NIST SPECIAL PUBLICATION 1800-22B

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume B:
Approach, Architecture, and Security Characteristics

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Jason Ajmo
R. Eugene Craft
Milissa McGinnis*
Kenneth Sandlin
Oksana Slivina
Julie Snyder
Paul Ward
The MITRE Corporation
McLean, VA

**Former employee; all work for this publication done while at employer.*

September 2023

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-22

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.

National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol. Spec. Publ. 1800-22B, 88 pages, (September 2023), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at mobile-nccoe@nist.gov.

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, easily 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 Cyber Security Framework and details the steps needed for another entity to recreate 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 Series 1800) 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.

This Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate enhancing the security of bring your own device (BYOD) solutions. This reference design is modular and can be deployed in whole or in part.

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

ABSTRACT

Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally owned devices. This practice guide provides an example solution demonstrating how to enhance security and privacy in Android and Apple phones and tablets used in BYOD deployments.

Incorporating BYOD deployments into an organization can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of traditional in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

However, some of the features that make BYOD mobile devices increasingly flexible and functional also present unique security and privacy challenges to both organizations and device owners. The unique nature of these challenges is driven by the differing risks posed by the type, age, operating system (OS), and other variances in mobile devices.

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks. Solutions that are designed to secure corporate devices and on-premises data do not provide an effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new privacy risks to employees by providing their employer a degree of access to their personal devices, opening up the possibility of observation and control that would not otherwise exist.

To help organizations benefit from BYOD's flexibility while protecting themselves from critical security and privacy challenges, this practice guide provides an example solution using standards-based, commercially available products and step-by-step implementation guidance.

KEYWORDS

Bring your own device; BYOD; mobile device management; mobile device security.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Donna Dodson*	NIST
Joshua M. Franklin*	NIST
Dylan Gilbert	NIST
Jeff Greene*	NIST
Natalia Martin	NIST

Name	Organization
William Newhouse	NIST
Cherilyn Pascoe	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Jessica Walton	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward*	IBM
Cesare Coscia*	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis*	Kryptowire (now known as Quokka)
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks

Name	Organization
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici*	Zimperium

**Former employee; all work for this publication done while at employer.*

The Technology Partners/Collaborators who participated in this build 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 Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

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.

PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

List of Figures

List of Tables

1 Summary

This section familiarizes the reader with

- Bring Your Own Device (BYOD) concepts
- Challenges, solutions, and benefits related to BYOD deployments

BYOD refers to the practice of performing work-related activities on personally owned devices. This practice guide provides an example solution demonstrating how to enhance security and privacy in Android and iOS mobile device BYOD deployments.

Incorporating BYOD capabilities in an organization can provide greater flexibility in how employees work and can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. Other organizations may adopt a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

Extending mobile device use by enabling BYOD capabilities in the enterprise can introduce new information technology (IT) risks to organizations. Solutions that are designed to help secure corporate devices and the data located on them do not always provide an effective cybersecurity solution for BYOD.

Deploying effective solutions can be challenging due to the unique risks that BYOD deployments impose. Some of the features that make personal mobile devices increasingly flexible and functional also present unique security and privacy challenges to both employers and device owners.

Additionally, enabling BYOD capabilities can introduce new privacy risks to employees by providing their employer a degree of access to their personal devices, opening the possibility of mobile device observation and control that would not otherwise exist.

This practice guide helps organizations deploy BYOD capabilities by providing an example solution that helps address BYOD challenges, solutions, and benefits. In this practice guide, the term mobile device is used to describe an Apple iOS or Google Android phone or tablet. This practice guide's scope for BYOD does not include deployment of laptops or devices similar to laptops.

1.1 Challenge

Many organizations now authorize employees to use their personal mobile devices to perform work-related activities. This provides employees with increased flexibility to access organizational information resources. However, BYOD architectures can also introduce vulnerabilities in the enterprise’s IT infrastructure because personally owned mobile devices are typically unmanaged and may lack security and privacy protections. Unmanaged devices are at greater risk of unauthorized access to sensitive information, tracking, email phishing, eavesdropping, misuse of device sensors, or compromise of organizational data due to lost devices to name but a few risks.

BYOD deployment challenges can include:

- **Supporting a broad ecosystem of mobile devices**
    - with diverse technologies that rapidly evolve and vary in manufacturer, operating system (OS), and age of the device
    - where each device has unique security and privacy requirements and capabilities
    - whose variety can present interoperability issues that might affect organizational integration
- **Reducing risk to the confidentiality, integrity, and availability of the enterprise's sensitive information**
    - posed by applications that may not usually be installed on devices issued by an organization
    - that result from lost, stolen, or sold mobile devices that still contain or have access to organizational data
    - created by a user who shares their personally owned device with friends and family members when that personally owned device may also be used for work activities
    - due to personally owned mobile devices being taken to places that increase the risk of loss of control for the device
    - that result from malicious applications compromising the device and subsequently the data to which the device has access
    - produced by network-based attacks that can traverse a device's always-on connection to the internet
    - caused by phishing attempts that try to collect user credentials or entice a user to install malicious software
    - that results from the increased value of employees' mobile devices due to enterprise data being present
- **Protecting the privacy of employees**
    - by helping to keep their personal photos, documents, location, and other data private and inaccessible to others (including the organization)
    - by helping to ensure separation between their work and personal data while simultaneously meeting the organization's objectives for business functions, usability, security, and employee privacy
    - by providing them with concise and understandable information about what data is collected and what actions are allowed and disallowed on their devices
- **Clearly communicating BYOD concepts**
    - among an organization's IT team so it can develop the architecture to address BYOD's unique security and privacy concerns while using a repeatable, standardized, and clearly communicated risk framework language
    - to organizational leadership and employees to obtain support and providing transparency in deploying BYOD

    - related to mobile device security technologies so that the organization can consistently plan for and implement the protection capabilities of their security tools

Given these challenges, it can be complex to manage the security and privacy aspects of personally owned mobile devices that access organizational information assets. This document provides an example solution to help organizations address these challenges.

1.2 Solution

To help organizations benefit from BYOD's flexibility while protecting themselves from many of its critical security and privacy challenges, this National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide provides an example solution using standards-based, commercially available products and step-by-step implementation guidance.

In our lab at the National Cybersecurity Center of Excellence (NCCoE), engineers built an environment that contains an example solution for managing the security and privacy of BYOD deployments. In this guide, we show how an enterprise can leverage the concepts presented in this example solution to implement enterprise mobility management (EMM), mobile threat defense (MTD), application vetting, a trusted execution environment (TEE) supporting secure boot/image authentication, and virtual private network (VPN) services to support a BYOD solution.

We configured these technologies to protect organizational assets and employee privacy and provide methodologies to enhance the data protection posture of the adopting organization. The standards and best practices on which this example solution is based help ensure the confidentiality, integrity, and availability of enterprise data on BYOD Android and iOS mobile devices as well as the predictability, manageability, and disassociability of employee's data.

The example solution in this practice guide helps:

- detect and protect against installing mobile malware, phishing attempts, and network-based attacks
- enforce passcode usage
- protect organizational data by enabling selective device wipe capability of organizational data and applications
- protect against organizational data loss by restricting an employee's ability to copy and paste, perform a screen capture, or store organizational data in unapproved locations
- organizations understand BYOD risks and remediate threats (e.g., risks from jailbroken or rooted devices)
- provide users with access to protected business resources (e.g., SharePoint, knowledge base, internal wikis, application data)
- support executed code authenticity, runtime state integrity, and persistent memory data confidentiality
- protect data from eavesdropping while traversing a network
- vet the security of mobile applications used for work-related activities
- organizations implement settings to protect employee privacy

- an organization deploy its own BYOD solution by providing a series of how-to guides, step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture, to help security and privacy engineers rapidly deploy and evaluate a mobile device solution in their test environment

Commercial, standards-based products such as the ones used in this practice guide are readily available and interoperable with existing IT infrastructure and investments. Organizations can use this guidance in whole or in part to help understand and mitigate common BYOD security and privacy challenges.

1.2.1 Standards and Guidance

This guide leverages many standards and guidance, including the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1], the *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2], NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017)* [3], the NIST Risk Management Framework [4], and the NIST Mobile Threat Catalogue [5]. For additional information, see Appendix D, Standards and Guidance.

1.2.2 Benefits of this Example Solution

Carrying two mobile devices, one for work and one for personal use, introduces inconveniences and disadvantages that some organizations and employees are looking to avoid. Recognizing that BYOD is being adopted, the NCCoE worked to provide organizations with guidance for improving the security and privacy of these BYOD solutions.

For organizations, the potential benefits of this example solution include:

- enhanced protection against both malicious applications and loss of data if a device is stolen or misplaced
- reduced adverse effects if a device is compromised
- visibility for system administrators into mobile security compliance, enabling automated identification and notification of a compromised device
- a vendor-agnostic, modular architecture based on technology roles
- demonstrated enhanced security options for mobile access to organizational resources such as intranet, email, contacts, and calendar

For employees, the potential benefits of this example solution include:

- safeguards to help protect their privacy
- better protected personal devices by screening work applications for malicious capability before installing them
- enhanced understanding about how their personal device will integrate with their organization through a standardized BYOD deployment

2 How to Use This Guide

This section familiarizes the reader with:

- this practice guide's content
- the suggested audience for each volume
- typographic conventions used in this volume

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this BYOD example solution. This reference design is modular and can be deployed in whole or in part.

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary* – high-level overview of the challenge, example solution, and benefits of the practice guide
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security, privacy, and technology officers will be interested in the *Executive Summary, NIST SP 1800-22A*, which describes the following topics:

- challenges that enterprises face in securing BYOD deployments
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology, security, or privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-22B*, which describes what we did and why. The following sections will be of particular interest:

- Appendix E, Example Security Subcategory and Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.
- Appendix F, Example Privacy Subcategory and Control Map, describes how the privacy control map identifies the privacy characteristic standards mapping for the products as they were used in the example solution.

You might share the *Executive Summary, NIST SP 1800-22A*, with your leadership team members to help them understand the importance of adopting standards-based BYOD deployments.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build 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.

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 this guide's example solution for BYOD security management. Your organization's security experts should identify the products that will effectively address the BYOD risks identified for your organization and that 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. Section 4.3, Technologies that Support the Security and Privacy Objectives of the Example Solution, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

For those who would like to see how the example solution can be implemented, this practice guide contains a volume titled NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice,* which explores an example scenario about a fictional company called Great Seneca Accounting. The example scenario shows how BYOD objectives can align with an organization's priority security and privacy capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice guide's supplement, *Example Scenario: Putting Guidance into Practice*.

- Appendix F of the Supplement describes the risk analysis we performed, using an example scenario.
- Appendix G of the Supplement describes how to conduct a privacy risk assessment and use it to improve mobile device architectures, using an example scenario.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to mobile-nccoe@nist.gov.

Acronyms used in figures can be found in Appendix A, List of Acronyms.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`Mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

This section familiarizes the reader with:

- this guide's intended audience, scope, and assumptions
- mobile device security and privacy risk assessments

To identify the cybersecurity challenges associated with deploying a BYOD solution, the team surveyed reports of mobile device security trends and invited the mobile device security community to engage in a discussion about pressing cybersecurity challenges.

Two broad and significant themes emerged from this research:

- Administrators wanted to better understand what policies and standards should be implemented.
- Employees were concerned about the degree to which enterprises have control over their personally owned mobile devices and potential visibility into the personal activity that takes place on them.

The team addressed these two challenges by reviewing the primary standards, best practices, and guidelines contained within Appendix D, Standards and Guidance.

3.1 Audience

This practice guide is intended for organizations that want to adopt a BYOD architecture that enables use of personal mobile devices. The target audience is executives, security managers, privacy managers, engineers, administrators, and others who are responsible for acquiring, implementing, communicating with users about, or maintaining mobile enterprise technology. This technology can include centralized device management, secure device/application security contexts, application vetting, and endpoint protection systems.

This document will interest system architects already managing mobile device deployments and those looking to integrate a BYOD architecture into existing organizational wireless systems. It assumes that readers have a basic understanding of mobile device technologies and enterprise security and privacy principles. Please refer to Section 2 of this document for how different audiences can effectively use this guide.

3.2 Scope

The scope of this build includes managing iOS or Android mobile devices deployed in a BYOD configuration with cloud-based EMM. We excluded laptops and mobile devices with minimal computing capability, including feature phones and wearables. We also do not address classified systems, devices, data, and applications within this publication.

While this document is primarily about mobile device security for BYOD implementations, BYOD introduces privacy risk to the organization and its employees who participate in the BYOD program. Therefore, the NCCoE found addressing privacy risk to be a necessary part of developing the BYOD architecture. The scope of privacy in this build is limited to those employees who use their devices as part of their organization's BYOD solution. The build does not explicitly address privacy considerations of other individuals (e.g., an employee's family members) whose information is processed by the organization through an employee's personal device.

We intend for the example solution proposed in this practice guide to be broadly applicable to enterprises, including both the public and private sectors.

3.3 Assumptions

This project is guided by the following assumptions:

- The example solution was developed in a lab environment. While the environment is based on a typical organization's IT enterprise, the example solution does not reflect the complexity of a production environment.
- The organization has access to the skills and resources required to implement a mobile device security and privacy solution.
- The example security and privacy control mappings provided as part of this practice guide are focused on mobile device needs, and do not include general control mappings that would also typically be used in an enterprise. Those general control mappings that do not specifically apply to this guide's mobile device security example solution are outside the scope of this guide's example solution.
- Because the organizational environment in which this build could be implemented represents a greater level of complexity than is captured in the current guide, we assume that organizations will first examine the implications for their current environment before implementing any part of the proposed example solution.
- The organization has either already invested or is willing to invest in the security of mobile devices used within it and in the privacy of participating employees, and in the organization's IT

systems more broadly. As such, we assume that the organization either has the technology in place to support this implementation or has access to the off-the-shelf technology used in this build, which we assume will perform as described by the respective product vendor.

- The organization has familiarized itself with existing standards and any associated guidelines (e.g., NIST Cybersecurity Framework [1]; *NIST Privacy Framework* [2]; NIST SP 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]; NIST SP 1800-4 *Mobile Device Security: Cloud and Hybrid Builds* [7]) relevant to implementation of the example solution proposed in this practice guide. We also assume that any existing technology used in the example solution has been implemented in a manner consistent with these standards.
- The organization has instituted relevant mobile device security and privacy policies, and these will be updated based on implementation of this example solution.
- The organization will provide guidance and training to its employees regarding BYOD usage and how to report device loss or suspected security issues in which their devices are involved. This guidance will be periodically reviewed and updated, and employees will be regularly trained on BYOD usage.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public. The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

Our BYOD risk assessments helped to identify and mitigate potential security threats, vulnerabilities, problematic data actions, and risks. The following sections define these terms.

3.4.1 Security Threats

NIST SP 800-30 Revision 1 defines a threat as "any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service". Threats are actions that may compromise a system's confidentiality, integrity, or availability [8]. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

3.4.2 Vulnerabilities

As defined in NIST SP 800-30 Revision 1, a vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" [8]. Vulnerabilities may exist in a broader context. That is, they may be found in organizational governance structures, external relationships, and mission/business processes.

3.4.3 Problematic Data Actions

This build considered operational activities of the example solution that interact with employee data during architectural processes ("data actions") and identified those that potentially cause problems to individuals ("problematic data actions").

The NIST Privacy Framework defines a problematic data action as "a data action that could cause an adverse effect for individuals."[9] Problematic data actions can result in privacy risk to individuals and prevent an organization from developing a solution that meets the privacy engineering objectives of:

- predictability: enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service
- manageability: providing the capability for granular administration of data, including alteration, deletion, and selective disclosure
- disassociability: enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

An organization should perform a risk assessment to determine contextual application of the problematic data actions. The discussion about problematic data actions and risks in Appendix G of the Great Seneca Supplement introduces the PRAM and provides a more detailed analysis of the privacy risks in this build.

3.4.4 Risks

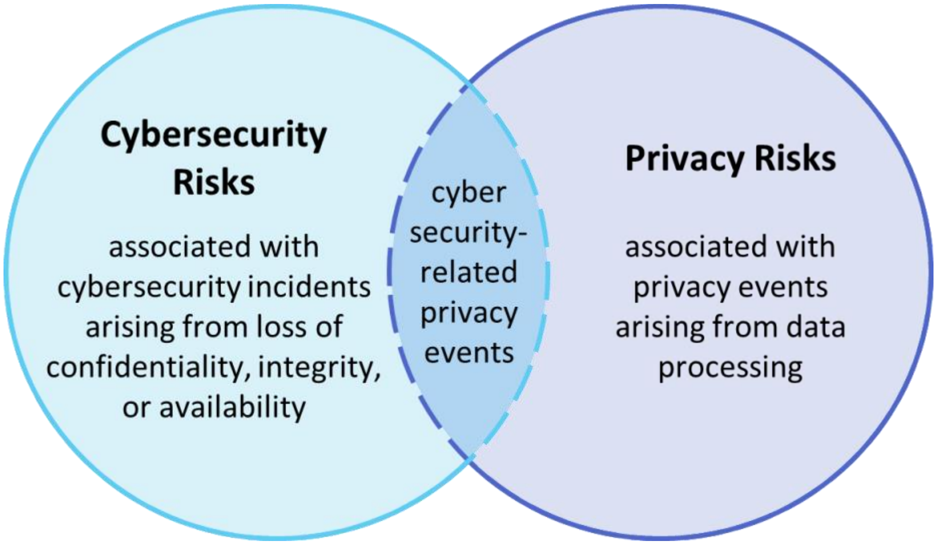
As noted in Section 3.4, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* defines risk as "a measure of the extent to which an entity is threatened by potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." [8]

Risk is the adverse impact or the result when a threat (attack) successfully leverages one or more vulnerabilities. As organizations consider risk, they should note that risk is not discreet. One may realize multiple risks based on a successful attack. And, those attacks may involve strictly cybersecurity threat events, the realization of privacy risks, or both.

3.5 Applying Risk Assessments to this BYOD Example Solution

We identified the security and privacy risks for this BYOD example solution by examining the relationship of risk between cybersecurity and privacy. Cybersecurity and privacy are two distinct risk areas, though the two intersect in significant ways. As noted in Section 1.2.1 of the NIST Privacy Framework [2], having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to cybersecurity risks. Allowing an unauthorized device to connect to the organization's network through its BYOD implementation is an example of a security risk that may not impact privacy.

Figure 3-1 Cybersecurity and Privacy Risk Relationship


Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

The security capabilities in this build help address some of the privacy risks that arise for employees. This build also uses the *NIST Privacy Framework* [2] and Privacy Risk Assessment Methodology (PRAM) [9] to identify and address privacy risks that are beyond the scope of security risks. Regardless of whether cybersecurity and privacy are situated in the same part of the organization or in different parts, the two capabilities must work closely together to address BYOD risks.

A risk assessment might include the following additional analysis areas. For more information on the example solution risk methodology employed for this BYOD example solution, see the referenced sections:

- **Security threats** and **objectives to remediate those threats,** see Section 4.1
- **Data actions** that introduce privacy problems (i.e., problematic data actions) and the methods to address those problems, see Section 4.1 and Appendix G of the Supplement
- **Vulnerabilities** that influenced the reference architecture, see Appendix Section F-5 of the Supplement
- **Risks** that influenced the architecture development, see Appendix Section F-6 of the Great Seneca Supplement
- **Security and Privacy Control Mapping** to cybersecurity and privacy standards and best practices, see Appendix E and Appendix F in this volume

4 Architecture

This section helps familiarize the reader with:

- threats to BYOD architectures

- example solution methods to remediate threats to BYOD architectures
- how organizations might leverage the Example Scenario: Putting Guidance into Practice supplement of this practice guide to implement their mobile device solution
- technologies to support the example solution objectives
- the example solution's architecture
- how the example solution's products were integrated
- mobile device data collection

4.1 Common BYOD Risks and Potential Objectives to Remediate Those Risks

This section contains examples of common security and privacy risks in BYOD deployments. We provide a list of objectives to manage those risks. Once completed, the example solution's architecture provides organizations with a security and privacy-enhanced design that can be leveraged for the BYOD deployments of mobile devices. The challenges addressed by the example solution's and risk remediation objectives are highlighted below, followed by the architecture that supports those objectives.

4.1.1 Threat Events

Leveraging a system life cycle approach [10], this build considered threats relating to BYOD deployments. Information from the Open Web Application Security Project Mobile Top 10 [11], which provides a consolidated list of mobile application risks, and information from the NIST Mobile Threat Catalogue [5], which examines the mobile information system threats in the broader mobile ecosystem, were used to develop applicable threats. Table 4-1 gives each threat an identifier for the purposes of this build, a description of each threat event (TE), and the related NIST Mobile Threat Catalogue Threat identifiers (IDs).

We limited inclusion of TEs to those that we generally expected to have a high likelihood of occurrence and high potential for adverse impact. Organizations applying this build should evaluate the NIST Mobile Threat Catalogue for additional threats that may be relevant to their architecture. For an example of how to determine the risk from these threats, see Appendix F in the Supplement.

The threat events are also used in Appendix F in the 1800-22 Supplement to identify relevant mobile threats in the example scenario and Appendix D in 1800-22 Volume C to test the security characteristics of the lab build.

Table 4-1 Examples of BYOD Deployment Threats

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-1	Intrusive application practices	APP-2, APP-12
TE-2	Account credential theft through phishing	AUT-9
TE-3	Outdated phones	APP-4, APP-26, STA-0, STA-9, STA-16

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-4	Sensitive data transmissions	APP-0, CEL-18, LPN-2
TE-5	Brute-force attacks to unlock a phone	AUT-2, AUT-4
TE-6	Application credential storage vulnerability	APP-9, AUT-0
TE-7	Unmanaged device protection	EMM-5
TE-8	Lost or stolen data protection	PHY-0
TE-9	Protecting enterprise data from being inadvertently backed up to a cloud service	EMM-9

4.1.2 Privacy Risks

In addition to the TEs just discussed, this practice guide's example solution also considers and helps mitigate privacy risks that can apply to BYOD deployments. Privacy risks for individuals can present themselves through problematic data actions. The NIST Privacy Framework defines a problematic data action as "a data action that could cause an adverse effect for individuals." [2] Example problematic data actions are shown in the table below:

Table 4-2: Example Privacy Risks and Problematic Data Actions

Privacy Risk ID	Description	Problematic Data Action
PR-1	Wiping Activities on the Employee's Device May Inadvertently Delete the Employee's Personal Data	Unwarranted Restriction
PR-2	Organizational Collection of Device Data May Subject Employees to Feeling of Being Surveilled	Surveillance
PR-3	Data Collection and Transmission Between Integrated Security Products May Expose Employee Data	Unanticipated Revelation
PR-4	Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations	Appropriation Induced Disclosure
PR-5	Unauthorized or Invasive Application Processing of Information Exposes Employee Data	Surveillance Unanticipated Revelation

The Privacy Risks are also used in Appendix F in the 1800-22 Supplement to identify relevant mobile privacy risks in the example scenario and Appendix D in 1800-22 Volume C to test the privacy characteristics of the lab build.

4.1.2.1 Privacy Risk Examples and Mitigation Methodologies

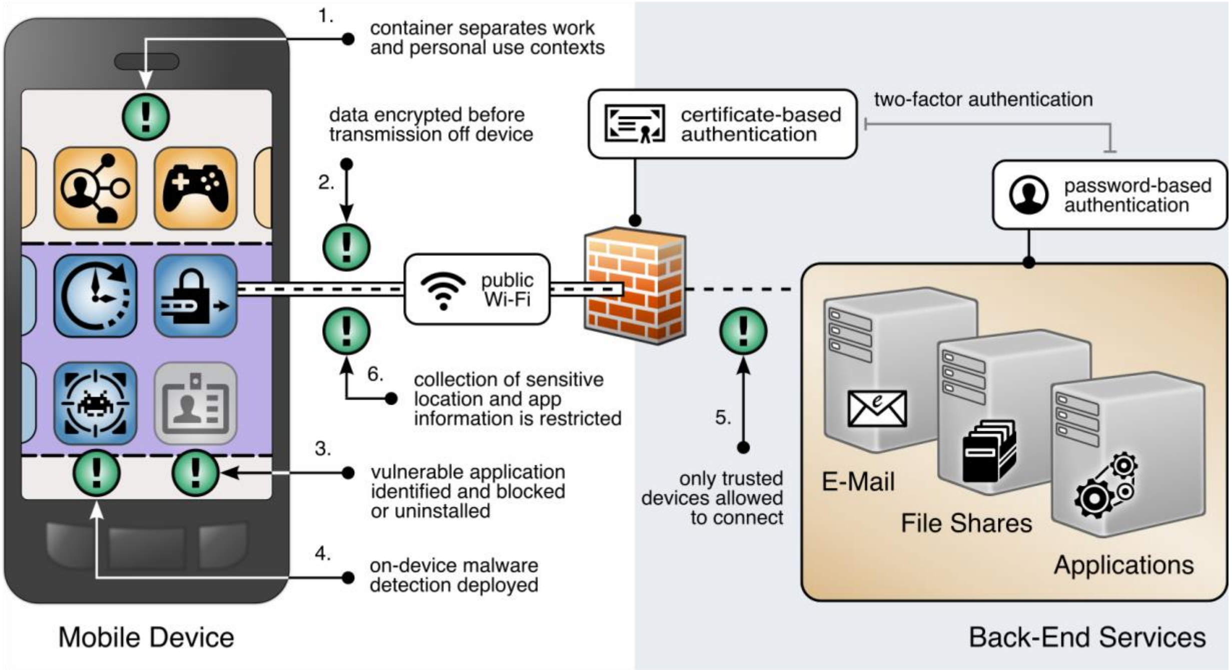
The example solution contained in this guide identifies and helps to mitigate some common privacy risks that a BYOD deployment may encounter. The privacy risks and their accompanying problematic data actions were identified using NIST-developed methodologies.

The NIST PRAM [9] and accompanying Catalog of Problematic Data Actions and Problems [12] (see Section 4.1.2) are standardized methodologies for identifying privacy challenges that were used to conduct our privacy risk analysis. This publication provides the results of our privacy risk analysis for a fictional organization as an exemplar for the reader's use, as well as suggested privacy architecture enhancements. See Appendix G of the Supplement for an example of how the privacy risks for this practice guide's BYOD deployment example solution were developed. The following section, 4.1.3, outlines the security and privacy objectives of this publication's example solution architecture.

4.1.3 Security and Privacy Objectives

To address the challenges stated in the previous sections, the architecture for this build addresses the high-level security and privacy objectives illustrated in Figure 4-1.

Figure 4-1 Security and Privacy Objectives


1.
container separates work and personal use contexts
data encrypted before transmission off device
2.
certificate-based authentication
two-factor authentication
password-based authentication
public Wi-Fi
6.
collection of sensitive location and app information is restricted
5.
3.
vulnerable application identified and blocked or uninstalled
only trusted devices allowed to connect
E-Mail
File Shares
Applications
4.
on-device malware detection deployed
Mobile Device
Back-End Services

The following are a list of security and privacy objectives (as highlighted above in Figure 4-1, with a green exclamation mark):

1. **Separate organization and personal information.** BYOD deployments can place organizational data at risk by allowing it to travel outside internal networks and systems when it is accessed on a personal device. BYOD deployments can also place personal data at risk by capturing information from employee devices. To help mitigate this, organizational and personal information can be separated by restricting data flow between organizationally managed and

unmanaged applications. The objectives include helping to prevent sensitive data from crossing between work and personal contexts.

2. **Encrypt data in transit.** Devices deployed in BYOD scenarios can leverage nonsecure networks, putting data at risk of interception. To help mitigate this, mobile devices can connect to the organization over a VPN or similar solution to encrypt all data before it is transmitted from the device, protecting otherwise unencrypted data from interception. A user would not be able to access the organization's resources without an active VPN connection and required certificates.

3. **Identify vulnerable applications.** Employees may install a wide range of applications on their personally owned devices, some of which may have security weaknesses. When vulnerable personal applications are identified, an organization can remove the employee's work profile (e.g., work applications such as work email) or configuration file from the device rather than uninstalling the employee's personal applications.

4. **Prevent or detect malware.** On personally owned devices, users may obtain applications outside official application stores, increasing the risk of installing malware in disguise. To help protect from this risk, an organization could deploy malware detection to devices to identify malicious applications within the work profile or managed applications and facilitate remediation. Additionally, security features that are built-in to the OS could aid in preventing or detecting the installation of malware.

5. **Trusted device access.** Because mobile devices can connect from unknown locations, an organization can provision mobile devices with a security certificate that allows identifying and authenticating them at the connection point, which combines with user credentials to create two-factor authentication from mobile devices. An employee would not be able to access the organization's resources without the required certificates.

6. **Restrict information collection.** Depending on how devices are enrolled, mobile device management tools can sometimes track application inventory and location information, including physical address, geographic coordinates, location history, internet protocol (IP) address, and service set identifier (SSID). These capabilities may reveal sensitive information about employees, such as frequently visited locations or habits. Device management tools can be configured to exclude application and location information. Excluding the collection of information further protects employee privacy when device and application data is shared outside the organization for monitoring and analytics.

4.2 Example Scenario: Putting Guidance into Practice

The example solution's high-level objectives underscore the need to use a thorough risk assessment process for organizations implementing mobile device security capabilities. To learn more about how your organization might implement this example solution, reference the NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice*. The supplement provides an example approach for developing and deploying a BYOD architecture that directly addresses the mobile device TEs and problematic data actions discussed in this guide.

The supplement shows how a fictional organization used the guidance in NIST's Cybersecurity Framework [1], Privacy Framework [2], RMF [10], and PRAM [9] to identify and address their BYOD security and privacy objectives.

4.3 Technologies that Support the Security and Privacy Objectives of the Example Solution

This section describes the mobile-specific technology components used within this example solution. These technologies were selected to address the security objectives, TEs, and problematic data actions identified in Section 4.1. This section provides a brief description of each technology and discusses the security and privacy capabilities that each component provides.

The technology components in this section are combined into a cohesive enterprise architecture to help address BYOD security threats and problematic data actions and provide security-enhanced access to enterprise resources from mobile devices. The technologies described in this section provide protection for enterprise resources accessed by BYOD users.

4.3.1 Trusted Execution Environment

A TEE is "a controlled and separated environment outside the high-level operating system that is designed to allow trusted execution of code and to protect against viruses, Trojans, and root kits." [13] By providing a controlled and separated environment, the TEE helps enable applications and features that can provide enhanced security and privacy functionality.

4.3.2 Enterprise Mobility Management

Organizations use EMM solutions to secure the mobile devices of users who are authorized to access organizational resources. Such solutions generally have two main components. The first is a backend service that mobile administrators use to manage the policies, configurations, and security actions applied to enrolled mobile devices. The second is an on-device agent, usually in the form of a mobile application, that integrates between the mobile OS and the solution's backend service. Both iOS and Android also support a bulk EMM enrollment use case (Apple Business Manager for iOS devices and Android Enterprise Enrollment for Android devices), which we do not discuss in this document.

At a minimum, an EMM solution can perform mobile device management (MDM) functions, which include the ability to provision configuration profiles to devices, enforce security policies on devices, and monitor compliance with those policies. The on-device MDM agent can typically notify the device user of any noncompliant settings and may be able to remediate some noncompliant settings automatically. The organization can use policy compliance data to inform its access control decisions so that it grants access only to a device that demonstrates the mandated level of compliance with the security policies in place.

EMM solutions commonly include any of the following capabilities: mobile application management, mobile content management, and implementations of or integrations with device- or mobile-OS-specific user profile solutions, such as Android Enterprise or iOS User Enrollment. These capabilities can be used in the following ways in a BYOD deployment:

- Mobile application management can be used to manage the installation and usage of an organization’s applications based on their trustworthiness and work relevance.
- Mobile content management can control how managed applications access and use organizational data.
- The EMM works with operating system data separation and isolation capabilities that can strengthen the separation between a user’s personal and professional usage of the device.
- Also, EMM solutions often have integrations with a diverse set of additional tools and security technologies that enhance their capabilities.

For further reading on this topic, NIST SP 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6] provides additional information on mobile device management with EMM solutions. The National Information Assurance Partnership’s (NIAP’s) *Protection Profile for Mobile Device Management Servers and Extended Package for Mobile Device Management Agents* [14] describes important capabilities and security requirements to look for in EMM systems.

EMMs can help BYOD deployments improve the security posture of the organization by providing a baseline of controls to limit attack vectors and help protect enterprise information that is on a personally owned device. EMMs can also provide an additional layer of separation between enterprise data and personal data on a mobile device.

In addition, EMMs may also provide mobile application wrapping functionality. The wrapping process encapsulates enterprise-developed applications in a vendor-created wrapper that intercepts application programming interface (API) calls and provides additional layers of security. Wrapping is useful in many different scenarios, for example, to force an application’s traffic to go through the corporate VPN. Wrapping typically occurs when applications are uploaded to the EMM’s app store for distribution to enrolled devices [15].

4.3.3 Virtual Private Network

A VPN gateway increases the security of remote connections from authorized mobile devices to an organization’s internal network. A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communication channel for data and system control information transmitted between networks. VPNs are used most often to protect communications carried over public networks from eavesdropping and interception. A VPN can provide several types of data protection, including confidentiality, integrity, authentication of data origin, replay protection, and access control that help reduce the risks of transmitting data between network components.

VPN connections apply an additional layer of encryption to the communication between remote devices and the internal network, and VPN gateways can enforce access control decisions by limiting what devices or applications can connect to them. Integration with other security mechanisms allows a VPN gateway to base access control decisions on more risk factors than it may be able to collect on its own; examples include a device’s level of compliance with mobile security policies, or the list of installed applications as reported by an integrated EMM and/or MTD.

NIAP’s *Module for Virtual Private Network (VPN) Gateways 1.0* [16], in combination with *Protection Profile for Network Devices* [17], describes important capabilities and security requirements to expect from VPN gateways.

In a BYOD deployment, an enterprise can also leverage a per-application or full enterprise profile VPN to provide a secure connection over the VPN tunnel strictly when using enterprise applications on the mobile device. Personal applications on the device would not be allowed to use the VPN, ensuring the enterprise only has visibility into enterprise traffic. This is especially important to BYOD deployments, whose devices may connect over a wide variety of wireless networks. It also provides a layer of privacy protection for employees by preventing personal mobile device traffic from being routed through the enterprise.

4.3.4 Mobile Application Vetting Service

Mobile application vetting services use a variety of static, dynamic, and behavioral techniques to determine if an application demonstrates any behaviors that pose a security or privacy risk. The risk may be to a device owner or user, to parties that own data on the device, or to external systems to which the application connects. The set of detected behaviors is often aggregated to generate a singular score that estimates the level of risk (or conversely, trustworthiness) attributed to an application. Clients can often adjust the values associated with given behaviors (e.g., hardcoded cryptographic keys) to tailor the score for their unique risk posture. Those scores may be further aggregated to present a score that represents the overall risk or trustworthiness posed by the set of applications currently installed on a given device.

Mobile applications, whether malicious or benign, can negatively affect both security and user privacy. A malicious application can contain code intended to exploit vulnerabilities present in potentially any targeted hardware, firmware, or software on the device. Alternatively, or in conjunction with exploit code, a malicious application may misuse any device, personal, or behavioral data to which it has been explicitly or implicitly granted access, such as contacts, clipboard data, or location services. Benign applications may still present vulnerabilities or weaknesses that malicious applications can exploit to gain unauthorized access to the device's data or functionality. Further, benign applications may place user privacy at risk by collecting more information than is necessary for it to deliver the functionality desired by the user.

While not specific to applications, some services may include device-based risks (e.g., a vulnerable OS version) in their analysis to provide a more comprehensive assessment of the risk or trustworthiness presented by a device when running an application or service.

While NIAP does not provide a protection profile for application vetting services, their *Protection Profile for Application Software* [18] describes security requirements to be expected from mobile applications. Many mobile application vetting vendors provide capabilities to automate evaluation of applications against NIAP's requirements.

Application vetting services help improve the security and privacy posture of mobile devices by assessing the risk of the applications that may be installed on a personally owned device. Depending on the deployment strategy, the application vetting service may analyze all installed applications, enterprise-only applications, or no applications.

4.3.5 Mobile Threat Defense

MTD generally takes the form of an application that is installed on the device that provides information about the device's threat posture based on risks, security, and activity on the device. This is also known as endpoint protection. Ideally, the MTD solution will be able to detect unwanted activity and properly inform the user and BYOD administrators so they can act to prevent or limit the harm that an attacker could cause. Additionally, MTD solutions may integrate with EMM solutions to leverage the MTD agent's greater on-device management controls and enforcement capabilities, such as blocking a malicious application from being launched until the user can remove it.

While detecting threats, MTD products typically analyze device-, application-, and network-based threats. Device-based threats include outdated OS versions, insecure configurations, elevation of privileges, unauthorized device profiles, and compromised devices. Application-based threat detection can provide similar functionality to that of dedicated application vetting services. However, application-based threat detection may not provide the same level of detail in its analysis as dedicated application vetting services. Network-based threats include use of unencrypted and/or public Wi-Fi networks and attacks such as active attempts to intercept and decrypt network traffic.

Because BYOD mobile devices can have a wide variety of installed applications and usage scenarios, an MTD profile helps improve the security and privacy posture by providing an agent-based capability to detect unwanted activity within the work profile.

To further enhance device protection and analytic capabilities, MTD services may offer additional integrations with 3rd party threat intelligence services such as MITRE ATT&CK for Mobile or VirusTotal. These services could aid in enriching the data acquired from devices, providing more contextual and technical information on the discovered threats. Then, the enriched data could be forwarded to other services for additional analysis or triage, such as a Security Information and Event Management service.

4.3.6 Mobile Operating System Capabilities

Mobile OS capabilities are available without the use of additional security features. They are included as part of the mobile device's core capabilities. The following mobile OS capabilities can be found in mobile devices.

4.3.6.1 Secure Boot

Secure boot is a general term that refers to a system architecture that is designed to prevent and detect any unauthorized modification to the boot process. A system that successfully completes a secure boot has loaded its start-up sequence information into a trusted OS. A common mechanism is for the first program executed (a boot loader) to be immutable (stored on read-only memory or implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified by either immutable or verified code prior to execution. This process establishes a chain of trust that can be traced back to immutable, implicitly trustworthy code.

4.3.6.2 Device Attestation

Device attestation is an extension of the secure boot process that involves the OS (or more commonly, an integrated TEE and/or Hardware Security Model) providing cryptographically verifiable proof that it has a known and trusted identity and is in a trustworthy state. This means that all software running on the device is free from unauthorized modification.

Device attestation requires cryptographic operations using an immutable private key that can be verified by a trusted third party, which is typically the original equipment manufacturer of the TEE or device platform vendor. Proof of possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique device identifiers, metadata, the results of integrity checks on mutable software, and possibly metrics from the boot or attestation process itself [19].

4.3.6.3 Mobile Device Management Application Programming Interfaces

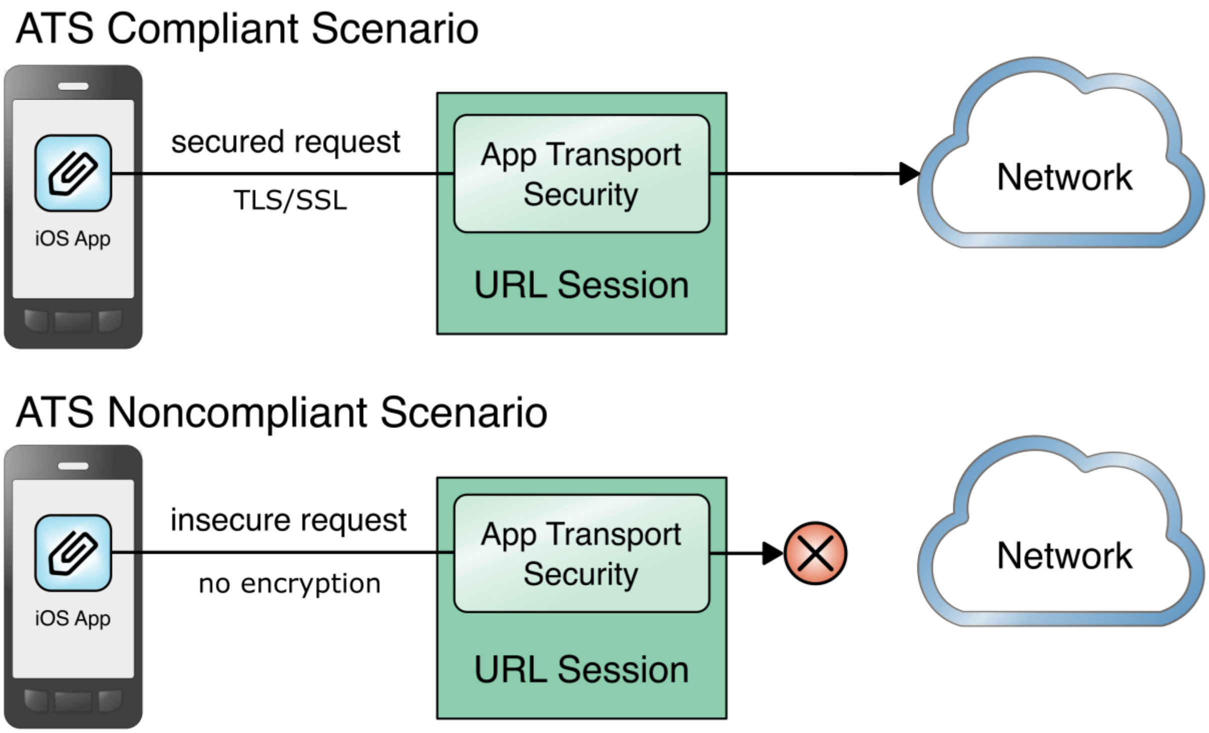
Mobile OS and platform-integrated firmware can provide a number of built-in security features that are generally active by default. Examples of how management APIs can enhance device security include verification of digital signatures for installed software and updates, requiring a device unlock code, initiating remote device lock actions, and requiring automatic device wipe following a series of failed device unlock attempts. The user can directly configure some of these features via a built-in application or through a service provided by the device platform vendor [20].

Additionally, mobile operating systems expose an API to MDM products that allow an organization that manages a device to have greater control over these and many more settings that might not be directly accessible to the device user. Management APIs allow enterprises using integrated EMM or MDM products to manage devices more effectively and efficiently than they could by using the built-in application alone.

4.3.6.4 iOS App Transport Security

App Transport Security (ATS) is a networking security feature on Apple iOS devices that increases data integrity and privacy for applications and extensions [21], [22]. ATS requires that the network connections made by applications are secured through the Transport Layer Security protocol, which uses reliable cipher suites and certificates. In addition, ATS blocks any connection that does not meet minimum security requirements. For applications linked to iOS 9.0 and later, ATS is enabled by default. Figure 4-2 shows how ATS compliant and noncompliant applications function. As demonstrated in the figure, secured application requests are allowed, and insecure requests are blocked.

Figure 4-2 iOS App Transport Security



4.3.6.5 Android Network Security Configuration

With data privacy becoming even more important, Google released mobile OS enhancements to protect data that traverses Android devices and endpoints [23], [24]. The Android Network Security Configuration prevents applications from transmitting sensitive data unintentionally in unencrypted cleartext. By default, `cleartextTrafficPermitted` is set to `false`. Through the Android Network Security Configuration feature, developers can designate what certification authorities are trusted and pin specific certificates to ensure secure communications and issue certificates.

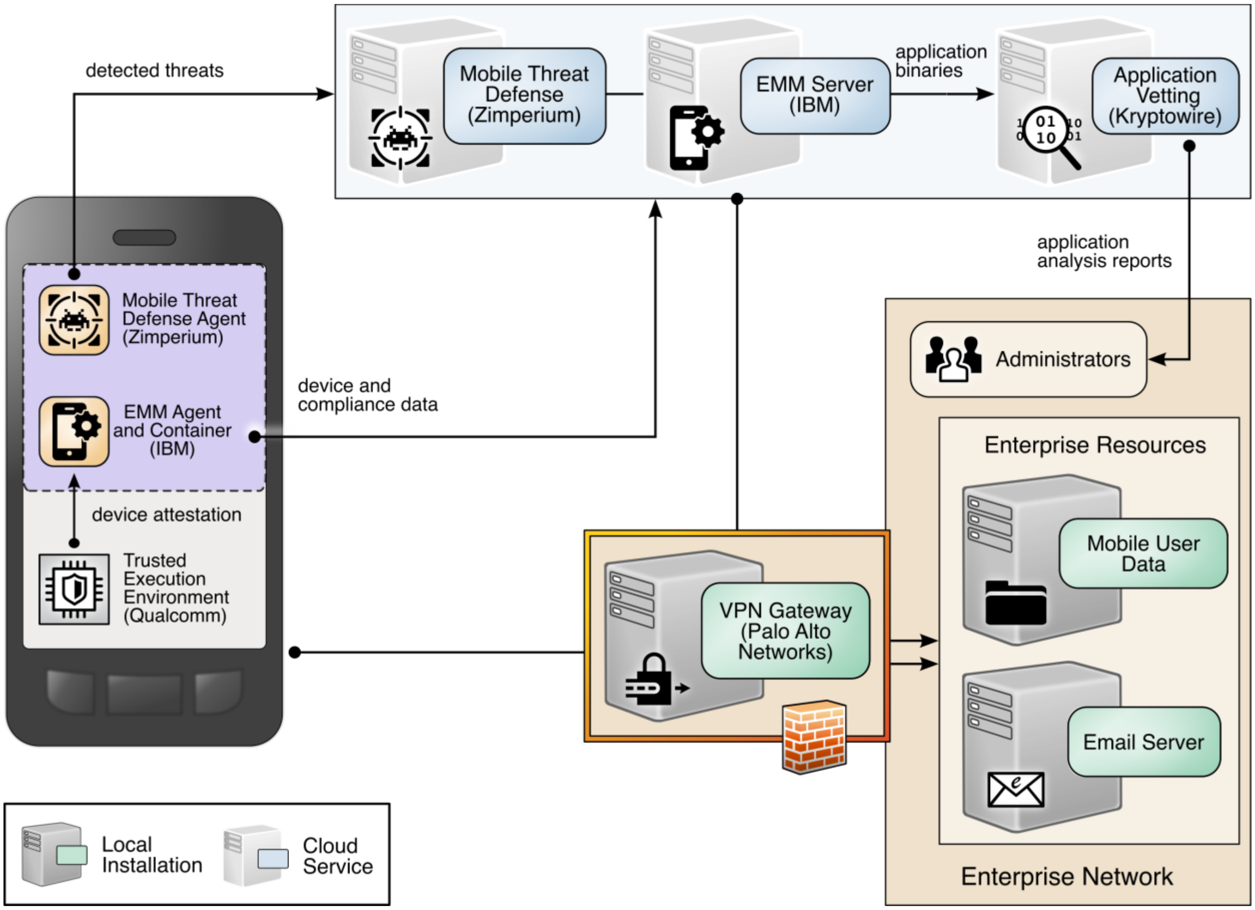
4.3.6.6 Application Sandboxing

Both Android and iOS impose sandboxing restrictions on applications running on the device. These security and privacy controls help isolate applications into their own runtime environments. The sandboxing restrictions then help prevent applications from accessing other applications' data or data on the underlying operating system not exposed by official APIs.

4.4 Architecture Description

The example solution architecture consists of the security technologies described in Section 4.3. The security technologies are further integrated with broader enterprise security mechanisms and a VPN gateway as shown in Figure 4-3. This example solution provides a broad range of capabilities to securely provision and manage devices, protect against and detect device compromise, and provide secure access to enterprise resources to only authorized mobile users and devices.

Figure 4-3 Example Solution Architecture


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Enterprise Network
Local Installation
Cloud Service

The NCCoE worked with industry experts to develop an open, standards-based architecture using commercially available products to address the threats and problematic data actions identified in Section 4.1.

Where possible, the architecture uses components that are present on the NIAP Product Compliant List, meaning that the product has been successfully evaluated against a NIAP-approved protection profile. The NIAP collaborates with a broad community, including industry, government, and international partners, to publish technology-specific security requirements and tests in the form of protection profiles. The requirements and tests in these protection profiles are intended to ensure that evaluated products address identified security threats and provide risk mitigation measures.

The security and privacy characteristics of the architecture result from many of the capability integrations outlined in Section 4.5.

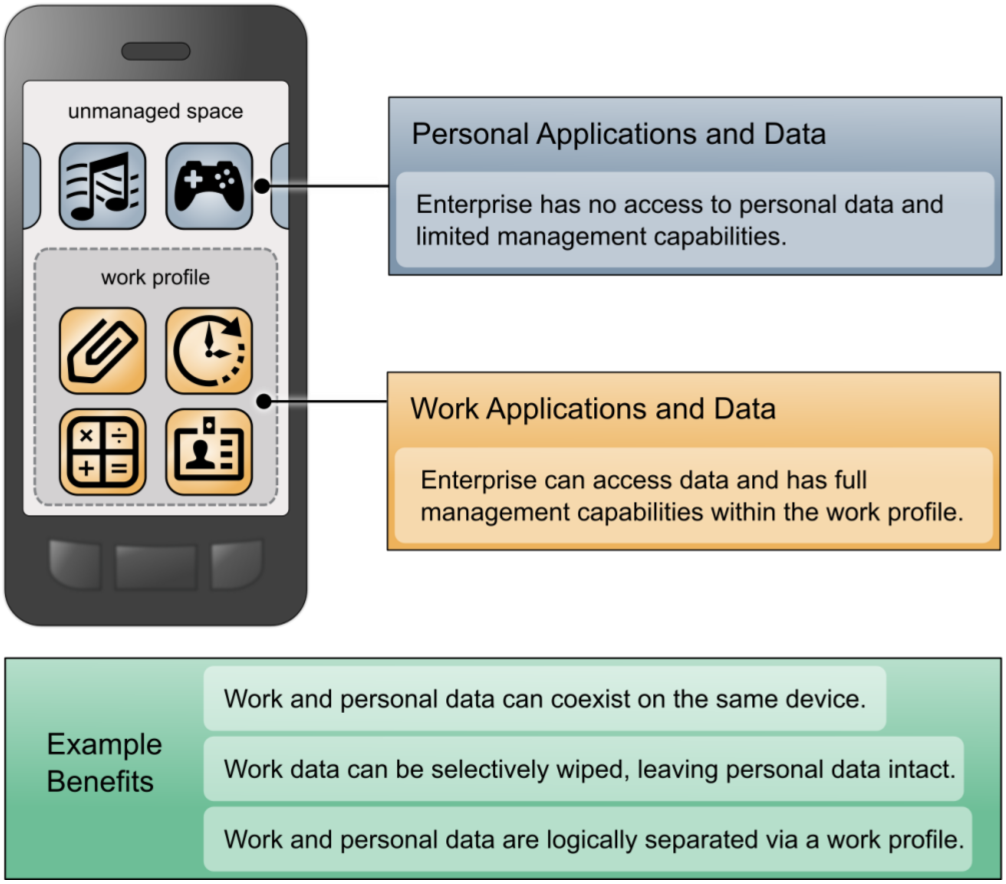
4.5 Enterprise Integration of the Employees' Personally Owned Mobile Devices

One key benefit of BYOD solutions for employees is the ability to access both work and personal data on the same device. While the technical approaches differ between iOS and Android devices, both operating systems offer the following types of features for managing the coexistence of work and personal data on devices [25], [26]:

- enterprise and personal application data isolation
- restriction of application installation from unofficial sources
- selective wiping to remove enterprise data and preserve personal data
- device passcode requirement enforcement
- enterprise application configuration control
- identity and certificate authority certificate support

Illustrating this concept, Figure 4-4 shows enterprise integration for managed and unmanaged applications on mobile devices. To protect sensitive work data and employee privacy, work applications can be separated into a work profile, with data access restricted between the personal and work container profile applications.

Figure 4-4 Mobile Device Application Management and Benefits


unmanaged space
work profile
Personal Applications and Data
Enterprise has no access to personal data and limited management capabilities.
Work Applications and Data
Enterprise can access data and has full management capabilities within the work profile.
Example Benefits
Work and personal data can coexist on the same device.
Work data can be selectively wiped, leaving personal data intact.
Work and personal data are logically separated via a work profile.

4.5.1 Microsoft Active Directory Integration

The example solution is integrated with Microsoft Active Directory (AD), which provides both enterprise identity management and certificate enrollment services via public key infrastructure. International

Business Machines (IBM) MaaS360 connects directly to the domain controller and the Network Device Enrollment Service (NDES) servers via an IBM Cloud Extender installed on the local intranet, while GlobalProtect connects to the domain controller via the Palo Alto Networks firewall’s Lightweight Directory Access Protocol service route.

By integrating directly with the AD infrastructure, administrators can configure MaaS360 to accept enrollment requests based on user groups in AD. GlobalProtect can inherit these roles and enforce access control protocols to restrict/deny permissions to the VPN. The AD integration is also used within MaaS360 to provide policy-based access to the MaaS360 administration console.

The Certificate Integration module within the MaaS360 Cloud Extender allows user certificates to be installed on the user’s devices when enrolling with MaaS360. These certificates are then validated in GlobalProtect during the VPN authentication sequence, along with the user’s corporate username and password. The Cloud Extender requests these certificates from the NDES server by using the Simple Certificate Enrollment Protocol.

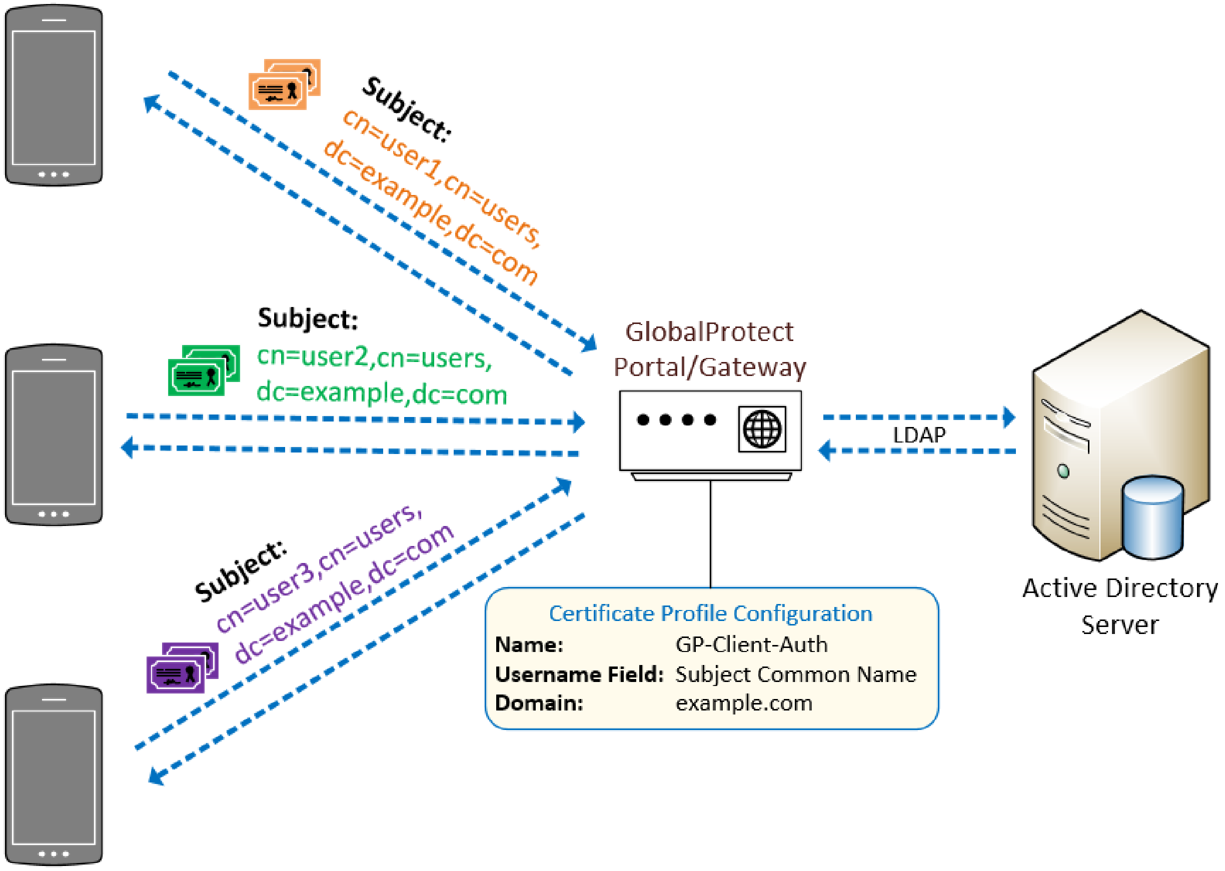
4.5.2 Mobile Device Enrollment

The example solution shown in Figure 4-5 mitigates the potential for Simple Certificate Enrollment Protocol (SCEP) to be remotely exploited by restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network. The uniform resource locator (URL) of the NDES server is resolvable only on this managed Wi-Fi network.

Furthermore, the NDES server is configured to require a dynamic challenge with each request. The Cloud Extender does this by including a one-time password with each request. This helps prevent unknown devices from requesting certificates. These certificates can then be used to prove identity when authenticating with the GlobalProtect VPN.

The certificate template includes the user’s username and email address. This allows the GlobalProtect gateway to enforce access control and identity verification.

Figure 4-5 Example Solution VPN Authentication Architecture



4.6 Mobile Components Integration

IBM MaaS360 supports integration of third-party applications and cloud services via a representational state transfer (REST) API [27]. External services are authenticated via access tokens, obtained through MaaS360 support. Zimperium and Kryptowire used the REST API [28].

Table 4-3 identifies the commercially available products used in this example solution and how they align with the mobile security technologies. For additional information, Appendices G and H contain a mapping of these technologies to the cybersecurity and privacy standards and best practices that each product provides in the example solution.

Table 4-3 Commercially Available Products Used

Commercially Available Product	Mobile Security Technology
IBM MaaS360 Mobile Device Management (SaaS) Version 10.82 IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)	mobile device management

Commercially Available Product	Mobile Security Technology
IBM MaaS360 Cloud Extender Cloud Extender Modules: Certificate Integration Module Version 2.96.000 Cloud Extender Base Module Version 2.96.000 Cloud Extender Basic Module Device Version 2.96.000 MaaS360 Configuration Utility Module Version 2.96.200 Mobile Device Management Module Version 2.31.020 User Authentication Module Version 2.96.200	
Kryptowire Cloud Service	application vetting
Palo Alto Networks PA-VM-100 Version 9.0.1 Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)	firewall virtual private network
Qualcomm (Version is mobile device dependent)	trusted execution environment
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense
Apple iOS Version 13 Google Android Version 10	mobile device operating system

4.6.1 Zimperium–MaaS360

Through the MaaS360 REST API, Zimperium can retrieve various device attributes such as device name, model, OS, OS version, and the owner's email address. It then continuously monitors the device's risk posture through the Zimperium Intrusion Prevention System (zIPS) application and reports any changes in the posture to MaaS360. This enables MaaS360 administrators to apply different device policies and enforcement actions based on the risk posture of a device.

When a device is enrolled with MaaS360, the zIPS application is automatically installed and configured in the work profile on the device. When the user first launches the zIPS application from within the work profile, it will automatically enroll the device in Zimperium's MTD service. zIPS will then continuously monitor the device for threats, and any detected threats will be reported to Zimperium. Zimperium can then report to MaaS360 if any changes in risk posture occurred.

MaaS360 can respond to the following risk posture levels, as assigned by Zimperium:

- low
- normal

- elevated
- critical

4.6.2 Kryptowire–MaaS360

Through the MaaS360 REST API, Kryptowire can retrieve a list of enrolled devices, device metadata (such as device ID, enterprise username, and device name), and the inventory of enterprise applications installed on those devices. This allows Kryptowire to automatically analyze all new applications installed on enrolled devices, ensuring that the risk posture of the devices, and therefore, the enterprise stays at an acceptable level.

Kryptowire also has configurable threat scores for various factors, such as requested permissions and hardcoded encryption keys.

The threat scores can be configured to one of four levels:

- low
- medium
- high
- critical

The administrator can configure a threat score alert threshold and an email address to receive alerts when an application's threat score is at or above the threshold. The administrator can then take appropriate action on the device in MaaS360.

Further, Kryptowire can provide information about applications including the latest version, when it was last seen, when tracking began, and the number of versions that have been seen.

4.6.3 Palo Alto Networks–MaaS360

Palo Alto Networks GlobalProtect VPN secures remote connections from mobile devices. MaaS360 offers specific configuration options for the GlobalProtect client, using certificate-based authentication to the GlobalProtect gateway and available for Android and iOS, that facilitate deployment of VPN clients and enabled VPN access. Section 4.5 presents details of the certificate enrollment process.

Two components of the Palo Alto Networks next-generation firewall compose the VPN architecture used in this example solution—a GlobalProtect portal and a GlobalProtect gateway. The portal provides the management functions for the VPN infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s). A GlobalProtect gateway provides security enforcement for network traffic. The GlobalProtect gateway in this example solution is configured to provide mobile device users with access to specific enterprise resources from the secure contexts after a successful authentication and authorization decision.

The VPN tunnel negotiation between the VPN endpoint/mobile device context and the VPN gateway has four steps: (1) The portal provides the client configuration, (2) a user logs into the system, (3) the agent automatically connects to the gateway and establishes a VPN tunnel, and (4) the security policy on the gateway enables access to internal and external applications.

For this example solution, a per-application VPN configuration is enforced on iOS and an always-on work profile VPN configuration on Android. This configuration forces the device to automatically establish a VPN connection to the GlobalProtect gateway whenever an application in the predefined list of applications runs on the device or when an application in the work profile is launched.

4.6.4 iOS and Android MDM Integration

Both iOS and Android integrate directly with MaaS360. iOS devices are enrolled into MaaS360 using User Enrollment, which is Apple's BYOD solution. User Enrollment creates a second persona on the device, which places the work data on a separate encrypted partition on the device. User Enrollment also requires managed user IDs, which are created in Apple Business Manager. This allows the enterprise to associate the work data with the managed Apple ID, while the user associates their personal data with their personal Apple ID.

Android devices are managed by Android Enterprise, which provides controls for both the device itself and the work profile. The work profile is a separated, isolated, and encrypted environment based on an SELinux user profile that stores all the enterprise applications and data, ensuring separation from personal applications and data.

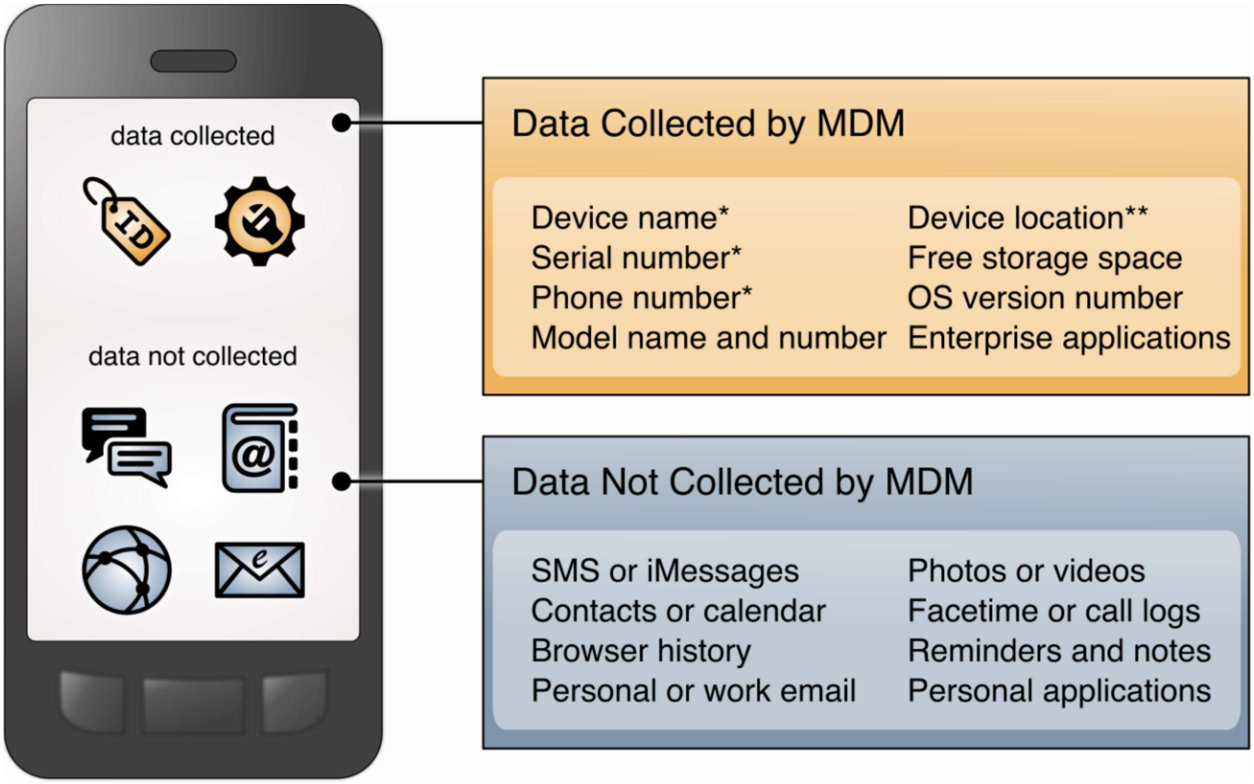
4.7 Privacy Settings: Mobile Device Data Processing

This section looks at components within the example architecture and the type of information an enterprise may access from an employee's personal mobile device through those components. Understanding the type of data an enterprise has access to can be helpful when understanding any privacy implications.

4.7.1 EMM: MaaS360

When a personal mobile device is connected to an EMM system, some data is collected and visible to the enterprise. While additional data can be collected (depending on how devices are enrolled), our example solution collects only the data shown in Figure 4-6 to help protect employee privacy. IBM provides documentation with more details on the information that MaaS360 collects and processes [29].

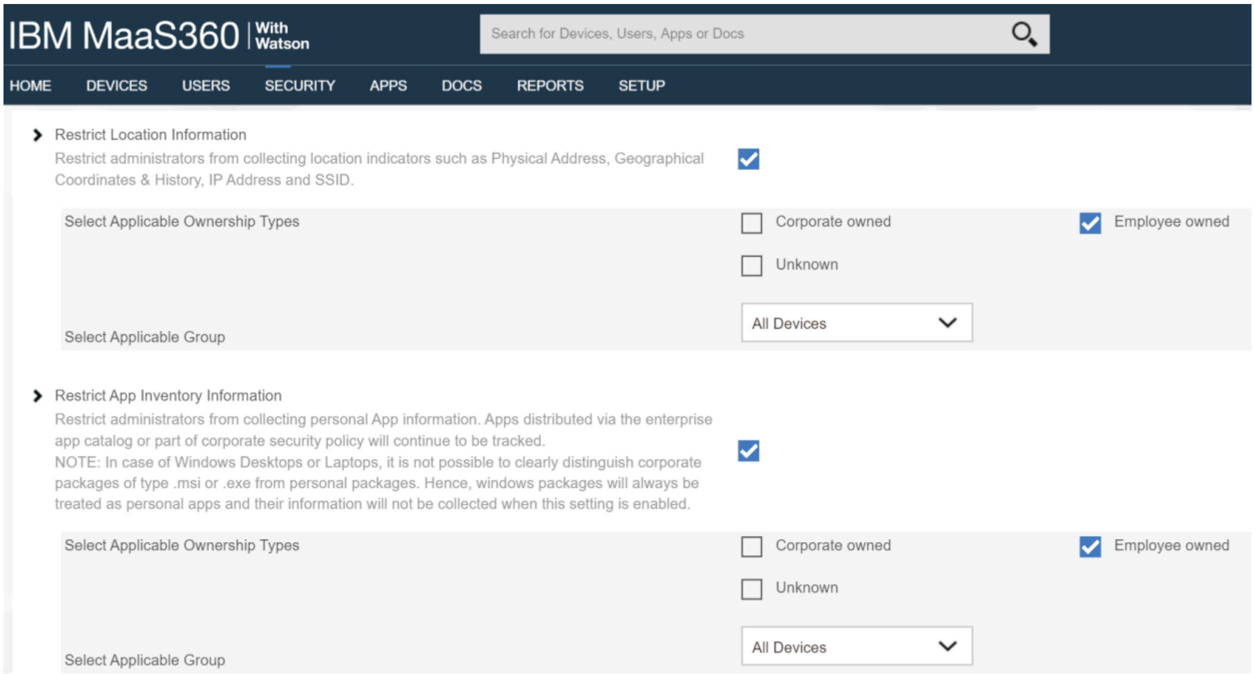
Figure 4-6 Data Collected by Example Solution Mobile Device Management



*: *Android only*
**: *With user consent*

As shown in Figure 4-7 below, administrators can restrict collection of location and/or application inventory information. When an administrator restricts location collection, the administrator cannot see any location information about devices. Similarly, when an administrator restricts application inventory information, MaaS360 will only collect applications that are distributed through the enterprise and, therefore, will not transmit any personal applications to third-party application-vetting services. Both privacy controls can be applied to specific device groups—for example, location collection can be disabled for personally owned devices. These privacy controls typically only apply to devices that are enrolled as fully managed devices. Devices enrolled using Android Enterprise (work profile mode) or Apple User Enrollment have controls in place that prevent the EMM from accessing application inventory and location collection regardless of privacy control configuration.

Figure 4-7 Example Solution Mobile Device Management Privacy Settings



Restrict Location Information ☑

Restrict administrators from collecting location indicators such as Physical Address, Geographical Coordinates & History, IP Address and SSID.

Select Applicable Ownership Types: □ Corporate owned ☑ Employee owned □ Unknown

Select Applicable Group: All Devices

Restrict App Inventory Information ☑

Restrict administrators from collecting personal App information. Apps distributed via the enterprise app catalog or part of corporate security policy will continue to be tracked.
NOTE: In case of Windows Desktops or Laptops, it is not possible to clearly distinguish corporate packages of type .msi or .exe from personal packages. Hence, windows packages will always be treated as personal apps and their information will not be collected when this setting is enabled.

Select Applicable Ownership Types: □ Corporate owned ☑ Employee owned □ Unknown

Select Applicable Group: All Devices

4.7.2 MTD: Zimperium

Zimperium provides configurable settings for what data is collected. In the list below, the top-level bullets can be disabled. Sub-bullets follow the enabled or disabled setting of the top-level. Zimperium also provides preset templates that can be utilized, including High, Medium, Low, and General Data Protection Regulation (GDPR). When using the Custom template type, the enterprise can configure exactly what data is collected. Data collected can include:

- device location (configurable granularity: street, city, county, none)
- device operating system
- device model
- device IP address
- device running processes (Android only)
- network connection details
    - SSID
    - BSSID
    - external IP address
    - gateway IP
    - gateway MAC
    - nearby Wi-Fi networks
    - ARP table

    - routing table
- carrier information
- attacker IP & MAC
- risky or unapproved sites
- phishing protection risky URLs
- application forensics
- application binaries (Android only)
- application inventory (Android only)

zIPS also collects some information that cannot be disabled. These items include:

- device root/jailbreak status
- USB debug mode status (Android only)
- developer mode status (Android only)
- 3rd party app store presence (Android only)
- mobile OS-specific vulnerability status (e.g., Stagefright)
- device encryption status (Android only)
- device protection status
- screen lock status

zIPS must collect certain data items to properly communicate with the zConsole. These items include:

- user credentials (email address, Zimperium-specific password)
- mobile network operator
- mobile network country code
- device operating system
- device push token
- hash of local z9 database
- time and name of threat detection when a threat occurs

4.7.3 Application Vetting: Kryptowire

Kryptowire collects certain pieces of device information through the MaaS360 REST API for analytics and application association purposes. The data collected includes:

- MDM device ID
- MDM device name
- MDM username
- last MDM sync date

- MDM enrollment data
- enterprise and non-app store installed applications

4.7.4 VPN: Palo Alto Networks

The Palo Alto Networks VPN uses information about the device as it establishes VPN connections. The data collected by the VPN includes information about:

- device name
- logon domain
- operating system
- app version
- mobile device network information to which the device is connected
- device root/jailbreak status

5 Security and Privacy Analysis

This section familiarizes the reader with:

- the example solution's assumptions and limitations
- results of the example solution's laboratory testing
- scenarios and findings that show the security and privacy characteristics addressed by the reference design
- the security and privacy control capabilities of the example solution

The purpose of the security and privacy characteristics evaluation is to understand the extent to which the project meets its objectives of demonstrating capabilities for securing mobile devices within an enterprise by deploying EMM, MTD, application vetting, secure boot/image authentication, and VPN services while also protecting the privacy of employees participating in the BYOD implementation.

5.1 Analysis Assumptions and Limitations

The security and privacy characteristics analysis has the following limitations:

- It is neither a comprehensive test of all security and privacy components nor a red-team exercise.
- It does not identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Build Testing

Test activities are provided to show how the example architecture addresses each TE and problematic data action. The NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into Practice*, provides insights into how an organization may determine its susceptibility to the threat before implementing the architecture detailed in this practice guide. Also, NIST SP 1800-22 Volume C, Appendix D shows the test activities that were used to demonstrate how this practice guide's example solution addresses TEs and privacy risks.

5.3 Scenarios and Findings

One aspect of the security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework and Privacy Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a subcategory. Using these subcategories as a basis for organizing the analysis allowed systematic consideration of how well the reference design supports the intended security and privacy characteristics.

This section of the publication provides findings for the security and privacy characteristics that the example solution was intended to support. These topics are described in the following subsections:

- development of the Cybersecurity Framework and NICE Framework mappings
- development of the Privacy Framework mappings
- TEs related to security and example solution architecture mitigations
- problematic data actions related to privacy and potential mitigations that organizations could employ

An example scenario that demonstrates how an organization may use NIST SP 1800-22 and other NIST tools to implement a BYOD use case is discussed more in the NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into Practice* of this practice guide.

5.3.1 Cybersecurity Framework, Privacy Framework, and NICE Framework Work Roles Mappings

As we installed, configured, and used the products in the architecture, we determined and documented the example solution's functions and their corresponding Cybersecurity Framework Subcategories, along with other guidance alignment.

This mapping will help users of this practice guide communicate with their organization's stakeholders regarding the security controls that the practice guide recommends for helping mitigate BYOD threats, and the workforce capabilities that the example solution will require.

The products, frameworks, security controls, and workforce mappings are in Appendix E (Cybersecurity Framework) and Appendix F (Privacy Framework).

Developing profiles utilizing frameworks such as the Cybersecurity and Privacy Frameworks can help with identifying whether or not an organization is meeting their security and privacy expectations.

5.3.2 Threat Events and Findings

As part of the findings, the TEs were mitigated in the example solution architecture using the concepts and technology shown in Table 5-1. Each TE was matched with functions that helped mitigate the risks posed by the TE.

Note: The TEE provided tamper-resistant processing environment capabilities that helped mitigate mobile device runtime and memory threats in the example solution. We do not show the Qualcomm TEE capability in the table because it is built into the phones used in this build.

Table 5-1 Threat Events and Findings Summary

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 1: Unauthorized access to sensitive information via a malicious or intrusive application practices	OS-level controls provide data separation between corporate and personal data.	EMM
Threat Event 2: Theft of credentials through a short message service or email phishing campaign	Utilized PAN-DB and URL filtering to block known malicious websites.	Firewall
Threat Event 3: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Alerted the user that their OS is non-compliant.	EMM MTD
Threat Event 4: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	Application vetting reports indicated if an application sent data without proper encryption.	Application vetting
Threat Event 5: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	The EMM enforces a required passcode. GlobalProtect requires periodic re-authentication.	EMM VPN
Threat Event 6: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	Application vetting reports indicated if an application used credentials improperly.	Application vetting
Threat Event 7: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	Devices that were not enrolled in the EMM system were not able to connect to the corporate VPN.	VPN

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 8: Loss of organizational data due to a lost or stolen device	Enforced passcode policies and device-wipe capabilities protected enterprise data.	EMM
Threat Event 9: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	Policies that enforce data loss prevention were pushed to devices.	EMM

The technologies in Table 5-1 are mapped to cybersecurity and privacy control mappings in Appendix E and Appendix F.

5.3.3 Privacy Risk Findings

The risk analysis found that five data actions in the build were potential privacy risks for individuals. We identified potential technical mitigations that an organization could use to lessen their impact, as shown below in Table 5-2. Organizations may also need to supplement these technical mitigations with supporting policies and procedures.

Table 5-2 Summary of Privacy Risks and Findings

Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
Privacy Risk 1: Wiping Activities on the Employee's Device May Inadvertently Delete the Employee's Personal Data **Related Problematic Data Action:** Unwarranted Restriction	In the event of a security issue, employee access to enterprise resources can be prevented by removing the device from EMM control or restricting device access to organizational systems instead of wiping the device. The EMM enables selective wiping of only corporate resources from the device. To further protect the employee's privacy, the ability to perform selective device information wipe activities can be limited to a small number of IT administrative staff.	EMM

Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
Privacy Risk 2: Organizational Collection of Device Data May Subject Employees to Feeling of Being Surveilled **Related Problematic Data Action:** Surveillance	The example solution restricts staff access to system capabilities that permit reviewing data about employees and their devices. Additionally, the example solution limits or disables collection of specific data elements (e.g., location data).	EMM
Privacy Risk 3: Data Collection and Transmission Between Integrated Security Products May Expose Employee Data **Related Problematic Data Action:** Unanticipated Revelation	The example solution: De-identifies employee data when it is not required to meet processing objectives. Encrypts data transmitted between parties. Limits or disables access to data. Limits or disables the collection of specific data elements.	EMM
Privacy Risk 4: Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations **Related Problematic Data Action:** Appropriation	The example solution provides a configurable pop-up banner to employees during device enrollment to provide notice regarding data processing practices in the BYOD solution, including what data is collected and what data is not collected. It can also provide information about where the employee can find more in-depth information regarding the organization's privacy policies and practices.	EMM
Privacy Risk 5: Unauthorized or Invasive Application Processing of Information Exposes Employee Data **Related Problematic Data Action:** Surveillance, Unanticipated revelation	EMM leverages OS-related separation between enterprise and employee personal data. The BYOD solution provides malware protection through Zimperium, which protects the device against advanced	EMM Zimperium

Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
	threats, while providing privacy protections.	

6 Example Scenario: Putting Guidance into Practice

To demonstrate how an organization may use NIST SP 1800-22 and other NIST tools to implement a BYOD use case, the NCCoE created the *Example Scenario: Putting Guidance into Practice* supplement document for this practice guide.

This example scenario shows how a fictional, small-to-mid-size organization (Great Seneca Accounting) can successfully navigate common enterprise BYOD security challenges.

In the narrative example, Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30 [8] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [9] to perform a privacy risk assessment. Appendix F and Appendix G of the Supplement of this practice guide, describe these risk assessments in more detail. These risk assessments produce two significant conclusions:

1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the controls discussed in the example solution are relevant to their environment.

2. The organization determines that it has a high-impact system, based on the impact guidance in NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* [30], and needs to implement more controls beyond those identified in NIST SP 1800-22 to support the additional system components in its own solution (e.g., underlying OS, the data center where the equipment will reside).

As part of their review of NIST FIPS 200, Great Seneca Accounting selects security and privacy controls from NIST SP 800-53 [31] for their BYOD architecture implementation. They then tailor the control baselines based on the needs identified through the priority subcategories in its cybersecurity and privacy Target Profiles.

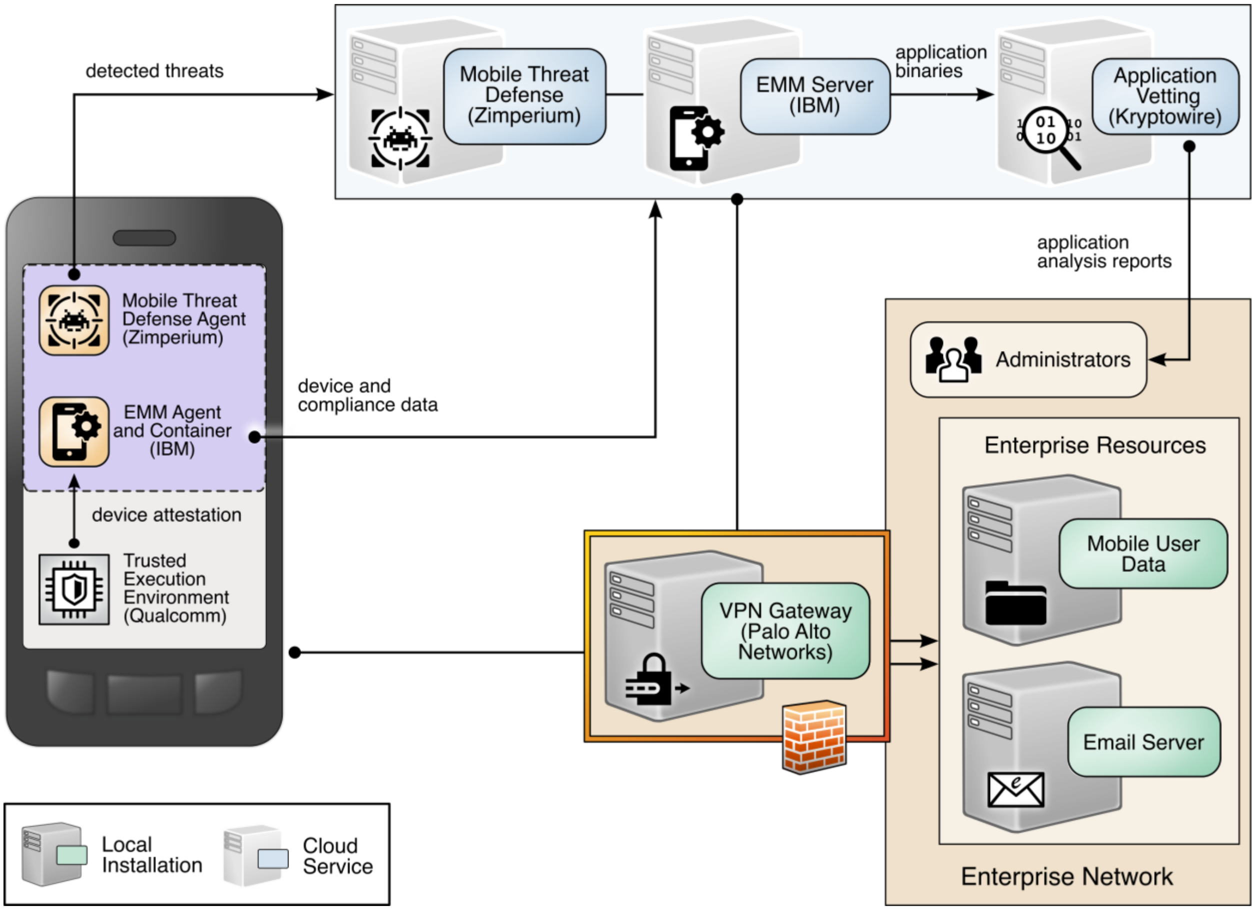
A detailed description of the implementation process that the fictional organization Great Seneca Accounting followed is provided in the NIST SP 1800-22 *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

7 Conclusion

This practice guide provides an explanation of mobile device security and privacy concepts and an example solution for organizations implementing a BYOD deployment. As shown in Figure 7-1, this example solution applied multiple mobile device security technologies. These included a cloud-based

EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities that support the example solution.

Figure 7-1 Example Solution Architecture


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Local Installation
Cloud Service
Enterprise Network

Our fictional Great Seneca Accounting organization example scenario contained in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide illustrates how the concepts and architecture from this guide may be applied by an organization. Great Seneca started with an IT infrastructure that lacked mobile device security architecture concepts. Great Seneca then employed multiple NIST cybersecurity and privacy risk management tools to understand the gaps in its architecture and the methods available today to enhance the security and privacy of its BYOD deployment.

In Volume C, this practice guide also includes a series of how-to guides, step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture, to help security engineers rapidly deploy and evaluate our example solution in their test environment.

The example solution uses standards-based, commercially available products that can be used by an organization interested in deploying a BYOD solution. The example solution provides recommendations for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted mobile security technologies. This practice guide provides an example solution that an organization may use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

8 Future Build Considerations

For future builds, the team is involved in projects that relate to mobile device security including Implementing a Zero Trust Architecture and Digital Identities – Mobile Driver's License (mDL).

Appendix A List of Acronyms

AD	Active Directory
API	Application Programming Interface
ATARC	Advanced Technology Academic Research Center
ATS	App Transport Security
BYOD	Bring Your Own Device
CIS	Center for Internet Security
CN	Common Name
COMSEC	Communications Security
COPE	Corporate-Owned Personally-Enabled
CRADA	Cooperative Research and Development Agreement
DHS	Department of Homeland Security
DN	Distinguished Name
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
ICS	Industrial Control System
IEC	International Electrotechnical Commission
iOS	iPhone Operating System
IP	Internet Protocol
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
mDL	Mobile Driver's License
MDM	Mobile Device Management
MSCT	Mobile Services Category Team
MTD	Mobile Threat Defense

NCCoE	National Cybersecurity Center of Excellence
NDES	Network Device Enrollment Service
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OS	Operating System
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
REST	Representational State Transfer
SCEP	Simple Certificate Enrollment Protocol
SMTP	Simple Mail Transport Protocol
SP	Special Publication
SSID	Service Set Identifier

Appendix B Glossary

Access Management Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [32].

Availability Ensure that users can access resources through remote access whenever needed [33].

Bring Your Own Device (BYOD) A non-organization-controlled telework client device [33].

Confidentiality Ensure that remote access communications and stored user data cannot be read by unauthorized parties [33].

Data Actions System operations that process personally identifiable information (PII) [34].

Disassociability Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [34].

Eavesdropping An attack in which an attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant [35] (definition located under eavesdropping attack).

Firewall Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [36].

Integrity Detect any intentional or unintentional changes to remote access communications that occur in transit [33].

Manageability Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [34].

Mobile Device A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [31].

Personally Identifiable Information (PII) Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [37] (adapted from Government Accountability Office Report 08-536).

Predictability Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system [34].

Privacy Event The occurrence or potential occurrence of problematic data actions [2].

Problematic Data Action A data action that could cause an adverse effect for individuals [2].

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [8].

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [8].

Appendix C References

[1] National Institute of Standards and Technology (NIST). NIST *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online]. Available: https://www.nist.gov/cyberframework.

[2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework.

[3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST Special Publication (SP) 800-181 rev. 1, NIST, Gaithersburg, Md., Nov. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

[5] NIST. Mobile Threat Catalogue. [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/.

[6] J. Franklin et al., *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST SP 800-124 Revision 2, NIST, Gaithersburg, Md., May. 2023. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/final.

[7] J. Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds,* NIST SP 1800-4, NIST, Gaithersburg, Md., Feb. 21, 2019. Available https://doi.org/10.6028/NIST.SP.1800-4.

[8] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments,* NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[9] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework/nist-pram.

[10] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[11] Open Web Application Security Project (OWASP). “OWASP Mobile Top 10,” [Online]. Available: https://owasp.org/www-project-mobile-top-10/.

[12] NIST. Privacy Engineering Program: Privacy Risk Assessment Methodology, Catalog of Problematic Data Actions and Problems. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[13] Qualcomm. “Mobile Security Solutions.” [Online]. Available: https://www.qualcomm.com/products/features/mobile-security-solutions.

[14] National Information Assurance Partnership (NIAP). U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 3.0. Nov. 21, 2016. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/ep_mdm_agent_v3.0.pdf.

[15] International Business Machines (IBM). About enterprise app wrapping. Aug. 09, 2022 last updated. [Online]. Available: https://www.ibm.com/docs/en/maas360?topic=overview-about-enterprise-app-wrapping.

[16] NIAP. U.S. Government Approved Protection Profile—Module for Virtual Private Network (VPN) Gateways 1.1. July 01, 2020. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=449&id=449.

[17] NIAP. U.S. Government Approved Protection Profile—collaborative Protection Profile for Network Devices Version 2.2e. Mar. 27, 2020. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=447&id=447.

[18] NIAP. Approved Protection Profiles. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[19] Qualcomm. “Qualcomm Secure Boot and Image Authentication Technical Overview.” [Online]. Available: https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview-v1-0.pdf.

[20] Google Android. Android Management API. [Online]. Available: https://developers.google.com/android/management.

[21] Apple Inc. “Preventing Insecure Network Connections.” [Online]. Available: https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

[22] Apple Inc. "Identifying the Source of Blocked Connections." [Online]. Available: https://developer.apple.com/documentation/security/preventing_insecure_network_connections/identifying_the_source_of_blocked_connections.

[23] Android.com. “Network security configuration.” Dec. 27, 2019. [Online]. Available: https://developer.android.com/training/articles/security-config.

[24] NowSecure.com. “A Security Analyst’s Guide to Network Security Configuration in Android P.” [Online]. Available: https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-to-network-security-configuration-in-android-p/.

[25] Apple Inc. “Overview: Managing Devices & Corporate Data on iOS.” July 2018. [Online]. Available: https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf.

[26] Google Android. “Build Android management solutions for enterprises.” [Online]. Available: https://developers.google.com/android/work.

[27] International Business Machines (IBM). “Web Services.” [Online]. Available: https://www.ibm.com/docs/en/maas360?topic=web-services.

[28] IBM. “IBM Community Public Wikis.” [Online]. Available: https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage.

[29] IBM. “MaaS360 Data Privacy Information.” [Online]. Available: https://www.ibm.com/support/pages/maas360-data-privacy-information

[30] NIST. *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available: https://csrc.nist.gov/publications/detail/fips/200/final.

[31] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53, NIST, Gaithersburg, Md., Jan. 2015. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[32] IDManagement.gov. “Federal Identity, Credential, and Access Management Architecture.” [Online]. Available: https://arch.idmanagement.gov/services/access/.

[33] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[34] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems,* NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[35] P. Grassi et al., *Digital Identity Guidelines,* NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[36] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* NIST SP 800-82 Revision 2, NIST, Gaithersburg, Md., May 2015. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[37] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[38] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE),* NIST SP 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available: https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment.

[39] NIST, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,* NIST SP 800-52 Revision 2, August 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final.

[40] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations (Final Public Draft),* NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[41] S. Frankel et al., *Guide to SSL VPNs,* NIST SP 800-113, NIST, Gaithersburg, Md., July 2008. Available: https://csrc.nist.gov/publications/detail/sp/800-113/final.

[42] M. Souppaya and K. Scarfone, *User's Guide to Telework and Bring Your Own Device (BYOD) Security,*, NIST SP 800-114 Revision 1, NIST, Gaithersburg, Md., July 2016. Available: https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final.

[43] M. Ogata et al., *Vetting the Security of Mobile Applications,* NIST SP 800-163 Revision 1, NIST, Gaithersburg, Md., Apr. 2019. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf.

[44] NIST, *Protecting Controlled Unclassified Information in Nonfederal SystemsI,* NIST SP 800-171 Revision 2, February 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[45] Center for Internet Security. Center for Internet Security home page. [Online]. Available: https://www.cisecurity.org/.

[46] Executive Office of the President, "Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," Aug. 23, 2012. Available: https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device.

[47] Federal CIO Council and Department of Homeland Security. *Mobile Security Reference Architecture Version 1.0.* May 23, 2013. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf.

[48] Digital Services Advisory Group and Federal Chief Information Officers Council. *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis.* Dec. 2012. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf.

[49] International Organization for Standardization. "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements." Oct. 2013. [Online]. Available: https://www.iso.org/standard/54534.html.

[50] "Mobile Computing Decision." [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf.

[51] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC). "Navigating the Future of Mobile Services." Oct. 2017. [Online]. Available: https://atarc.org/wp-content/uploads/2019/01/ATARC-MSCT-Report-Navigating-Future-of-Mobile-Services-2.pdf.

[52] Mobile Services Category Team (MSCT). "Device Procurement and Management Guidance." Nov. 2016. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance.

[53] Mobile Services Category Team (MSCT). “Mobile Device Management (MDM), MDM Working Group Document.” Aug. 2017. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf.

[54] Mobile Services Category Team (MSCT). “Mobile Services Roadmap (MSCT Strategic Approach).” Sept. 23, 2016. [Online]. Available: https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/.

[55] NIAP. U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0. Dec. 31, 2014. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf.

[56] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1,. June 16, 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417.

[57] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0. Apr. 25, 2019. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=428&id=428.

[58] NIAP. Product Compliant List. [Online]. Available: https://www.niap-ccevs.org/Product/.

[59] Office of Management and Budget, Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services, Aug. 4, 2016. Available: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_20.pdf.

[60] NIST. United States Government Configuration Baseline (in development). [Online]. Available: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline.

[61] Department of Homeland Security (DHS). “DHS S&T Study on Mobile Device Security.” Apr. 2017. [Online]. Available: https://www.dhs.gov/publication/csd-mobile-device-security-study.

[62] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*, Mar. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf.

[63] NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53, Revision 5 Crosswalk. [Online]. Available: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.

Appendix D Standards and Guidance

The following are references that informed the writing of this publication.

- National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) Version 1.1 [1]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2]
- NIST Mobile Threat Catalogue [5]
- NIST Risk Management Framework [4]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [7]
- NIST SP 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* [38]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [8]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [10]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [33]
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [39]
- NIST SP 800-53 Revision 4 (Final)*, Security and Privacy Controls for Information Systems and Organizations* [31]
- NIST SP 800-53 Revision 5 (Final), *Security and Privacy Controls for Information Systems and Organizations* [40]
- NIST SP 800-63-3, *Digital Identity Guidelines* [35]
- NIST SP 800-113, *Guide to SSL VPNs* [41]
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [42]
- NIST SP 800-124 Revision 2*, Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [43]
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [44]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017)* [3]
- NIST Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* [30]
- NIST Privacy Risk Assessment Methodology [9]
- Center for Internet Security [45]

- Executive Office of the President, Bring Your Own Device toolkit [46]
- Federal Chief Information Officers Council and Department of Homeland Security *Mobile Security Reference Architecture*, Version 1.0 [47]
- Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis* [48]
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, "Information technology – Security techniques – Information security management systems – Requirements" [49]
- Mobile Computing Decision example case study [50]
- MSCT ATARC, "Navigating the Future of Mobile Services," Working Group Document [51]
- MSCT, "Device Procurement and Management Guidance" [52]
- MSCT, "Mobile Device Management (MDM)," MDM Working Group Document [53]
- MSCT, "Mobile Services Roadmap, MSCT Strategic Approach" [54]
- National Information Assurance Partnership (NIAP), U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0 [55]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1 [56]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0 [57]
- NIAP, Product Compliant List [58]
- Office of Management and Budget, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* [59]
- United States Government Configuration Baseline [60]
- Department of Homeland Security (DHS), "DHS S&T Study on Mobile Device Security" [61]
- NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework* [62]

Appendix E Example Security Subcategory and Control Map

Using the developed risk information as input, the security characteristics of the example solution were identified. A security control map was developed documenting the example solution's capabilities with applicable Subcategories from the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1]; NIST Special Publication (SP) 800-53 Revision 5*, Security and Privacy Controls for Information Systems and Organizations* [40]; International Organization for Standardization (ISO); International Electrotechnical Commission (IEC) 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* [49]; the Center for Internet Security's (CIS) control set Version 6 [45]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

Table E-1 below identifies the security characteristic standards mapping for the products as they were used in the example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the mapping not be used as a reference for all of the security capabilities these products may be able to address.

Table E-1 Example Solution's Cybersecurity Standards and Best Practices Mapping

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Kryptowire Cloud Service	Application Vetting	**ID.RA-1:** Asset vulnerabilities are identified and documented.	**CA-2, CA-7, CA-8:** Security Assessment and Authorization **RA-3, RA-5:** Risk Assessment **SA-4:** Acquisition Process **SI-7:** Software, Firmware, and Information Integrity	**A.12.6.1:** Control of technical vulnerabilities **A.18.2.3:** Technical Compliance Review	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **SP-ARC-002:** Security Architect **OM-ANA-001:** Systems Security Analyst

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		ID.RA-3: Threats, both internal and external, are identified and documented.	**RA-3:** Risk Assessment **SI-7:** Software, Firmware, and Information Integrity **PM-12, PM-16:** Insider Threat Program	**6.1.2:** Information risk assessment process	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **OM-ANA-001:** Systems Security Analyst **OV-SPP-001:** Cyber Workforce Developer and Manager **OV-TEA-001:** Cyber Instructional Curriculum Developer **PR-VAM-001:** Vulnerability Assessment Analyst **PR-VAM-001:** Vulnerability Assessment Analyst

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		DE.CM-4: Malicious code is detected.	**SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses **CSC 12:** Boundary Defense	**PR-CIR-001:** Cyber Defense Incident Responder **PR-CDA-001:** Cyber Defense Analyst
		DE.CM-5: Unauthorized mobile code is detected.	**SC-18:** Mobile Code **SI-7:** Software, Firmware, and Information Integrity	**A.12.5.1:** Installation of Software on Operational Systems **A.12.6.2:** Restrictions on Software Installation	**CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses	**PR-CDA-001:** Cyber Defense Analyst **SP-DEV-002:** Secure Software Assessor

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Zimperium Console version vGA-4.23.1	Cloud service that complements the zIPS Agent	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**CM-8:** Information System Component Inventory **PM-5:** Information System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets	**CSC 1:** Inventory of Authorized and Unauthorized Devices	**OM-STS-001:** Technical Support Specialist **OM-NET-001:** Network Operations Specialist **OM-ADM-001:** System Administrator
zIPS agent Version 4.9.2 (iOS), 4.9.2 (Android)	Endpoint security for mobile device threats	**ID.AM-2:** Software platforms and applications within the organization are inventoried.	**CM-8:** Information System Component Inventory **PM-5:** Information System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets **A.12.5.1:** Installation of Software on Operational Systems	**CSC 2:** Inventory of Authorized and Unauthorized Software	**SP-DEV-002:** Secure Software Assessor **SP-DEV-001:** Software Developer **SP-TRD-001:** Research and Development Specialist

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		DE.CM-8: Vulnerability scans are performed.	**RA-5:** Vulnerability Monitoring and Scanning	**A.12.6.1:** Management of technical vulnerabilities	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 20:** Penetration Tests and Red Team Exercises	**PR-VAM-001:** Vulnerability Assessment Analyst **PR-INF-001:** Cyber Defense Infrastructure Support Specialist **PR-CDA-001:** Cyber Defense Analyst
		DE.AE-5: Incident alert thresholds are established.	**IR-4:** Incident Handling **IR-5:** Incident Monitoring **IR-8:** Incident Response Plan	**A.16.1.4:** Assessment of and decision on information security events	**CSC 6:** Maintenance, Monitoring, and Analysis of Audit Logs **CSC 19:** Incident Response and Management	**PR-CIR-001:** Cyber Defense Incident Responder **AN-TWA-001:** Threat/Warning Analyst

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		DE.CM-5: Unauthorized mobile code is detected.	**SC-18:** Mobile Code **SI-7:** Software, Firmware, and Information Integrity	**A.12.5.1:** Installation of Software on Operational Systems **A.12.6.2:** Restrictions on Software Installation	**CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses	**PR-CDA-001:** Cyber Defense Analyst **SP-DEV-002:** Secure Software Assessor
IBM MaaS360 Mobile Device Management (SaaS) Version 10.73	Enforces organizational mobile endpoint security policy	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**CM-8:** System Component Inventory **PM-5:** System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets	**CSC 1:** Inventory of Authorized and Unauthorized Devices	**OM-STS-001:** Technical Support Specialist **OM-NET-001:** Network Operations Specialist **OM-ADM-001:** System Administrator

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		ID.AM-2: Software platforms and applications within the organization are inventoried.	**CM-8:** System Component Inventory **PM-5:** System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets **A.12.5.1:** Installation of Software on Operational Systems	**CSC 2:** Inventory of Authorized and Unauthorized Software	**SP-DEV-002:** Secure Software Assessor **SP-DEV-001:** Software Developer **SP-TRD-001:** Research and Development Specialist

		PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	**AC-3:** Access Enforcement **IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11:** Identification and Authentication Family	**A.9.2.1:** User Registration and De-Registration **A.9.2.2:** User Access Provisioning **A.9.2.3:** Management of Privileged Access Rights **A.9.2.4:** Management of Secret Authentication Information of Users **A.9.2.6:** Removal or Adjustment of Access Rights **A.9.3.1:** Use of Secret Authentication Information **A.9.4.2:** Secure logon Procedures **A.9.4.3:** Password Management System	**CSC 1:** Inventory of Authorized and Unauthorized Devices **CSC 5:** Controlled Use of Administrative Privileges **CSC 15:** Wireless Access Control **CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OM-ADM-001:** System Administrator **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.AC-3: Remote access is managed.	**AC-1:** Access Control Policy and Procedures **AC-17:** Remote Access **AC-19:** Access Control for Mobile Devices **AC-20:** Use of External Systems **SC-15:** Collaborative Computing Devices and Applications	**A.6.2.1:** Mobile Device Policy **A.6.2.2:** Teleworking **A.11.2.6:** Security of equipment and assets off premises **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures	**CSC 12:** Boundary Defense	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**AC-1, AC-3:** Access Control Policy and Procedures **IA-2, IA-4, IA-5:** Identification and Authentication **PE-2:** Physical Access Authorizations	**A.7.1.1:** Screening **A.9.2.1:** User Registration and De-Registration	**CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		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).	**CM-8:** System Component Inventory **SA-10:** Developer Configuration Management	**A.12.1.2:** Change Management **A.12.5.1:** Installation of Software on Operational Systems **A.12.6.2:** Restrictions on Software Installation **A.14.2.2:** System Change Control Procedures **A.14.2.3:** Technical Review of Applications After Operating Platform Changes **A.14.2.4:** Restrictions on Changes to Software Packages	**CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers **CSC 9:** Limitation and Control of Network Ports, Protocols, and Services **CSC 11:** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**SP-ARC-002:** Security Architect **OV-SPP-002:** Cyber Policy and Strategy Planner **SP-SYS-001:** Information Systems Security Developer **OM-ADM-001:** System Administrator **PR-VAM-001:** Vulnerability Assessment Analyst

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)	Endpoint software that compliments IBM MaaS360 Mobile Device Management console–provides root/jailbreak detection and other functions	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**SC-16:** Transmission of Security and Privacy Attributes **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware **A.12.5.1:** Installation of Software on Operational Systems **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions **A.14.2.4:** Restrictions on Changes to Software Packages	**CSC 2:** Inventory of Authorized and Unauthorized Software **CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**OV-SPP-002:** Cyber Policy and Strategy Planner **SP-ARC-001:** Enterprise Architect

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Qualcomm (version is mobile device dependent)	Secure boot and image integrity	**PR.DS-1:** Data-at-rest is protected.	**SC-28:** Protection of Information at Rest	**A.8.2.3:** Handling of Assets	**CSC 13:** Data Protection **CSC 14:** Controlled Access Based on the Need to Know	**OV-SPP-002:** Cyber Policy and Strategy Planner **PR-INF-001:** Cyber Defense Infrastructure Support Specialist **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**SA-10(1):** Developer Configuration Management **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware **A.12.5.1:** Installation of Software on Operational Systems **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions **A.14.2.4:** Restrictions on Changes to Software Packages	**CSC 2:** Inventory of Authorized and Unauthorized Software **CSC 3:** Secure Configurations for Hardware and Software on Mobile	**OV-SPP-002:** Cyber Policy and Strategy Planner **PR-CDA-001:** Cyber Defense Analyst **SP-ARC-001:** Enterprise Architect

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	**SA-10:** Developer Configuration Management **SI-7:** Software, Firmware, and Information Integrity	**A.11.2.4:** Equipment maintenance	Not applicable	**OM-ADM-001:** System Administrator **SP-ARC-001:**Enterprise Architect
		DE.CM-4: Malicious code is detected.	**SC-35:** External Malicious Code Identification **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses **CSC 12:** Boundary Defense	**PR-CDA-001:** Cyber Defense Analyst **PR-INF-001:** Cyber Defense Infrastructure Support Specialist

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Palo Alto Networks PA-220	Enforces network security policy for remote devices	**PR.AC-3:** Remote access is managed.	**AC-1, AC-3:** Access Control Policy and Procedures **AC-19:** Access Control for Mobile Devices	**A.6.2.1:** Mobile Device Policy **A.6.2.2:** Teleworking **A.11.2.6:** Security of equipment and assets off-premises **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures	**CSC 12:** Boundary Defense	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	**AC-3:** Access Enforcement **SC-7:** Boundary Protection	**A.13.1.1:** Network Controls **A.13.1.3:** Segregation in Networks **A.13.2.1:** Information Transfer Policies and Procedures **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions	**CSC 9:** Limitation and Control of Network Ports, Protocols, and Services **CSC 14:** Controlled Access Based on the Need to Know **CSC 15:** Wireless Access Control **CSC 18:** Application Software Security	**PR-CDA-001:** Cyber Defense Analyst **OM-ADM-001:** System Administrator

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**AC-3:** Access Enforcement **IA-2, IA-4, IA-5, IA-8:** Identification and Authentication (Organizational Users) **PE-2:** Physical Access Authorizations **PS-3:** Personnel Screening	**A.7.1.1:** Screening **A.9.2.1:** User Registration and De-Registration	**CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.DS-2: Data-in-transit is protected.	**AC-17(2):** Protection of Confidentiality and Integrity Using Encryption **SC-8:** Transmission Confidentiality and Integrity	**A.8.2.3:** Handling of Assets **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures **A.13.2.3:** Electronic Messaging **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions	**CSC 13:** Data Protection **CSC 14:** Controlled Access Based on the Need to Know	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager

Specific product used	Function	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.PT-4: Communications and control networks are protected.	**AC-3, AC-4, AC-17, AC-18:** Access Control Family **CP-2:** Contingency Plan **SC-7, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-38, SC-39, SC-40, SC-41, SC-43:** System and Communications Protection Family	**A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures **A.14.1.3:** Protecting Application Services Transactions	**CSC 8:** Malware Defenses **CSC 12:** Boundary Defense **CSC 15:** Wireless Access Control	**PR-INF-001:** Cyber Defense Infrastructure Support Specialist **OV-SPP-002:** Cyber Policy and Strategy Planner **PR-CDA-001:** Cyber Defense Analyst

Appendix F Example Privacy Subcategory and Control Map

Using the developed privacy information as input, we identified the privacy characteristics of the example solution. We developed a privacy control map documenting the example solution's capabilities with applicable Functions, Categories, and Subcategories from the National Institute of Standards and Technology *(NIST) Privacy Framework* [2]; and NIST SP 800-53 Revision 5 [40]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

The table that follows maps component functions in the build to the related Subcategories in the NIST Privacy Framework as well as to controls in the NIST SP 800-53, Revision 5 controls catalog. Each column maps independently to the build component's functions and, given the specific capabilities of this mobile device security solution, may differ from other NIST-provided mappings for the Privacy Framework and SP 800-53 revision. For example, build functions may provide additional capabilities beyond what is contemplated by a Privacy Framework Subcategory or that are implemented by additional controls beyond those that NIST identified as an informative reference for the Subcategory.

The table also identifies the privacy characteristic mapping for the products as they were used in the example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the mapping not be used as a reference for all the privacy capabilities these products may be able to address. The comprehensive mapping of the NIST Privacy Framework to NIST SP 800-53, Revision 5 controls can be found on the NIST Privacy Framework Resource Repository website, in the event an organization's mobile device security solution is different to determine other controls that are appropriate for their environment [63].

Table F-1 Example Solution's Privacy Standards and Best Practices Mapping

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
IBM MaaS360	MaaS360 can be used to capture an inventory of the types and number of devices deployed and shows the administrators what data is collected from each enrolled device.	**ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	**CM-12:** Information Location **CM-13:** Data Action Mapping **PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **PT-3:** Personally Identifiable Information Processing Purposes **RA-3:** Risk Assessment **RA-8:** Privacy Impact Assessment	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **OV-TEA-001:** Cyber Instructional Curriculum Developer
	Administrators can view data elements in the administration portal. Users can see collected data within the MaaS360 application on their device. Users are advised about data collection practices in a window during enrollment. Data can be edited and deleted from within the	**CT.DM-P1:** Data elements can be accessed for review.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-3(14):** Access Enforcement | Individual Access **PM-21:** Accounting of Disclosures	**OM-DTA-002:** Data Analyst
		CT.DM-P3: Data elements can be accessed for alteration.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-3(14):** Access Enforcement | Individual Access **PM-21:** Accounting of Disclosures **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	administration console.	**CT.DM-P4:** Data elements can be accessed for deletion.	**AC-2:** Account Management **AC-3:** Access Enforcement **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst
		CT.DM-P5: Data are destroyed according to policy.	**MP-6**: Media Sanitization **SA-8(33):** Security and Privacy Engineering Principles | Minimization **SI-18:** Personally Identifiable Information Quality Operations **SR-12:** Component Disposal	**OM-DTA-002:** Data Analyst
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	**CM-6:** Configuration Settings **SA-8(33):** Minimization **SC-42(5):** Collection Minimization **SI-12(1):** Information Management and Retention | Limit Personally Identifiable Information Elements	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager
	Devices may be backed up to the cloud.	**PR.PO-P3:** Backups of information are conducted, maintained, and tested.	**CP-4:** Contingency Plan Testing **CP-6:** Alternate Storage Site **CP-9:** System Backup	**OM-ADM-001:** System Administrator

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	Devices are issued identity certificates via on-premises certificate infrastructure.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**IA-2:** Identification and Authentication (Organizational Users) **IA-3:** Device Identification and Authentication **IA-4:** Identifier Management **IA-4(4):** Identifier Management | Identifier User Status	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
	MaaS360 enforces a device personal identification number for access.	**PR.AC-P2:** Physical access to data and devices is managed.	**PE-2:** Physical Access Authorizations **PE-3:** Physical Access Control **PE-3(1):** System Access **PE-4:** Access Control for Transmission **PE-5:** Access Control for Output Devices **PE-6:** Monitoring Physical Access **PE-18:** Location of System Components **PE-20:** Asset Monitoring and Tracking	**OM-DTA-001:** Database Administrator **OM-DTA-002:** Data Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		PR.DS-P1: Data-at-rest is protected.	**MP-2:** Media Access **MP-4:** Media Storage **PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**OM-DTA-001:** Database Administrator **OM-DTA-002:** Data Analyst
	Data flowing between the device and MaaS360 is encrypted with Transport Layer Security.	**PR.DS-P2:** Data-in-transit is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity	**PR-CIR-001:** Cyber Defense Incident Responder
	Restrictions are used that prevent data flow between enterprise and personal applications.	**PR.DS-P5:** Protections against data leaks are implemented.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **AC-4:** Information Flow Enforcement	**PR-CIR-001:** Cyber Defense Incident Responder
	Devices that are jailbroken or otherwise modified beyond original equipment manufacturer status can be detected.	**PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SI-7:** Software, Firmware, and Information Integrity **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
Zimperium	Zimperium checks the device for unauthorized modifications.	**PR.DS-P1:** Data-at-rest is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.DS-P2: Data-in-transit is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity **SC-11:** Trusted Path	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SC-16:** Transmission of Security Attributes **SI-7:** Boundary Protection **SI-10:** Network Disconnect **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
Kryptowire (now known as Quokka)	Kryptowire can identify applications that do not use best practices, such as lack of encryption or hardcoded credentials.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	**AC-8:** System Use Notification	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		CM.AW-P3: System/ product/ service design enables data processing visibility.	**PL-8:** Security and Privacy Architecture **PM-5(1):** System Inventory | Inventory of Personally Identifiable Information	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure.	**AC-16:** Security and Privacy Attributes **SC-16:** Transmission of Security Attributes	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.DS-P1: Data-at-rest is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		PR.DS-P2: Data-in-transit is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity **SC-11:** Trusted Path	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
Palo Alto Networks PA-220	Provides firewall and virtual private network capabilities.	**PR.DS-P2:** Data-in-transit is protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity **SC-11:** Trusted Path	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-5:** Separation of Duties **AC-6:** Least Privilege **AC-24:** Access Control Decisions	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**AC-4:** Information Flow Enforcement **AC-10:** Access Control **SC-7:** Boundary Protection **SC-10:** Network Disconnect	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		PR.PT-P3: Communications and control networks are protected.	**AC-12:** Session Termination **AC-17:** Remote Access **AC-18**: Wireless Access **SC-5:** Denial of Service Protection **SC-7:** Boundary Protection **SC-10:** Network Disconnect **SC-11:** Trusted Path **SC-21:** Secure Name/Address Resolution Service (Recursive or Caching Resolver) **SC-23:** Session Authenticity	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **PR-CDA-001:** Cyber Defense Analyst
Qualcomm	The trusted execution environment provides data confidentiality and integrity.	**PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SC-16:** Transmission of Security and Privacy Attributes **SI-7:** Software, Firmware, and Information Integrity **SI-10:** Information Input Validation **SI-18:** Personally Identifiable Information Quality Operations	**PR-INF-001:** Cyber Defense Infrastructure Support Specialist **OM-ANA-001:** Systems Security Analyst