NIST SPECIAL PUBLICATION 1800-35E

Implementing a Zero Trust Architecture

Volume E:
Risk and Compliance Management

Alper Kerman
Murugiah Souppaya
National Institute of Standards and Technology
Gaithersburg, Maryland

Parisa Grayeli
Susan Symington
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

William Barker
Dakota Consulting
Silver Spring, Maryland

Peter Gallagher
Aaron Palermo
Appgate
Coral Gables, Florida

Corey Bonnell
Dean Coclin
DigiCert
Lehi, Utah

Ryan Johnson
Dung Lam
F5
Seattle, Washington

Harmeet Singh
Krishna Yellepeddy
IBM
Armonk, New York

Ken Durbin
Earl Matthews
Mandiant
Reston, Virginia

Chris Jensen
Joshua Moll
Tenable
Columbia, Maryland

Peter Bjork
Keith Luck
VMware
Palo Alto, California

September 2023

SECOND PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-35E, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3E, 173 pages, September 2023, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback for any part of this document. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: nccoe-zta-project@list.nist.gov.

Public comment period: September 12, 2023. through October 31, 2023.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

A zero trust architecture (ZTA) focuses on protecting data and resources. It enables secure authorized access to enterprise resources that are distributed across on-premises and multiple cloud environments, while enabling a hybrid workforce and partners to access resources from anywhere, at any time, from any device in support of the organization's mission. Each access request is evaluated by verifying the context available at access time, including criteria such as the requester's identity and role, the requesting device's health and credentials, the sensitivity of the resource, user location, and user behavior consistency. If the enterprise's defined access policy is met, a secure session is created to protect all information transferred to and from the resource. A real-time and continuous policy-driven,

risk-based assessment is performed to establish and maintain the access. In this project, the NCCoE and its collaborators use commercially available technology to build interoperable, open, standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. This NIST Cybersecurity Practice Guide explains how commercially available technology can be integrated and used to build various ZTAs. This volume of the NIST Cybersecurity Practice Guide discusses risks addressed by the ZTA reference architecture. It also maps ZTA security characteristics to Cybersecurity Framework Subcategories, NIST SP 800-53r5 (Security and Privacy Controls for Information Systems and Organizations) security controls, and Executive Order (EO) 14028 security measures.

KEYWORDS

Cybersecurity Framework; identity credential and access management (ICAM); risk; security controls; zero trust; zero trust architecture (ZTA).

ACKNOWLEDGMENTS

We are grateful to the following individuals for reviewing the document.

Name	Organization
Timothy Jones	Forescout
Tim LeMaster	Lookout
Kevin Stine	NIST
Wade Ellery	Radiant Logic
Deborah McGinn	Radiant Logic

The Technology Partners/Collaborators who participated in this project submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Collaborators		
Appgate	IBM	Ping Identity
AWS	Ivanti	Radiant Logic
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
F5	Okta	VMware
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

Collaborators listed above who have already contributed technologies may also provide additional components for integration in future builds.

DOCUMENT CONVENTIONS

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nccoe-zta-project@list.nist.gov

Contents

List of Tables

167

1 Introduction

In this project, the NCCoE and its collaborators use commercially available technology to build interoperable, open, standards-based zero trust architecture (ZTA) implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture* [1]. This volume of the NIST Cybersecurity Practice Guide discusses risks addressed by the ZTA reference architecture. It also maps ZTA security characteristics to Cybersecurity Framework Subcategories, NIST SP 800-53 security controls, and Executive Order (EO) 14028 security measures. The mappings include both general ZTA logical component capabilities and specific ZTA example implementation capabilities.

1.1 How to Use this Guide

This NIST Cybersecurity Practice Guide helps users develop a plan for migrating to ZTA. It demonstrates a standards-based reference design for implementing a ZTA and describes various example implementations of this reference design known as *builds*. The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

This guide contains five volumes:

- NIST SP 1800-35A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-35B*: Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-35C: *How-To Guides* – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project
- NIST SP 1800-35D: *Functional Demonstrations* – use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations
- NIST SP 1800-35E*: Risk and Compliance Management* – risk analysis and mapping of ZTA security characteristics to cybersecurity standards and recommended practices **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-35A*, which describes the following topics:

- challenges that enterprises face in migrating to the use of ZTA
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-35B*, which describes what we did and why.

Also, Section 4 of this guide, *NIST SP 1800-35E,* will be of particular interest. Section 4, *Mappings*, maps logical components of the general ZTA reference design to security characteristics listed in various cybersecurity documents, including the NIST Cybersecurity Framework (CSF), NIST SP 800-53 (*Security and Privacy Controls for Information Systems and Organizations*), and *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028*.

You might share the *Executive Summary, NIST SP 1800-35A*, with your leadership team members to help them understand the importance of migrating toward standards-based ZTA implementations.

IT professionals who want to implement similar solutions will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-35C*, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. Also, you can use *Functional Demonstrations, NIST SP 1800-35D*, which provides the use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations. Finally, this guide, *NIST SP 1800-35E,* will be helpful in explaining the security functionality that the components of each build provide.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a ZTA. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated. We seek feedback on the publication's contents and welcome your input. Comments, suggestions, and success

stories will improve subsequent versions of this guide. Please contribute your thoughts to nccoe-zta-project@list.nist.gov.

2 Risks Addressed by the ZTA Reference Architecture

Conventional network security has focused on perimeter defense. Historically, most organization resources have been located within and protected by the enterprise's network perimeter, which tended to be large and static. Subjects that are inside the network perimeter are often assumed to be implicitly trusted and are given broad access to the resources within the network perimeter. Attempts to access resources from outside the network perimeter, i.e., from the internet, are often subject to more scrutiny than those originating from within. However, a subject can be compromised regardless of whether it is inside or outside of the network perimeter. Once a subject is compromised, malicious actors—through impersonation and escalation—can gain access to the resources that the subject is authorized to access and move laterally within the network perimeter to access adjacent resources.

By protecting each resource individually and employing extensive identity, authentication, and authorization measures to verify a subject's requirement to access each resource, zero trust can ensure that authorized users, applications, and systems have access to only those resources that they absolutely have a need to access in order to perform their duties, not to a broad set of resources that all happen to be within the network perimeter. This way, if a malicious actor does manage to gain unauthorized access to one resource, this access will not provide them with any advantage when trying to move laterally to other nearby resources. To compromise those other resources, the attacker would be required to figure out how to circumvent the mechanisms that are protecting those resources individually because it is not possible to reach those resources from nearby compromised resources. In this way, ZTA limits the insider threat because instead of having permission to access all resources within the network perimeter, malicious insiders would only be permitted to access those resources they require to perform their official roles.

In addition, once a subject is granted access to a resource, this access is often permitted to continue for a substantial period of time without being reevaluated based on a defined policy. The access session is often not monitored or subject to behavioral analysis, and the configuration and health of the devices being used to access resources may be subject to initial, but not ongoing, scrutiny. So, if a subject does manage to gain unauthorized access to a resource, the subject often has ample time to exfiltrate or modify valuable information or further compromise the resource and/or use it as a point from which to pivot and attack other corporate resources. ZTA limits these threats by performing continual verification of a subject's identity and authorization to access a resource. It may also perform behavioral analysis and validation of each system's health and configuration, and consider other factors such as day, time, and location of subject and resource. Based on the organization's defined policy, ZTA makes dynamic ongoing assessments of the risk of each access request in real-time to ensure it poses an acceptable level of risk according to organization policy.

A number of trends, including cloud computing and remote work, have also introduced additional security threats. The growth in cloud computing has meant that enterprises are now storing critical resources (e.g., databases, applications, servers) in the cloud (i.e., outside of the traditional network perimeter) as well as on-premises. As a result, these resources cannot be protected by the network perimeter strategy. A new protection paradigm is needed that focuses on protecting resources individually, no matter where they are located, so that they are not at risk of being subjected to security policies that are not under organization control or not enforced consistently across all enterprise resources. Often the clouds in which resources are hosted are multitenant, meaning that different enterprises have authorized access to their own portions of the cloud infrastructure, with each tenant reliant on the cloud service provider to enforce this separation. If a malicious actor were to figure out how to subvert cloud security and move from one tenant's account to the next, the organization's resources would be at risk. Use of ZTA to protect each resource individually serves as further assurance that the resources will not be accessible to cloud users from other enterprises, nor will they be accessible to users from within the enterprise who do not have a need to access them.

The growth of the remote workforce, as well as collaboration with partners and dependence on contractors are other trends that are also challenging the conventional security paradigm. The subjects requesting authorized access to resources may not necessarily be within the network perimeter. They may be employees working from home or from a coffee shop's public Wi-Fi via the internet, or a partner, contractor, customer, or guest that requires access to some resources but must be restricted from accessing other resources. By relying on strong identity, authentication, and authorization services to determine precisely which resources a subject is authorized to access with respect to their role in or relationship to the organization, ZTA can restrict subjects to accessing only those resources that they have a need to access and ensure that they are not permitted to access any other resources.

While implementing ZTA addresses many risks, it also has limitations. It cannot remove all risk, and the ZTA implementation itself may introduce additional risks that need to be addressed. For more information on the limitations of ZTA, see Section 5 of SP 800-207.

3 ZTA Reference Architecture Security Mappings

A *mapping* indicates that one concept is related to another concept. This publication provides mappings for ZTA cybersecurity functions. They include both functions performed by the ZTA reference design's logical components (see NIST SP 1800-35B Section 4.1) as well as functions performed by specific technologies used in the project's builds. The ZTA cybersecurity functions are based on the tenets of zero trust described in NIST SP 800-207. These tenets are a set of principles and strategies for system and security architects to use when designing, deploying, or upgrading systems and workflows. Architects and planners can use the zero trust tenets and the ZTA cybersecurity functions that are based on them when designing systems to help meet their cybersecurity requirements.

For this mapping, we have used the supportive relationship mapping style as defined in Section 4.2 of draft NIST Internal Report (IR) 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings* [2].

3.1 Use Cases

Each set of mappings in this publication involves the ZTA cybersecurity functions and one of the following:

- Subcategories from the NIST Cybersecurity Framework (CSF) 1.1 [3] (Note: Future versions of this document are expected to map to *The NIST Cybersecurity Framework 2.0 (CSF 2.0)* [4])
- Security controls from NIST SP 800-53r5 (*Security and Privacy Controls for Information Systems and Organizations*) [5]
- Security measures defined in *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028* [6] in support of Executive Order (EO) 14028 [7]

All of the elements in these mappings—the ZTA cybersecurity functions, CSF Subcategories, SP 800-53 controls, and EO 14028 security measures—are concepts involving ways to reduce cybersecurity risk.

The mappings in this publication were developed to support two primary use cases. The mappings are not intended to be comprehensive, but rather to capture the strongest relationships involving ZTA cybersecurity functions.

1. **Why should organizations implement ZTA?** This use case identifies how implementing ZTA can support an organization with achieving CSF Subcategories, SP 800-53 controls, and EO 14028 security measures. This helps communicate to an organization's senior management that expending resources to implement ZTA can also aid in fulfilling other security requirements.
2. **How can organizations implement ZTA?** This use case identifies how an organization's existing implementations of CSF Subcategories, SP 800-53 controls, and EO 14028 security measures can help support a ZTA implementation. An organization wanting to implement ZTA might first assess its current security capabilities so that it can plan how to add missing capabilities and enhance existing capabilities in order to implement ZTA. Organizations can leverage their existing security investments and prioritize future security technology deployment to address the gaps.

These mappings are intended to be used by any organization that is interested in implementing ZTA or that has begun or completed a ZTA implementation.

3.2 Mapping Producers

The NCCoE ZTA project team performed the initial mapping between the cybersecurity functions performed by the ZTA reference design's logical components and the security characteristics in the cybersecurity documents, with input and feedback from the collaborators who have contributed

technology to demonstrate ZTA capabilities. The collaborators performed the technology-specific mappings between the cybersecurity functions performed by collaborator products used in the project's ZTA builds and the security characteristics in the cybersecurity documents. In some cases, collaborators have not yet produced mappings for their products. These mappings are expected to be included in future versions of this document as collaborators develop them.

3.3 Mapping Approach

The NCCoE asked each collaborator to indicate the mapping between the cybersecurity functions its technology components provide in one or more builds and the security characteristics in the cybersecurity documents. The logical components in the ZTA reference design were used as the organizing principle for enumerating collaborator products and mapping the cybersecurity functions of those products to security characteristics. Using this approach, the product-specific technology mappings are instantiations of the general reference design logical component mappings for each cybersecurity document.

3.3.1 Mapping Terminology

In this publication, we use the following relationship types from NIST IR 8477 [2] to describe how the functions in our ZTA reference design are related to the NIST reference documents. Note that the *Supports* relationship applies to use case 1 only and the *Is Supported B*y relationship applies to use case 2 only.

- **Supports**: ZTA function X *supports* security control/Subcategory/measure Y when X can be applied alone or in combination with one or more other functions to achieve Y in whole or in part.
- **Is Supported By**: ZTA function X *is supported by* security control/Subcategory/measure Y when Y can be applied alone or in combination with one or more other security controls/Subcategories/measures to achieve X in whole or in part.
- **Equivalent**: ZTA function X is *equivalent* to security control/Subcategory/measure Y when X is the function that Y describes.

Each relationship of type *Supports* (A supports B) or *Is Supported By* (B is supported by A) has one of the following properties assigned to it:

- **Example of**: The supporting concept A is one way (an *example*) of achieving the supported concept B in whole or in part. However, B could also be achieved without applying A.
- **Integral to**: The supporting concept A is *integral to* and a component of the supported concept B. A must be applied as part of achieving B.
- **Precedes**: The supporting concept A *precedes* the supported concept B when A must be achieved before applying B. In other words, A is a prerequisite for B.

When determining whether a ZTA function's support for a given CSF Subcategory, SP 800-53 control, or EO 14028 security measure is integral to that support versus an example of that support, we do not consider how that function may in general be used to support the Subcategory, control, security measure, or other item. Rather, we consider only how that function is intended to support that Subcategory, control, security measure, or other item within the context of our ZTA reference design.

Also, when determining whether a ZTA function is supported by a CSF Subcategory with the relationship property of *precedes*, we do not consider whether or not it is possible to apply the function without first achieving the Subcategory. Rather, we consider whether or not, according to our ZTA reference design, the Subcategory is to be achieved prior to applying that function.

There may be cases in which a conflict arises between zero trust principles and a compliance control. This conflict may be due to the control assuming a particular architecture or process in place. A control's description may use language to indicate a particular role, technology, or process that would not necessarily be relevant in a ZTA. For example, some controls may include references to "remote access" or "perimeter defenses", which seem irrelevant in a ZTA. In an ideal ZTA, the network location should not matter (tenet 2 in SP 800-207). Likewise, while zero trust does acknowledge that perimeters exist, wide-scale perimeter defenses should not be the sole location where access policies are enforced. The mappings in this document do not ignore controls with descriptions that seem to conflict with ZTA. Instead, the mappings attempt to meet the spirit of the control while noting that a ZTA principle may go beyond the baseline requirement.

3.3.2 Mapping Process

The process that the NCCoE used to create the mapping from the logical components of the ZTA reference design to the security characteristics of a given document was as follows:

1. Create a table that lists each of the logical components of the ZTA reference design in column 1.
2. Describe each logical component's cybersecurity function in column 2.
3. Map each cybersecurity function to each of the security characteristics in the document to which the function is most strongly related, and list each of these security characteristics on different sub-rows within column 3. Begin each security characteristic entry with an underlined keyword that describes the mapping's relationship type (e.g., *Supports*, *Is Supported By*, *or Equivalent).* After the keyword describing the relationship type, put in parentheses the underlined keyword(s) describing the relationship's property if applicable (e.g., *Example of*, *Integral to*, or *Precedes*).
4. In the fourth column, provide a brief explanation of why that relationship type and property apply to the mapping.

5. After completing the mapping table entries as described above for all the logical components in the reference design, examine the mapping in the other direction, i.e., starting with the security characteristics listed in the document and considering whether they have a relationship to the logical components' cybersecurity functions in the reference design. In other words, step through each of the security characteristics in the document and determine if there is some logical component in the reference design that has a strong relationship to that security characteristic. If so, add an entry for that security characteristic mapping to that logical component's row in the table. By examining the mapping in both directions in this manner, security characteristic mappings are less likely to be overlooked or omitted.

The NCCoE applied this mapping process separately for each reference document. None of the mappings are intended to be exhaustive; they all focus on the strongest relationships involving each cybersecurity function in order to help organizations prioritize their work. Mapping every possible relationship, no matter how tenuous, would create so many mappings that they would not have any value in prioritization.

4 Mappings

The mappings organized in the remainder of this document as follows:

- Section 4.1 – NIST CSF 1.1 Subcategory mappings. These include:
  - Section 4.1.1 – Mappings between the security functions provided by the logical components of the ZTA reference design and NIST CSF Subcategories
  - Section 4.1.2 – Mappings between the ZTA build functionality provided by each collaborator's products and NIST CSF Subcategories
- Section 4.2 – NIST SP 800-53 control mappings. These include:
  - Section 4.2.1 – Mappings between the security functions provided by the logical components of the ZTA reference design and NIST SP 800-53r5 controls
  - Section 4.2.2 – Mappings between the ZTA build functionality provided by each collaborator's products and NIST SP 800-53r5 controls
- Section 4.3 – EO 14028 security measure mappings. These include:
  - Section 4.3.1 – Mappings between the security functions provided by the logical components of the ZTA reference design and EO 14028 security measures
  - Section 4.3.2 – Mappings between the ZTA build functionality provided by each collaborator's products and EO 14028 security measures

The product-specific mappings are organized by collaborator. Only collaborators who have provided mappings for their products are included. Sections for additional collaborators and the mappings for

their products are expected to be included in future drafts of this document as those collaborators make the mappings for their products available.

The builds that the collaborator technologies are used in are denoted using the abbreviations defined in volume B, where *E1B1*, for example, refers to Build 1 of the example implementation in Enterprise 1, *E2B1* refers to Build 1 of the example implementation in Enterprise 2, and *E1B2* refers to Build 2 of the example implementation in Enterprise 1. The composition of each build is described in an appendix of volume B.

4.1 NIST CSF Subcategory Mappings

This section provides mappings between ZTA functionality and NIST CSF 1.1 Subcategories.

4.1.1 Mapping Between ZTA Reference Design Functions and NIST CSF Subcategories

Table 4-1 provides a mapping between the functions of the ZTA reference design's components and the NIST CSF Subcategories. This table indicates how ZTA functions help support CSF Subcategories and vice versa.

Table 4-1 Mapping Between ZTA Reference Design Functions and NIST CSF Subcategories

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, information from functional components, and a trust algorithm	Supports (integral to) PR.AC-3: Remote access is managed	The PE makes remote access decisions based on policy. In a ZTA, the PE must be applied to help manage remote access. Note that in ZTA, the same policy applies to all access requests, regardless of whether they are remote or local. Although ZTA does not differentiate between local and remote access policy, however, compliance frameworks might.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) PR.AC-3: Remote access is managed	The PA supports the enforcement of remote access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced. In a ZTA, the PA must be applied to help manage remote access.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) PR.AC-3: Remote access is managed	The PEP enforces remote access decisions. In a ZTA, the PEP must be applied in order to help manage remote access.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	The PEP can prevent unauthorized access to the portions of the enterprise that it guards. If it is used to protect a single resource, it does not necessarily provide network segregation or network segmentation. However, it can be deployed to protect and segregate discrete network segments. Network segmentation may also be provided by other mechanisms besides a PEP.
		Supports (integral to) PR.DS-5: Protections against data leaks are implemented	The PEP prevents unauthorized transfer of information out of the portion of the enterprise that it guards. In a ZTA, the PEP must be applied to help protect against data leaks.
		Supports (integral to) PR.PT-4: Communications and control networks are protected	To support ZTA, the data plane and control plane (networks) must be logically separate. The PEP is the only component that can send and receive messages from both planes. It protects the planes from each other and ensures that the control plane is not directly accessible by enterprise assets and resources.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	The PEP may be used to monitor connections between a subject and an enterprise resource to detect prohibited or suspicious activity. However, it must not necessarily be configured to do so. Network monitoring may also be provided by other mechanisms besides a PEP.
		Supports (integral to) RS.MI-1: Incidents are contained	In a ZTA, the PEP is central to containing incidents. If a resource is compromised, the PEPs protecting other resources prevent attackers from moving laterally from the compromised resource to the resources protected by those other PEPs.
ICAM - Identity Management	Creates and manages enterprise user and device accounts,	Is supported by (precedes) ID.AM-6: Cybersecurity roles and	Identity Management supports the creation, storage, and management of digital representations of cybersecurity

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	roles and their associated permissions and responsibilities. It also supports the assignment of roles to user identities. To be able to create, store, and manage these representations of user roles and responsibilities, the roles and responsibilities themselves must have already been established.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Identity Management supports issuance, storage, management, and revocation of identities and their associated roles and credentials. It also supports the verification of credentials when performing user and device authentication.
		Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege and separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege and separation of duties, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Identity Management stores and manages the association of identities with credentials.
ICAM - Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which	Is supported by (precedes) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	To determine whether an access request is authorized, the Access and Credential Management component authenticates the user or device that is requesting access by verifying the credentials that are bound to the user or device and asserted as part of the access request. The user and device identities must be asserted for this component to be able to authenticate them.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	access requests are authorized.	Supports (integral to) PR-AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The key function of the Access and Credential Management component is to perform user and device authentication.
		Supports (example of) RS.MI-1: Incidents are contained	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the Access and Credential Management component will limit the attacker to accessing only those resources that the legitimate user's role or attributes allow. This is one example of how incidents can be contained.
		Supports (example of) RS.MI-2: Incidents are mitigated	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the attacker will only be allowed to access that resource in the way that the legitimate user's role allows (e.g., read-only vs. read-write). This is one example of how incidents can be mitigated.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The Access and Credential Management component can perform ongoing, intermittent user authentication and authorization, thereby monitoring for unauthorized users and devices.
ICAM - Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to	Is supported by (precedes) ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g.,	The Federated Identity component enables enforcement of the cybersecurity roles and responsibilities that have been established and stored for many different groups—the enterprise workforce and third-party stakeholders (e.g., suppliers, customers, partners) to be managed and enforced. These roles and responsibilities

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	suppliers, customers, partners) are established	must already be established before they can be enforced.
ICAM - Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	A key function of the Identity Governance component is to support the auditing of identities and credentials.
		Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	The Identity Governance component manages access permissions and authorizations in a way that incorporates the principles of least privilege and separation of duties.
		Is supported by (precedes) ID.GV-1: Organizational cybersecurity policy is established and communicated	The Identity Governance component ensures that the organization's cybersecurity policy is enforced in such a way that it complies with regulatory, legal, and other governance-related requirements. This policy must already be established before it can be enforced by the Identity Governance component.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	The Identity Governance component supports the coordination and alignment of cybersecurity roles and responsibilities with internal roles and external partners to ensure that the organization operates in accordance with regulatory, legal, and other governance-related requirements.
		Is supported by (precedes) ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	The processes that the Identity Governance component follows have been defined to ensure that the organization operates in conformance with all legal and regulatory requirements. These requirements must be well understood in order to define the Identity Governance processes. As these requirements change, they must be managed on an ongoing basis, and they may require changes to identity governance processes.
		Supports (integral to) ID.GV-4: Governance and risk management processes address cybersecurity risks	The processes that the Identity Governance component follows are defined and managed with the objective of addressing cybersecurity risks.
		Supports (integral to) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The Identity Governance component performs logging and audits all identity management activities in accordance with policy and regulations.
ICAM - Multi-Factor Authentication (MFA)	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks	The MFA component enables users to be authenticated using a second factor, which is required for higher-risk access requests.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		and other organizational risks)	
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to be enrolled into a UEM/MDM system, the device must be known to be part of the organization's inventory.
		Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The UEM/MDM installs, manages, configures, and updates applications on UEM/MDM-managed devices, so it provides inventory information regarding these applications.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The UEM/MDM may be able to identify and remediate device vulnerabilities by updating software on managed devices, for example.
		Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	The UEM/MDM may monitor for suspicious activity; detect and disable malware, viruses, and other malicious traffic; and repair infected files on managed devices.
		Supports (integral to) PR.AC-3: Remote access is managed	The UEM/MDM may prevent a remote device that it is managing from being able to access any resources until the device is brought into compliance.
		Supports (example of) PR.DS-1: Data-at-rest is protected	The UEM/MDM may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
		Supports (example of) PR-DS-2: Data-in-transit is protected	The UEM/MDM may encrypt data sent from the device, but this data could also be encrypted via a different mechanism.
		Supports (example of) PR.DS-5: Protections against data leaks are implemented	The UEM/MDM may track user activity on the device and monitor for unauthorized traffic to help prevent, detect, and mitigate data leaks.
		Supports (example of) PR.DS-6: Integrity checking mechanisms	The UEM/MDM may use integrity checking to verify updates prior to installing them. It may also use integrity

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	activity on devices, and detects and addresses security issues on the device.	are used to verify software, firmware, and information integrity	checking to verify compliance of device software and firmware.
		Supports (example of) PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	The UEM/MDM may rely on device attestation or similar mechanisms that use integrity checking to verify the hardware integrity of the device before trusting the device.
		Supports (integral to) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The UEM/MDM ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. UEM/MDM enforces and maintains these baselines at endpoints.
		Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The baseline configuration on the endpoints that the UEM/MDM enforces must have been developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. UEM/MDM operation depends on the existence of such baselines.
		Supports (example of) PR.IP-6: Data is destroyed according to policy	The UEM/MDM can remotely delete applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
		Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	The UEM/MDM can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before the UEM/MDM can enforce them, and they constitute at least one portion of the

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			organization's vulnerability management plan.
		Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	The UEM/MDM can restrict the use of removable media as required by policy.
		Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The UEM/MDM can be used to configure devices to provide only essential capabilities.
		Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The UEM/MDM can monitor user activity for suspicious behavior.
		Supports (example of) DE.CM-4: Malicious code is detected	The UEM/MDM prevents, detects, and disables numerous types of malicious code.
		Supports (example of) DE.CM-5: Unauthorized mobile code is detected	The UEM/MDM may be able to detect unauthorized mobile code.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The UEM/MDM monitors the device for unauthorized software and connections.
		Supports (integral to) RS.MI-1: Incidents are contained	The UEM/MDM performs many activities that help to contain incidents, such as detecting and disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) RS.MI-2: Incidents are mitigated	The UEM/MDM performs many activities that help to mitigate incidents, such as detecting and disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.
Endpoint Security - Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections;	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to have EDR/EPP software installed on it, the device must be known to be part of the organization's inventory.
		Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The EDR/EPP can inventory software on the device.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The EDR/EPP scans the device to detect missing patches or outdated software and report them. It can also install patches if instructed to do so later.
		Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (integral to) PR.AC-3: Remote access is managed	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (example of) PR.DS-1: Data-at-rest is protected	The EDR/EPP may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (example of) PR-DS-2: Data-in-transit is protected	The EDR/EPP may encrypt data sent from the device, but this data could also be encrypted via a different mechanism.
		Supports (example of) PR.DS-5: Protections against data leaks are implemented	The EDR/EPP may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (example of) PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	The EDR/EPP may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
		Supports (integral to) and Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The EDR/EPP ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. This baseline that the EDR/EPP enforces must have been developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. So EDR/EPP operation depends on the existence of such baselines, but it also enforces and maintains these baselines.
		Supports (example of) PR.IP-6: Data is destroyed according to policy	The EDR/EPP can remotely delete applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
		Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	The EDR/EPP can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before the EDR/EPP can enforce them, and they constitute at least one portion of the organization's vulnerability management plan.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	The EDR/EPP can restrict the use of removable media as required by policy.
		Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The EDR/EPP can be used to configure devices to provide only essential capabilities.
		Supports (example of) DE.CM-4: Malicious code is detected	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (example of) DE.CM-5: Unauthorized mobile code is detected	The EDR/EPP may be able to detect unauthorized mobile code.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The EDR/EPP monitors the device for unauthorized software and connections.
		Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The EDR/EPP can monitor user activity for suspicious behavior.
		Supports (integral to) RS.MI-1: Incidents are contained	The EDR/EPP performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) RS.MI-2: Incidents are mitigated	The EDR/EPP performs many activities that help to mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
Endpoint Security - Endpoint Compliance	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to have EDR/EPP software installed on it, the device must be known to be part of the organization's inventory.
		Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The EDR/EPP can inventory software on the device.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The EDR/EPP scans the device to detect missing patches or outdated software and report them. It can also install patches if instructed to do so later.
Security Analytics - Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and	Supports (example of) DE.AE-2: Detected events are analyzed to understand attack targets and methods	The SIEM collects security and event information from many components. This aggregated data may be analyzed to understand attack targets and methods.
		Supports (integral to) DE.AE-3: Event data are collected and correlated from multiple sources and sensors	A key function of the SIEM is to collect and correlate security event data from multiple sources.
		Supports (example of) DE.AE-4: Impact of events is determined	Security analysts may use SIEM data to help them determine the impact of events.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	logs the data to adhere to data compliance requirements.	Supports (example of) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The SIEM can aggregate logs of security information and event activity as required by policy.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	SIEM logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
		Supports (example of) RS.AN-2: The impact of the incident is understood	The SIEM logs can provide data that helps security analysts to understand the impact of cybersecurity incidents.
		Supports (example of) RS.AN-3: Forensics are performed	The SIEM logs can provide data that can help security analysts to perform forensic analysis of cybersecurity incidents.
Security Analytics - Identity Monitoring	Monitors the identity of subjects to detect and send alerts for indicators that user accounts or credentials may be compromised, or to detect sign-in risks for a particular access session.	Supports (example of) ID.RA-3: Threats, both internal and external, are identified and documented	The Identity Monitoring component can potentially identify users whose accounts have been compromised or users who may be insider threats.
		Is supported by (precedes) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	In order to be able to monitor the activity of particular subjects for risks, those subjects must have been issued digital identities.
		Is supported by (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	If a subject has clearly defined and well-managed access permissions that incorporate the principles of least privilege and separation of duties and the subject is attempting to deviate from these permissions, the identity monitoring component may use this behavior as an indicator of potential compromise.
		Is supported by (integral to) PR.AC-6: Identities	In order to be able to monitor the interactions of a particular subject

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		are proofed and bound to credentials and asserted in interactions	identity, the subject identity must be asserted in interactions.
		Is supported by (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	One way to detect that an account or credential has been compromised is to notice differences between expected user identity, authentication, and sign-in behavior and actual behavior.
Security Analytics – User Behavior Analytics	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Performing user behavior analytics is an essential part of monitoring the activity of personnel to detect potential cybersecurity events.
Security Analytics - Security Monitoring	Monitors and detects malicious or suspicious user actions based on access activity	Is supported by (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	One way to detect malicious or suspicious user actions is to notice differences between expected access activity and actual access activity.
		Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Monitoring for malicious or suspicious user access activity is one example of how personnel activity can be monitored to detect potential cybersecurity events.
Security Analytics - Application Protection and Response	Protects particular applications from phishing, spam, malware and other zero day attacks	Supports (example of) DE.CM-4: Malicious code is detected	Use of an Application Protection and Response component is one way to detect malicious code.
Security Analytics - Cloud Access Permission Manager	Provides visibility and control of permissions used by identities in various cloud platforms	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	This component provides the visibility and control necessary to enable permissions used by identities in the cloud to be managed.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Security Analytics – Endpoint Monitoring	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts (devices or VMs) that are connected to the network	Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Endpoint Monitoring is essential for detecting unauthorized software and is also a good way to detect unauthorized devices and connections.
		Supports (integral to) DE.CM-4: Malicious code is detected	Endpoint monitoring is essential for detecting malicious code.
Security Analytics - Vulnerability Scanning and Assessment	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) DE.CM-8: Vulnerability scans are performed	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans.
Security Analytics - Security Orchestration, Automation, and Response (SOAR)	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the	Supports (example of) RS.RP-1: Response plan is executed during or after an incident	A SOAR can execute predefined incident response workflows.
		Supports (example of) RS.AN-2: The impact of the incident is understood	Security analysts can use a SOAR to visualize security events and their impacts, thereby enabling incidents to be better understood.
		Supports (example of) RS.AN-3: Forensics are performed	Security analysts can use a SOAR to help them perform forensic analysis of cybersecurity incidents.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	operations required to respond.		
Security Analytics - Security Controls Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows.	Is supported by (integral to) DE.CM-1: The network is monitored to detect potential cybersecurity events	The network must be monitored to have visibility into network traffic.
		Is supported by (example of) ID.AM-3: Organizational communication and data flows are mapped	To determine what controls should be implemented and validated, the organization should have a good understanding of what communication and data flows are needed to support the organization's mission. This understanding can be obtained by mapping organizational communication and data flows.
		Is supported by (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	One way to validate implemented controls by observing network traffic and transaction flows is to have a set of expected flows against which to compare the set of observed flows.
		Supports (integral to) DE.DP-3: Detection processes are tested	Security Controls Validation is used to test and verify the effectiveness of detection processes and other ZTA cybersecurity controls.
		Supports (example of) DE.DP-5: Detection processes are continuously improved	The organization can use Security Controls Validation to continuously monitor, measure, and validate the effectiveness of cybersecurity controls, thereby enabling the organization to continuously improve the detection processes.
Security Analytics - Traffic Inspection	Intercepts, examines, and records relevant traffic transmitted on the network.	Supports (integral to) DE.CM-1: The network is monitored to detect potential cybersecurity events	Traffic inspection is an essential part of monitoring the network to detect potential cybersecurity events.
Security Analytics -	Discovers, classifies, and assesses the risk	Supports (integral to) ID.RA-3: Threats, both internal and external,	A key function of Network Discovery is to monitor the network to find, identify, and document unknown and/or unexpected

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Network Discovery	posed by devices and users on the network.	are identified and documented	devices and activity that may pose a threat to the organization.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	Network Discovery can help identify unknown and/or unexpected devices and activity that may be indicative of suspicious events, making it an example of how the network can be monitored to detect potential cybersecurity events.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	A key function of the Network Discovery component is to discover unauthorized devices and connections on the network.
Security Analytics - Network Monitoring	Aggregates and analyzes network telemetry—information generated by network devices—to provide network visibility both on premises and in clouds and to detect and respond to threats.	Equivalent DE.CM-1: The network is monitored to detect potential cybersecurity events	The network monitoring component monitors network traffic to detect potential cybersecurity events.
Security Analytics - Security Analytics and Access Monitoring	Monitors cloud resource access sessions for conformance to policy	Is supported by (integral to) DE.CM-1: The network is monitored to detect potential cybersecurity events	Network access within the cloud must be monitored in order to have visibility into cloud resource access sessions.
		Is supported by (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	One way to validate that cloud resource access sessions conform to policy is to have a set of expected access flows against which to compare the set of observed access sessions.
Data Security – Data Discovery	Scans and classifies digital assets,	Supports (example of) PR.DS-1: Data-at-rest is protected	Finding and classifying data stored in the cloud and on-premises helps ensure that it can be protected appropriately.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	including unstructured data		
Data Security - Data Encryption	Provides strong encryption and key management capabilities for both structured and unstructured data both on premises and in the cloud	Supports (integral to) PR.DS-1: Data-at-rest is protected	Encryption and key management are essential for protecting the confidentiality of data, whether the data is at rest or in transit.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	Encryption and key management are essential for protecting the confidentiality of data, whether the data is at rest or in transit.
Data Security - Data Access Protection	Restricts access to/actions on data based on permanent or transient attributes of the entity accessing the data, with the ability to revoke access as needed. Includes all data access policies and rules needed to secure access to enterprise information and resources	Supports (example of) PR.DS-1: Data-at-rest is protected	Providing policy-based protection of the data according to its classification is one way to help protect data stored in the cloud and on-premises.
General - Remote Connectivity	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (example of) PR.AC-3: Remote access is managed	Requiring remote users to access the enterprise via VPN is one mechanism that can be used to manage remote access.
		Supports (example of) PR.DS-2: Data-in-transit is protected	VPNs are one method of encrypting data in transit.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	Traffic sent on the VPN can be monitored to detect prohibited or suspicious activity.
General - Certificate Management	Provides automated capabilities to issue, install, inspect,	Is supported by (precedes) ID.AM-2: Software platforms and applications within the	Servers and software must be identified and known to be within the organization's inventory in order for them to be issued certificates.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	revoke, renew, and otherwise manage TLS certificates.	organization are inventoried	
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Verification (i.e., authentication) of the identity of servers depends on the issuance, use, and management of TLS certificates.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Proofing (i.e., authenticating) server identities requires TLS certificates.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The setup of encrypted TLS transport connections depends on TLS certificates.
		Supports (integral to) PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates. Any integrity mechanism that relies on public key cryptography is supported by TLS certificates.
General - Configuration Management	Enables the management and configuration of resources such as virtual machines and containers on-premises and in other clouds	Supports (example of) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	The configuration management component is a tool that helps the organization create and maintain a baseline configuration of IT systems.
General - Secure Admin Workstation	Securely configured workstation that is dedicated to performing sensitive tasks	Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Use of a dedicated workstation that is configured securely is one way to ensure that the workstation will provide only essential capabilities in accordance with the principle of least functionality.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
General - Virtual Desktop	Enables the secure streaming of the desktop experience from the cloud to an endpoint or handheld device.	Supports (example of) PR.DS-2: Data-in-transit is protected	Encryption of the streamed desktop content protects this data while in transit.
Resource Protection - Cloud Workload Protection	Secures cloud work-loads to protect them from known se-curity risks and pro-vides alerts to enable real-time reaction to prevent security events from develop-ing. Monitors traffic to and from cloud and web applications and provides session control to prevents sensitive information from leaving.	Is supported by (integral to) DE.CM-1: The network is monitored to detect potential cybersecurity events	Cloud workload protection relies on the ability to monitor traffic to and from the cloud and web applications and to provide visibility into workload behavior to help detect and respond to incidents.
		Is supported by (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	One way to secure cloud workloads is to segment the cloud data center into small segments, define security controls for each segment, and run one workload on each segment to protect individual workloads and isolate them from each other so malware and breaches cannot migrate from workload to workload.
		Supports (example of) PR.DS-5: Protections against data leaks are implemented	The cloud workload protection component may provide session control to help prevent sensitive information from leaving the environment.
		Is supported by (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	One way that a cloud workload protection component can monitor workload behavior is by comparing observed behavior to a baseline of expected behavior.
		Supports (example of) RS.MI-1: Incidents are contained	The cloud workload protection component may implement micro-segmentation or use hypervisors to isolate workloads and thereby prevent a compromise of one workload from propagating to other workloads.
		Supports (example of) RS.MI-2: Incidents are mitigated	The cloud workload protection component is designed to react to detected incidents in real-time to prevent security events from developing.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The cloud workload protection component provides visibility into and the ability to configure workloads to help ensure that they provide only essential capabilities. It also enables workload monitoring and log management to be performed more uniformly. It can also help identify unnecessary applications, permissions, etc., thereby reducing potential attack vectors.
Resource Protection - Cloud Security Posture Management	Continually assesses the security posture of cloud resources.	Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The Cloud Security Posture Management component can inventory software in the cloud.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The Cloud Security Posture Management component continually assesses cloud resources to detect missing or outdated software or other posture vulnerabilities and report or remediate them.
Resource Protection- Application Connector	Component that is deployed to be the front-end for an internal resource (whether located on-premises or in the cloud) and act as a proxy for it. Requests to access the resource are directed to the connector, which responds by initiating a secure connection to the PEP. A connector enables access to a resource to be controlled without requiring the resource to be visible on the network.	Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	The application connector segregates a resource/application from the rest of the network.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Resource Protection - PaaS/Kubernetes security	Create a per-pod secure connection to the PEP, enabling authorized service to service and service to resource communication without the Pod or the resource visible on the Internet.	Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	The PaaS/Kubernetes security component segregates a resource or Pod from the rest of the network.

4.1.2 Mapping Between Collaborator Technologies in the ZTA Builds and NIST CSF Subcategories

In this section we map between the technologies that various collaborators have contributed to the project's ZTA builds and the NIST CSF Subcategories. There is a separate subsection describing the mappings for each collaborator. Some collaborators have not yet provided the mappings for their technologies. The mappings for those collaborator technologies are planned for inclusion in a future draft of this document as the collaborators develop them.

4.1.2.1 Mapping Between Appgate Technologies and NIST CSF Subcategories

Table 4-2 lists the technologies that Appgate has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST CSF Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. Appgate technologies have been included in Build E1B4.

Table 4-2 Mapping Between Appgate ZTA Functionality and NIST CSF Subcategories

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Appgate SDP Controller	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource;	Supports (integral to) PR.AC-3: Remote access is managed	The Appgate SDP Controller makes policy-based access decisions, regardless of whether the access is remote or local. Access decisions are based on device security posture, user authN, and

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		forwards requests to and receives commands from the PA		MFA, and often include compliance data obtained from external sources.
Policy Administrator (PA)	Appgate SDP Controller	Executes the PE's policy decision by sending a set of entitlements (list of protected resources defined by hostname/IP, port, and protocol) and conditions for access to a PEP	Supports (integral to) PR.AC-3: Remote access is managed	The Appgate SDP Controller executes its access policy decisions (both remote and local).
Policy Enforcement Point (PEP)	Appgate SDP Gateway	Receives signed entitlement tokens and dynamically adjusts access between subject and resource as conditions change	Supports (integral to) PR.AC-3: Remote access is managed	Appgate SDP Gateways enforce the access decisions made by the Appgate SDP Controller.
			Supports (integral to) PR.DS-5: Protections against data leaks are implemented	Appgate SDP Gateways prevent unauthorized transfer of information out of the resources that they guard. All access to and from one of the resources must be explicitly permitted by an Appgate SDP Gateway.
			Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	The Gateway monitors connections between a subject and an enterprise resource to detect, log, and prevent prohibited or suspicious activity.
Endpoint Security - Endpoint Compliance	Appgate SDP Client	Enforces policies based on a defined set of endpoint compliance checks to allow or deny user/endpoint access to a resource, but does not perform the functions of an EPP solution to	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Devices using the Appgate SDP Client software for secure access report physical, network, OS, and user information as needed to authorize access and determine access level.
			Supports (example of) ID.AM-2: Software platforms	The Appgate SDP Client can inventory software, processes, certificates, etc.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		automatically remediate an endpoint	and applications within the organization are inventoried	as part of the device compliance assessment.
General - Remote Connectivity	Appgate SDP	Provides remote users with connectivity to on-premises or cloud resources.	Supports (example of) PR.AC-3: Remote access is managed	Users access enterprise and cloud resources via Appgate's per-site tunnel connection.
			Supports (example of) PR.DS-2: Data-in-transit is protected	Mutual-TLS 1.2 or 1.3 based tunnels are used to encrypt data in transit.
Resource Protection - PaaS/ Kubernetes security	Appgate Injector (Appgate for Kubernetes)	Creates a per-pod secure connection to the PEP, enabling authorized service-to-service and service-to-resource communication without the Pod or the resource visible on the Internet	Supports (example of) PR.AC-5: Network integrity is protected	All traffic from Pods/containers to corporate APIs and protected resources is encrypted and restricted to least-privilege access. Pods, containers, APIs, and protected resources can be located on-premises or in the cloud.
			Supports (example of) PR.DS-2: Data-in-transit is protected	Mutual-TLS 1.2 or 1.3 based tunnels are used to encrypt data in transit.

4.1.2.2 Mapping Between Digicert Technologies and NIST CSF Subcategories

Table 4-3 lists the technologies that Digicert has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST CSF Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. Digicert technologies have been included in all of the ZTA builds.

470 **Table 4-3 Mapping Between Digicert Functionality and NIST CSF Subcategories**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
General - Certificate Management	DigiCert CertCentral TLS Manager	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	DigiCert CertCentral TLS Manager provides the capability to manage TLS certificates throughout the certificate lifecycle process from issuance to expiration or revocation.

471 ### *4.1.2.3 Mapping Between F5 Technologies and NIST CSF Subcategories*

472 **Table 4-4** lists the technologies that F5 has contributed to the ZTA builds implemented in this project
473 and details the mappings between the functionality performed by these technologies and the NIST CSF
474 Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. F5
475 technologies have been included in Builds E3B1, E3B2, and E3B3.

476 **Table 4-4 Mapping Between F5 Functionality and NIST CSF Subcategories**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	F5 BIG-IP	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) PR.AC-3: Remote access is managed	F5 BIG-IP can enforce access decisions for the resources that it protects.
			Supports (integral to) PR.DS-5: Protections against data leaks are implemented	F5 BIG-IP prevents unauthorized transfer of information out of the resources that it guards. All access to and from the resource must be explicitly permitted by F5 BIG-IP.

4.1.2.4 Mapping Between IBM Technologies and NIST CSF Subcategories

Table 4-5 lists the technologies that IBM has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST CSF Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. IBM technologies have been included in Builds E1B1, E2B1, E1B2, E1B3, E2B3, E4B3, and E1B4.

Table 4-5 Mapping Between IBM Functionality and NIST CSF Subcategories

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	IBM Security Verify	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, identity, authorization, and endpoint compliance information received from supporting components, and a trust algorithm	Supports (integral to) PR.AC-3: Remote access is managed	IBM Security Verify makes policy-based access decisions regardless of whether the access is remote or local.
Policy Administrator (PA)	IBM Security Verify	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) PR.AC-3: Remote access is managed	IBM Security Verify supports the enforcement of access decisions (both remote and local) by conveying the access decision information to the PEP, where the decision can be enforced.
Policy Enforcement Point (PEP)	IBM Security Verify	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) PR.AC-3: Remote access is managed	IBM Security Verify enforces the access decisions it makes.
			Supports (integral to) PR.DS-5: Protections against data leaks are implemented	IBM Security Verify prevents unauthorized transfer of information out of the resources that it guards. All access to and from the resource must be explicitly permitted by IBM Security Verify.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
ICAM - Identity Management	IBM Security Verify	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time	Is supported by (precedes) ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	IBM Security Verify supports the creation, storage, and management of digital representations of cybersecurity roles and their associated permissions and responsibilities. It also supports the assignment of roles to user identities. To be able to create, store, and manage these representations of user roles and responsibilities, the roles and responsibilities themselves must have already been established.
			Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IBM Security Verify supports issuance, storage, management, and revocation of identities and their associated roles and credentials. It also supports the verification of credentials when performing user and device authentication.
ICAM - Access & Credential Management	IBM Security Verify	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which access requests are authorized.	Is supported by (precedes) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	IBM Security Verify supports the ability to determine whether an access request is authorized. It authenticates the user or device that is requesting access by verifying the credentials that are bound to the user or device and asserted as part of the access request. The user and device identities must be asserted for this component to be able to authenticate them.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			Supports (integral to) PR-AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	IBM Security Verify performs user and device authentication.
			Supports (example of) RS.MI-1: Incidents are contained	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, IBM Security Verify will limit the attacker to accessing only those resources that the legitimate user's role or attributes allow. This is one example of how incidents can be contained.
			Supports (example of) RS.MI-2: Incidents are mitigated	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the attacker will only be allowed to access that resource in the way that the legitimate user's role allows (e.g., read-only vs. read-write). This is one example of how incidents can be mitigated.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	IBM Security Verify performs ongoing, intermittent user authentication and authorization, thereby monitoring for unauthorized users and devices.
ICAM - Federated Identity	IBM Security Verify	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	Is supported by (precedes) ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	The Federated Identity component supported by IBM Security Verify enables management and enforcement of the cybersecurity roles and responsibilities that have already been established and stored for many different groups—the enterprise workforce and third-party stakeholders (e.g., suppliers, customers, partners).
ICAM - Identity Governance	IBM Security Verify	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IBM Security Verify supports the auditing of identities and credentials.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		reporting) to ensure compliance with requirements and regulations.	Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	IBM Security Verify supports the management of access permissions and authorizations in a way that incorporates the principles of least privilege and separation of duties.
			Is supported by (precedes) ID.GV-1: Organizational cybersecurity policy is established and communicated	IBM Security Verify ensures that the organization's cybersecurity policy is enforced in such a way that it complies with regulatory, legal, and other governance-related requirements. This policy must already be established before it can be enforced by the Identity Governance component.
			Supports (integral to) ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	IBM Security Verify supports the coordination and alignment of cybersecurity roles and responsibilities with internal roles and external partners to ensure that the organization operates in accordance with regulatory, legal, and other governance-related requirements.
			Is supported by (precedes) ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are	The identity governance processes that IBM Security Verify uses are defined to ensure that the organization operates in conformance with all legal and regulatory requirements. These requirements must be well understood in order to serve as a basis for defining the

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			understood and managed	identity governance processes. As these requirements change, they must be managed on an ongoing basis, and they may require changes to identity governance processes.
			Supports (integral to) ID.GV-4: Governance and risk management processes address cybersecurity risks	The identity governance processes that IBM Security Verify uses are defined and managed with the objective of addressing cybersecurity risks.
			Supports (integral to) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	IBM Security Verify performs logging and audits all identity management activities in accordance with policy and regulations.
ICAM - Multi-Factor Authentication (MFA)	IBM Security Verify	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IBM Security Verify supports the auditing of identities and credentials.
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	IBM Security MaaS360	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	IBM Security MaaS360 involves device enrollment into a UEM/MDM system. The device must be known to be part of the organization's inventory before it can be enrolled.
			Supports (integral to) ID.AM-2:	IBM Security MaaS360 installs, manages, configures, and

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.	Software platforms and applications within the organization are inventoried	updates applications on UEM/MDM-managed devices, so it provides inventory information regarding these applications.
			Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	IBM Security MaaS360 supports the identification and remediation of device vulnerabilities by updating software on managed devices.
			Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	IBM Security MaaS360 monitors for suspicious activity; detects and disables malware, viruses, and other malicious traffic; and repairs infected files on managed devices.
			Supports (integral to) PR.AC-3: Remote access is managed	IBM Security MaaS360 prevents a remote device that it is managing from being able to access any resources until the device is brought into compliance.
			Supports (example of) PR.DS-1: Data-at-rest is protected	IBM Security MaaS360 encrypts data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (example of) PR-DS-2: Data-in-transit is protected	IBM Security MaaS360 encrypts data sent from the device, but this data could also be encrypted via a different mechanism.
			Supports (example of) PR.DS-5: Protections against data leaks are implemented	IBM Security MaaS360 tracks user activity on the device and monitors for unauthorized traffic to help prevent, detect, and mitigate data leaks.
			Supports (example of) PR.DS-6:	IBM Security MaaS360 uses integrity checking to verify

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			Integrity checking mechanisms are used to verify software, firmware, and information integrity	updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
			Supports (example of) PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	IBM Security MaaS360 relies on device attestation or similar mechanisms that use integrity checking to verify the hardware integrity of the device before trusting the device.
			Supports (integral to) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	IBM Security MaaS360 ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. It enforces and maintains these baselines at endpoints.
			Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The baseline configuration that IBM Security MaaS360 enforces should be developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. IBM Security MaaS360 operation depends on the existence of such baselines.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			Supports (example of) PR.IP-6: Data is destroyed according to policy	IBM Security MaaS360 remotely deletes applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
			Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	IBM Security MaaS360 mitigates and remediates vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before IBM Security MaaS360 can enforce them, and they constitute at least one portion of the organization's vulnerability management plan.
			Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	IBM Security MaaS360 restricts the use of removable media as required by policy.
			Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	IBM Security MaaS360 may be used to configure devices to provide only essential capabilities.
			Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential	IBM Security MaaS360 monitors user activity for suspicious behavior.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			cybersecurity events	
			Supports (example of) DE.CM-4: Malicious code is detected	IBM Security MaaS360 prevents, detects, and disables numerous types of malicious code.
			Supports (example of) DE.CM-5: Unauthorized mobile code is detected	IBM Security MaaS360 detects unauthorized mobile code.
			Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	IBM Security MaaS360 monitors the device for unauthorized software and connections.
			Supports (integral to) RS.MI-1: Incidents are contained	IBM Security MaaS360 performs many activities that help to contain incidents, such as detecting and disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.
			Supports (integral to) RS.MI-2: Incidents are mitigated	IBM Security MaaS360 performs many activities that help to mitigate incidents, such as detecting and

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
				disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.
Endpoint Security - Endpoint Protection Platform (EPP)	IBM Security MaaS360	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections;	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	IBM Security MaaS360 involves installation of EDR/EPP software on the device. The device must be known to be part of the organization's inventory before the EDR/EPP software can be installed.
			Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	IBM Security MaaS360 inventories software on the device.
			Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	IBM Security MaaS360 scans the device to detect missing patches or outdated software and report them. It can also install patches if instructed to do so later.
			Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	IBM Security MaaS360 detects and disables malware, viruses, and other signature-based threats.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (integral to) PR.AC-3: Remote access is managed	IBM Security MaaS360 includes a firewall that blocks unauthorized connections to and from the device.
			Supports (example of) PR.DS-1: Data-at-rest is protected	IBM Security MaaS360 encrypts data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (example of) PR-DS-2: Data-in-transit is protected	IBM Security MaaS360 encrypts data sent from the device, but this data could also be encrypted via a different mechanism.
			Supports (example of) PR.DS-5: Protections against data leaks are implemented	IBM Security MaaS360 includes a firewall that blocks unauthorized traffic to and from the device.
			Supports (example of) PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	IBM Security MaaS360 uses integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
			Supports (integral to) and Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating	IBM Security MaaS360 ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. This baseline that IBM Security MaaS360 enforces must have been developed based on security principles, such as the concept of least functionality, in

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			security principles (e.g., concept of least functionality)	accordance with the organization's policies. So IBM Security MaaS360 operation depends on the existence of such baselines, but it also enforces and maintains these baselines.
			Supports (example of) PR.IP-6: Data is destroyed according to policy	IBM Security MaaS360 remotely deletes applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
			Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	IBM Security MaaS360 mitigates and remediates vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before IBM Security MaaS360 can enforce them, and they constitute at least one portion of the organization's vulnerability management plan.
			Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	IBM Security MaaS360 restricts the use of removable media as required by policy.
			Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide	IBM Security MaaS360 can configure devices to provide only essential capabilities.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			only essential capabilities	
			Supports (example of) DE.CM-4: Malicious code is detected	IBM Security MaaS360 detects and disables malware, viruses, and other signature-based threats.
			Supports (example of) DE.CM-5: Unauthorized mobile code is detected	IBM Security MaaS360 can detect unauthorized mobile code.
			Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	IBM Security MaaS360 monitors the device for unauthorized software and connections.
			Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	IBM Security MaaS360 monitors user activity for suspicious behavior.
			Supports (integral to) RS.MI-1: Incidents are contained	IBM Security MaaS360 performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device,

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
				which limits the data's usefulness if it is exfiltrated.
			Supports (integral to) RS.MI-2: Incidents are mitigated	IBM Security MaaS360 performs many activities that help to mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
Endpoint Security - Endpoint Compliance	IBM Security MaaS360	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	IBM Security MaaS360 involves installation of EDR/EPP software onto devices that are known to be part of the organization's inventory. The device must be known to be part of the organization's inventory before the software can be installed.
			Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	IBM Security MaaS360 has both the capability and the policy to inventory software on the device.
			Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	IBM Security MaaS360 scans the device to detect missing patches or outdated software and report them. It can also install patches if instructed to do so later.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Security Analytics – Security Information and Event Management (SIEM)	IBM Security QRadar XDR	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Supports (example of) DE.AE-2: Detected events are analyzed to understand attack targets and methods	IBM QRadar is a SIEM that collects security and event information from many components. This aggregated data may be analyzed to understand attack targets and methods.
			Supports (integral to) DE.AE-3: Event data are collected and correlated from multiple sources and sensors	IBM QRadar is a SIEM that collects and correlates security event data from multiple sources.
			Supports (example of) DE.AE-4: Impact of events is determined	Security analysts may use data collected and correlated in IBM QRadar to help them determine the impact of events.
			Supports (example of) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The IBM QRadar SIEM supports aggregating logs of security information and event activity as required by policy.
			Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	The IBM QRadar SIEM supports logs that can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
			Supports (example of) RS.AN-2: The impact of the	The IBM QRadar SIEM supports logs that can provide data that helps security analysts to understand the

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			incident is understood	impact of cybersecurity incidents.
			Supports (example of) RS.AN-3: Forensics are performed	The IBM QRadar SIEM supports logs that can provide data that can help security analysts to perform forensic analysis of cybersecurity incidents.
Security Analytics - Security Orchestration, Automation, and Response (SOAR)	IBM Cloud Pak for Security	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (example of) RS.RP-1: Response plan is executed during or after an incident	IBM Cloud Pak for Security supports a security integration platform that can execute predefined incident response workflows.
			Supports (example of) RS.AN-2: The impact of the incident is understood	IBM Cloud Pak for Security supports security analysts who want to use a security integration platform to visualize security events and their impacts, thereby enabling incidents to be better understood.
			Supports (example of) RS.AN-3: Forensics are performed	IBM Cloud Pak for Security supports security analysts who want to use a security integration platform to help them perform forensic analysis of cybersecurity incidents.
Security Analytics – User Behavior Analytics	IBM Security Verify/Trusteer	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	IBM Trusteer's support for user behavior analytics is an essential part of monitoring the activity of personnel to detect potential cybersecurity events.
Data Security – Data Encryption	IBM Security Guardium Data	Provides strong encryption and key management	Supports (integral to) PR.DS-1: Data-at-rest is protected	IBM Security GDE supports encryption and key management, which are essential for protecting the

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	Encryption (GDE)	capabilities for both structured and unstructured data both on premises and in the cloud		confidentiality of data, whether the data is at rest or in transit.
			Supports (integral to) PR.DS-2: Data-in-transit is protected	IBM Security GDE supports encryption and key management, which are essential for protecting the confidentiality of data, whether the data is at rest or in transit.
Data Security - Data Access Protection	IBM Security Guardium Data Encryption (GDE)	Discovers, classifies, and labels sensitive business critical data in the cloud and on-premises and provides protection by preventing unauthorized access and minimizing the risk of data theft and data leaks using security policy rules.	Supports (example of) PR.DS-1: Data-at-rest is protected	IBM Security GDE supports and provides policy-based protection of the data according to its classification. This is one way to help protect data stored in the cloud and on-premises.

4.1.2.5 Mapping Between Mandiant Technologies and NIST CSF Subcategories

Table 4-6 lists the technologies that Mandiant has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST CSF Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. Mandiant technologies have been included in all builds of the project.

488 **Table 4-6 Mapping Between Mandiant Functionality and NIST CSF Subcategories**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Security Analytics - Security Controls Validation	Mandiant Security Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows	Supports (integral to) DE.DP-3: Detection processes are tested	Security Validation is used to test and verify the effectiveness of detection processes and other ZTA cybersecurity controls.
			Supports (example of) DE.DP-5: Detection processes are continuously improved	The organization can use Security Validation to continuously monitor, measure, and validate the effectiveness of cybersecurity controls, thereby enabling the organization to continuously improve detection processes.

489 ### *4.1.2.6 Mapping Between Tenable Technologies and NIST CSF Subcategories*

490 **Table 4-7** lists the technologies that Tenable has contributed to the ZTA builds implemented in this
491 project and details the mappings between the functionality performed by these technologies and the
492 NIST CSF Subcategories. It indicates how these components help support CSF Subcategories and vice
493 versa. Tenable technologies have been included in all builds of the project.

494 **Table 4-7 Mapping Between Tenable Functionality and NIST CSF Subcategories**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Security Analytics – Endpoint Monitoring	Tenable.io	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts	Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	Tenable.io inventories software on the endpoints. A key function of the Endpoint Monitoring component is to check endpoints for missing patches, updates, and upgrades.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		(devices or VMs) that are connected to the network		
Security Analytics - Vulnerability Scanning and Assessment	Tenable.io and Tenable.ad	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) DE.CM-8: Vulnerability scans are performed	A key function of Tenable.io and Tenable.ad is to perform vulnerability scans.
Security Analytics - Traffic Inspection	Tenable NNM	Interception, examination, and recording of relevant traffic transmitted on the network.	Supports (integral to) DE.CM-1: The network is monitored to detect potential cybersecurity events	Traffic inspection, which is performed by Tenable NNM, is an essential part of monitoring the network to detect potential cybersecurity events.
Security Analytics - Network Discovery	Tenable NNM	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	Network Discovery, which is performed by Tenable NNM, can help identify unknown and/or unexpected devices and activity that may be indicative of suspicious events, making it an example of how the network can be monitored to detect potential cybersecurity events.

4.1.2.7 Mapping Between VMware Technologies and NIST CSF Subcategories

Table 4-8 lists the technologies that VMware has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST CSF Subcategories. It indicates how these technologies help support CSF Subcategories and vice versa. VMware technologies have been included in build E2B3.

500 **Table 4-8 Mapping Between VMware Functionality and NIST CSF Subcategories**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	VMware Workspace ONE UEM	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to be enrolled into VMware Workspace ONE UEM, the device must be part of the organization's inventory.
			Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	VMware Workspace ONE UEM installs, manages, configures, and updates applications on UEM/MDM-managed devices, so it provides inventory information regarding these applications.
			Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	VMware Workspace ONE UEM may be able to identify and remediate device vulnerabilities by updating software on managed devices, for example.
			Supports (integral to) PR.AC-3: Remote access is managed	VMware Workspace ONE UEM may prevent a remote device that it is managing from being able to access any resources until the device is brought into compliance.
			Supports (example of) PR.DS-1: Data-at-rest is protected	VMware Workspace ONE UEM may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (integral to) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and	VMware Workspace ONE UEM ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. VMware Workspace ONE UEM

			maintained incorporating security principles (e.g., concept of least functionality)	enforces and maintains these baselines at endpoints.
			Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The baseline configuration on the endpoints that VMware Workspace ONE UEM enforces must have been developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. VMware Workspace ONE UEM operation depends on the existence of such baselines.
			Supports (example of) PR.IP-6: Data is destroyed according to policy	VMware Workspace ONE UEM can remotely delete applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
			Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	VMware Workspace ONE UEM can mitigate and remediate vulnerabilities and threats in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before VMware Workspace ONE UEM can enforce them, and they constitute at least one portion of the organization's vulnerability management plan.
			Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	VMware Workspace ONE UEM can restrict the use of removable media as required by policy.

			Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	VMware Workspace ONE UEM can be used to configure devices to provide only essential capabilities.
			Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	VMware Workspace ONE UEM monitors the device for unauthorized software.

4.2 NIST SP 800-53 Control Mappings

This section provides mappings between ZTA functionality and NIST SP 800-53 Controls.

4.2.1 Mapping Between ZTA Reference Design Functions and NIST SP 800-53 Controls

Table 4-9 provides a mapping between the functions provided by the logical components of the ZTA reference design and NIST SP 800-53 security controls. This table indicates how ZTA functions help support NIST SP 800-53 controls. Because hundreds of NIST SP 800-53 controls can help support ZTA functions, we have omitted use case 2 (see Section 3.1), identifying how existing SP 800-53 controls can help support a ZTA implementation. Readers needing to determine how their SP 800-53 implementations apply to a ZTA implementation can follow the Risk Management Framework.

Table 4-9 Mapping Between ZTA Reference Design Functions and NIST SP 800-53 Controls

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, information from functional	Supports (integral to) AC-17: Remote Access	The PE authorizes each type of remote access to the system prior to allowing such connections.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PE authorizes the connection of mobile devices to organizational systems.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	components, and a trust algorithm	Supports (integral to) AC-20: External Systems	The PE authorizes or denies access to systems that are used by but are not part of on-premises systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness.
		Supports (integral to) AC-24: Access Control Decisions	The key function of the PE is to make access control decisions based on policy.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PE permits or prohibits remote activation of collaborative computing devices and applications.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) AC-3: Access Enforcement	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-17: Remote Access	The PA supports the enforcement of remote access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PA conveys mobile device access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-20: External Systems	The PA conveys external system access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PA conveys collaborative computing device activation decision information from the PE to the PEP, where the decision can be enforced.
	Guards the trust zone that hosts an	Supports (integral to) AC-2: Account Management	The PEP enforces authorized access to the system based on

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA		valid access authorization or intended system usage.
		Supports (integral to) AC-3: Access Enforcement	The PEP enforces access decisions.
		Supports (integral to) AC-4: Information Flow Enforcement	The PEP enforces approved authorizations for controlling the flow of information within the system and between connected systems. The data plane and control plane (networks) are logically separate. The PEP is the only component that can send and receive messages from both planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.
		Supports (integral to) AC-12: Session Termination	The PEP can terminate connections to enforce compliance with policies.
		Supports (integral to) AC-17: Remote Access	The PEP can enforce remote access decisions.
		Supports (integral to) AC-18: Wireless Access	The PEP can enforce wireless access decisions.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PEP can enforce access decisions regarding connection to mobile devices.
		Supports (integral to) AC-20: External Systems	The PEP can enforce access decisions regarding connection to external systems.
		Supports (integral to) CA-7: Continuous Monitoring	The PEP monitors connections between a subject and an enterprise resource to detect prohibited or suspicious activity.
		Supports (integral to) IR-4: Incident Handling	If a resource is compromised, incidents are contained because attackers cannot move laterally from the compromised resource to any resources that are not also in that part of the

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			enterprise guarded by the compromised resource's PEP.
		Supports (example of) SC-7: Boundary Protection	The PEP can enforce access decisions to key internal managed interfaces within the system including publicly accessible system components that are separated from internal organizational networks. It can prevent unauthorized access to the portions of the enterprise that it guards. If it is used to protect a single resource, it does not necessarily provide network segregation or network segmentation. However, it can be deployed to protect and segregate discrete network segments.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PEP can enforce access decisions regarding activation of collaborative computing devices.
		Supports (integral to) SC-23: Session Authenticity	The PEP is the only component that can send and receive messages from both the data and control planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.
		Supports (integral to) SC-32: System Partitioning	The PEP can enforce approved authorizations for controlling the flow of information within the system.
		Supports (integral to) SC-41: Port and I/O Device Access	The PEP can enforce authorizations for access to I/O ports and devices.
		Supports (integral to) SC-43: Usage Restrictions	The PEP can enforce authorization and control of usage restrictions for system components.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) SI-4: System Monitoring	The PEP monitors connections between a subject and an enterprise resource to detect prohibited or suspicious activity.
ICAM - Identity Management	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	Supports (integral to) AC-2: Account Management	The Identity Management function includes account management such as definition of the types of accounts allowed and specifically prohibited for use within the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account.
		Supports (integral to) AC-3: Access Enforcement	The Identity Management function enforces approved authorizations associated with logical access to information and system resources in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Identity Management function is a necessary component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of separation of duties, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) AC-6: Least Privilege	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-17: Remote Access, including enhancement #1	The Identity Management function authorizes each type of remote access to the system prior to allowing such connections.
		Supports (integral to) AC-24: Access Control Decisions	The Identity Management function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	The Identity Management function is necessary for unique identification and authentication of organizational users.
		Supports (integral to) IA-5: Authentication Management	The Identity Management function permits verification, as part of the initial authenticator distribution, of the identity of the individual receiving the authenticator.
		Supports (integral to) IA-8: Identification and Authentication (Non-organizational Users)	The Identity Management function is necessary for unique identification and authentication of non-organizational users.
		Supports (integral to) PE-2: Physical Access Authorizations	The Identity Management function is the basis for

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			authorization of credentials for facility access, including physical access to security-critical devices.
ICAM - Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which access requests are authorized.	Supports (integral to) AC-2: Account Management	The Access and Credential Management function includes account management such as definition of the types of accounts allowed and specifically prohibited for use within the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account by performing user authentication.
		Supports (integral to) AC-3: Access Enforcement	The Access and Credential Management function enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Access and Credential Management function is a necessary component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	Access and Credential Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of separation of duties, and to manage each user's roles

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-6: Least Privilege	Access and Credential Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-24: Access Control Decisions	The Access and Credential Management function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
		Supports (integral to) IA-1: Policy and Procedures	The Access and Credential Management function is integral to implementation of the organization's identification and authentication policies and procedures.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	Access and Credential Management is a necessary element of uniquely identifying and authenticating organizational users. To determine whether an access is authorized, the Access and Credential Management component authenticates the user or device that is requesting access by verifying the

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			credentials that are bound to the user or device and asserted as part of the access request. These credentials must be asserted for this IDAM component to be able to authenticate the user request.
		Supports (precedes) IA-3: Device Identification and Authentication	The Access and Credential Management function is necessary in order to uniquely identify and authenticate organization-defined devices and/or types of devices.
		Supports (integral to) IA-5: Authentication Management	The Access and Credential Management function permits verification, as part of the initial authenticator distribution, of the identity of the individual receiving the authenticator.
		Supports (integral to) IA-8: Identification and Authentication (Non-Organizational Users)	The Access and Credential Management function is necessary for unique identification and authentication of non-organizational users.
		Supports (integral to) IA-9: Service Identification and Authentication	The Access and Credential Management function is necessary for authorization of user/system connections to services employing identification and authentication mechanisms.
		Supports (example of) IR-4: Incident Handling	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the Access and Credential Management component will limit the attacker to accessing only those resources that the legitimate user's role allows.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
ICAM - Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	Supports (example of) IA-5: Authentication Management	An extension of IA-5 (9) requires acceptance and verification of federated or PKI credentials.
		Supports (example of) IA-8: Identification and Authentication (Non-Organizational Users)	Extensions of IA-8 (5 and 6) require acceptance and verification of federated or PKI credentials.
		Supports (example of) IA-12: Identity Proofing	An extension of IA-12 (6) calls for accepting externally proofed identities, a fundamental component of managing federated identities across agencies and organizations.
ICAM - Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) AC-2: Account Management	The Identity Governance function includes account management such as authorized users of the system, access authorizations (i.e., privileges), and assignment of organization-defined attributes.
		Supports (integral to) AC-3: Access Enforcement	The Identity Governance function enforces approved authorizations for logical access to information and system resources by identified users in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Identity Governance function is a necessary component of the identity component of access authorizations on which information flow enforcement depends.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) AC-5: Separation of Duties	The Identity Governance component can manage access permissions and authorizations in a way that incorporates the separation of duties principle.
		Supports (integral to) AC-6: Least Privilege	The Identity Governance component can manage access permissions and authorizations in a way that incorporates the least privilege principle.
		Supports (integral to) AC-24: Access Control Decisions	The Identity Governance function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement and that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
		Supports (integral to) AU-2: Event Logging	The Identity Governance component logs all identity management activities in accordance with policy and regulations.
		Supports (integral to) AU-12: Audit Record Generation	The Identity Governance component audits all identity management activities in accordance with policy and regulations.
ICAM - Multi-Factor Authentication (MFA)	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	The MFA component enables users to be authenticated using a second factor, which is required for access to privileged accounts and processes and in some cases, non-privileged accounts and processes.
Endpoint Security - Unified Endpoint	Manages and secures enterprise desktop computers, laptops,	Supports (integral to) AC-1: Policy and Procedures	UEM/MDM devices enforce access control policies and procedures and associated access controls.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Management (UEM)/Mobile Device Management (MDM)	and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.	Supports (integral to) AC-2: Account Management	The UEM/MDM can monitor the use of accounts user activity for prohibited use.
		Supports (integral to) AC-6: Least Privilege	The UEM/MDM can be used to configure devices to provide only essential capabilities.
		Supports (integral to) AC-17: Remote Access	The UEM/MDM enforces usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed and authorizes each type of remote access to the system prior to allowing such connections. May use encrypted VPNs to enhance confidentiality and integrity for remote connections.
		Supports (integral to) AC-18: Access Control for Wireless Access	The UEM/MDM enforces configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorizes each type of wireless access to the system prior to allowing such connections. An AC-18 extension (1) requires protection of wireless access to the system using authentication of users and devices and encryption.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The UDM/MDM enforces configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas and authorizes the connection of mobile devices to organizational systems.
		Supports (integral to) AC-20: Use of External Systems	The UDM/MDM enforces organization-defined controls

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing only authorized individuals to access the system from external systems and processing, storing, or transmitting organization-controlled information using external systems.
		Supports (integral to) CA-7: Least Functionality	The UEM/MDM enforces configuration of the system to provide only organization-defined mission essential capabilities. The UEM/MDM can monitor user activity to ensure that users are granted only the minimum access necessary to perform an operation and that such access is granted only for the minimum amount of time necessary.
		Supports (integral to) CM-2: Baseline Configuration	The UEM/MDM ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware.
		Supports (integral to) CM-4: Impact Analysis	The UEM/MDM ensures that the devices are compliant with organizational policy regarding analysis of changes to the system to determine potential security and privacy impacts prior to change implementation.
		Supports (integral to) CM-5: Access Restrictions for Change	The UEM/MDM enforces physical and logical access restrictions associated with changes to the system.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) CM-6: Configuration Settings	The UEM/MDM enforces configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations and implements the configuration settings.
		Supports (integral to) CM-10: Software Usage Restrictions	The UEM/MDM can monitor user activity for violation of usage restrictions.
		Supports (example of) CM-11: User Installed Software	The UEM/MDM can monitor user activity to enforce software installation policies.
		Supports (example of) CM-14: Signed Components	The UEM/MDM may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
		Supports (integral to) IR-4: Incident Handling	The UEM/MDM performs many activities that help to contain and mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
		Supports (example of) MP-6: Media Sanitization	The UEM/MDM can remotely delete applications and data from devices as needed according to policy (not complete sanitization).

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) MP-7: Media Use	The UEM/MDM can restrict the use of removable media as required by policy.
		Supports (integral to) PM-5: System Inventory	The UEM/MDM installs, manages, configures, and updates applications on UEM/MDM managed devices, so it provides inventory information regarding these applications.
		Supports (example of) RA-3: Risk Assessment	The UEM/MDM may be able to identify device vulnerabilities by updating software, for example. The UEM/MDM may monitor for suspicious activity; detect and disable malware, viruses, and other malicious traffic; and repair infected files. The UEM/MDM can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
		Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	The UEM/MDM can monitor device software, firmware, and configurations for vulnerabilities and threats.
		Supports (integral to) SC-18: Mobile Code	The UEM/MDM may be able to detect unauthorized mobile code.
		Supports (example of) SC-3: Security Function Isolation	The UEM/MDM can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities.
		Supports (example of) SC-8: Transmission Confidentiality and Integrity	The UEM/MDM can provide cryptographic protection for transmitted information.
		Supports (integral to) SC-13: Cryptographic Protection	The UEM/MDM may provide cryptographic protection to

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			support a variety of security solutions.
		Supports (example of) SC-28: Protection of Data at Rest	The UEM/MDM can provide cryptographic protection for data that is stored onsite.
		Supports (integral to) SI-2: Flaw Remediation	The UEM/MDM mitigates and remediates vulnerabilities that it detects in device software, firmware, and configuration.
		Supports (integral to) SI-3: Malicious Code Protection	The UEM/MDM prevents, detects, and disables malware, viruses, and other malicious traffic. It also repairs infected files when possible. When malicious code is detected, it provides alerts and may recommend remediation action.
		Supports (integral to) SI-4: System Monitoring	The UEM/MDM monitors the device for unauthorized software and connections. The UEM/MDM monitors the system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives and unauthorized local, network, and remote connections to identify unauthorized use of the system.
Endpoint Security – Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect	Supports (integral to) AC-2: Account Management	The EDR/EPP can monitor the use of accounts.
		Supports (integral to) AC-4: Information Flow Enforcement	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) AC-17: Remote Access	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The EDR/EPP may include a firewall that blocks

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.		unauthorized connections to and from the device.
		Supports (integral to) AC-20: Use of External Systems	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) CA-7: Continuous Monitoring	The EDR/EPP scans the device to detect missing patches or outdated software and report them.
		Supports (integral to) CM-2: Baseline Configuration	The EDR/EPP ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software. It is a prerequisite that the compliance policies incorporate appropriate security principles.
		Supports (integral to) CM-7: Least Functionality	The EDR/EPP can be used to configure devices to provide only essential capabilities.
		Supports (integral to) CM-8: System Component Inventory	For a device to have EDR/EPP software installed on it, the device must be known to be part of the organization's inventory.
		Supports (integral to) IR-4: Incident Handling	The EDR/EPP performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) MP-2: Media Access	The EDR/EPP can restrict the use of removable media as required by policy.
		Supports (example of) MP-6: Media Sanitization	The EDR/EPP can remotely delete applications and data from devices as needed according to policy (not full sanitization).
		Supports (example of) MP-7: Media Use	The EDR/EPP can restrict the use of organization-defined types of system media on organization-defined systems or system.
		Supports (example of) PM-5: System Inventory	The EDR/EPP can inventory software on the device.
		Supports (integral to) RA-3: Risk Assessment	The EDR/EPP supports Identification of threats to and vulnerabilities in the system by scanning the device to detect missing patches or outdated software and reporting them. The EDR/EPP also detects malware, viruses, and other signature-based threats.
		Supports (integral to) SC-7: Boundary Protection	The EDR/EPP may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The EDR/EPP may encrypt data sent from the device and may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (example of) SC-10: Software Usage Restrictions	The EDR/EPP can monitor user activity to enforce usage restrictions.
		Supports (example of) SC-11: User-Installed Software	The EDR/EPP can monitor activity to enforce software installation policies.
		Supports (integral to) SC-13: Cryptographic Protection	The EDR/EPP may encrypt data sent from the device or stored on the device.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The EDR/EPP may include a firewall that blocks unauthorized remote activation of collaborative computing devices and applications.
		Supports (integral to) SC-18: Mobile Code	The EDR/EPP may be able to detect unauthorized mobile code.
		Supports (integral to) SC-28: Protection of Information at Rest	The EDR/EPP may encrypt data stored on the device.
		Supports (example of) SI-2: Flaw Remediation	The EDR/EPP can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
		Supports (integral to) SI-3: Malicious Code Protection	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (integral to) SI-4: System Monitoring	The EDR/EPP monitors the device for unauthorized software and connections.
		Supports (example of) SI-7: Software, Firmware, and Information Integrity	The EDR/EPP may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
Endpoint Security – Endpoint Compliance	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Supports (example of) SI-3: Malicious Code Protection	SI-3 requires configuration of malicious code protection mechanisms to perform periodic scans of the system. A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans.
		Supports (integral to): RA-5: Vulnerability Monitoring and Scanning	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Security Analytics – Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Supports (integral to) AU-2: Event Logging	The SIEM logs security information and event activity as required by policy.
		Supports (integral to) AU-6: Audit Record Review, Analysis, and Reporting	The SIEM collects security and event information from many components. This data may be analyzed to understand attack targets and methods. Security analysts rely at least in part on SIEM data to help them determine the impact of events.
		Supports (example of) AU-7: Audit Record Reduction and Report Generation	The SIEM logs can provide helpful data that can help with forensic analysis of cybersecurity incidents.
		Supports (integral to) CA-7: Continuous Monitoring	The SIEM collects security and event information from many components.
		Supports (integral to) IR-4: Incident Handling	The SIEM collects security and event information from many components. This data may be analyzed to understand attack targets and methods and the impact of cybersecurity incidents.
		Supports (integral to) IR-5: Incident Monitoring	The SIEM collects security and event information from many components to support tracking and documentation of events. The SIEM logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
		Supports (integral to) RA-3: Risk Assessment	Security analysts rely at least in part on SIEM data to help them determine the impact of events.
		Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	The SIEM acts as a vulnerability scanning and assessment tool.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) SC-7: Boundary Protection	The SIEM collects and correlates event information. The SIEM logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
Security Analytics – Security Controls Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows.	Supports (integral to) AC-4: Information Flow Enforcement	Provides visibility into network traffic and transaction flows necessary to validate controls intended to enforce approved authorizations for controlling the flow of information within the system and between connected systems.
		Supports (integral to) CA-2: Control Assessments	Provides visibility into network traffic and transaction flows necessary to validate assessment of controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirement.
		Is supported by (Integral to) CA-7: Continuous Monitoring	The network must be monitored to have visibility into network traffic.
		Is supported by (integral to) SI-4: System Monitoring	To determine what security controls should be implemented and validated, the organization should have a good understanding of what communication and data flows are needed to support the organization's mission. This understanding can be obtained by mapping organizational communication and data flows.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) SI-10: Information Input Validation	Security Controls Validation is used to test and verify the inputs to detection processes and other ZTA cybersecurity controls.
Security Analytics–-Identity Monitoring	Monitors the identity of subjects to detect and send alerts for indicators that user accounts or credentials may be compromised, or to detect sign-in risks for a particular access session.	Supports (integral to) AC-3: Access Enforcement	Monitoring the identities of subjects supports enforcement of approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
		Supports (integral to) AC-24: Access Control Decisions	Monitoring the identities of subjects supports ensuring that organization-defined access control decisions are applied to each access request prior to access enforcement.
		Is supported by (integral to) IA-2: Identification and Authentication (Organizational Users)	Uniquely identifying and authenticating users and associating that unique identification with processes acting on behalf of those users are necessary to effectively monitor the identities of subjects. In order to be able to monitor the activity of particular subjects for risks, those subjects must have been issued digital identities.
		Is supported by (integral to) IA-4: Identifier Management	Management of identifiers is necessary for effective monitoring of subject identities.
		Is supported by (integral to) IA-8: Identification and Authentication (Non-organizational Users)	Uniquely identifying and authenticating users and associating that unique identification with processes acting on behalf of those users are necessary to effectively monitor the identities of subjects. In order to be able to monitor the activity of particular subjects for risks, those subjects

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			must have been issued digital identities.
Security Analytics – User Behavior Analytics	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) AC-2 (12): Account Management (Account Monitoring for Atypical Usage)	Performing user behavior analytics is an essential part of monitoring the activity of personnel to detect potential cybersecurity events.
		Supported by (integral to) CA-7: Continuous Monitoring	Continuous monitoring provides the information required for analysis of user behavior.
Security Analytics - Security Monitoring	Monitors and detects malicious or suspicious user actions based on access activity	Supported by (example of) AC-2: Account Management	Detection of unauthorized actions is assisted by knowing the access authorizations for each account.
		Supports (example of) AC-4: Information Flow Enforcement	One way to detect unauthorized information flows (e.g., exfiltration) is to notice differences between expected flows and actual flows.
		Supported by (integral to) CA-7: Continuous Monitoring	Continuous monitoring is necessary for security monitoring functions.
		Supports (example of) SI-4: System Monitoring	System monitoring capabilities are achieved through a variety of tools and techniques including intrusion detection, scanning tools, audit record monitoring, and network monitoring.
Security Analytics - Application Protection and Response	Protects particular applications from phishing, spam, malware and other zero day attacks	Supports (example of) SI-3: Malicious Code Protection	Use of an application protection response component is one way to detect malicious code.
		Supports (example of) SI-8: Spam Protection	Use of an application protection response component is one way to detect spam.
Security Analytics - Cloud Access Permission Manager	Provides visibility and control of permissions used by identities in various cloud platforms	Supports (example of) AC-2; Account Management	This component provides the visibility and control necessary to specify authorized users of the system and access authorizations for each account.
		Supports (example of) AC-3: Access Enforcement	This component provides the visibility and control necessary

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			to enforce approved authorizations for logical access to information and systems resources.
		Supports (example of) AC-6: Least Privilege	This component provides the visibility and control necessary to enforce least privilege.
		Supports (example of) AC-24: Access Control Decisions	This component provides the visibility and control necessary for access control decisions.
Security Analytics – Endpoint Monitoring	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts (devices or VMs) that are connected to the network	Supported by (integral to) CA-7: Continuous Monitoring	Continuous monitoring is essential for detecting unauthorized software on endpoints and is also a good way to detect unauthorized devices and connections.
Security Analytics – Vulnerability Scanning and Assessment	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to): RA-5: Vulnerability Monitoring and Scanning	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans.
Security Analytics – Security Orchestration, Automation, and Response (SOAR)	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help	Supports (integral to) CP-10: System Recovery and Reconstitution	A SOAR can provide for the recovery and reconstitution of the system to a known state within an organization-defined time period consistent with recovery time and recovery point objectives after a

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.		disruption, compromise, or failure.
		Supports (example of) IR-4: Incident Handling	The SOAR can be used to implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
Security Analytics - Traffic Inspection	Intercepts, examines, and records relevant traffic transmitted on the network.	Supports (integral to) CA-7: Continuous Monitoring	Traffic inspection is an essential part of monitoring the network to detect potential cybersecurity events.
Security Analytics - Network Discovery	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (integral to) AU-13: Monitoring for Information Disclosure	A key function of Network Discovery is to monitor the network to find, identify, and document unknown and/or unexpected devices and activity that may pose a threat to the organization.
		Supports (example of) CA-7: Continuous Monitoring	A key function of Network Discovery is to monitor the network.
		Supports (example of) RA-3: Risk Assessment	Network Discovery can support risk assessment through predictive cyber analytics using automated threat discovery and response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine assisted decision tools.
		Supports (example of) SC-7: Boundary Protection	Key functions of the Network Discovery component include monitoring and controlling communications at the external managed interfaces to the sys-

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			tem and at key internal managed interfaces within the system.
		Supports (example of) SI-4: System Monitoring	Key functions of the Network Discovery component include monitoring the system to detect attacks and indicators of potential attacks; unauthorized local, network, and remote connections and identifying unauthorized use of the system.
Security Analytics - Network Monitoring	Aggregates and analyzes network telemetry—information generated by network devices—to provide network visibility both on premises and in clouds and to detect and respond to threats	Supports (integral to) AU-13: Monitoring for Information Disclosure	A key function of Network Monitoring is to monitor the network to find, identify, and document unknown and/or unexpected devices and activity that may pose a threat to the organization. Note that the EDR/EPP can monitor the device for unauthorized network connections. Other network monitoring technologies can be used instead of EDR/EPP to do this.
		Supports (integral to) CA-7: Continuous Monitoring	A key function of Network Monitoring is to monitor the network at all times.
		Supports (example of) RA-3: Risk Assessment	Network Monitoring can support risk assessment through predictive cyber analytics using automated threat discovery and response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine assisted decision tools.
		Supports (integral to) SC-7: Boundary Protection	Key functions of the Network monitoring component include monitoring and controlling communications at the external

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			managed interfaces to the system and at key internal managed interfaces within the system. Note that the PEP may be used to monitor connections between a subject and an enterprise resource to detect prohibited or suspicious activity. However, it must not necessarily be configured to do so. Network monitoring may also be provided by other mechanisms besides a PEP.
		Supports (example of) SI-4: System Monitoring	Key functions of the Network Monitoring component include monitoring the system to detect attacks and indicators of potential attacks; unauthorized local, network, and remote connections and identifying unauthorized use of the system.
Security Analytics - Security Analytics and Access Monitoring	Monitors cloud resource access sessions for conformance to policy	Supports (example of) AC-4: Information Flow Enforcement	One way to validate that cloud resource access conforms to policy is to have a set of expected access flows against which to compare observed access sessions.
		Is supported by (integral to) CA-7: Continuous Monitoring	Network access within the cloud must be monitored in order to have visibility into cloud resource access sessions.
		Supports (example of) SI-4: System Monitoring	Network access within the cloud must be monitored in order to have visibility into cloud resource access sessions.
Data Security - Data Discovery	Scans and classifies digital assets, including unstructured data	Supports (example of) SC-28: Protection of Information at Rest	Finding and classifying data stored in the cloud and on-premises helps ensure that it can be protected appropriately.
Data Security - Data Encryption	Provides strong encryption and key	Supports (example of) AC-17: Remote Access	Data Encryption devices implement cryptographic mechanisms to protect the

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	management capabilities for both structured and unstructured data both on premises and in the cloud		confidentiality and integrity of remote access sessions [AC-17 (2)].
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	Data Encryption devices protect information from unauthorized disclosure and modification during transmission.
		Supports (example of) SC-12: Cryptographic Key Establishment and Management	Some Data Encryption devices establish and manage cryptographic keys when cryptography is employed. Others use keys provided by other key management components.
Data Security - Data Access Protection	Discovers, classifies, and labels sensitive business critical data in the cloud and on-premises and provides protection by preventing unauthorized access and minimizing the risk of data theft and data leaks using security policy rules.	Supports (example of) AC-16: Security and Privacy Attributes	Provides a means to associate security and privacy attributes with organization-defined security and privacy attribute values.
		Supports (example of) SC-4: Information in Shared System Resources	Classifying, labeling, and providing policy-based protection of the data according to its label is one way to help protect data stored in the cloud and on-premises from unauthorized and unintended information transfer via shared system resources.
		Supports (example of) SC-28: Protection of Information at Rest	Preventing unauthorized access and minimizing the risk of data theft and data leaks protects information at rest.
General - Remote Connectivity	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (integral to) AC-17: Remote Access	Requiring remote users to access the enterprise via VPN is one mechanism that helps manage remote access.
		Supports (integral to) AC-20: Use of External Systems	Limiting external users to access the enterprise via VPN is one mechanism that helps manage remote access.
		Supports (example of) CA-7: Continuous Monitoring	Traffic sent on the VPN can be monitored to detect prohibited or suspicious activity.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) SC-8: Transmission Confidentiality and Integrity	VPNs encrypt data in transit.
		Supports (integral to) SC-13: Cryptographic Protection	VPNs encrypt data in transit.
General - Certificate Management	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (integral to) AC-16: Security and Privacy Attributes	Proofing server identities requires TLS certificates.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	Verification of the identity of servers depends on the issuance, use, and management of TLS certificates.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The setup of encrypted TLS transport connections depends on TLS certificates.
		Supports (integral to) SC-16: Transmission of Security and Privacy Attributes	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates.
		Supports (integral to) SI-7: Software, Firmware, and Information Integrity	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates.
General - Configuration Management	Enables the management and configuration of resources such as virtual machines and containers on-premises and in other clouds	Supports (integral to) CM-2: Baseline Configuration	The configuration management component is a tool that helps the organization create and maintain a baseline configuration of IT systems.
		Supports (integral to) CM-6: Configuration Settings	The configuration management component is a tool that helps the organization create and maintain configuration settings.
General - Secure Admin Workstation	Securely configured workstation that is dedicated to performing sensitive tasks.	Supports (example of) CM-7: Least Functionality	Use of a dedicated workstation that is configured securely is one way to ensure that the workstation will provide only essential capabilities in accordance with the principle of least functionality.
General - Virtual Desktop	Enables the secure streaming of the desktop experience from	Supports (example of) SC-8: Transmission Confidentiality and Integrity	Encryption of the streamed desktop content protects this data while in transit.

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	the cloud to an end-point or handheld device.		
Resource Protection - Cloud Workload Protection	Secures cloud workloads to protect them from known security risks and provides alerts to enable real-time reaction to prevent security events from developing. Monitors traffic to and from cloud and web applications and provides session control to prevents sensitive information from leaving.	Supported by (example of) AU-13: Monitoring for Information Disclosure	Cloud workload protection relies on the ability to monitor traffic to and from the cloud and web applications and to provide visibility into workload behavior to help detect and respond to incidents.
		Supports (example of) CM-7: Least Functionality	The cloud workload protection component provides visibility into and the ability to configure workloads to help ensure that they provide only essential capabilities.
		Supports (example of) IR-4: Incident Handling	The cloud workload protection component is designed to react to detected incidents in real-time to prevent security events from developing.
		Supports (example of) SC-3: Security Function Isolation	One way to secure cloud workloads is to segment the cloud data center into small segments, define security controls for each segment, and run one workload on each segment to protect individual workloads and isolate them from each other so malware and breaches cannot migrate from workload to workload.
		Supports (example of) SC-39: Process Isolation	One way to secure cloud workloads is to segment the cloud data center into small segments, define security controls for each segment, and run one workload on each segment to protect individual workloads and isolate them from each other so malware and breaches cannot migrate from workload to workload. The

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			cloud workload protection component may implement micro-segmentation or use hypervisors to isolate workloads.
		Is supported by (example of) SI-4: System Monitoring	Cloud workload protection relies on the ability to monitor traffic to and from the cloud and web applications and to provide visibility into workload behavior to help detect and respond to incidents.
Resource Protection - Cloud Security Posture Management	Continually assesses the security posture of cloud resources.	Supports (example of) PL-9: Central Management	Automated tools (e.g., security information and event management tools and enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with central management of controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.
		Is supported by (integral to) CA-7: Continuous Monitoring	The cloud security posture management component relies on the ability to monitor traffic to and from the cloud and web applications and to provide visibility required for continuous assessment of the security posture of cloud resources.
		Supports (example of) PM-5: System Inventory	The cloud security posture management component can inventory software in the cloud.
		Supports (example of) RA-5: Vulnerability Monitoring and Scanning	The cloud security posture management component continually scans and assesses

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			the security posture of cloud resources.
		Is supported by (example of) SI-4: System Monitoring	The cloud security posture management component relies on system monitoring for assessment of the security posture of cloud resources.
Resource Protection-Application Connector	Component that is deployed to be the front-end for an internal resource (whether located on-premises or in the cloud) and act as a proxy for it. Requests to access the resource are directed to the connector, which responds by initiating a secure connection to the PEP. A connector enables access to a resource to be controlled without requiring the resource to be visible on the network.	Supports (example of) SC-7: Boundary Protection	Boundary protection includes dynamic isolation and segregation of components. The application connector segregates a resource/application from the rest of the network.
Resource Protection - PaaS/Kubernetes security	Create a per-pod secure connection to the PEP, enabling authorized service to service and service to resource communication without the Pod or the resource visible on the Internet.	Supports (example of) SC-7: Boundary Protection	The PaaS/Kubernetes security component segregates a resource or Pod from the rest of the network.

4.2.2 Mapping Between Collaborator Technologies in the ZTA Builds and NIST SP 800-53 Controls

This section maps between the technologies that various collaborators have contributed to the project's ZTA builds and the NIST SP 800-53 controls. There is a separate subsection describing the mappings for

each collaborator. Some collaborators have not yet provided the mappings for their technologies; those mappings are planned for inclusion in a future draft of this document as the collaborators develop them.

4.2.2.1 Mapping Between Appgate Technologies and NIST SP 800-53 Controls

Table 4-10 lists the technologies that Appgate has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these technologies help support NIST SP 800-53 controls and vice versa. Appgate technologies have been included in Build E1B4.

Table 4-10 Mapping Between Appgate ZTA Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Appgate SDP Controller	Decides what protected resources to grant, deny, or revoke access to, based on enterprise policy, identity, authorization, and endpoint compliance information received from supporting components	Supports (integral to) AC-17: Remote Access	The Appgate SDP Controller authorizes both user and device to access a finite set of protected resources. Protects information about remote access mechanisms from unauthorized use and disclosure.
			Supports (integral to) AC-19: Access Control for Mobile Devices	The Appgate SDP Controller authorizes both user and device to access a finite set of protected resources.
Policy Administrator (PA)	Appgate SDP Controller	Executes the PE's policy decision by sending a set of entitlements (list of protected resources defined by hostname/IP, port, and protocol) and conditions for access to a PEP	Supports (integral to) AC-16: Security and Privacy Attributes	The Appgate SDP Controller authorizes both user and device to access a finite set of protected resources at login and continuously monitors for changes that may affect access.
Policy Enforcement Point (PEP)	Appgate SDP Gateway	Receives signed entitlement tokens and dynamically adjusts access between subject and resource as conditions change	Supports (integral to) AC-3: Access Enforcement	The Appgate SDP Gateway enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Enforcement is performed at

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				the hostname/IP(s), port(s), and protocol level of the defined protected resource(s).
Endpoint Security - Endpoint Compliance	Appgate SDP Client	Has capabilities to enforce policies based on a defined set of endpoint compliance checks to allow or deny user/endpoint access to a resource but does not perform the functions of an EPP solution to automatically remediate an endpoint.	Supports (integral to) AC-17: Remote Access	The Appgate SDP Client continuously monitors device and user attributes for changes and sends updates to the PEP which can dynamically adjust access to protected resources. Employs automated mechanisms to monitor and control remote access methods.
General - Remote Connectivity	Appgate SDP Controller	Provides remote users' connectivity to both cloud and on-premises resources.	Supports (integral to) AC-17: Remote Access	The Appgate SDP Controller authorizes both user and device to access a finite set of protected resources. Protects information about remote access mechanisms from unauthorized use and disclosure.
Resource Protection - PaaS/Kubernetes security	Appgate Injector (Appgate for Kubernetes)	Creates a per-pod secure connection to the PEP, enabling authorized service to service and service to resource communication without the Pod or the resource visible on the Internet.	Supports (integral to) AC-17: Remote Access	Service/Pod network traffic destined for protected resources is securely transmitted over mTLS tunnels to an Appgate SDP Gateway where mTLS encryption is removed and data passes in the native format/protocol to the protected resource. Services/Pods can be in the cloud or on-premises. Protected resources can be in the cloud or on-premises and do not need to be collocated with Services/Pods they communicate with.

4.2.2.2 Mapping Between Digicert Technologies and NIST SP 800-53 Controls

Table 4-11 lists the technologies that Digicert has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these technologies help support NIST SP 800-53 controls and vice versa. Digicert technologies have been included in all of the ZTA builds.

Table 4-11 Mapping Between Digicert Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
General - Certificate Management	DigiCert CertCentral TLS Manager	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (integral to) IA-5: Authenticator Management	DigiCert CertCentral TLS Manager provides the capability to manage TLS certificates throughout the certificate lifecycle process from issuance to expiration or revocation.

4.2.2.3 Mapping Between F5 Technologies and NIST SP 800-53 Controls

Table 4-12 lists the technologies that F5 has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these components help support NIST SP 800-53 controls and vice versa. F5 technologies have been included in Builds E3B1, E3B2, and E3B3.

Table 4-12 Mapping Between F5 Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	F5 BIG-IP	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to	Supports (integral to) AC-3: Access Enforcement	BIG-IP authenticates the user against Azure AD. Once authenticated, BIG-IP proxies the user to applications.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		and receives commands from the PA		

4.2.2.4 Mapping Between IBM Technologies and NIST SP 800-53 Controls

Table 4-13 lists the technologies that IBM has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these technologies help support NIST SP 800-53 controls and vice versa. IBM technologies have been included in Builds E1B1, E2B1, E1B2, E1B3, E2B3, and E4B3.

Table 4-13 Mapping Between IBM Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	IBM Security Verify	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, identity, authorization, and endpoint compliance information received from supporting components, and a trust algorithm	Supports (integral to) AC-17: Remote Access	IBM Security Verify authorizes each type of remote access to the system prior to allowing such connections.
			Supports (integral to) AC-19: Access Control for Mobile Devices	IBM Security Verify authorizes the connection of mobile devices to organizational systems.
			Supports (integral to) AC-20: External Systems	IBM Security Verify authorizes or denies access to systems that are used by but are not part of on-premises systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness.
			Supports (integral to) AC-24: Access Control Decisions	IBM Security Verify supports key functions needed to make access control decisions based on policy.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SC-15: Collaborative Computing Devices and Applications	IBM Security Verify permits or prohibits remote activation of collaborative computing de-vices and applications.
Policy Administrator (PA)	IBM Security Verify	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) AC-3: Access Enforcement	IBM Security Verify supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
			Supports (integral to) AC-17: Remote Access	IBM Security Verify supports the enforcement of remote access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
			Supports (integral to) AC-19: Access Control for Mobile Devices	IBM Security Verify conveys mobile device access decision information from the PE to the PEP, where the decision can be enforced.
			Supports (integral to) AC-20: External Systems	IBM Security Verify conveys external system access decision information from the PE to the PEP, where the decision can be enforced.
			Supports (integral to) SC-15: Collaborative Computing Devices and Applications	IBM Security Verify conveys collaborative computing device activation decision information from the PE to the PEP, where the decision can be enforced.
Policy Enforcement Point (PEP)	IBM Security Verify	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the	Supports (integral to) AC-2: Account Management	IBM Security Verify enforces authorized access to re-sources based on valid access authorization or intended sys-tem usage.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) AC-3: Access Enforcement	IBM Security Verify acts as a PEP to enforce access decisions.
			Supports (integral to) AC-4: Information Flow Enforcement	IBM Security Verify enforces approved authorizations for controlling the flow of information within the system and between connected systems. The data plane and control plane (networks) are logically separate. The PEP is the only component that can send and receive messages from both planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.
			Supports (integral to) AC-12: Session Termination	IBM Security Verify terminates connections to enforce compliance with policies.
			Supports (integral to) AC-17: Remote Access	IBM Security Verify enforces remote access decisions.
			Supports (integral to) AC-18: Wireless Access	IBM Security Verify enforces wireless access decisions.
			Supports (integral to) AC-19: Access Control for Mobile Devices	IBM Security Verify enforces access decisions regarding connection to mobile devices.
			Supports (integral to) AC-20: External Systems	IBM Security Verify enforces access decisions regarding connection to external systems.
			Supports (integral to) CA-7: Continuous Monitoring	IBM Security Verify monitors connections between a subject and an enterprise resource to detect prohibited or suspicious activity.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) IR-4: Incident Handling	If a resource is compromised, IBM Security Verify helps contain incidents by preventing attackers from moving laterally from the compromised resource to any resources that are not also in that part of the enterprise guarded by the compromised resource's PEP.
			Supports (example of) SC-7: Boundary Protection	IBM Security Verify can enforce access to key internal managed interfaces within the organization including publicly accessible system components that are separated from internal organizational networks. It can prevent unauthorized access to the portions of the enterprise that it guards. If it is used to protect a single resource, then it does not necessarily provide network segregation or network segmentation. However, it can be deployed to protect and segregate discrete network segments.
			Supports (integral to) SC-15: Collaborative Computing Devices and Applications	IBM Security Verify enforces access decisions regarding activation of collaborative computing devices.
			Supports (integral to) SC-23: Session Authenticity	As a PEP, IBM Security Verify can send and receive messages from both the data and control planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SC-32: System Partitioning	IBM Security Verify enforces approved authorizations for controlling the flow of information within the system.
			Supports (integral to) SC-41: Port and I/O Device Access	IBM Security Verify enforces authorizations for access to I/O ports and devices.
			Supports (integral to) SC-43: Usage Restrictions	IBM Security Verify enforces authorization and control of usage restrictions for system components.
			Supports (example of) SI-4: System Monitoring	IBM Security Verify can monitor connections between a subject and an enterprise resource to detect prohibited or suspicious activity.
ICAM - Identity Management	IBM Security Verify	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	Supports (integral to) AC-2: Account Management	By performing user authentication, IBM Security Verify supports identity management, including account management functions such as definition of the types of accounts allowed and prohibited for use within the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account.
			Supports (integral to) AC-3: Access Enforcement	IBM Security Verify supports the identity management function by enforcing approved authorizations associated with logical access to information and system resources in accordance with applicable access control policies.
			Supports (precedes) AC-4:	IBM Security Verify supports the identity management

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Information Flow Enforcement	function, which is a necessary component of access authorizations on which information flow enforcement depends.
			Supports (integral to) AC-5: Separation of Duties	IBM Security Verify is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of separation of duties, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
			Supports (integral to) AC-6: Least Privilege	IBM Security Verify is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
			Supports (integral to) AC-17: Remote Access, including enhancement #1	IBM Security Verify supports the identity management function by authorizing each type of remote access to the system prior to allowing such connections.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) AC-24: Access Control Decisions	IBM Security Verify supports the identity management function as a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement.
			Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	IBM Security Verify supports the identity management function as necessary for unique identification and authentication of organizational users.
			Supports (integral to) IA-5: Authentication Management	IBM Security Verify supports verification, as part of the initial authenticator distribution, of the identity of the individual receiving the authenticator.
			Supports (integral to) IA-8: Identification and Authentication (Non-organizational Users)	IBM Security Verify supports the identity management function necessary for unique identification and authentication of non-organizational users.
			Supports (integral to) PE-2: Physical Access Authorizations	IBM Security Verify supports the identity management function that serves as a basis for authorization of credentials for facility access, including physical access to security-critical devices.
ICAM - Access & Credential Management	IBM Security Verify	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which	Supports (integral to) AC-2: Account Management	By performing user authentication, IBM Security Verify supports access and credential management, including the account management function such as definition of the types of accounts allowed and prohibited for use within

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		access requests are authorized.		the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account.
			Supports (integral to) AC-3: Access Enforcement	IBM Security Verify enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
			Supports (precedes) AC-4: Information Flow Enforcement	IBM Security Verify is a necessary component of access authorizations, on which information flow enforcement depends.
			Supports (integral to) AC-5: Separation of Duties	IBM Security Verify is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, to assign users to roles that best match their responsibilities based on the principle of separation of duties, and to manage each user's roles as their responsibilities in the enterprise change or as they leave employment.
			Supports (integral to) AC-6: Least Privilege	IBM Security Verify is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, to assign users to roles that best match their responsibilities based on the principle of least privilege,

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				and to manage each user's roles as their responsibilities in the enterprise change or as they leave employment.
			Supports (integral to) AC-24: Access Control Decisions	IBM Security Verify is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
			Supports (integral to) IA-1: Policy and Procedures	IBM Security Verify's access and credential management functionality is integral to implementation of the organization's identification and authentication policies and procedures.
			Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	IBM Security Verify is a necessary element of uniquely identifying and authenticating organizational users. To determine whether access is authorized, IBM Security Verify authenticates the user or device that is requesting access by verifying the credentials that are bound to the user or device and asserted as part of the access request. These credentials must be asserted for IBM Security Verify to be able to authenticate the user request.
			Supports (precedes) IA-3: Device Identification and Authentication	IBM Security Verify identifies and authenticates organization-defined devices and/or types of devices before establishing a local, remote, or network connection.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) IA-5: Authentication Management	IBM Security Verify verifies the identity of the individual receiving the authenticator as part of the initial authenticator distribution.
			Supports (integral to) IA-8: Identification and Authentication (Non-Organizational Users)	IBM Security Verify identifies and authenticates non-organizational users.
			Supports (integral to) IA-9: Service Identification and Authentication	IBM Security Verify authorizes user/system connections to services by employing identification and authentication mechanisms.
ICAM - Federated Identity	IBM Security Verify	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	Supports (example of) IR-4: Incident Handling	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, IBM Security Verify will limit the attacker to accessing only those resources that the legitimate user's role allows.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
ICAM - Identity Governance	IBM Security Verify	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) AC-2: Account Management	IBM Security Verify supports identity governance, including account management functions such as authorized users of the system, access authorizations (i.e., privileges), and assignment of organization-defined attributes.
			Supports (integral to) AC-3: Access Enforcement	IBM Security Verify enforces approved authorizations for logical access to information and system resources by identified users in accordance with applicable access control policies.
			Supports (precedes) AC-4: Information Flow Enforcement	IBM Security Verify supports the identity governance function as a necessary component of the identity component of access authorizations on which information flow enforcement depends.
			Supports (integral to) AC-5: Separation of Duties	IBM Security Verify supports the identity governance and can manage access permissions and authorizations in a way that incorporates the separation of duties principle.
			Supports (integral to) AC-6: Least Privilege	IBM Security Verify supports identity governance and can manage access permissions and authorizations in a way that incorporates the least privilege principle.
			Supports (integral to) AC-24: Access Control Decisions	IBM Security Verify supports identity governance function as a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement and

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
			Supports (integral to) AU-2: Event Logging	IBM Security Verify supports identity governance and logs all identity management activities in accordance with policy and regulations.
			Supports (integral to) AU-12: Audit Record Generation	IBM Security Verify supports identity governance and audits all identity management activities in accordance with policy and regulations.
ICAM - Multi-Factor Authentication (MFA)	IBM Security Verify	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	IBM Security Verify supports MFA and enables users to be authenticated using a second factor, which is required for access to privileged accounts and processes and in some cases, non-privileged accounts and processes.
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	IBM Security MaaS360	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses,	Supports (integral to) AC-1: Policy and Procedures	IBM Security MaaS360 enforces access control policies and procedures and associated access controls.
			Supports (integral to) AC-2: Account Management	IBM Security MaaS360 supports the ability to monitor the use of accounts user activity for prohibited use.
			Supports (integral to) AC-6: Least Privilege	IBM Security MaaS360 supports the configuration of devices to provide only essential capabilities.
			Supports (integral to) AC-17: Remote Access	IBM Security MaaS360 supports the enforcement of usage restrictions, configuration/connection requirements, and implementation

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.		guidance for each type of remote access allowed, and it authorizes each type of remote access to the system prior to allowing such connections. IBM Security MaaS360 may use encrypted VPNs to enhance confidentiality and integrity for remote connections.
			Supports (integral to) AC-18: Access Control for Wireless Access	IBM Security MaaS360 supports the enforcement of configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorizes each type of wireless access to the system prior to allowing such connections. An AC-18 extension (1) requires protection of wireless access to the system using authentication of users and devices and encryption.
			Supports (integral to) AC-19: Access Control for Mobile Devices	IBM Security MaaS360 supports the enforcement of configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas and authorizes the connection of mobile devices to organizational systems.
			Supports (integral to) AC-20: Use of External Systems	IBM Security MaaS360 supports the enforcement of organization-defined controls asserted to be implemented

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems; allowing only authorized individuals to access the system from external systems and process, store, or transmit organization-controlled information using external systems.
			Supports (integral to) CA-7: Least Functionality	IBM Security MaaS360 supports the enforcement of configuration of the system to provide only organization-defined mission essential capabilities. IBM Security MaaS360 can monitor user activity to ensure that users are granted only the minimum access necessary to perform an operation and that such access is granted only for the minimum amount of time necessary.
			Supports (integral to) CM-2: Baseline Configuration	IBM Security MaaS360 ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware.
			Supports (integral to) CM-4: Impact Analysis	IBM Security MaaS360 ensures that the devices are compliant with organizational policy regarding analysis of changes to the system to determine potential security and privacy impacts prior to change implementation.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) CM-5: Access Restrictions for Change	IBM Security MaaS360 enforces physical and logical access restrictions associated with changes to the system.
			Supports (integral to) CM-6: Configuration Settings	IBM Security MaaS360 enforces configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations and implements the configuration settings.
			Supports (integral to) CM-10: Software Usage Restrictions	IBM Security MaaS360 monitors user activity for violation of usage restrictions.
			Supports (example of) CM-11: User Installed Software	IBM Security MaaS360 monitors user activity to enforce software installation policies.
			Supports (example of) CM-14: Signed Components	IBM Security MaaS360 uses integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
			Supports (integral to) IR-4: Incident Handling	IBM Security MaaS360 performs many activities that help to contain and mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
			Supports (example of) MP-6: Media Sanitization	IBM Security MaaS360 remotely deletes applications and data from devices as needed according to policy (not complete sanitization).
			Supports (example of) MP-7: Media Use	IBM Security MaaS360 restricts the use of removable media as required by policy.
			Supports (integral to) PM-5: System Inventory	IBM Security MaaS360 installs, manages, configures, and updates applications on UEM/MDM managed devices, so it provides inventory information regarding these applications.
			Supports (example of) RA-3: Risk Assessment	IBM Security MaaS360 is able to identify device vulnerabilities by updating software, for example. It may monitor for suspicious activity; detect and disable malware, viruses, and other malicious traffic; and repair infected files. It can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
			Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	IBM Security MaaS360 monitors device software, firmware, and configurations for vulnerabilities and threats.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SC-18: Mobile Code	IBM Security detects unauthorized mobile code.
			Supports (example of) SC-3: Security Function Isolation	IBM Security MaaS360 restricts access to security functions using access control mechanisms and by implementing least privilege capabilities.
			Supports (example of) SC-8: Transmission Confidentiality and Integrity	IBM Security MaaS360 provides cryptographic protection for transmitted information.
			Supports (integral to) SC-13: Cryptographic Protection	IBM Security MaaS360 provides cryptographic protection to support a variety of security solutions.
			Supports (example of) SC-28: Protection of Data at Rest	IBM Security MaaS360 provides cryptographic protection for data that is stored onsite.
			Supports (integral to) SI-2: Flaw Remediation	IBM Security MaaS360 mitigates and remediates vulnerabilities that it detects in device software, firmware, and configuration.
			Supports (integral to) SI-3: Malicious Code Protection	IBM Security MaaS360 prevents, detects, and disables malware, viruses, and other malicious traffic. It also repairs infected files when possible. When malicious code is detected, it provides alerts and may recommend remediation action.
			Supports (integral to) SI-4: System Monitoring	IBM Security MaaS360 monitors the device for unauthorized software and connections. It monitors the system

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives and unauthorized local, network, and remote connections to identify unauthorized use of the system.
Endpoint Security - Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	IBM Security MaaS360	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (integral to) AC-2: Account Management	IBM Security MaaS360 monitors the use of accounts.
			Supports (integral to) AC-4: Information Flow Enforcement	IBM Security MaaS360 includes a firewall that blocks unauthorized connections to and from the device.
			Supports (integral to) AC-17: Remote Access	IBM Security MaaS360 includes a firewall that blocks unauthorized connections to and from the device.
			Supports (integral to) AC-19: Access Control for Mobile Devices	IBM Security MaaS360 includes a firewall that blocks unauthorized connections to and from the device.
			Supports (integral to) AC-20: Use of External Systems	IBM Security MaaS360 includes a firewall that blocks unauthorized connections to and from the device.
			Supports (integral to) CA-7: Continuous Monitoring	IBM Security MaaS360 scans the device to detect missing patches or outdated software and report them.
			Supports (integral to) CM-2: Baseline Configuration	IBM Security MaaS360 ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software. It is a prerequisite that the compliance policies incorporate appropriate security principles.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) CM-7: Least Functionality	IBM Security MaaS360 can be used to configure devices to provide only essential capabilities.
			Supports (integral to) CM-8: System Component Inventory	In order to have IBM Security MaaS360 EDR/EPP software installed on it, a device must be known to be part of the organization's inventory.
			Supports (integral to) IR-4: Incident Handling	IBM Security MaaS360 performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
			Supports (example of) MP-2: Media Access	IBM Security MaaS360 restricts the use of removable media as required by policy.
			Supports (example of) MP-6: Media Sanitization	IBM Security MaaS360 remotely deletes applications and data from devices as needed according to policy (not full sanitization).
			Supports (example of) MP-7: Media Use	IBM Security MaaS360 restricts the use of organization-defined types of system media on organization-defined systems or system.
			Supports (example of) PM-5: System Inventory	IBM Security MaaS360 inventories software on the device.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) RA-3: Risk Assessment	IBM Security MaaS360 identifies threats to and vulnerabilities in the system by scanning the device to detect missing patches or outdated software and reporting them. It also detects malware, viruses, and other signature-based threats.
			Supports (integral to) SC-7: Boundary Protection	IBM Security MaaS360 may include a firewall that blocks unauthorized traffic to and from the device.
			Supports (integral to) SC-8: Transmission Confidentiality and Integrity	IBM Security MaaS360 may encrypt data sent from the device and may include a firewall that blocks unauthorized traffic to and from the device.
			Supports (example of) SC-10: Software Usage Restrictions	IBM Security MaaS360 monitors user activity to enforce usage restrictions.
			Supports (example of) SC-11: User-Installed Software	IBM Security MaaS360 monitors activity to enforce software installation policies.
			Supports (integral to) SC-13: Cryptographic Protection	IBM Security MaaS360 may encrypt data sent from the device or stored on the device.
			Supports (integral to) SC-15: Collaborative Computing Devices and Applications	IBM Security MaaS360 may include a firewall that blocks unauthorized remote activation of collaborative computing devices and applications.
			Supports (integral to) SC-18: Mobile Code	IBM Security MaaS360 may be able to detect unauthorized mobile code.
			Supports (integral to) SC-28: Protection of Information at Rest	IBM Security MaaS360 may encrypt data stored on the device.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (example of) SI-2: Flaw Remediation	IBM Security MaaS360 can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
			Supports (integral to) SI-3: Malicious Code Protection	IBM Security MaaS360 detects and disable malware, viruses, and other signature-based threats.
			Supports (integral to) SI-4: System Monitoring	IBM Security MaaS360 monitors the device for unauthorized software and connections.
			Supports (example of) SI-7: Software, Firmware, and Information Integrity	IBM Security MaaS360 may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
Endpoint Security - Endpoint Compliance	IBM Security MaaS360	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Supports (example of) SI-3: Malicious Code Protection	IBM Security MaaS360 supports the configuration of malicious code protection mechanisms to perform periodic scans of the system. A key function of the vulnerability scanning and assessment functionality of IBM Security MaaS360 is to perform vulnerability scans.
			Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	A key function of the vulnerability scanning and assessment functionality of IBM Security MaaS360 is to perform vulnerability scans.
Security Analytics – Security	IBM Security QRadar XDR		Supports (integral to) AU-2: Event Logging	IBM Security QRadar XDR supports the logging of security

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Information and Event Management (SIEM)		Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.		information and event activity as required by policy.
			Supports (integral to) AU-6: Audit Record Review, Analysis, and Reporting	IBM Security QRadar XDR collects security and event information from many components. This data may be analyzed to understand attack targets and methods. Security analysts rely at least in part on SIEM data collected by IBM Security QRadar XDR to help them determine the impact of events.
			Supports (example of) AU-7: Audit Record Reduction and Report Generation	IBM Security QRadar XDR can provide helpful data that can help with forensic analysis of cybersecurity incidents.
			Supports (integral to) CA-7: Continuous Monitoring	IBM Security QRadar XDR collects security and event information from many components.
			Supports (integral to) IR-4: Incident Handling	IBM Security QRadar XDR collects security and event information from many components. This data may be analyzed to understand attack targets and methods and the impact of cybersecurity incidents.
			Supports (integral to) IR-5: Incident Monitoring	IBM Security QRadar XDR collects security and event information from many components to support tracking and documentation of events. Its logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anom-

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				alous behavior and other indicators of potential cybersecurity events.
			Supports (integral to) RA-3: Risk Assessment	IBM Security QRadar XDR support the security analysts who rely at least in part on SIEM data to help them determine the impact of events.
			Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	IBM Security QRadar XDR acts as a vulnerability scanning and assessment tool.
			Supports (integral to) SC-7: Boundary Protection	IBM Security QRadar XDR collects and correlates event information. Its logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
Security Analytics - Security Orchestration, Automation, and Response (SOAR)	IBM Cloud Pak for Security	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (integral to) CP-10: System Recovery and Reconstitution	IBM Cloud Pak for Security can provide for the recovery and reconstitution of the system to a known state within an organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.
			Supports (example of) IR-4: Incident Handling	IBM Cloud Pak for Security can be used to implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Security Analytics – User Behavior Analytics	IBM Security Verify/Trusteer	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) AC-2 (12): Account Management (Account Monitoring for Atypical Usage)	IBM Security Trusteer support for user behavior analytics is an essential part of monitoring the activity of personnel to detect potential cybersecurity events.
			Supported by (integral to) CA-7: Continuous Monitoring	IBM Security Trusteer supports continuous monitoring by providing the information required for analysis of user behavior.
Security Analytics – Data Encryption	IBM Security Guardium Data Encryption (GDE)	Provides strong encryption and key management capabilities for both structured and unstructured data both on premises and in the cloud	Supports (example of) AC-17: Remote Access	IBM GED implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions [AC-17 (2)].
			Supports (integral to) SC-8: Transmission Confidentiality and Integrity	IBM GED supports protects information from unauthorized disclosure and modification during transmission.
			Supports (example of) SC-12: Cryptographic Key Establishment and Management	IBM GED supports the establishment and management of cryptographic keys for some devices when cryptography is employed. Other devices use keys provided by other key management components.
Data Security - Data Access Protection	IBM Security Guardium Data Encryption (GDE)	Discovers, classifies, and labels sensitive business critical data in the cloud and on-premises and provides protection by preventing unauthorized access and minimizing the risk of data theft and data leaks using security policy rules.	Supports (example of) AC-16: Security and Privacy Attributes	IBM GED provides a means to associate security and privacy attributes with organization-defined security and privacy attribute values.
			Supports (example of) SC-4: Information in Shared System Resources	IBM GED supports classifying, labeling, and providing policy-based protection of data according to its label. These mechanisms help protect data stored in the cloud and on-premises from unauthorized

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				and unintended information transfer via shared system resources.
			Supports (example of) SC-28: Protection of Information at Rest	IBM GED prevents unauthorized access and minimizes the risk of data theft and data leaks to protect Information at rest.

4.2.2.5 Mapping Between Mandiant Technologies and NIST SP 800-53 Controls

Table 4-14 lists the technologies that Mandiant has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these technologies help support NIST SP 800-53 controls and vice versa. Mandiant technologies have been included in all builds of the project.

Table 4-14 Mapping Between Mandiant Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Security Analytics - Security Controls Validation	Mandiant Security Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows.	Supports (integral to) CA-2: Control Assessments	Mandiant Security Validation is used to test and verify the effectiveness of detection processes and other ZTA cybersecurity controls.
			Is supported by (integral to) CA-7: Continuous Monitoring	Mandiant Security Validation can continuously monitor, measure, and validate the effectiveness of cybersecurity controls, thereby enabling an organization to continuously improve its detection processes.
			Supports (integral to) SI-10: Information Input Validation	Mandiant Security Validation is used to test and verify the inputs to detection processes and other ZTA cybersecurity controls.

4.2.2.6 Mapping Between Tenable Technologies and NIST SP 800-53 Controls

Table 4-15 lists the technologies that Tenable has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these components help support NIST SP 800-53 controls and vice versa. Tenable technologies have been included in all builds of the project.

Table 4-15 Mapping Between Tenable Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Security Analytics – Endpoint Monitoring	Tenable.io	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts (devices or VMs) that are connected to the network	Supported by (integral to) CA-7: Continuous Monitoring	A key function of Tenable.io is to check endpoints for missing patches, updates, and upgrades.
Vulnerability Scanning and Assessment	Tenable.io and Tenable.ad	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	A key function of Tenable.io and Tenable.ad is to perform vulnerability scans.
Security Analytics - Traffic Inspection	Tenable NNM	Interception, examination, and recording of relevant	Supports (example of) CA-7: Continuous Monitoring	Traffic inspection, which is performed by Tenable NNM, is an essential part of monitoring the network to

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		traffic transmitted on the network.		detect potential cybersecurity events.
Security Analytics - Network Discovery	Tenable NNM	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (example of) CA-7: Continuous Monitoring	A key function of Network Discovery is to monitor the network at all times, which can be accomplished by Tenable NNM.

4.2.2.7 Mapping Between VMware Technologies and NIST SP 800-53 Controls

Table 4-16 lists the technologies that VMware has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the NIST SP 800-53 controls. It indicates how these technologies help support NIST SP 800-53 controls and vice versa. VMware technologies have been included in build E2B3.

Table 4-16 Mapping Between VMware Functionality and NIST SP 800-53 Controls

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	VMware Workspace ONE UEM	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they	Supports (integral to) AC-1: Policy and Procedures	VMware Workspace ONE UEM enforces access control policies and procedures and associated access controls.
			Supports (integral to) AC-6: Least Privilege	VMware Workspace ONE UEM can be used to configure devices to provide only essential capabilities.
			Supports (integral to) AC-17: Remote Access	VMware Workspace ONE UEM enforces usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorizes each type of remote access to the system prior to allowing such

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.		connections. May use encrypted VPNs to enhance confidentiality and integrity for remote connections.
			Supports (integral to) AC-18: Access Control for Wireless Access	VMware Workspace ONE UEM enforces configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorizes each type of wireless access to the system prior to allowing such connections. An AC-18 extension (1) requires protection of wireless access to the system using authentication of users and devices and encryption.
			Supports (integral to) AC-19: Access Control for Mobile Devices	VMware Workspace ONE UEM enforces configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas and authorizes the connection of mobile devices to organizational systems.
			Supports (integral to) AC-20: Use of External Systems	VMware Workspace ONE UEM enforces organization-defined controls asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing only authorized

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
				individuals to access the system from external systems and processing, storing, or transmitting organization-controlled information using external systems.
			Supports (integral to) CM-2: Baseline Configuration	VMware Workspace ONE UEM ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware.
			Supports (integral to) CM-4: Impact Analysis	VMware Workspace ONE UEM ensures that the devices are compliant with organizational policy regarding analysis of changes to the system to determine potential security and privacy impacts prior to change implementation.
			Supports (integral to) CM-6: Configuration Settings	VMware Workspace ONE UEM enforces configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations and implements the configuration settings.
			Supports (example of) CM-11: User Installed Software	VMware Workspace ONE UEM can monitor user activity to enforce software installation policies.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (example of) MP-6: Media Sanitization	VMware Workspace ONE UEM can remotely delete applications and data from devices as needed according to policy (not complete sanitization).
			Supports (example of) MP-7: Media Use	VMware Workspace ONE UEM can restrict the use of removable media as required by policy.
			Supports (integral to) PM-5: System Inventory	VMware Workspace ONE UEM installs, manages, configures, and updates applications on UEM/MDM managed devices, so it provides inventory information regarding these applications.
			Supports (example of) RA-3: Risk Assessment	VMware Workspace ONE UEM can mitigate and remediate vulnerabilities and threats that are detected in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
			Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	VMware Workspace ONE UEM can monitor device software, firmware, and configurations for known vulnerabilities and threats.
			Supports (integral to) SC-18: Mobile Code	VMware Workspace ONE UEM may be able to detect unauthorized mobile code.
			Supports (example of) SC-8: Transmission Confidentiality and Integrity	VMware Workspace ONE UEM can provide cryptographic protection for transmitted information.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SC-13: Cryptographic Protection	VMware Workspace ONE UEM may provide cryptographic protection to support a variety of security solutions.
			Supports (example of) SC-28: Protection of Data at Rest	VMware Workspace ONE UEM can provide cryptographic protection for data that is stored onsite.
			Supports (integral to) SI-2: Flaw Remediation	VMware Workspace ONE UEM mitigates and remediates known vulnerabilities in device software, firmware, and configuration.
			Supports (integral to) SI-4: System Monitoring	VMware Workspace ONE UEM monitors the device for unauthorized software.

4.3 EO 14028 Security Measure Mappings

This section provides mappings between ZTA functionality and EO 14028 security measures.

4.3.1 Mapping Between ZTA Reference Design Functions and EO 14028 Security Measures

Table **4-17** provides a mapping between the functions performed by the logical components of the ZTA reference design and the EO 14028 security measures. This table indicates how ZTA functions help support EO 14028 security measures for EO-critical software and EO-critical software platforms, and vice versa.

Table 4-17 Mapping Between ZTA Reference Design Functions and EO 14028 Security Measures

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or	Supports (integral to) SM 1.4: Employ	The PE makes access decisions based on policy.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	revoke access to a resource, based on enterprise policy, information from functional components, and a trust algorithm	boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The PE makes access decisions based on policy.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
Policy Enforcement Point (PEP)	Guards the trust zone that hosts an enterprise resource; enables, monitors,	Supports (integral to) SM 1.4: Employ boundary protection techniques as	The PEP prevents unauthorized access to the portions of the enterprise that it guards.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The PEP enforces access decisions. The PEP can be placed in front of a single or multiple resources, making access control as fine-grained as desired.
		Supports (example of) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	The PEP can monitor connections between a subject and an EO-critical software platform to detect prohibited or suspicious activity.
ICAM - Identity Management	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	Identity Management is used to create and manage the identities that are verified using MFA.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
ICAM - Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which access requests are authorized.	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	Access & Credential Management is used to perform MFA.
		Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Performing user and device authentication is necessary for mutual authentication.
ICAM - Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data	Supports (example of) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	Federated identities can be verified using MFA.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	Supports (example of) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Federated identities can be used with digital representations of roles and associated access authorizations.
ICAM - Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	The Identity Governance component manages user identity functions.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The Identity Governance component manages access control functions.
		Supports (integral to) SM 4.1: Configure logging to record the necessary information about security events	The Identity Governance component performs logging and audits all identity management activities in accordance with policy and regulations.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		involving EO-critical software platforms and all software running on those platforms.	
ICAM - MFA	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	The MFA component enables users to be authenticated using a second factor.
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data.	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	The UEM/MDM may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
		Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The UEM/MDM installs, manages, configures, and updates software on UEM/MDM-managed devices, so it provides inventory information regarding this software.
		Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The UEM/MDM installs, manages, configures, and updates software on UEM/MDM-managed devices.
		Supports (integral to) SM 4.1: Configure logging to record the	The UEM/MDM component performs security event logging on UEM/MDM-managed devices.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.	necessary information about security events involving EO-critical software platforms and all software running on those platforms.	
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	The UEM/MDM component provides several forms of endpoint security protection on UEM/MDM-managed devices.
Endpoint Security - Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection,	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	The EDR/EPP may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
		Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The EDR/EPP inventories software on the device.
		Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The EDR/EPP installs, manages, configures, and updates software on EDR/EPP-managed devices.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The EDR/EPP ensures that devices are compliant with organizational policy in terms of having the expected software configurations.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	The EDR/EPP provides several forms of endpoint security protection on EDR/EPP-managed devices.
		Supports (example of) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	The EDR/EPP can monitor the device for unauthorized network connections. Other network monitoring technologies can be used instead of EDR/EPP to do this.
Endpoint Security - Endpoint Compliance	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Part of endpoint compliance is continuously monitoring security tools and services to ensure they are running and their integrity has not been compromised.
		Is supported by (example of) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection is one way of performing device health checks.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Security Analytics - Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Is supported by (precedes) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	The SIEM aggregates logs of security information and security event activity generated by EO-critical software platforms.
		Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The SIEM can collect, analyze, and correlate security information and security event data from many platforms.
Security Analytics – Security Controls Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows.	Is supported by (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	Network security protection is needed to have visibility into network traffic and transaction flows for validating controls.
		Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The ZTA's cybersecurity controls are a subset of the EO-critical software platforms' controls, so continuous monitoring of the ZTA's cybersecurity controls achieves a part of continuous monitoring for EO-critical software platforms.
Security Analytics - Identity Monitoring	Monitors the identity of subjects to detect and send alerts for indicators that user accounts or credentials may be compromised, or to detect sign-in risks	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Identity monitoring, including generating alerts for potentially compromised accounts and attacks against accounts, is one part of continuous monitoring.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	for a particular access session.		
Security Analytics – User Behavior Analytics	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Monitoring user behavior for unusual activity is one part of continuous monitoring.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection on platforms includes monitoring of user behavior.
Security Analytics - Security Monitoring	Monitors and detects malicious or suspicious user actions based on access activity	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Continuous security monitoring of software and software platforms includes monitoring of user actions.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection on platforms includes monitoring of user actions.
Security Analytics - Application Protection and Response	Protects particular applications from phishing, spam, malware and other zero day attacks	Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection on platforms includes protecting applications running on that platform.
		Supports (integral to) SM 4.4: Employ network	Network security protection includes protecting applications from network-

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	based attacks and detecting and stopping attacks before reaching their target.
Security Analytics - Cloud Access Permission Manager	Provides visibility and control of permissions used by identities in various cloud platforms	Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	A key function of the Cloud Access Permission Manager component is to provide control over and management of access permissions for data and resources.
Security Analytics – Endpoint Monitoring	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts (devices or VMs) that are connected to the network	Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The endpoint monitoring inventories software on the endpoints.
		Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Endpoint Monitoring component is to check endpoints for missing patches, updates, and upgrades.
		Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and	A key function of the Endpoint Monitoring component is to check endpoints for misconfigurations.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		all software deployed to those platforms.	
		Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Endpoint monitoring includes continuous monitoring of the state of the endpoint.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection on platforms includes continuous endpoint monitoring.
Security Analytics – Vulnerability Scanning and Assessment	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans for missing patches.
		Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans for misconfigurations.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Security Analytics – Security Orchestration, Automation, and Response (SOAR)	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The SOAR component can support monitoring of security data from many platforms.
Security Analytics - Traffic Inspection	Intercepts, examines, and records relevant traffic transmitted on the network.	Supports (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	Inspecting network traffic is a fundamental element of network security protection.
Security Analytics - Network Discovery	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	Discovering, classifying, and assessing the risk posed by devices on the network is vital for monitoring and analyzing network traffic to and from devices.
Security Analytics - Network Monitoring	Aggregates and analyzes network telemetry—information generated by	Supports (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-	Monitoring network traffic is at the core of network security protection.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	network devices—to provide network visibility both on premises and in clouds and to detect and respond to threats.	critical software platforms to protect the platforms and their software using networks.	
Security Analytics - Security Analytics and Access Monitoring	Monitors cloud resource access sessions for conformance to policy.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Continuous security monitoring of software and software platforms includes monitoring of access to cloud resources.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection on platforms includes monitoring of access to cloud resources.
Data Security – Data Discovery	Scans and classifies digital assets, including unstructured data	Supports (integral to) SM 2.1: Establish and maintain a data inventory for EO-critical software and EO-critical platforms.	Discovering and classifying sensitive unstructured data is a key component of having a data inventory.
Data Security Data Encryption	Provides strong encryption and key management capabilities for both structured and unstructured data both on premises and in the cloud	Supports (integral to) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Strong encryption and key management capabilities are essential for protecting data at rest.
		Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and	Strong encryption and key management capabilities are essential for protecting data in transit.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	
Data Security Data Access Protection	Discovers, classifies, and labels sensitive business critical data in the cloud and on-premises and provides protection by preventing unauthorized access and minimizing the risk of data theft and data leaks using security policy rules.	Supports (integral to) SM 2.1: Establish and maintain a data inventory for EO-critical software and EO-critical platforms.	Discovering and classifying sensitive business-critical data effectively creates a partial data inventory.
		Is supported by (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Fine-grained access control is necessary for preventing unauthorized access to sensitive data.
		Is supported by (integral to) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Encrypting sensitive data at rest is necessary for protecting the data from unauthorized access and theft/leaks.
		Is supported by (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent	Encrypting sensitive data in transit is necessary for protecting the data from unauthorized access and theft/leaks.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		with NIST's cryptographic standards.	
General - Remote Connectivity	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (example of) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	VPNs are one method of encrypting data in transit.
General - Certificate Management	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (example of) SM 1.2: Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	Services can be identified and authenticated through the use of TLS certificates.
		Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	TLS certificates are widely used for mutual authentication and communications encryption—for example, in HTTPS.
General - Configuration Management	Enables the management and configuration of resources such as virtual machines and containers on-premises and in other clouds	Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Configuration Management component is to maintain software and software platforms regardless of location.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
General - Secure Admin Workstation	Securely configured workstation that is dedicated to performing sensitive tasks	Supports (integral to) SM 1.3: Follow privileged access management principles for network-based administration of EO-critical software and EO critical software platforms.	Having separate workstations for secure administration tasks is a vital component of privileged access management.
General - Virtual Desktop	Enables the secure streaming of the desktop experience from the cloud to an endpoint or handheld device.	Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Encryption of the streamed desktop content protects this data while in transit.
Resource Protection - Cloud Workload Protection	Secures cloud workloads to protect them from known security risks and provides alerts to enable real-time reaction to prevent security events from developing. Monitors traffic to and from cloud and web applications and provides session control to prevents sensitive information from leaving.	Is supported by (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Fine-grained access control for data and resources is necessary for securing cloud workloads.
		Is supported by (integral to) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Protecting data at rest through encryption is necessary for securing cloud workloads.
		Is supported by (integral to) SM 2.4: Protect data	Protecting data in transit is necessary for controlling and protecting cloud sessions.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	
		Is supported by (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	Enabling real-time reactions to security events is dependent on logging being configured and implemented for the cloud workload.
		Is supported by (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Identifying security events within a cloud workload is dependent on performing continuous monitoring within that workload.
		Is supported by (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Endpoint security protection employed for cloud workloads is necessary for protecting the workloads.
		Is supported by (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms	Network security protection, including traffic monitoring, is necessary for keeping cloud workloads secure.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		and their software using networks.	
Resource Protection - Cloud Security Posture Management	Continually assesses the security posture of cloud resources.	Is supported by (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	Patch management includes the identification of vulnerabilities and missing patches, which is vital to assessing security posture.
		Is supported by (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	Configuration management includes the identification of misconfigurations, which is vital to assessing security posture.
		Is supported by (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	Cybersecurity event logging is vital to assessing security posture.
		Is supported by (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	Continuously monitoring software security is vital to assessing security posture.
		Is supported by (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	Using endpoint security protection for cloud resources is vital to assessing the security posture of those resources.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		Is supported by (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	Using network security protection to monitor and protect cloud resources is vital to assessing the security posture of those resources.
Resource Protection-Application Connector	Component that is deployed to be the front-end for an internal resource (whether located on-premises or in the cloud) and act as a proxy for it. Requests to access the resource are directed to the connector, which responds by initiating a secure connection to the PEP. A connector enables access to a resource to be controlled without requiring the resource to be visible on the network.	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	The Application Connector is part of the boundary protection architecture for ZTA.
Resource Protection - PaaS/Kubernetes security	Create a per-pod secure connection to the PEP, enabling authorized service to service and service to resource communication without the Pod or the resource visible on the Internet.	Supports (integral to) SM 1.2: Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	Services must be identified and authenticated for secure service-to-service and service-to-resource communications.
		Is supported by (integral to) SM 2.4: Protect data in transit by using	Protecting data in transit is necessary for protecting connections to the PEP and

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	service-to-service and service-to-resource communications.

4.3.2 Mapping Between Collaborator Technologies in the ZTA Builds and EO 14028 Security Measures

This section maps between the technologies that various collaborators have contributed to the project's ZTA builds and EO 14028 security measures. There is a separate subsection describing the mappings for each collaborator. Some collaborators have not yet provided the mappings for their technologies; these mappings are planned for inclusion in a future draft of this document as the collaborators develop them.

4.3.2.1 Mapping Between Appgate Technologies and EO 14028 Security Measures

Table 4-18 lists the technologies that Appgate has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the EO 14028 security measures. It indicates how these technologies help support EO 14028 security measures and vice versa. Appgate technologies have been included in Build E1B4.

Table 4-18 Mapping Between Appgate ZTA Functionality and EO 14028 Security Measures

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Appgate SDP Controller	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource;	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct	The Appgate SDP Controller defines protected resources and the conditions under which those resources can be accessed.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
		forwards requests to and receives commands from the PA	access to EO-critical software, EO-critical software platforms, and associated data.	
Policy Administrator (PA)	Appgate SDP Controller	Executes the PE's policy decision by sending a set of entitlements (list of protected resources defined by hostname/IP, port, and protocol) and conditions for access to a PEP	Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The Appgate SDP Controller determines access control on a default-deny basis and can use logic (simple or complex) that considers user, device, and other context information.
Policy Enforcement Point (PEP)	Appgate SDP Gateway	Receives signed entitlement tokens and dynamically adjusts access between subject and resource as conditions change	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data. Examples of such techniques include network segmentation, isolation, software-defined perimeters, and proxies	The Appgate SDP Gateway creates user-specific micro-firewalls to ensure least privilege access to protected resources. The Gateway cloaks itself and the network/resource while securely allowing authenticated and authorized end user traffic to reach protected resources.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
Endpoint Security - Endpoint Compliance	Appgate SDP Client	Has capabilities to enforce policies based on a defined set of endpoint compliance checks to allow or deny user/endpoint access to a resource, but does not perform the functions of an EPP solution to automatically remediate an endpoint.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The Appgate SDP Client continuously performs endpoint checks (customizable) and sends changes to the PEP which can immediately change (limit or grant) access to protected resources.
General - Remote Connectivity	Appgate SDP Controller	Provides remote users connectivity to on-premises or cloud hosted resources.	Supports (example of) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	User data is securely transmitted over mTLS tunnels to an Appgate SDP Gateway where mTLS encryption is removed and data passes in the native format/protocol to the protected resource.
Resource Protection - PaaS/Kubernetes security	Appgate Injector (Appgate for Kubernetes)	Creates a per-pod secure connection to the PEP, enabling authorized service to service and service to resource communication without the Pod or the resource visible on the Internet.	Supports (example of) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-	Service/Pod data is securely transmitted over mTLS tunnels from the Appgate Injector to an Appgate SDP Gateway where mTLS encryption is removed and data passes in the native format/protocol to the protected resource.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
			critical software platforms consistent with NIST's cryptographic standards.	

4.3.2.2 Mapping Between Digicert Technologies and EO 14028 Security Measures

Table 4-19 lists the technologies that Digicert has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the EO 14028 security measures. It indicates how these technologies help support EO 14028 security measures and vice versa. Digicert technologies have been included in all of the ZTA builds.

Table 4-19 Mapping Between Digicert Functionality and EO 14028 Security Measures

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
General - Certificate Management	DigiCert CertCentral TLS Manager	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (integral to) SM 1.2: Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	DigiCert CertCentral TLS Manager provides the capability to manage TLS certificates throughout the certificate lifecycle process from issuance to expiration or revocation.
			Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting	DigiCert CertCentral TLS Manager provides the capability to issue and manage TLS certificates that provide a basis for authenticating endpoints and encrypting connections.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 security measures (and Relationship Properties)	Relationship Explanation
			sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	

587 *4.3.2.3 Mapping Between F5 Technologies and EO 14028 Security Measures*

588 **Table 4-20** lists the technologies that F5 has contributed to the ZTA builds implemented in this project
589 and details the mappings between the functionality performed by these technologies and the EO 14028
590 security measures. It indicates how these technologies help support EO 14028 security measures and
591 vice versa. F5 technologies have been included in Builds E3B1, E3B2, and E3B3.

592 **Table 4-20 Mapping Between F5 Functionality and EO 14028 Security Measures**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	F5 BIG-IP	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	BIG-IP authenticates user against Azure AD. Once authenticated, BIG-IP proxies user to applications.

4.3.2.4 Mapping Between IBM Technologies and EO 14028 Security Measures

Table 4-21 lists the technologies that IBM has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the EO 14028 security measures. It indicates how these technologies help support EO 14028 security measures and vice versa. IBM technologies have been included in Builds E1B1, E2B1, E1B2, E1B3, E2B3, and E4B3.

Table 4-21 Mapping Between IBM Functionality and EO 14028 Security Measures

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	IBM Security Verify	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, identity, authorization, and endpoint compliance information received from supporting components, and a trust algorithm	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	IBM Security Verify makes access decisions based on policy.
			Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify makes access decisions based on policy.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Policy Administrator (PA)	IBM Security Verify	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	IBM Security Verify supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
			Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
Policy Enforcement Point (PEP)	IBM Security Verify	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	IBM Security Verify prevents unauthorized access to the portions of the enterprise that it guards.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify enforces access decisions. It can be placed in front of a single or multiple resources, making access control as fine-grained as desired.
			Supports (example of) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	IBM Security Verify can monitor connections between a subject and an EO-critical software platform to detect prohibited or suspicious activity.
ICAM - Identity Management	IBM Security Verify	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	IBM Security Verify creates and manages the identities that are verified using MFA.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		resources at the appropriate time.	Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify defines and manages digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it manages each user's roles as their responsibilities in the enterprise change or as they leave employment.
ICAM - Access & Credential Management	IBM Security Verify	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which access requests are authorized.	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	IBM Security Verify performs MFA.
			Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with	IBM Security Verify performs the user and device authentication that is necessary for mutual authentication.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			NIST's cryptographic standards.	
ICAM - Federated Identity	IBM Security Verify	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	Supports (example of) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	IBM Security Verify supports the verification of federated identities using MFA.
			Supports (example of) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify supports federated identities to be used with digital representations of roles and associated access authorizations.
ICAM - Identity Governance	IBM Security Verify	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-	IBM Security Verify manages user identity functions.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		compliance with requirements and regulations.	critical software platforms.	
			Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM Security Verify manages access control functions.
			Supports (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	IBM Security Verify performs logging and audits all identity management activities in accordance with policy and regulations.
ICAM - Multi-Factor Authentication (MFA)	IBM Security Verify	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-	IBM Security Verify enables users to be authenticated using a second factor.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			critical software platforms.	
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	IBM Security MaaS360	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	IBM Security MaaS360 encrypts data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	IBM Security MaaS360 installs, manages, configures, and updates software on UEM/MDM-managed devices, so it provides inventory information regarding this software.
			Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	IBM Security MaaS360 manages, configures, and updates software on UEM/MDM-managed devices.
			Supports (integral to) SM 4.1:	IBM Security MaaS360 performs security event

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		security issues on the device.	Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	logging on UEM/MDM-managed devices.
			Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	IBM Security MaaS360 provides several forms of endpoint security protection on UEM/MDM-managed devices.
Endpoint Security - Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	IBM Security MaaS360	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	IBM Security MaaS360 encrypts data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms	IBM Security MaaS360 inventories software on the device.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	
			Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	IBM Security MaaS360 installs, manages, configures, and updates software on EDR/EPP-managed devices.
			Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	IBM Security MaaS360 ensures that devices are compliant with organizational policy in terms of having the expected software configurations.
			Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	IBM Security MaaS360 provides several forms of endpoint security protection on EDR/EPP-managed devices.
			Supports (example of) SM 4.4: Employ network security	IBM Security MaaS360 monitors the device for unauthorized network

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	connections. Other network monitoring technologies can be used instead of EDR/EPP to do this.
Endpoint Security - Endpoint Compliance	IBM Security MaaS360	Performs device health checks by validating specific tools or services within the endpoint including antivirus, data encryption, intrusion prevention, EPP, and firewall.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	IBM MaaS360 Endpoint agent performs periodic scans of the system for vulnerabilities.
			Is supported by (example of) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	IBM MaaS360 Endpoint agent performs vulnerability scans to protect the endpoint and software running on it.
Security Analytics – Security Information and Event Management (SIEM)	IBM Security QRadar XDR	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and	Is supported by (precedes) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software	IBM Security QRadar aggregates logs of security information and security event activity generated by EO-critical software platforms.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	platforms and all software running on those platforms.	
			Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	IBM Security QRadar XDR collects, analyzes, and correlates security information and security event data from many platforms.
Security Analytics - Security Orchestration, Automation, and Response (SOAR)	IBM Cloud Pak for Security	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	IBM Cloud Pak for Security supports monitoring of security data from many platforms.
Security Analytics - User Behavior Analytics	IBM Security Verify/Trusteer	Monitors and analyzes user behavior to detect unusual patterns or anomalies that might indicate an attack.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	IBM Security Trusteer supports monitoring user behavior for unusual activity as one aspect of continuous monitoring.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	IBM Security Trusteer supports monitoring of user behavior.
Data Security – Data Encryption	IBM Security Guardium Data Encryption (GDE)	Provides strong encryption and key management capabilities for both structured and unstructured data both on premises and in the cloud	Supports (integral to) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	IBM GDE supports strong encryption and key management capabilities, which are essential for protecting data at rest.
			Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	IBM GDE supports strong encryption and key management capabilities, which are essential for protecting data in transit.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Data Security - Data Access Protection	IBM Security Guardium Data Encryption (GDE)	Discovers, classifies, and labels sensitive business critical data in the cloud and on-premises and provides protection by preventing unauthorized access and minimizing the risk of data theft and data leaks using security policy rules.	Supports (integral to) SM 2.1: Establish and maintain a data inventory for EO-critical software and EO-critical platforms.	IBM GDE supports discovering and classifying sensitive business-critical data, which effectively creates a partial data inventory.
			Is supported by (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	IBM GDE supports fine-grained access control which is necessary for preventing unauthorized access to sensitive data.
			Is supported by (integral to) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	IBM GDE supports encrypting sensitive data at rest which is necessary for protecting the data from unauthorized access and theft/leaks.
			Is supported by (integral to) SM 2.4: Protect data in transit by using mutual	IBM GDE supports encrypting sensitive data in transit, which is necessary for protecting the data from unauthorized access and theft/leaks.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	

599 *4.3.2.5 Mapping Between Mandiant Technologies and EO 14028 Security Measures*

600 **Table 4-22** lists the technologies that Mandiant has contributed to the ZTA builds implemented in this
601 project and details the mappings between the functionality performed by these technologies and the EO
602 14028 security measures. It indicates how these technologies help support EO 14028 security measures
603 and vice versa. Mandiant technologies have been included in all builds of the project.

604 **Table 4-22 Mapping Between Mandiant Functionality and EO 14028 Security Measures**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Security Analytics - Security Controls Validation	Mandiant Security Validation	Validates the ZTA cybersecurity controls implemented through visibility into network traffic and transaction flows.	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The ZTA's cybersecurity controls are a subset of the EO-critical software platforms' controls, so continuous monitoring of the ZTA's cybersecurity controls achieves a part of continuous monitoring for EO-critical software platforms.

4.3.2.6 Mapping Between Tenable Technologies and EO 14028 Security Measures

Table 4-23 lists the technologies that Tenable has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the EO 14028 security measures. It indicates how these components help support EO 14028 security measures and vice versa. Tenable technologies have been included in all builds of the project.

Table 4-23 Mapping Between Tenable Functionality and EO 14028 Security Measures

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Security Analytics – Endpoint Monitoring	Tenable.io	Discovers all IP-connected endpoints and performs continuous collection, examination, and analysis of software versions, configurations, and other information regarding hosts (devices or VMs) that are connected to the network	Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	Tenable.io inventories software on the endpoints. A key function of Tenable.io is to check endpoints for missing patches, updates, and upgrades
Security Analytics - Vulnerability Scanning and Assessment	Tenable.io and Tenable.ad	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of Tenable.io and Tenable.ad is to perform vulnerability scans.
Security Analytics - Traffic Inspection	Tenable NNM	Interception, examination, and recording of relevant	Supports (integral to) SM 4.4: Employ network security protection to	Traffic inspection, which is performed by Tenable NNM, is an essential part of monitoring the network to

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		traffic transmitted on the network.	monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks	detect potential cybersecurity events.
Security Analytics - Network Discovery	Tenable NNM	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks	Network Discovery, which is supported by Tenable NNM, can help identify unknown and/or unexpected devices and activity that may be indicative of suspicious events, making it an example of how the network can be monitored to detect potential cybersecurity events.

4.3.2.7 Mapping Between VMware Technologies and EO 14028 Security Measures

Table 4-24 lists the technologies that VMware has contributed to the ZTA builds implemented in this project and details the mappings between the functionality performed by these technologies and the EO 14028 security measures. It indicates how these technologies help support EO 14028 security measures and vice versa. VMware technologies have been included in build E2B3.

616 **Table 4-24 Mapping Between VMware Functionality and EO 14028 Security Measures**

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Endpoint Security - Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	VMware Workspace ONE UEM	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards. Using the encryption capabilities of the OS. Policy can be enforced to require encryption.	VMware Workspace ONE UEM may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
			Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	VMware Workspace ONE UEM installs, manages, configures, and updates software on UEM/MDM-managed devices, so it provides inventory information regarding this software.
			Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all	VMware Workspace ONE UEM installs, manages, configures, and updates software on UEM/MDM-managed devices.

ZTA Architecture Component	Product	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
			software deployed to those platforms.	
			Supports (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	VMware Workspace ONE UEM performs security event logging on UEM/MDM-managed devices.

Appendix A References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Gaithersburg, Md., August 2020, 50 pp. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final

[2] K. Scarfone, M. Souppaya, and M. Fagan, Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Content Mappings, National Institute of Standards and Technology (NIST) Internal Report (IR) 8477, Gaithersburg, Md., August 2023, 26 pp. Available: https://dFoi.org/10.6028/NIST.IR.8477.ipd

[3] NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[4] NIST. The NIST Cybersecurity Framework 2.0, August 2023 draft. Available: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

[5] Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Gaithersburg, Md., September 2020, 465 pp. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[6] Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, National Institute of Standards and Technology (NIST). Available: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2

[7] Executive Order no. 14028, *Improving the Nation's Cybersecurity*, Federal Register Vol. 86, No.93, May 17, 2021. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity