NIST SPECIAL PUBLICATION 1800-31B

Improving Enterprise Patching for General IT Systems:

Utilizing Existing Tools and Performing Processes in Better Ways

Volume B:
Security Risks and Capabilities

Tyler Diamond*
Alper Kerman
Murugiah Souppaya
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brian Johnson
Chris Peloquin
Vanessa Ruffin
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

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

FINAL

April 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-31

The draft publication is available free of charge from
https://www.nccoe.nist.gov/publications/practice-guide/nist-sp-1800-31-improving-enterprise-patching-general-it-systems-draft

DISCLAIMER

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

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

National Institute of Standards and Technology Special Publication 1800-31B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-31B, 49 pages, (April 2022), 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 cyberhygiene@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, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Patching is the act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities. Despite widespread recognition that patching is effective and attackers regularly exploit unpatched software, many organizations cannot or do not adequately patch. There are myriad reasons why, not the least of which are that it's resource-intensive and that the act of patching can reduce system and service availability. Also, many organizations struggle to prioritize patches, test patches before deployment, and adhere to policies for how quickly patches are applied in different situations. To address these challenges, the NCCoE collaborated with cybersecurity technology providers to develop an example

solution that addresses these challenges. This NIST Cybersecurity Practice Guide explains how tools can be used to implement the patching and inventory capabilities organizations need to handle both routine and emergency patching situations, as well as implement isolation methods or other emergency mitigations as alternatives to patching. It also explains recommended security practices for patch management systems themselves.

KEYWORDS

cyber hygiene; enterprise patch management; firmware; patch; patch management; software; update; upgrade; vulnerability management

ACKNOWLEDGMENTS

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

Name	Organization
Peter Romness	Cisco
Matthew Hyatt	Cisco
John Loucaides	Eclypsium
Travis Raines	Eclypsium
Timothy Jones	Forescout
Tom May	Forescout
Michael Correa	Forescout
Jeffrey Ward	IBM MaaS360 with Watson
Joseph Linehan	IBM MaaS360 with Watson
Cesare Coscia	IBM MaaS360 with Watson
Jim Doran	IBM Research Team
Shripad Nadgowda	IBM Research Team

Name	Organization
Victoria Mosby	Lookout
Tim LeMaster	Lookout
Dan Menicucci	Microsoft
Steve Rachui	Microsoft
Parisa Grayeli	The MITRE Corporation
Yemi Fashina	The MITRE Corporation
Nedu Irrechukwu	The MITRE Corporation
Joshua Klosterman	The MITRE Corporation
Allen Tan	The MITRE Corporation
Josh Moll	Tenable
Chris Jensen	Tenable
Jeremiah Stallcup	Tenable
John Carty	VMware
Kevin Hansen	VMware
Rob Robertson	VMware
Rob Hilberding	VMware
Brian Williams	VMware

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
Cisco	Cisco Firepower Threat Defense (FTD) Cisco Identity Services Engine (ISE)
Eclypsium	Eclypsium Administration and Analytics Service
Forescout	Forescout Platform
IBM	IBM Code Risk Analyzer IBM MaaS360 with Watson
Lookout	Lookout Mobile Endpoint Security
Microsoft	Microsoft Endpoint Configuration Manager
Tenable	Nessus Tenable.io Tenable.sc
VMware	VMware vRealize Automation SaltStack Config

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 Tables

1 Summary

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) recognizes the challenges that organizations face in keeping software up to date with patches. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Patches can also add new features, including security capabilities. Sometimes there are alternatives to patches, such as temporary mitigations involving software or security control reconfiguration before patches are ready, but these mitigations are not permanent fixes and they may impact functionality.

The NCCoE developed the Critical Cybersecurity Hygiene: Patching the Enterprise (Patching) project to provide approaches for improving enterprise patching practices for general information technology (IT) systems. The aim is to help organizations balance security with mission impact and business objectives.

This project utilizes commercial tools to aid with functions that include asset discovery characterization and prioritization, and patch implementation tracking and verification. It includes actionable and prescriptive guidance on establishing policies and processes for the entire patching lifecycle. This volume explains why we built the example solution to address patching challenges, including the risk analysis we performed and the security capabilities that the example solution provides.

1.1 Challenge

There are a few root causes for many data breaches, malware infections such as ransomware, and other security incidents, and known—but unpatched—vulnerabilities in software are one of them. Implementing a few security hygiene practices, such as patching, can address those root causes. *Patching* is the act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities. Patching can prevent many incidents from occurring by minimizing the attack surface and lower the potential impact of incidents that occur. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause.

Unfortunately, security hygiene is easier said than done. Despite widespread recognition that (a) patching is effective and (b) attackers regularly exploit unpatched software, many organizations cannot or do not adequately patch. There are myriad reasons why, not the least of which are that it is resource-intensive and that the act of patching is perceived to reduce system and service availability. However, delaying patch deployment gives attackers a larger window of opportunity to take advantage of the exposure. Many organizations struggle to inventory their assets, prioritize patches, have defined and consistent processes and procedures for deployment, and adhere to policies and metrics for how quickly patches are applied in different situations. Also, deploying enterprise patch management tools that

operate with privileged access within an enterprise can itself create additional security risks for an organization if the tools are not secured properly.

1.2 Solution

To address these challenges, the NCCoE collaborated with cybersecurity technology providers to develop an example solution. It demonstrates how tools can be used to 1) implement the inventory and patching capabilities organizations need to handle both routine and emergency patching situations, as well as 2) implement temporary mitigations, isolation methods, or other alternatives to patching. The solution also demonstrates recommended security practices for protecting the patch management systems themselves against threats.

This draft covers both phases of the example solution, which involves patching, updating, and configuring two types of general IT assets. Phase 1 focuses on desktop and laptop computers and on-premises servers, and phase 2 adds mobile devices and containers.

The NCCoE has also created a companion publication, NIST Special Publication (SP) 800-40 Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. It complements the implementation focus of this guide by recommending creation of an enterprise strategy to simplify and operationalize patching while also reducing risk.

1.3 Benefits

The demonstrated approach offers several benefits to organizations that implement it, including the following:

- Vulnerabilities in the organization's IT systems that are susceptible to cyber attacks are addressed more quickly, which reduces risk and lowers the likelihood of an incident occurring.
- Increased automation provides a traceable and repeatable process and leads to a decrease in hours worked by the organization's security administrators, system administrations, and others who have patching responsibilities.
- It improves compliance with laws, regulations, mandates, local organization policy, and other requirements to keep the organization's software patched.
- The practices it demonstrates can play an important role as your organization embarks on a journey to zero trust.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information they need to replicate the proposed approach for improving enterprise

patching practices for general IT systems. This design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-31A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving the challenge
- NIST SP 1800-31B: *Security Risks and Capabilities* – why we built the example implementation, including the risk analysis performed and the security capabilities provided by the implementation **(you are here)**
- NIST SP 1800-31C: *How-To Guides* – what we built, with instructions for building the example implementation, including all the details that would allow you to replicate all or parts of this project

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-31A*, which describes the following topics:

- challenges that enterprises face in mitigating risk from software vulnerabilities
- example solution built at the NCCoE
- benefits of adopting the example solution

Business decision makers can also use *NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*.

Technology or security 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 1800-31B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5.1, Threats, Vulnerabilities, and Risks, provides a description of the risk analysis we performed.
- Section 3.5.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-31A*, with your leadership team members to help them understand the importance of adopting standards-based, automated patch management. Also, *NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* may be helpful to you and your leadership team.

IT professionals who may be interested in implementing an approach similar to ours will find the entire practice guide useful. In particular, the How-To portion of the guide, *NIST SP 1800-31C* could be used to replicate all or parts of the build created in our lab. Furthermore, the How-To portion of the guide

provides specific product installation, configuration, and integration instructions for implementing the example solution. We have omitted the general installation and configuration steps outlined in manufacturers' product documentation since they are typically made available by manufacturers. Instead, we focused on describing how we incorporated the products together in our environment to create the example solution.

This guide assumes that the reader of this document is a seasoned IT professional with experience in implementing security solutions within an enterprise setting. 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 an automated enterprise patch management system. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and recommended practices. Section 4.2, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this example solution.

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 cyberhygiene@nist.gov.

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`**

Typeface/Symbol	Meaning	Example
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

The NCCoE issued an open invitation to technology providers to participate in demonstrating how organizations can use technologies to improve enterprise patch management for their general IT assets. Cooperative Research and Development Agreements (CRADAs) were established with qualified respondents, and a build team was assembled. The team fleshed out the initial architecture, and the collaborators' components were composed into an example implementation, i.e., build. The build team documented the architecture and design of the build. As the build progressed, the team documented the steps taken to install and configure each component of the build.

Finally, the team verified that the build provided the desired capabilities. This included conducting a risk assessment and a security characteristic analysis, then documenting the results, including mapping the security contributions of the demonstrated approach to the *Framework for improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), NIST SP 800-53, the *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028*, and other relevant standards and guidelines.

3.1 Audience

This guide is intended for chief information officers (CIOs), chief information security officers (CISOs), cybersecurity directors and managers, and others who are responsible for managing organizational risk related to patch management. It also contains information of use for security engineers and architects, system administrators, security operations personnel, and others who are involved in enterprise patch management.

3.2 Scope

This project only covers general IT systems: desktops/laptops, servers, virtual machines and containers, and mobile devices running current software. There are additional challenges with patching legacy IT systems, as well as industrial control systems (ICS), Internet of Things (IoT) devices, and other technologies stemming from operational technology (OT), so they will not be covered in this project.

All aspects of security hygiene other than those related to patching are out of the scope of this project.

3.3 Assumptions

This project is guided by the following assumptions:

- An IT endpoint for an enterprise would have firmware, operating system(s), and application(s) to be patched. The endpoint may be in a fixed location within the organization's own facilities or in a fixed location at a third-party facility (e.g., a data center), or it may be intended for use in multiple locations, such as a laptop used at the office and for telework. The proposed approach for improving enterprise patching practices would have to account for all these possibilities.
- Problems sometimes occur with patches, such as a failure during installation, a patch that cannot take effect until the endpoint is rebooted, or a patch that is uninstalled because of operational concerns or because an attacker rolled it back in order to have an entry point to the system. This project follows a "verify everything and trust nothing" philosophy that does not assume installing a patch automatically means the patch is successfully and permanently applied.
- There are no standard protocols, formats, etc. for patch management, including patch distribution, integrity verification, installation, and installation verification. It is also highly unlikely for a single patch management system to be able to handle all patch management responsibilities for all software on IT endpoints. For example, some applications may handle patching themselves and not be capable of integrating with a patch management system for patch acquisition and installation.

3.4 Scenarios

This project addresses all the scenarios described below.

3.4.1 Scenario 0: Asset identification and assessment

This scenario identifies the assets and classifies them based on vulnerability impact levels to prioritize the order of remediation. It leverages tools to discover assets across the enterprise and the cloud and to enumerate their firmware, operating systems (OS), and applications. Knowing which software and software versions are in use and predetermining remediation priorities are critically important to all other patching processes. Without accurate, up-to-date, and comprehensive information, an organization will have difficulties effectively and efficiently performing patching processes, thus increasing risk. While many enterprises have constant asset attrition, it is important to have full and accurate inventory of critical assets and the best possible inventory for the full enterprise.

3.4.2 Scenario 1: Routine patching

This is the standard procedure for patches that are on a regular release cycle and haven't been elevated to an active emergency status (see Scenario 3). Routine patching includes endpoint firmware, OS, and applications, and server OS and applications hosted on-premises or in the cloud (e.g., Infrastructure as a

Service). Most patching falls under this scenario or Scenario 2. However, because routine patching does not have the urgency of emergency patching, and routine patch installation can interrupt operations (e.g., device reboots), it is often postponed and otherwise neglected. This provides many additional windows of opportunity for attackers.

3.4.3 Scenario 2: Routine patching with cloud delivery model

This is the standard procedure for patches that are delivered through a cloud delivery model, such as a "Windows as a Service (WaaS)" model with Windows operating systems, Apple Software Update, and mobile device software updates for Android and iOS devices provided by device manufacturers or mobile operators. This scenario is similar in importance to Scenario 1, Routine Patching. However, organizations may not be as accustomed to cloud-delivered patches (which are frequently cumulative for the whole system vs. discrete patches), so this scenario is somewhat more likely to be overlooked by organizations, which increases risk.

3.4.4 Scenario 3: Emergency patching

This is the emergency procedure to address active patching emergencies in a crisis situation, such as extreme severity vulnerabilities like the Server Message Block (SMB) vulnerability detailed in MS17-010, as well as vulnerabilities that are being actively exploited in the wild. The scope of targets is the same as Scenario 1. Emergency patching needs to be handled as efficiently as possible to prevent imminent exploitation of vulnerable devices. Key characteristics include identifying vulnerable assets, triaging and applying patches based on a priority list, and tracking and monitoring the state of those assets.

3.4.5 Scenario 4: Emergency mitigation (and backout if needed)

This is the emergency procedure in a crisis situation to temporarily mitigate risk for vulnerabilities prior to a vendor releasing a patch. It is typically required when the vulnerability is being actively exploited in the wild. The mitigation can vary and may or may not need to be rolled back afterward. The scope of targets is the same as Scenario 1. Organizations need to be prepared to quickly implement a wide variety of emergency mitigations to protect vulnerable devices. Without processes, procedures, and tools in place to implement emergency mitigations, too much time may be lost and vulnerable devices may be compromised before mitigations are in place. This may require disabling system functionality, having automated mechanisms to apply these changes, and having capabilities to revert back these changes when a permanent and approved patch is released.

3.4.6 Scenario 5: Isolation of unpatchable assets

This is the reference architecture and implementation of isolation methods to mitigate the risk of systems which cannot be easily patched. This is typically required if routine patching is not able to accommodate these systems within a reasonable timeframe (usually X days or less). Most systems in this scope are legacy unsupported systems or systems with very high operational uptime requirements.

Isolation is a form of mitigation that can be highly effective at stopping threats against vulnerable devices. Organizations need to be prepared to implement isolation methods when needed and to undo the isolation at the appropriate time to restore regular device access and functionality.

3.4.7 Scenario 6: Patch management system security (or other system with administrative privileged access)

This is a reference architecture and implementation of recommended security practices for systems like patch management systems which have administrative privileged access over many other systems. This includes practices like least privilege, privileged access workstations, and software updates.

3.5 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. Also, the NIST Cybersecurity Framework and NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* informed our risk assessment and subsequent recommendations from which we developed the security characteristics of the build and this guide.

3.5.1 Threats, Vulnerabilities, and Risks

The objective of this project is to demonstrate example solutions for each of the scenarios described in Section 3.4. Scenarios 0 through 5 collectively address improving the mitigation of software vulnerabilities in small to large IT enterprises for general IT assets. The last scenario, Scenario 6 (see Section 3.4.7) focuses on the security of the patch management technologies themselves. Scenario 6 has a different set of threats, vulnerabilities, and risks than the other scenarios, so it is discussed separately in this section. See NIST SP 1800-31 Volume C for information on which technologies we used to demonstrate each of the scenarios.

Scenarios 0 through 5

Collectively, the objective of Scenarios 0 through 5 is to ensure that software vulnerabilities are mitigated, either through patching or by using additional security controls, for firmware, operating systems, applications, and any other forms of software. The pertinent threats encompass the enormous range of attackers and attacks that target software vulnerabilities. Major risks can be grouped into three categories:

- **Vulnerabilities aren't mitigated, leaving them susceptible to compromise.** Potential causes of this include organizations being unaware of vulnerabilities or vulnerable assets, patching being delayed because of limited resources, users declining to install patches or reboot devices in order for patches to take effect, and organizations choosing not to implement isolation techniques or other mitigations to protect unpatchable assets.
- **Installing patches causes unintended side effects.** Examples include breaking the patched software or other software on the asset, inadvertently altering configuration settings to weaken security, adding software functionality without adequately securing that functionality, and disrupting interoperability with other software or assets.
- **Patch integrity is compromised.** A patch's integrity could be compromised at several places in the path from vendor to asset. Examples include the software vendor itself being compromised, the organization downloading patches from an unauthorized source, patches being tampered with while in transit to the organization, and patches being altered in storage at the organization.

Scenario 6

The objective of Scenario 6 is to protect the example solution itself from compromise. To be effective, the example solution requires administrative privileged access for many assets, so this makes it an attractive target for attackers. The example solution also holds sensitive information regarding what computing assets the organization has and what vulnerabilities each asset has, so safeguarding this information from attackers is important. Vulnerabilities that the example solution might have include software vulnerabilities in its own components, misconfigurations, and security design errors, such as not encrypting its network communications.

3.5.2 Security Control Map

Table 3-1 provides a security mapping for Scenarios 0 through 5. It maps the characteristics of the commercial products comprising the example solution (as detailed in Table 4-1) to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and NIST SP 800-53 Revision 5. This exercise is meant to demonstrate the real-world applicability of standards and recommended practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 3-1: Mapping Security Characteristics of the Example Solution for Scenarios 0-5

Cybersecurity Framework Category	Cybersecurity Framework Subcategory	SP 800-53 Revision 5 Controls
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CM-8**, System Component Inventory
	ID.AM-2: Software platforms and applications within the organization are inventoried	**CM-8**, System Component Inventory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**AC-3**, Access Enforcement
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**AC-3**, Access Enforcement
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	**SI-7**, Software, Firmware, and Information Integrity

Cybersecurity Framework Category	Cybersecurity Framework Subcategory	SP 800-53 Revision 5 Controls
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-3:** Configuration change control processes are in place	**CM-3**, Configuration Change Control
	PR.IP-12: A vulnerability management plan is developed and implemented	**RA-3**, Risk Assessment **RA-5**, Vulnerability Monitoring and Scanning **RA-7**, Risk Response **SI-2**, Flaw Remediation
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**AU-6**, Audit Record Review, Analysis, and Reporting
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CA-7,** Continuous Monitoring
	DE.CM-8: Vulnerability scans are performed	**RA-3**, Risk Assessment **SI-4**, System Monitoring

Table 3-2 provides a security mapping for Scenario 6 for the example solution. Although it has the same format as Table 3-1, the two tables have different functions. Table 3-1 lists the Cybersecurity Framework Subcategories and SP 800-53 Revision 5 security controls that the example solution supports. Table 3-2 lists the Cybersecurity Framework Subcategories and SP 800-53 Revision 5 security controls that are needed to support the example solution—to mitigate the risks of the solution itself.

Table 3-2: Mapping Security Characteristics of the Example Solution for Scenario 6

Cybersecurity Framework Category	Cybersecurity Framework Subcategory	SP 800-53 Revision 5 Controls
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**AC-3**, Access Enforcement **AC-5**, Separation of Duties **AC-6**, Least Privilege
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**AC-2**, Account Management **IA-2**, Identification and Authentication (Organizational Users) **IA-3**, Device Identification and Authentication **IA-4**, Identifier Management **IA-5**, Authenticator Management **IA-9**, Service Identification and Authentication
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**SC-28**, Protection of Information at Rest
	PR.DS-2: Data-in-transit is protected	**SC-8**, Transmission Confidentiality and Integrity
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**CM-7**, Least Functionality

4 Components of the Example Solution

This section highlights the components of the example solution and the collaborators who contributed those components and participated in the solution design, implementation, configuration, troubleshooting, and/or testing. More information on each component, including instructions for installing and configuring it as part of the example solution, is provided in NIST SP 1800-31C, How-To Guides.

4.1 Collaborators

Collaborators that participated in this build and the capabilities of their contributions to the example solution are described briefly in the subsections below.

4.1.1 Cisco

Cisco Systems is a provider of enterprise, telecommunications, and industrial networking solutions. Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure, micro-segmented network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments. Cisco Firepower Threat Defense (FTD) is a threat-focused, next-generation firewall with unified management. It provides advanced threat protection before, during, and after attacks. By delivering comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint, it increases visibility and security posture while reducing risks.

4.1.2 Eclypsium

Eclypsium is an enterprise firmware security company. The cloud-based solution identifies, verifies, and fortifies firmware and hardware in laptops, servers, network gear, and devices. Eclypsium Administration and Analytics Service secures against persistent and stealthy firmware attacks, provides continuous device integrity, delivers firmware patching at scale, and prevents ransomware and malicious implants. Eclypsium also provides an on-premises version that has parity with the cloud-based platform.

4.1.3 Forescout

Forescout assesses device security posture in real time upon connection and initiates remediation workflows with your existing security tools to enforce compliance. It continuously monitors all devices for new threats and reassesses their patch level hygiene every time the device leaves and returns to the corporate network. Forescout works to assess all device types, including transient devices often missed by point-in-time scans, without requiring agents. Forescout's solution goes beyond simple device authentication to identify every device, assess its security posture, trigger remediation workflows, and

implement access control across heterogeneous networks to unpatched assets. It continuously monitors all connected devices and automates response when noncompliance or unpatched assets are detected.

4.1.4 IBM

IBM MaaS360 with Watson is a unified endpoint management (UEM) solution that transforms how organizations support users, apps, content, and data across every type of mobile device: laptops, smartphones, tablets, and IoT. IBM MaaS360 was built almost twenty years ago as a cloud-based Software-as-a-Service (SaaS) platform that integrates with preferred security and productivity tools, allowing modern business leaders to derive immediate value. IBM MaaS360 is the only UEM platform that leverages the power of the Watson Artificial Intelligence engine to deliver contextually relevant security insights for administrators, while ensuring continuous monitoring of the riskiest end users.

IBM Code Risk Analyzer was developed in conjunction with IBM Research projects and customer feedback. It enables developers to quickly assess and remediate security and legal risks that they are potentially introducing into their source code, and it provides feedback directly in Git artifacts (for example, pull/merge requests) as part of continuous delivery in a DevOps pipeline. IBM Code Risk Analyzer is provided as a set of Tekton tasks, which can be easily incorporated into delivery pipelines.

4.1.5 Lookout

Lookout is an integrated endpoint-to-cloud security solution provider with mobile endpoint protection offerings. Lookout's Mobile Endpoint Security (MES) solution provides cloud-centric behavior-based detection capabilities; it performs behavioral analysis based on telemetry data from nearly 200 million devices and over 120 million apps. This analysis enables Lookout to deliver efficient protection with a lightweight app on the device that optimizes processor speed and battery life. In addition, continuously monitoring changes to the endpoint enables detection of risks that span from jailbreaking or rooting a device to advanced device compromise. With insight into both real-time changes on a device and the aggregate view of behavior across the broader mobile ecosystem, Lookout endpoint protection can detect zero-day threats.

4.1.6 Microsoft

Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure in the cloud and on-premises. Endpoint Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers. Endpoint Manager combines several services, including Configuration Manager (Microsoft Endpoint Configuration Manager), an on-premises management solution for desktops, servers, and laptops that are on your network or internet-based. Endpoint Configuration Manager can be integrated with Intune, Azure Active Directory (AD), Microsoft Defender for Endpoint, and other cloud services. Endpoint Configuration Manager can deploy apps, software updates, and operating systems, and also be used to monitor compliance and to query and act on clients in real time.

4.1.7 Tenable

Tenable.sc is Tenable's on-premises vulnerability management solution. Built on Nessus technology, the Tenable.sc family of products identifies, investigates, and prioritizes vulnerabilities. You get real-time, continuous assessment of your security and compliance posture so you can discover unknown assets and vulnerabilities, monitor unexpected network changes, and prioritize weaknesses to minimize your cyber risk and prevent breaches. Tenable.sc includes over 350 pre-built, highly customizable dashboards and reports to give you immediate insight into your security compliance, effectiveness, and risk. You can continuously measure, analyze, and visualize the effectiveness of your security program, based on high-level business objectives and underlying customizable policies that executives care about.

Powered by Nessus technology and managed in the cloud, Tenable.io provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first. Using an advanced asset identification algorithm, Tenable.io provides the most accurate information about dynamic assets and vulnerabilities in ever-changing environments. As a cloud-delivered solution, its intuitive dashboard visualizations, comprehensive risk-based prioritization, and seamless integration with third-party solutions help security teams maximize efficiency and scale for greater productivity.

4.1.8 VMware

VMware vRealize Automation includes SaltStack Config, a modern configuration management platform with the performance, speed, and agility IT teams need to manage large, complex IT systems and improve efficiency at scale. For this project, vRealize Automation SaltStack Config provides device configuration and software distribution capabilities. Specifically, it allows for configuration changes to be made to devices by updating or removing software as well as updating settings such as network information.

SaltStack SecOps, an add-on to the vRealize products, gives system administrators the ability to create security policies and scan assets to determine whether they are compliant with supported, industry-recognized security benchmarks. SaltStack SecOps also has the ability to scan your system for Common Vulnerabilities and Exposures (CVEs), then immediately apply the updates or patches to remediate the advisories.

4.2 Technologies

Table 4-1 lists all the technologies used in this project, the primary functions that each technology provides to the project, and the Cybersecurity Framework Subcategories that the technology supports in this project. Please refer to Table 3-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes.

Table 4-1: Technologies Used in the Build

Technology	Primary Functions	Cybersecurity Framework Subcategories
Cisco Firepower Threat Defense (FTD) and Cisco Firepower Management Center (FMC)	Network policy enforcement	PR.AC-4, PR.AC-5, DE.CM-1
Cisco Identity Services Engine (ISE)	Asset discovery and inventory; network access control	ID.AM-2, PR.AC-4, PR.AC-5
Eclypsium Administration and Analytics Service	Hardware and firmware inventory; firmware vulnerability assessment, integrity monitoring, and updating	ID.AM-1, ID.AM-2, PR.DS-6, PR.IP-12
Forescout Platform	Asset discovery and inventory; security policy enforcement	ID.AM-2, PR.AC-4, PR.AC-5, PR.IP-3, PR.PT-1
IBM Code Risk Analyzer	Vulnerability scanning for source code	PR.IP-12
IBM MaaS360 with Watson	Asset inventory; configuration management; software updates	ID.AM-2, PR.IP-3, PR.IP-12
Lookout Mobile Endpoint Security (MES)	Security policy enforcement; vulnerability scanning and reporting; software discovery and inventory; firmware vulnerability assessment and policy enforcement	PR.AC-4, PR.IP-3, PR.IP-12
Microsoft Endpoint Configuration Manager	Asset discovery; configuration management; software updates	ID.AM-2, PR.IP-3, PR.IP-12
Tenable.sc, Tenable.io, and Nessus	Asset discovery and inventory; vulnerability scanning and reporting	ID.AM-2, PR.PT-1, DE.CM-8
VMware vRealize Automation SaltStack Config and SaltStack SecOps	Vulnerability scanning and remediation; configuration management; software updates	PR.IP-3, PR.IP-12, DE.CM-8

The following sections summarize the security capabilities that each technology provided to the example solution.

4.2.1 Cisco Firepower Threat Defense (FTD) & Firepower Management Center (FMC)

Cisco Firepower Threat Defense (FTD) is a virtual firewall that was utilized as the networking backbone that connected all of the lab subnets. This build also used the Cisco FTD firewall to provide network access management capabilities, including enforcing network access control using firewall rules. Cisco FTD was deployed and managed in the lab via a separate Cisco Firepower Management Center (FMC) virtual machine.

To support the unpatchable asset scenario (Scenario 5), the integration between Cisco FTD and Cisco Identity Services Engine (ISE) via Cisco Platform Exchange Grid (pxGrid) allowed for the firewall to ingest security group tags (SGTs) that were applied by ISE. SGTs were then used in custom firewall rules to restrict network access to any machine that was given a quarantine tag. Section 4.2.2 has more information on this integration.

4.2.2 Cisco Identity Services Engine (ISE)

In this build Cisco Identity Services Engine (ISE) provided asset discovery, asset inventory, and network access control to enforce administrator-created security and access control policies. Cisco ISE had integrations with several other example solution technologies, including the following:

- An integration between ISE and AD allowed the user of a device to be identified. This information could then be used in custom policy.
- A Dynamic Host Configuration Protocol (DHCP) relay was established between ISE and the lab DHCP server. This integration allowed for ISE to identify any device that was assigned an IP address. This allowed devices to be discovered as they joined the network.
- Cisco ISE was configured to integrate with Tenable.sc via an adapter. Cisco ISE leveraged this adapter to prompt Tenable to scan devices newly connected to the network. Cisco ISE could then ingest this scan data to find the Common Vulnerability Scoring System (CVSS) scores of device vulnerabilities. An ISE policy was written to apply a quarantine action, via SGTs, to any device with a CVSS score equal to or greater than 7 (corresponding to high and critical vulnerabilities).
- Cisco pxGrid was configured to share contextual information about authenticated devices to the firewall. Cisco ISE was utilized to apply SGTs to devices as they were assessed for vulnerabilities. These SGTs were then passed to the lab firewall via pxGrid, where they could be used in custom firewall rules. pxGrid was also used to share communications between Forescout and Cisco ISE. Forescout could apply a quarantine tag to observed devices, which would then be shared with ISE.

4.2.3 Eclypsium Administration and Analytics Service

In this build, we utilized Eclypsium Administration and Analytics Service to provide agent-based identification of hardware and firmware for our laptop, desktop, and server endpoints while also monitoring the firmware for vulnerable or end-of-life versions. Eclypsium monitored laptop and virtual machine (VM) firmware integrity, and alerted if a component or its associated firmware changed. It also monitored endpoints for known security vulnerabilities from out-of-date firmware. Finally, we utilized Eclypsium's beta firmware update script, which automatically finds the latest known Basic Input/Output System (BIOS) firmware version for the system, downloads the update, and executes it to update the BIOS.

4.2.4 Forescout Platform

In this build the Forescout platform was configured to perform endpoint discovery by detecting endpoints and determining software information about those endpoints based on a set of attributes. Forescout also provided the capability to isolate or restrict assets that cannot be patched and to respond to emergency scenarios, such as providing an emergency mitigation or deploying an emergency patch. Forescout had several integrations with other example solution technologies:

- The User Directory plugin was configured so that the Forescout platform integrated with the lab's AD Domain Controller. This plugin provided Lightweight Directory Access Protocol (LDAP) services to Forescout, allowing directory-based users to log in to Forescout as well as providing user directory information such as the current active domain users logged into each endpoint.
- The Domain Name System (DNS) Query Extension configuration setting allowed Forescout to query the DNS server to determine the hostnames of devices identified by Forescout.
- The Tenable VM plugin provided the Forescout platform with vulnerability and scan status information which can be used to create custom policies. This plugin also enabled Forescout to utilize vulnerability management information that Tenable.sc collected from endpoints, and allowed Forescout to determine if scans had been performed on endpoints within the lab.
- The Microsoft Systems Management Server (SMS)/System Center Configuration Manager (SCCM) module was configured to allow the Forescout platform to integrate with Microsoft Endpoint Configuration Manager. This module allowed for a custom policy to be created that used data from Microsoft Endpoint Configuration Manager.
- The Linux plugin was configured to collect information from and manage Linux-based endpoints via two methods: secure shell (SSH) access to the endpoint, and agent-based integration with the endpoint.
- The HPS Inspection Engine was configured to collect information from Windows endpoints via two methods. The first method utilized a directory-based integration with the lab's AD Domain Services instance, which collected domain-based information on the Windows endpoint. The

second method utilized an agent-based integration called SecureConnector that allowed Forescout to collect and manage Windows endpoints.

- The pxGrid plugin was configured to integrate with Cisco ISE. This plugin gave the Forescout platform the ability to utilize Cisco ISE to apply adaptive network control (ANC) policies to endpoints for restricting their network access.
- The Switch plugin was configured to integrate Forescout with the physical Cisco switch located in the lab. The plugin used information from the switch to collect information about endpoints that were physically connected to the switch.

Our implementation utilized multiple policies to support the use case scenarios. Examples of capabilities that the policies provided are described below:

- Check for a particular application running on Windows; if present, stop execution and uninstall it.
- Check an endpoint for known critical vulnerabilities; if any are present, use Cisco ISE to quarantine the endpoint via the pxGrid plugin.
- Force a Windows update to occur on an endpoint with Windows Update enabled.
- Determine if a Windows endpoint has the Microsoft Endpoint Configuration Manager agent installed.

4.2.5 IBM Code Risk Analyzer

IBM Code Risk Analyzer was used to demonstrate vulnerability scanning and reporting for pre-deployed code as part of a DevOps pipeline to deliver a cloud-native application. Integration with Git allowed the Code Risk Analyzer to perform vulnerability assessments against applications and base images. The Code Risk Analyzer would then print a bill-of-materials, which indicates the composition of a deployment. This allows an administrator to see all of an application's dependencies and their sources, providing visibility into application components which could have vulnerabilities.

4.2.6 IBM MaaS360 with Watson

IBM MaaS360 with Watson was used to demonstrate how to securely manage an enterprise's devices by enabling deployment, control of content, and policy controls. Enterprises can manage organization-owned and user-owned devices using this product. The lab used MaaS360 for asset identification and assessment, routine patching and emergency patching, emergency mitigations, and isolation of assets that cannot be patched. The first phase of this lab build used MaaS360's comprehensive enterprise mobility management (EMM) capability to manage a MacBook Pro and a Windows 10 virtual desktop. The second phase used MaaS360's Mobile Device Manager (MDM) capability to manage Android and Apple iOS devices.

This build also used Maas360's Cloud Extender, which allows enterprises to integrate mobile devices with corporate on-premises and cloud-based resources. The Cloud Extender was installed on the AD server to allow users to log in with AD accounts.

4.2.7 Lookout

Lookout MES was used in this build to perform security compliance, vulnerability scanning, and firmware/software discovery for mobile endpoints. Our implementation of Lookout MES was integrated with IBM MaaS360. Lookout MES shared custom device attributes, such as device threat, with MaaS360, which could in turn provide policy enforcement. The Lookout for Work mobile client was able to provide firmware and application vulnerability assessment for mobile endpoints. Administrators could use Lookout to see which vulnerabilities were affecting deployed endpoints and find risk grades (i.e., A, B, C, D, or F) for installed applications.

4.2.8 Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager was used in this build to perform configuration management, including software and firmware patching, for Windows-based hosts. Our implementation of Endpoint Configuration Manager included Windows Server Update Services (WSUS), an update service primarily used for downloading, distributing, and managing updates for Microsoft Windows-based systems. The example build used Microsoft Endpoint Configuration Manager to demonstrate the identification of endpoints utilizing Heartbeat discovery and Windows Domain discovery methods, the patching of Windows endpoints via Microsoft updates and third-party update sources, and the deployment of custom scripts to endpoints.

4.2.9 Tenable.io

In the example build, Tenable.io was used to provide vulnerability scanning and reporting for Docker container images. Containers are built from images and vulnerabilities are patched in images, not deployed containers, so images are the focus of scanning. Tenable.io scanned the repository of a Red Hat OpenShift cluster in the lab environment. Tenable.io was scheduled to routinely pull the latest images from the OpenShift cluster and perform vulnerability scans on them. Scan information was reported in the container security section of the Tenable.io Web Console. Administrators could see vulnerability information for containers deployed in their respective networks.

4.2.10 Tenable.sc and Nessus

This example build utilized two Tenable products in the first phase of this project, Nessus and Tenable.sc. We used Nessus to scan Linux, Windows, and macOS endpoints and network switches for vulnerability data, and then feed this information to Tenable.sc for reporting. Tenable.sc, a vulnerability management product, collected the information from Nessus and reported that information to

administrators using dashboards and reports. Also, Tenable.sc had integrations with other example solution technologies:

- An integration between Tenable.sc and Cisco ISE was performed to initiate scans of any newly connected network devices. Tenable.sc would pass scan data to Cisco ISE, where a custom policy was written to quarantine devices based on their CVSS scores.
- An integration between Forescout and Tenable was leveraged to scan devices as hosts joined the network. Forescout could prompt Tenable to scan hosts to determine if an endpoint had critical vulnerabilities. This information was ingested by Forescout for the purpose of quarantining endpoints.

4.2.11 VMware vRealize Automation SaltStack Config

In this example build, VMware vRealize Automation SaltStack Config was used to provide configuration management and patch deployment. In the first phase of the build, it was used to manage Windows workstations and servers, a macOS laptop, and Linux/Unix-based VMs and servers. SaltStack Config was configured to run jobs, applying different states or configurations, on endpoints. The job that was written for this project, in support of the emergency mitigation scenario, could uninstall an application based on the current version of the product. SaltStack Config also had an add-on component called SaltStack SecOps which was utilized to scan devices for known vulnerabilities and provide mitigation actions, including missing updates for endpoints.

4.2.12 Additional Information

See NIST SP 1800-31 Volume C for additional information on each of the technologies we used to demonstrate the scenarios. It explains each technology, summarizes their integration into the laboratory environment, and documents our security decisions and associated configurations.

Appendix A Patch Management System Security Practices

Section 3.4.7 describes Scenario 6, "Patch management system security (or other system with administrative privileged access)." In support of Scenario 6, this appendix describes recommended security practices for systems like patch management systems which have administrative privileged access over many other systems as defined as "critical software" in Executive Order (EO) 14028. It then summarizes how the example solution components described in this practice guide could support each of those recommended security practices.

A.1 Security Measures

The table below defines security measures for software of critical importance. Note that these security measures are not intended to be comprehensive. They are based on those in the NIST publication *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028*. A *security measure (SM)* is a high-level security outcome statement that is intended to apply to critical software or to all platforms, users, administrators, data, or networks (as specified) that are part of running critical software. The security measures are grouped by five objectives:

1. Protect critical software and *critical software platforms* (the platforms on which critical software runs, such as endpoints, servers, and cloud resources) from unauthorized access and usage.
2. Protect the confidentiality, integrity, and availability of data used by critical software and critical software platforms.
3. Identify and maintain critical software platforms and the software deployed to those platforms to protect the critical software from exploitation.
4. Quickly detect, respond to, and recover from threats and incidents involving critical software and critical software platforms.
5. Strengthen the understanding and performance of humans' actions that foster the security of critical software and critical software platforms.

Each row in the table defines one security measure and lists mappings to it from the NIST Cybersecurity Framework and NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. These mappings are in the forms of Cybersecurity Framework Subcategories and SP 800-53 security controls, respectively. The mappings are general and informational; any particular situation might have somewhat different mappings.

Security Measure (SM)	Cybersecurity Framework Subcategories	SP 800-53 Rev. 5 Controls
Objective 1: Protect critical software and critical software platforms from unauthorized access and usage.		
SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of critical software and critical software platforms.	PR.AC-1, PR.AC-7	AC-2, IA-2, IA-4, IA-5
SM 1.2: Uniquely identify and authenticate each service attempting to access critical software or critical software platforms.	PR.AC-1, PR.AC-7	AC-2, IA-9
SM 1.3: Follow privileged access management principles for network-based administration of critical software and critical software platforms. Examples of possible implementations include using hardened platforms dedicated to administration and verified before each use, requiring unique identification of each administrator, and proxying and logging all administrative sessions to critical software platforms.	PR.AC-1, PR.AC-7, PR.MA-1, PR.MA-2	AC-2, IA-2, SC-2, SC-7 enhancement 15
SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to critical software, critical software platforms, and associated data. Examples of such techniques include network segmentation, isolation, software-defined perimeters, and proxies.	PR.AC-3, PR.AC-5	SC-7
Objective 2: Protect the confidentiality, integrity, and availability of data used by critical software and critical software platforms.		
SM 2.1: Establish and maintain a data inventory for critical software and critical software platforms.	ID.AM-3, DE.AE-1	CM-8, PM-5
SM 2.2: Use fine-grained access control for data and resources used by critical software and critical software platforms to enforce the principle of least privilege to the extent possible.	PR.AC-4	AC-2, AC-3, AC-6
SM 2.3: Protect data at rest by encrypting the sensitive data used by critical software and critical software platforms consistent with NIST's cryptographic standards.	PR.DS-1	SC-28
SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for critical software and critical software platforms consistent with NIST's cryptographic standards.	PR.AC-3, PR.AC-7, PR.DS-2, PR.PT-4, DE.CM-7	AC-4, AC-17, SC-8

Security Measure (SM)	Cybersecurity Framework Subcategories	SP 800-53 Rev. 5 Controls
SM 2.5: Back up data, exercise backup restoration, and be prepared to recover data used by critical software and critical software platforms at any time from backups.	PR.IP-4	CP-9, CP-10
Objective 3: Identify and maintain critical software platforms and the software deployed to those platforms to protect the critical software from exploitation.		
SM 3.1: Establish and maintain a software inventory for all platforms running critical software and all software (both critical and non-critical) deployed to each platform.	ID.AM-1, ID.AM-2, ID.SC-2	CM-8, PM-5, RA-9
SM 3.2: Use patch management practices to maintain critical software platforms and all software deployed to those platforms. Practices include: ▪ rapidly identify, document, and mitigate known vulnerabilities (e.g., patching, updating, upgrading software to supported version) to continuously reduce the exposure time ▪ monitor the platforms and software to ensure the mitigations are not removed outside of change control processes	ID.RA-1, ID.RA-2, ID.RA-6, PR.IP-12, DE.CM-8, RS.MI-3	CA-7, RA-5, SI-2, SI-5, SR-8
SM 3.3: Use configuration management practices to maintain critical software platforms and all software deployed to those platforms. Practices include: ▪ identify the proper hardened security configuration for each critical software platform and all software deployed to that platform (hardened security configurations enforce the principles of least privilege, separation of duties, and least functionality) ▪ implement the configurations for the platforms and software ▪ control and monitor the platforms and software to ensure the configuration is not changed outside of change control processes	ID.RA-1, ID.RA-2, ID.RA-6, PR.AC-4, PR.IP-1, PR.IP-3, PR.PT-3, DE.CM-8, RS.MI-3	AC-5, AC-6, CA-7, CM-2, CM-3, CM-6, CM-7, RA-5, SI-5
Objective 4: Quickly detect, respond to, and recover from threats and incidents involving critical software and critical software platforms.		
SM 4.1: Configure logging to record the necessary information about security events involving critical software platforms and all software running on those platforms.	PR.PT-1	AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12

Security Measure (SM)	Cybersecurity Framework Subcategories	SP 800-53 Rev. 5 Controls
SM 4.2: Continuously monitor the security of critical software platforms and all software running on those platforms.	DE.CM-7	CA-7, SI-4
SM 4.3: Employ endpoint security protection on critical software platforms to protect the platforms and all software running on them. Capabilities include: ▪ protecting the software, data, and platform by identifying, reviewing, and minimizing the attack surface and exposure to known threats ▪ permitting only verified software to execute (e.g., file integrity verification, signed executables, allowlisting) ▪ proactively detecting threats and stopping them when possible ▪ responding to and recovering from incidents ▪ providing the necessary information for security operations, threat hunting, incident response, and other security needs	PR.DS-5, PR.DS-6, DE.AE-2, DE.CM-4, DE.CM-7, DE.DP-4	SI-3, SI-4, SI-7
SM 4.4: Employ network security protection to monitor the network traffic to and from critical software platforms to protect the platforms and their software using networks. Capabilities include: ▪ proactively detecting threats at all layers of the stack, including the application layer, and stopping them when possible ▪ providing the necessary information for security operations, threat hunting, incident response, and other security needs	PR.DS-5, DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.DP-4	AU-13, AU-14, SC-7, SI-3
SM 4.5: Train all security operations personnel and incident response team members, based on their roles and responsibilities, on how to handle incidents involving critical software or critical software platforms.	PR.AT-5, PR.IP-9, PR.IP-10	AT-3, CP-3, IR-2
Objective 5: Strengthen the understanding and performance of humans' actions that foster the security of critical software and critical software platforms.		
SM 5.1: Train all users of critical software, based on their roles and responsibilities, on how to securely use the software and the critical software platforms.	PR.AT-1	AT-2, AT-3

Security Measure (SM)	Cybersecurity Framework Subcategories	SP 800-53 Rev. 5 Controls
SM 5.2: Train all administrators of critical software and critical software platforms, based on their roles and responsibilities, on how to securely administer the software and/or platforms.	PR.AT-2	AT-3, CP-3
SM 5.3: Conduct frequent awareness activities to reinforce the training for all users and administrators of critical software and platforms, and to measure the training's effectiveness for continuous improvement purposes.	PR.AT-1, PR.AT-2	AT-3

A.2 Component Support of Security Measures

This section provides summary tables for how each technology provider's components in the example solution could support the security measures defined above. The technical mechanisms, configuration settings, or other ways in which the components could provide this support were not necessarily utilized in the example solution build. The information is provided here to offer examples of how these security measures might be implemented, not to serve as recommendations for how to implement them.

Each table in this section has the same four columns:

- **SM #**: This lists a security measure ID from the previous section and links to the definition of that ID.
- **Question**: This contains a question NIST asked the technology providers to answer for their components regarding the associated security measure.
- **Technical Mechanism or Configuration**: This is a summary of the answer from the component's technology provider. The content submitted by each technology provider has been edited for brevity.
- **Refs.**: This provides hyperlinks to any applicable references specified by the technology provider. This column is blank if no reference was needed or available, or if there is a single reference for all entries in a table, in which case the reference is defined immediately before the table.

In each table, rows with no answer or an answer of "no" or "not applicable" have been omitted for brevity.

A.2.1 Cisco FTD Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	Certificates from a Personal Identity Verification (PIV) card or Common Access Card (CAC) can be used along with soft certificates to authenticate admin users.	Ref1
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	Services using the pxGrid solution to gather data from the system or publish require the use of certificates to secure the communications channel.	Ref1
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	The Cisco FMC admin console supports role-based access control. There are predefined roles, and custom roles with permissions can be created.	Ref1
SM 1.4	Does the system allow for the use of discretionary access control lists (DACLs), network segmentation, or isolation for access to the platform?	Administrators can limit access by IP address and port.	Ref1
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	The Cisco FMC admin console and command-line interface (CLI) both support role-based access control.	Ref1
SM 2.5	Does the system support performing regular backups and restorations?	Cisco FMC enables backup and restore of configuration and monitoring. FMC also provides backup and restore of the devices it manages.	Ref1
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	Cisco distributes several types of upgrades and updates for Firepower deployments. These include OS versions, patches, vulnerability databases, intrusion rules, and geolocation databases. These are all deployed centrally from FMC.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or Security Information and Event Management (SIEM)?	FMC allows for sending all logs to a third-party SIEM using syslog or eStreamer.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.4	Does the platform allow for logging connection events to the tool?	The system can generate logs of the connection events its managed devices detect. Connection events include Security Intelligence events (connections blocked by the reputation-based Security Intelligence feature.)	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Cisco provides training resources through direct offering, partner, knowledge partners, and on-demand through Cisco Live.	
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Cisco provides training resources through direct offering, partner, knowledge partners, and on-demand through Cisco Live.	
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Cisco regularly collects metrics from completed user training to make improvements and updates.	

A.2.2 Cisco ISE Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	Certificates from a PIV or CAC can be used along with soft certificates to authenticate admin users.	Ref1
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	Services using the ISE pxGrid solution to gather data from the system or publish require the use of certificates to secure the communications channel.	Ref1
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	The Cisco ISE admin console and CLI both support role-based access control.	Ref1
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	Both the admin user interface (UI) and CLI can be configured to limit IP access to the system.	Ref1
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	The Cisco ISE admin console and CLI both support role-based access control.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	Cisco ISE can be configured for Federal Information Processing Standards (FIPS) compliance. In this mode, only the protocols listed here are allowed to be used for authentication: EAP-TLS, PEAP, EAP-FAST, and EAP-TTLS.	Ref1
SM 2.5	Does the system support performing regular backups and restorations?	Cisco ISE backs up both the configuration and event data to a repository. The system provides high-availability (HA) capabilities with redundant service pairs.	Ref1
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	Cisco ISE provides a centralized patching mechanism through the admin node to apply patches to all systems that are a member of the deployment. Patches are rollups, so administrators do not have to install multiple patches. Patches include vulnerability fixes and bug fixes.	Ref1
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	Cisco ISE allows administrators to turn on and off features and functions. Cisco ISE does not allow access to the underlying OS, so services are only enabled and disabled based on the packages needed to support the enabled services.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	Log events for the following categories are sent by all nodes in the deployment to the logging targets: Administrative and Operational Audit, System Diagnostics, and System Statistics.	Ref1
SM 4.4	Does the platform allow for logging connection events to the tool?	The web interface can specify remote syslog server targets to which system log messages are sent. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (RFC 3164).	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Cisco provides training resources through direct offering, partner, knowledge partners, and on-demand through Cisco Live.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Cisco provides training resources through direct offering, partner, knowledge partners, and on-demand through Cisco Live.	
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Cisco regularly collects metrics from completed user training to make improvements and updates.	

A.2.3 Eclypsium Administration and Analytics Service Support of Security Measures

All entries in this table have the same two references: the Eclypsium-supplied Solution Guide and Deployment Guide. The Solution Guide is built into the product, and Eclypsium provides the Deployment Guide at purchase, so it was not possible to provide hyperlinks for this table.

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	Eclypsium integrates with multiple authentication mechanisms, many of which support multi-factor authentication (MFA).	
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	Unique application programming interface (API) tokens are managed by Eclypsium administrators.	
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	The Eclypsium platform contains Admin/User access roles. Only administrators can change systemwide analysis policies.	
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	The Linux OS hosting Eclypsium can be configured to allow for the creation of network-based access restrictions.	
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	The Eclypsium platform contains Admin/User access roles. Only administrators can change systemwide analysis policies.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	The data-at-rest encryption implementation is done as part of the backend platform onto which Eclypsium is deployed. In the cloud, the provider's key management system may be used. In an on-premises deployment, the OS or hardware-based encryption on the physical servers may be used.	
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	All communications occur over Transport Layer Security (TLS). FIPS mode can be enabled and utilized where desired.	
SM 2.5	Does the system support performing regular backups and restorations?	Backups of the Eclypsium backend are performed as part of the platform onto which it is deployed. Standard mechanisms for Linux server backup/restore will operate normally.	
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	This information is in the Solution Guide. When scanning firmware on target systems, similar information may be inferred from binary analysis.	
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	The cloud version is managed by Eclypsium to provide updates. The on-premises version is the responsibility of the customer. The OS can be configured to perform updates. On target systems, Eclypsium will indicate whether firmware is up to date.	
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	Eclypsium directly manages the configuration of cloud deployments. In an on-premises environment, configuration management becomes the responsibility of the customer. Normal configuration management for Linux servers will apply to the Eclypsium backend.	
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	In most instances, syslog is integrated with SIEM tools. Eclypsium alerts for target systems are forwarded over syslog to such tools when configured.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	There is an audit trail of users who have logged in and the actions they performed. Updates are also sent out to help remediate software running on the platform.	
SM 4.3	Is anti-malware or antivirus able to be installed on the system running your platform?	Eclypsium scanners and the Eclypsium backend are compatible with running other endpoint security software on the same device.	
SM 4.4	Does the platform allow for logging connection events to the tool?	In cloud deployments, Eclypsium manages network security protections. In an on-premises deployment, this would be inherited from the environment into which Eclypsium is deployed.	
SM 4.5	Are there training courses or procedures in the event of an incident involving the tool or platform?	Eclypsium security operations personnel receive security and incident response training. Customer training is available from Eclypsium to cover firmware security and incident response scenarios.	
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Eclypsium has the latest training catalog.	
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Eclypsium has the latest training catalog.	
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Eclypsium has the latest training catalog.	

A.2.4 Forescout Platform Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	The Forescout platform's integration with PIV and Homeland Security Presidential Directive 12 (HSPD-12) cards allows for this capability.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	The Forescout platform supports a range of accounts with different access levels as required to support least privilege.	Ref1
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	Forescout supports the use of DACLs, virtual local area network (VLAN) assignment, and any other network-based control offered by the network devices in use for device isolation as needed.	Ref1
SM 2.1	Does the software list and maintain an inventory of all software criticalities and integrations?	This is enabled via Forescout's native policy.	Ref1
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	The Forescout platform supports a range of accounts with different access levels as required to support least privilege.	Ref1
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	Forescout natively encrypts the data at rest on the hard drives but can also verify and establish the encryption level of managed endpoints.	Ref1
SM 2.5	Does the system support performing regular backups and restorations?	Forescout supports backup/restore of data and configurations of all appliances.	Ref1
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	Forescout can identify applications and services that are installed and/or running on Windows, Linux, and macOS. Remote inspection capabilities are enabled either by integration with AD (LDAP) or via an agent (Secure Connector). This in turn can be enhanced by creating Forescout security policies to identify all software with enhanced privileges and known CVEs.	
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	Forescout integrates with a variety of patch and OS management tools. Forescout has native remediations via scripting on endpoints via policy.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	Forescout can perform control actions against any managed endpoint. Services as a property are an attribute detected running/installed on the endpoint. These attributes (services) can in turn can be stopped/started or removed as required via policy.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	The Forescout platform sends rich device context information to a SIEM system for logging and event analysis.	Ref1 Ref2
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	Forescout supports a default Windows Vulnerability CVE/Patch plugin (published by Microsoft) to actively scan all Windows clients/servers in real time via policy. The Forescout platform also provides Security Policy Templates (SPT) covering zero-day information and assesses software and hardware for these issues. SPT includes vulnerability and response templates with relevant data for vulnerabilities as documented by Forescout security labs.	Ref1
SM 4.4	Does the platform allow for logging connection events to the tool?	All successful and failed connections to the Forescout platform are logged in system event logs. Administrators can view these logs. An option is also available to forward event messages to third-party logging systems via syslog.	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Forescout offers training and certifications for administrators.	Ref1
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Forescout offers training and certifications for engineers.	Ref1

A.2.5 IBM Code Risk Analyzer Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	It leverages the IBM Cloud authentication mechanism, which provides multi-factor authentication for all users and administrators.	
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	All users and machines are identified using the Identity and Access Management feature of IBM Cloud.	
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	Accounts can be created and assigned to appropriate roles that have different access levels. This functionality is provided by the Identify and Access Management feature of IBM Cloud.	
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	Network segmentation and isolation is done by using Kubernetes clusters and Istio as the service mesh. Strict policies exist for egress and ingress.	
SM 2.1	Does the software list and maintain an inventory of all software criticalities and integrations?	The software keeps a bill of materials for each component. This bill of materials contains a full list of third-party dependencies. Integration is allowed with only IBM-authorized software.	
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	This feature is achieved by using the Identity and Access Management (IAM) feature of IBM Cloud. IAM has comprehensive features for granular access for users, administrators, and machines.	
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	All data at rest, whether in databases or file systems, is encrypted using NIST-certified cryptographic standards.	
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	All data in transit is encrypted using NIST-certified cryptographic standards. This includes data that is flowing between microservices inside a cluster.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 2.5	Does the system support performing regular backups and restorations?	The system data is backed up regularly for offsite storage. Disaster recovery procedures are reviewed and tested regularly by IBM engineers.	
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	A bill of materials is created for each microservice. Integrations with databases and other systems are tracked. Change management is rigorously followed.	
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	The OS, middleware, and application components are regularly patched using automated pipelines. These components are scanned for any vulnerabilities and patches are deployed within strict timeframes.	
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	The system is configured and deployed using various standard techniques such as Kubernetes Helm charts and YAML files. The service can be disabled in all regions within minutes by disabling DNS entries, reverse proxies, etc.	
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	Syslog data is streamed to centralized logging mechanisms. The security events data is also made available to clients using the Activity Tracker mechanism.	
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	Continuous monitoring for security is accomplished by using firewalls and service mesh.	
SM 4.3	Is anti-malware or antivirus able to be installed on the system running your platform?	All systems running the system have anti-malware software running on them. Comprehensive reports are generated to ensure compliance.	
SM 4.4	Does the platform allow for logging connection events to the tool?	All successful and unsuccessful connections are logged in the Activity Tracker and in the Identity and Access Management system of IBM Cloud.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.5	Are there training courses or procedures in the event of an incident involving the tool or platform?	Process documentation, runbooks, training, and technology are in place to respond to incidents in a timely manner. High-severity incidents are tracked at executive levels. Root-cause analysis is performed and actionable tasks are documented. Best practices are shared across all teams in IBM Cloud.	
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Self-service tutorials are available to users based on their roles. Comprehensive documentation is available as well.	
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	IBM Garage teams host courses for all aspects of the IBM Cloud platform.	
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Regular trainings are conducted for all developers and administrators who are responsible for operating the IBM Cloud. The training materials are revised as new best practices become available.	

A.2.6 IBM MaaS360 with Watson Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	Connections to IBM MaaS360 are authenticated with API keys or credentials.	Ref1
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	In the MaaS360 admin console, roles can be assigned to each administrator based on their individual needs.	Ref1
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	In the MaaS360 admin console, custom roles can be defined with granular access rights.	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	IBM MaaS360 offers training courses that are catered to the role an individual will hold for utilizing the product.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	IBM MaaS360 offers training courses for administrative users.	Ref1 Ref2
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Release Notes are regularly updated with new and updated feature information, and the "MaaS360 Latest" panel provides videos and tutorials on new and updated capabilities. Each training course has a star rating system for effectiveness and improvement purposes.	Ref1

A.2.7 Lookout MES Support of Security Measures

SM #	Description	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	Organizations can integrate their existing Security Assertion Markup Language (SAML) 2.0 MFA solutions for authorization purposes into the Lookout MES Console.	
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	Lookout identifies and authenticates each user or machine account that attempts to access the platform. Audit logs also collect actions taken by each account.	
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	Lookout allows for the creation of several administrative types with decreasing levels of access.	
SM 2.1	Does the software list and maintain an inventory of all software criticalities and integrations?	The Lookout MES Console provides a full application inventory list of all devices within the customer's user fleet.	
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	Lookout allows for the creation of several administrative types with decreasing levels of access.	
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit encryption.	

SM #	Description	Technical Mechanism or Configuration	Refs.
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	Data in transit is encrypted using TLS version 1.2.	
SM 2.5	Does the system support performing regular backups and restorations?	Daily backups and snapshots of the production environment are taken and stored via Amazon's S3 service within multiple zones and U.S. regions. Regular integrity checks occur through restorations occurring multiple times annually. These restores populate new production instances which are then verified and monitored.	
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	The Lookout MES Console provides a full application inventory list of all devices within the customer's user fleet.	
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	Patches to the Lookout MES Console are controlled and maintained by Lookout backoffice support.	
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	Lookout uses a representational state transfer (REST) API to capture and send all console-related logs (e.g., device changes, threat information, system audit events) to SIEMs and syslog readers.	
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	Lookout is Federal Risk and Authorization Management Program (FedRAMP) Moderate and therefore follows strict patch management controls for patching our own software.	
SM 4.4	Does the platform allow for logging connection events to the tool?	Lookout captures connection events to the tool and activities conducted within the tool via our auditing capabilities.	
SM 4.5	Are there training courses or procedures in the event of an incident involving the tool or platform?	Internally, Lookout has established procedures for how to respond to a security incident (leak, compromise, etc.). These procedures follow strict FedRAMP Moderate policies.	

SM #	Description	Technical Mechanism or Configuration	Refs.
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Lookout provides first-touch training and guidance for using the Lookout MES and for integration guidance with a customer's MDM. Additionally, frequently asked questions (FAQs), integration guides, and console user guides are available to all administrators via the Lookout Support Knowledge portal.	
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Lookout provides first-touch training and guidance for using the Lookout MES and for integration guidance with a customer's MDM. Additionally, FAQs, integration guides, and console user guides are available to all administrators via the Lookout Support Knowledge portal.	

A.2.8 Microsoft Endpoint Configuration Manager (ECM) Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	Access to ECM Site Collections can be restricted via strong authentication. This can include MFA and passwordless options like Windows Hello for Business.	Ref1
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	ECM natively audits logins and activities and can be reported on by utilizing ECM Reports.	Ref1
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	ECM supports achieving least privilege through security roles, scopes, and collections.	Ref1
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	Microsoft provides guidance around the ports and protocols required by ECM. Customers can use this to implement firewalls between services and clients.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 2.1	Does the software list and maintain an inventory of all software criticalities and integrations?	Configuration Manager uses an in-console service method called Updates and Servicing. It makes it easy to find and install recommended updates for your Configuration Manager infrastructure.	Ref1
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	ECM supports achieving least privilege through security roles, scopes, and collections.	Ref1
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	ECM supports encryption at rest natively and through the use of BitLocker.	Ref1
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	ECM supports encryption for data in transport.	Ref1
SM 2.5	Does the system support performing regular backups and restorations?	Backup and restore operations are core resiliency capabilities in ECM.	Ref1
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	ECM lists the software dependencies that are required for the platform to operate on the server in addition to client end nodes.	Ref1
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	Configuration Manager uses an in-console service method called Updates and Servicing. It makes it easy to find and install recommended updates for your Configuration Manager infrastructure.	Ref1
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	Configuration Manager supports installing specific roles, for example management points, distribution points, and software update points, which contain the services required to run that service only.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	Logs are stored in the ECM database, log files, and Windows Event Logs. Implementation guidance is specific to the capabilities of the SIEM.	

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	Configuration Manager includes software update monitoring, which can be used to identify vulnerable software on its infrastructure.	Ref1
SM 4.3	Is anti-malware or antivirus able to be installed on the system running your platform?	Anti-malware and anti-virus solutions can be installed on the host operating system. Microsoft recommends allowlisting the files and processes related to ECM.	Ref1
SM 4.4	Does the platform allow for logging connection events to the tool?	Client and management point logging can be configured at various levels to meet customer requirements.	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Microsoft offers training courses that are catered to the role an individual will have for utilizing the product.	Ref1
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Microsoft provides e-learning and certification preparation guides for ECM on the Microsoft Learn portal. Hands-on or train-the-trainer models are provided through an implementation partner.	Ref1
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Courses and certifications are periodically updated based on product enhancements and feedback from customers.	

A.2.9 Tenable.sc Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.1	Does the software platform allow for the use of a two-factor authentication method for access?	MFA is achieved through certificate-based authentication and SAML authentication.	Ref1 Ref2
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	This is default behavior. Connections are authenticated with API keys or credentials, then handled via session cookie.	Ref1 Ref2
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	This is default behavior provided by role-based access control.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	Tenable.sc can bind the HTTPS interface to a single IP/network interface card (NIC) and utilize sideband networks for management/administration.	Ref1 Ref2
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	This is default behavior provided by role-based access control.	Ref1
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	Tenable.sc provides encryption for critical resources (target credentials). For vulnerability data and application configuration information, an external data-at-rest solution is required.	Ref1
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	This is default behavior.	Ref1
SM 2.5	Does the system support performing regular backups and restorations?	Tenable supports administrator backup of the opt/sc directory. Backups can be scripted to run on the host OS.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	The Tenable.sc application can use the host OS's syslog implementation to leverage an external syslog or SIEM.	Ref1
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	Tenable.sc can scan an environment passively (with the use of Nessus Network Monitor/NNM) and actively to achieve continuous monitoring.	Ref1 Ref2
SM 4.3	Is anti-malware or antivirus able to be installed on the system running your platform?	Anti-malware and anti-virus solutions can be installed. Tenable recommends allowlisting the files and processes related to Nessus and Tenable.sc.	Ref1 Ref2
SM 4.4	Does the platform allow for logging connection events to the tool?	NNM not only does passive analysis for vulnerabilities, but it can also provide logging of connection events as Informational events.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.5	Are there training courses or procedures in the event of an incident involving the tool or platform?	Tenable has many training options available to customers of our products, including instructional videos, free trainings, and paid trainings for deeper dives and larger groups.	Ref1 Ref2 Ref3
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	Tenable offers training courses that are catered to the role an individual will have utilizing the product.	Ref1 Ref2 Ref3
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	Tenable offers training courses for administrative users.	Ref1 Ref2 Ref3
SM 5.3	Are trainings updated and metrics collected to improve trainings?	Tenable continually collects feedback and introduces changes based on product updates and user feedback.	

A.2.10 VMware vRealize Automation SaltStack Config Support of Security Measures

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 1.2	Does the software platform identify and authenticate users and machine accounts that try to access the platform?	This can be set up in the SaltStack Config component or done through integration with LDAP, AD, SAML, or OpenID Connect (OIDC) providers.	Ref1
SM 1.3	Does the system allow for creating accounts with different access levels to enforce least management?	This can be set up in SaltStack Config or done through integration with LDAP, AD, SAML, or OIDC providers.	Ref1
SM 1.4	Does the system allow for the use of DACLs, network segmentation, or isolation for access to the platform?	The Linux OS hosting SaltStack Config can be configured to perform network isolation.	
SM 2.1	Does the software list and maintain an inventory of all software criticalities and integrations?	VMware tracks each product used by SaltStack Config and any updates and vulnerabilities in those products.	
SM 2.2	Does the system allow for creating accounts with different access levels to enforce least management?	This can be set up in SaltStack Config or done through integration with LDAP, AD, SAML, or OIDC providers.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 2.3	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data at rest?	SaltStack Config has a FIPS-compliant mode that can be configured at installation time to support encryption of data at rest.	Ref1
SM 2.4	Does the system use or contain an option to enable the use of NIST-certified cryptographic standards for protecting data in transit?	SaltStack Config supports encryption for data in transit by default. Key generation uses standard algorithms found in the OpenSSL library. These algorithms rely on OS-generated random seed data.	
SM 2.5	Does the system support performing regular backups and restorations?	SaltStack Config allows administrators to perform manual backups.	Ref1
SM 3.1	Does the product list all software dependencies and currently installed applications/services?	SaltStack provides a list of all dependent software and libraries used within the product.	
SM 3.2	Does the platform allow for the deployment of patches and OS updates?	The Linux system hosting SaltStack can be updated by administrators. The SaltStack SecOps component can be utilized to perform updates on SaltStack nodes and client end nodes.	Ref1
SM 3.3	Does the platform allow for configuration management practices such as removal or disabling of services to maintain security?	SaltStack Config allows for configuration management through the implementation of Salt states, the beacon and reactor system, and/or orchestration.	Ref1
SM 4.1	Does the security tool support logging and sending that data to rsyslog or a SIEM?	Salt returners can be used/configured to send logs to third-party tools like rsyslog and Splunk.	Ref1
SM 4.2	Does the platform monitor the security and vulnerabilities associated with all software and dependencies used?	VMware tracks each product used by SaltStack Config and tracks any updates and vulnerabilities that are announced by the product owners.	
SM 4.3	Is anti-malware or antivirus able to be installed on the system running your platform?	Anti-malware and anti-virus solutions can be installed on the host Linux OS.	
SM 4.4	Does the platform allow for logging connection events to the tool?	You can set the logging level to debug or turn on the audit trail, and that will provide connection events.	Ref1

SM #	Question	Technical Mechanism or Configuration	Refs.
SM 4.5	Are there training courses or procedures in the event of an incident involving the tool or platform?	There is official training for customers of the platform. Also, support contracts can be purchased to help troubleshoot and fix incidents with the product.	Ref1
SM 5.1	Are there training courses in how to use the products? Are there different courses for different roles?	VMware provides training on the underlying platform (SaltStack Config and vRealize Automation) as well as the security operations product.	Ref1
SM 5.2	Are there training courses for teaching administrators how to utilize the platform?	VMware provides training on the underlying platform (SaltStack Config and vRealize Automation) as well as the security operations product.	Ref1

Appendix B List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
ANC	Adaptive Network Control
API	Application Programming Interface
BIOS	Basic Input/Output System
CAC	Common Access Card
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLI	Command-Line Interface
CRADA	Cooperative Research and Development Agreement
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DACL	Discretionary Access Control List
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECM	(Microsoft) Endpoint Configuration Manager
EMM	Enterprise Mobility Management
EO	Executive Order
FAQ	Frequently Asked Questions
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FMC	(Cisco) Firepower Management Center
FTD	(Cisco) Firepower Threat Defense
HA	High Availability

HSPD-12	Homeland Security Presidential Directive 12
IAM	Identity and Access Management
ICS	Industrial Control System
IoT	Internet of Things
IP	Internet Protocol
ISE	(Cisco) Identity Services Engine
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Manager
MES	(Lookout) Mobile Endpoint Security
MFA	Multi-Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NNM	(Tenable) Nessus Network Monitor
OIDC	OpenID Connect
OS	Operating System
OT	Operational Technology
PC	Personal Computer
PIV	Personal Identity Verification
REST	Representational State Transfer
RMF	Risk Management Framework
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCCM	(Microsoft) System Center Configuration Manager

SGT	Security Group Tag
SIEM	Security Information and Event Management
SM	Security Measure
SMS	(Microsoft) Systems Management Server
SP	Special Publication
SPT	(Forescout) Security Policy Templates
SSH	Secure Shell
TLS	Transport Layer Security
UEM	Unified Endpoint Management
UI	User Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
WaaS	Windows as a Service
WSUS	(Microsoft) Windows Server Update Services