NIST SPECIAL PUBLICATION 1800-21B

Mobile Device Security:

Corporate-Owned Personally-Enabled (COPE)

Volume B:
Approach, Architecture, and Security Characteristics

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

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

September 2020

Final

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-21B Natl. Inst. Stand. Technol. Spec. Publ. 1800-21B, 147 pages, (September 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, 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

Mobile devices provide access to vital workplace resources while giving employees the flexibility to perform their daily activities. Securing these devices is essential to the continuity of business operations.

While mobile devices can increase efficiency and productivity, they can also leave sensitive data vulnerable. Mobile device management tools can address such vulnerabilities by helping secure access to networks and resources. These tools are different from those required to secure the typical computer workstation.

This practice guide focuses on security enhancements that can be made to corporate-owned personally-enabled (COPE) mobile devices. COPE devices are owned by an enterprise and issued to an employee. Both the enterprise and the employee can install applications onto the device.

To address the challenge of securing COPE mobile devices while managing risks, the NCCoE at NIST built a reference architecture to show how various mobile security technologies can be integrated within an enterprise's network.

This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their mobile device security and privacy needs.

KEYWORDS

Corporate-owned personally-enabled; COPE; mobile device management; mobile device security, on-premise; bring your own device; BYOD

ACKNOWLEDGMENTS

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

Name	Organization
Donna Dodson	NIST
Vincent Sritapan	Department of Homeland Security, Science and Technology Directorate
Jason Frazell	Appthority (acquired by Symantec—A division of Broadcom)
Joe Midtlyng	Appthority (acquired by Symantec—A division of Broadcom)
Chris Gogoel	Kryptowire
Tom Karygiannis	Kryptowire
Tim LeMaster	Lookout
Victoria Mosby	Lookout
Michael Carr	MobileIron

Name	Organization
Walter Holda	MobileIron
Farhan Saifudin	MobileIron
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Lura Danley	The MITRE Corporation
Eileen Durkin	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Marisa Harriston	The MITRE Corporation
Milissa McGinnis	The MITRE Corporation
Nick Merlino	The MITRE Corporation
Doug Northrip	The MITRE Corporation
Titilayo Ogunyale	The MITRE Corporation
Oksana Slivina	The MITRE Corporation
Tracy Teter	The MITRE Corporation
Paul Ward	The MITRE Corporation

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
Appthority*	Appthority Cloud Service, Mobile Threat Intelligence
Kryptowire	Kryptowire Cloud Service, Application Vetting
Lookout	Lookout Cloud Service/Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android), Mobile Threat Defense
MobileIron	MobileIron Core Version 9.7.0.1, MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android), Enterprise Mobility Management
Palo Alto Networks	Palo Alto Networks PA-220
Qualcomm	Qualcomm Trusted Execution Environment (version is device dependent)

* Appthority (acquired by Symantec—A division of Broadcom).

Contents

List of Figures

List of Tables

1 Summary

This section helps familiarize the reader with:

- Corporate-Owned Personally-Enabled (COPE) concepts
- COPE challenges, solutions, and benefits as related to this practice guide

---

COPE mobile devices are owned by an enterprise and issued to an employee. Both the enterprise and the employee can install applications onto the device.

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide seeks to help address COPE mobile device security implementation challenges in several ways: by analyzing a set of mobile security and privacy threats; exploring mitigating technologies; and describing a reference design based upon those technologies to help mitigate the identified threats.

Mobile devices provide greater flexibility in how employees access resources. For some organizations, this flexibility supports a hybrid approach enhancing their in-office processes with mobile device communication and workflows.

For others, this flexibility, combined with growing mobile functionality, fosters a mobile-first approach in which their employees primarily communicate and collaborate using mobile devices. However, some of the features that make mobile devices increasingly flexible and functional also make them challenging to deploy and manage with security in mind.

Further, organizations are becoming progressively cognizant of the privacy implications that arise from using mobile security technologies. Therefore, developing a successful mobile deployment strategy requires organizations to evaluate their security and privacy requirements.

To help organizations address mobile device security and privacy risks, this document's reference design provides:

- a description of a mobile device deployment example solution featuring an on-premises enterprise mobility management (EMM) solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities in support of a COPE mobile device usage scenario
- a series of how-to guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture to help security engineers rapidly deploy and evaluate our example solution in their test environment

The example solution of our reference design uses standards-based, commercially available products. It can be used directly by any organization with a COPE usage scenario by implementing a security infrastructure that supports integration of on-premises with cloud-hosted mobile security technologies.

Alternatively, an organization may use our reference design and example solution in whole or part as the basis for a custom solution that realizes the security and privacy characteristics that best support its unique mobile device usage scenario.

1.1 Challenge

Mobile devices are a staple within modern workplaces, and as employees use these devices to perform tasks, organizations are challenged with ensuring that devices process, modify, and store sensitive data securely. They bring unique threats to the enterprise and need to be managed differently from desktop platforms.

Due to their unique capabilities, mobile devices' specific security challenges can include:

- securing their always-on connections to the internet from network-based attacks
- securing the data on devices to prevent compromise via malicious applications
- protecting them from phishing attempts that try to collect user credentials or entice a user to install software
- selecting from the many mobile device management tools available and implementing their protection capabilities consistently
- identifying threats to mobile devices and how to mitigate them

Given these challenges, managing the security of workplace mobile devices and minimizing the risk posed can be complex. By providing an example solution that organizations can make immediate use of, this guide provides an example solution to help simplify deployment of mobile device security capabilities.

1.2 Solution

In our lab at the National Cybersecurity Center of Excellence (NCCoE), NIST engineers built an environment that contains an example solution for managing the security of mobile devices. In this guide, we show how an enterprise can leverage this infrastructure to implement on-premises EMM, mobile threat defense (MTD), mobile threat intelligence (MTI), application vetting, secure boot/image authentication, and virtual private network (VPN) services.

Further, these technologies were configured to protect organizational assets and end-user privacy, providing methodologies to enhance the security posture of the adopting organization. The foundation of this architecture is based on federal United States guidance, including that from the NIST 800 series publications [1], the National Information Assurance Partnership (NIAP) [2], the Department of Homeland Security [3], and the Federal Chief Information Officers (CIO) Council [4]. These standards, best practices, and certification programs help ensure the confidentiality, integrity, and availability of enterprise data on mobile systems.

This guide provides:

- a detailed example solution with capabilities that mitigate common mobile threats
- a demonstration of an approach that uses commercially available products
- step-by-step installation how-to guidance for implementers, which is designed to integrate with existing systems to improve the organization's mobile security posture with minimal disruption to operations

The NCCoE sought existing technologies that provided the following capabilities:

- ability to help protect data on the mobile device
- utilization of centralized management systems to deploy policies and configurations to devices
- vetting the security of mobile applications
- ability to help protect data from eavesdropping
- privacy settings to enable the predictability, manageability, and disassociability of end-users' personally identifiable information (PII)

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing information technology (IT) infrastructure and investments.

1.2.1 Standards and Guidance

This guide leverages many standards and guidance, including the NIST *Cybersecurity Framework Version 1.1* [5], the NIST *Privacy Risk Assessment Methodology (PRAM)* [6], the *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [7], the NIST *Risk Management Framework* [8], and the *NIST Mobile Threat Catalogue* [9]. For additional information, see Appendix D, Standards and Guidance.

1.3 Benefits

The potential benefits of the example solution explored by this project are to:

- provide users with enhanced protection against both malicious applications and loss of personal and business data when a device is stolen or misplaced
- reduce adverse effects on an organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- provide visibility for system administrators into mobile security events, enabling automated identification and notification of a compromised device
- provide modular architecture based on technology roles while remaining vendor-agnostic
- facilitate multiple mobile device usage scenarios using COPE devices

- apply robust, standards-based technologies using industry best practices
- demonstrate secure mobile access to organizational resources
- illustrate the application of the NIST Risk Management Framework to mobility scenarios

2 How to Use This Guide

This section helps familiarize the reader with:

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

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate how to improve the security and privacy of organization-owned mobile devices. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-21A: *Executive Summary*
- NIST SP 1800-21B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-21C: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-21A*, which describes the following topics:

- challenges that enterprises face in securing organization-owned mobile devices from threats that are distinct from desktop platforms
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-21B,* which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed

- Section 4.3, 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 1800-21A,* with your leadership team members to help them understand the importance of adopting standards-based solutions to improve mobile device security with on-premises mobile device management solutions.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-21C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that information technology (IT) professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of this guide's example solution for on-premises mobile device security management. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used, and Appendix I maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to mobile-nccoe@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 detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**

Typeface/ Symbol	Meaning	Example
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

This section helps familiarize the reader with:

- this guide's intended audience, scope, and assumptions
- the fictional organization used in the example scenario
- the risk assessment, including the privacy risk assessment
- the example solution's goals and the technologies it uses

The NIST build team surveyed reports of mobile device security trends and openly invited the mobile device security community—including vendors, researchers, administrators, and users—to engage in a discussion about pressing cybersecurity challenges. The community expressed two significant messages.

First, administrators experienced confusion about which policies and standards—out of myriad sources—should be implemented. Second, mobile device users were frustrated by the degrees to which enterprises have control over their mobile devices and maintain visibility into their personal activity.

Therefore, the NIST build team reviewed the primary standards, best practices, and guidelines from government sources and implemented a COPE usage scenario within this build. This effort highlights several security characteristics and capabilities that are documented within the Mobile Device Security for Enterprises building block [10].

3.1 Audience

This practice guide is for organizations that want to enhance the security and privacy of corporate-owned mobile devices. It is intended for executives, security managers, engineers, administrators, and others who are responsible for acquiring, implementing, and maintaining mobile enterprise technology, including centralized device management, application vetting, and endpoint protection systems.

This document will be of particular interest to system architects already managing mobile deployment solutions and those looking to deploy mobile devices in the near term. It assumes readers have a basic understanding of mobile device technologies and enterprise security principles. Please refer to Section 2 for how different audiences can effectively use this guide.

3.2 Scope

The scope of this build includes managing mobile phones and tablets with on-premises EMM. Mobile devices in general are commonly defined as:

> A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [11].

Laptops are excluded from the scope of this publication, as the security controls available today for laptops differ significantly from those available for mobile phones and tablets, although this is changing with the emergence of unified endpoint management capabilities.

Devices with minimal computing capability are also excluded, including feature phones, wearables, and devices classified as part of the Internet of Things. Classified systems, devices, data, and applications are not addressed within this publication.

The build team devised a fictional scenario centered around a mock organization (Orvilia Development) to provide context to our risk assessment and to enable us to build a reference design to solve common enterprise mobile security challenges. Using a fictional scenario exemplifies the issues that an organization may face when addressing common enterprise mobile security challenges. We intend for the example solution proposed in this practice guide to be broadly applicable to enterprises, including both the public and private sectors.

The example solution does not incorporate insider threats and their corresponding mitigations. It focuses on external threats and how the example solution can address them.

Additional options for deployment of Android, Apple, and Samsung Knox managed devices are discussed in Appendix E.

3.2.1 Orvilia Development

The fictional organization, Orvilia Development, is a start-up company providing IT services to many private sector organizations. Its service offerings include developing scalable web applications, improving existing IT systems, project management, and procurement. Orvilia recently won its first government contract. Given the organization's current security posture, particularly in its use of mobile devices, complying with government regulations and heightened cybersecurity standards presents it with new challenges.

Orvilia has a deployment of on-premises IT resources. It hosts its own Microsoft Active Directory (AD) domain, Microsoft Exchange email server, and web-based resources for employees, such as timekeeping and travel support. All enterprise resources can be directly accessed by employees locally or remotely from any internet-connected device by using password-based authentication. Orvilia also provides its employees with corporate-owned mobile devices. These may be used for personal activity, including phone calls, instant messaging, and installation and use of social applications. Employees also regularly work outside the office and frequently use public Wi-Fi networks at hotels, airports, and coffee shops.

Orvilia's mobile device deployment practice is still developing; it has minimal mobile device policies and has not implemented any additional security mechanisms such as enterprise mobility management. All policy and security enforcement actions are performed manually on an ad-hoc basis. Employees are expected to secure their own COPE devices, for instance via the timely installation of operating system (OS) updates, and to exercise good judgment regarding any personal use.

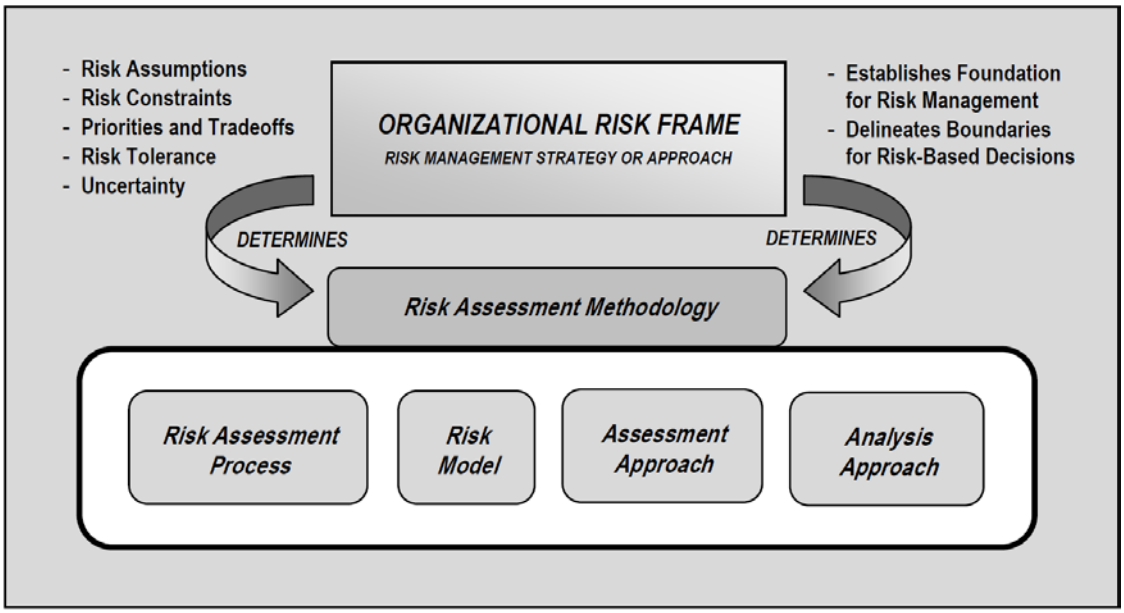
However, no mechanisms have been put into place to prevent or detect misuse or device compromise. Further, corporate policy prohibits access to the corporate network from personally owned mobile devices, but no technical safeguards have been implemented to prevent employees from doing so. This posture had been promoted based on the organization's small size, high level of employee technical acumen, and lack of awareness that it has been significantly impacted by any cybersecurity incidents.

However, Orvilia's new status as a contractor to a civilian government agency calls for it to achieve and maintain compliance with government policies, which require compliance with cybersecurity best practices and applicable standards. For example, Orvilia is required to secure its access to and storage of sensitive government information, which its employees will need to access from their mobile devices, both locally at agency sites and remotely from Orvilia or during travel.

In addition to meeting compliance requirements rising from its contractual obligations to a government agency, Orvilia leadership is concerned about the potential for future incidents where nation-state malicious actors might obtain sensitive government data from unsecured devices and infrastructure.

Therefore, a risk assessment as described in NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12], was performed using the risk management concepts shown in Figure 3-1.

Figure 3-1 Risk Management Approach



The risk assessment revealed that Orvilia's current mobile infrastructure places the organization at risk of intrusion and compromise of sensitive data. The results of the risk assessment process are presented in Appendix F.

Based on the risk assessment findings, Orvilia chose to invest in security improvements to its mobile infrastructure. Details of Orvilia's new mobile device security infrastructure are provided in Section 4. As described in Section 4's architecture design, Orvilia's new infrastructure addressed the concerns identified in its risk assessment. Orvilia's risk assessment team reviewed guidance by standards organizations and government agencies as part of its process and identified the standards and guidance identified in Appendix D as applicable to its organizational mobile use case.

3.3 Assumptions

This project is guided by the following assumptions:

- The solution was developed in a lab environment based on a typical organization's IT enterprise. It does not reflect the complexity of a production environment.
- An organization has access to the skills and resources required to implement a mobile device security solution.

- The benefits of adopting this particular mobile device security solution outweigh any additional performance, reliability, or security risks that may be introduced. However, we draw the reader's attention to the fact that implementation of any security controls has the potential to increase or decrease the attack surface within an enterprise, the actual impact of which will vary from organization to organization. Because the organizational environment in which this build could be implemented represents a greater level of complexity than is captured in the current guide, we assume that organizations will first examine the implications for their current environment before implementing any part of the proposed solution.
- Organizations have either already invested or are willing to invest in the security of mobile devices used within their organization and of their IT systems more broadly. As such, we assume they either have the technology in place to support this implementation or have access to the off-the shelf information security technology used in this build, which we assume will perform as described by the respective product vendor.
- Organizations have familiarized themselves with existing standards and any associated guidelines (e.g., NIST Cybersecurity Framework [5], NIST SP 800-124 Revision 2 Draft [13], NIST SP 1800-4 [14]) relevant to implementation of the solution proposed in this practice guide. We also assume that any existing technology to be used in the proposed solution has been implemented in a manner consistent with these standards.
- Organizations have instituted relevant mobile device security policies and that these will be updated based on implementation of this solution.

3.3.1 Systems Engineering

Some organizations use a systems engineering-based approach in planning and implementing their IT projects. Organizations wishing to implement IT systems are encouraged to conduct robust requirements development, taking into consideration the operational needs of each system stakeholder.

The information contained within Section 4 of this volume provides architecture details to help understand the operational capabilities of the example solution. Guidance is also provided in standards such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE) 15288:2015, *Systems and software engineering–System life cycle processes* [15]; and NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [16], which provide guidance in this endeavor. With these standards, organizations may choose to adopt only those sections that are relevant to their environment and business context.

3.4 Risk Assessment

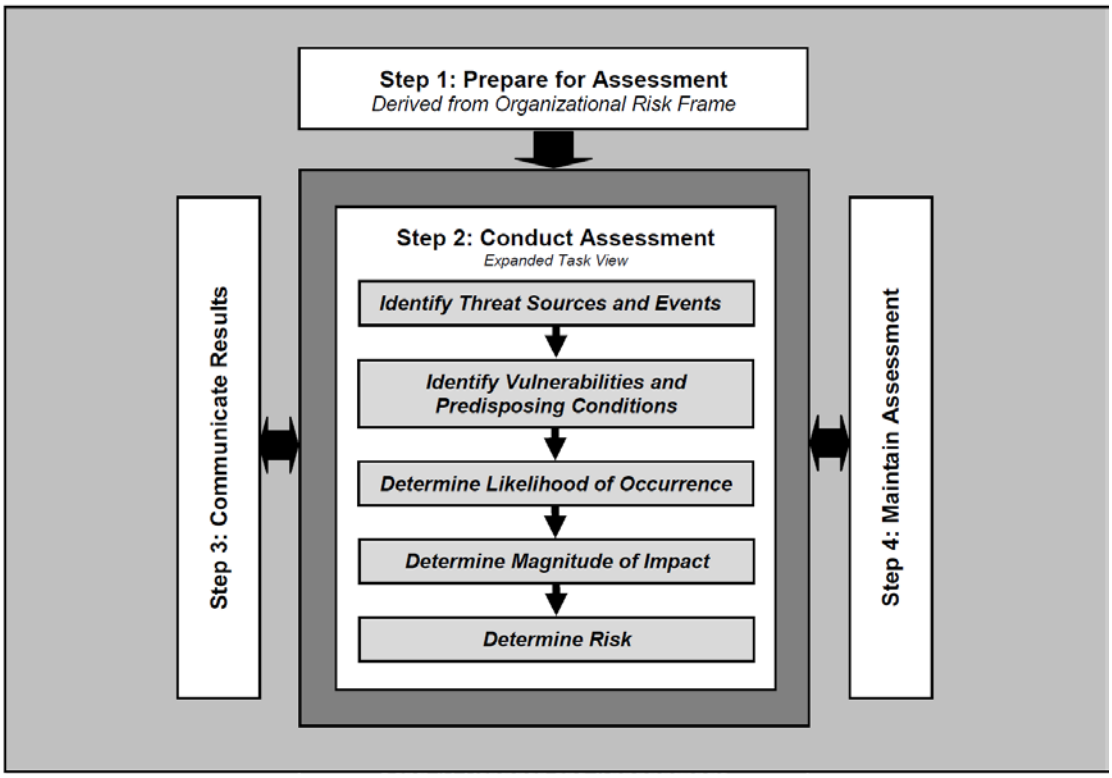
NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12], states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) 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* [17]–material that is available to the public. The Risk Management Framework (RMF) guidance [8], 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.

This section provides information on the risk assessment process employed to improve the mobile security posture of Orvilia Development. Typically, a NIST SP 800-30 Revision 1-based risk assessment follows a four-step process as shown in Figure 3-2: Prepare for assessment, conduct assessment, communicate results, and maintain assessment. Full details of the risk assessment can be found in Appendix F.

Figure 3-2 Risk Assessment Process



The purpose of Orvilia Development's risk assessment is to identify and document risk-impacting changes to its mission resulting from Orvilia's new status as a contractor to government agencies and COPE mobile deployment.

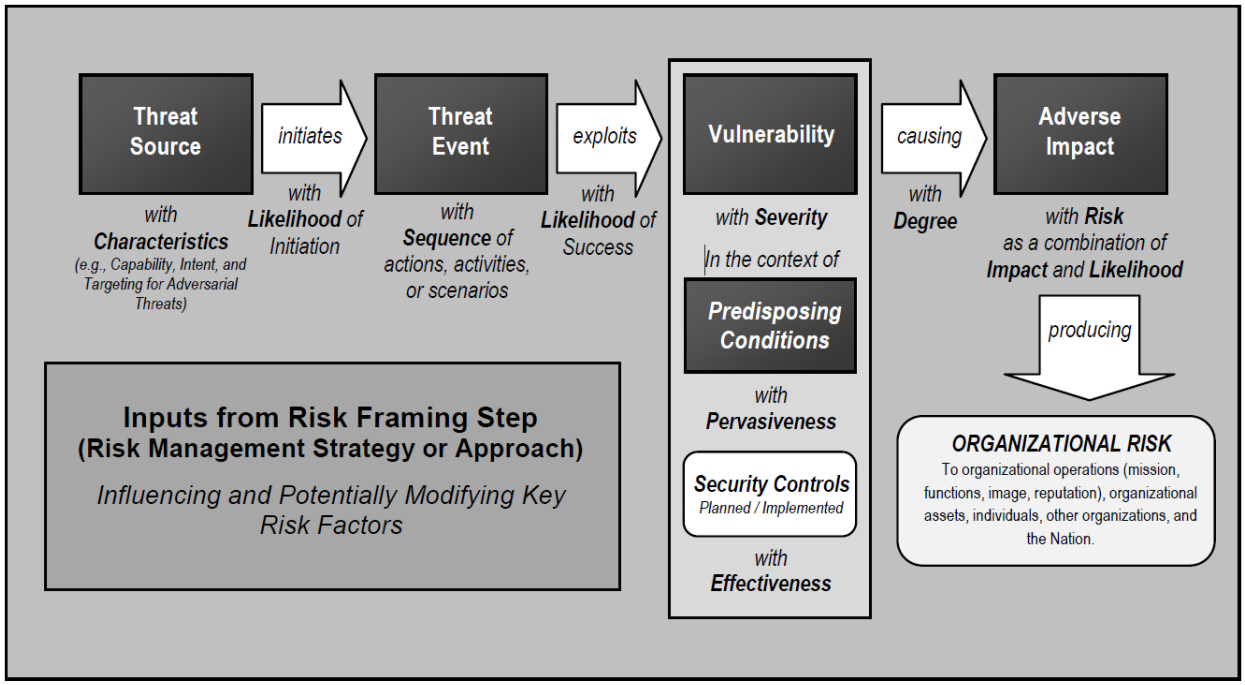
3.4.1 Risk Assessment of the Fictional Organization Orvilia Development

This risk assessment is scoped to Orvilia's mobile deployment, which consists of mobile devices used to access Orvilia enterprise resources along with any backend IT components used to manage or provide services to those mobile devices.

Risk assessment assumptions and constraints were developed using a NIST SP 800-30 Revision 1 Generic Risk Model as shown in Figure 3-3 to identify the following necessary components of the risk assessment:

- threat sources
- threat events
- vulnerabilities
- predisposing conditions
- security controls
- adverse impacts
- organizational risks

Figure 3-3 NIST 800-30 Generic Risk Model



3.4.2 Development of Threat Event Descriptions

Orvilia examined the sample tables in NIST SP 800-30 Revision 1—Table F-1, Table F-2, Table F-3, Table F-4, and Table F-5—and analyzed the sources of mobile threats. Using this process, Orvilia leadership identified the potential mobile device threat events that are described in the following subsections. A mapping of the threat events considered in this guide's example solution to the Mobile Threat Catalogue can be found in Table 3-1.

A note about selection of the threat events: These threat events were developed by identifying threats from the NIST Mobile Threat Catalogue [9] that would have the ability to significantly disrupt Orvilia's processes. In the interest of brevity, we limited our identified threat events of concern to those that were presumed to average a foreseeably high likelihood of occurrence and high potential for adverse impact in Orvilia's specific scenario. The threats from the NIST Mobile Threat Catalogue that could have less impact to Orvilia were not prioritized as high and did not become part of the following 12 threat events that Orvilia prioritized for inclusion in its mobile device security architecture.

Table 3-1 Threat Event Mapping to the Mobile Threat Catalogue

Threat Event (TE)	NIST Mobile Threat Catalogue Threat ID
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-5, AUT-10, APP-31, APP-40, APP-32, APP-2
TE-4	STA-9, APP-4, STA-16, STA-0, APP-26
TE-5	APP-32, APP-36
TE-6	STA-7, EMM-3
TE-7	CEL-18, APP-0, LPN-2
TE-8	AUT-2, AUT-4
TE-9	APP-9, AUT-0
TE-10	EMM-5
TE-11	PHY-0
TE-12	EMM-9

3.4.2.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

Summary: A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, camera roll), and general device data available to any application (e.g., International Mobile Equipment Identity , device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the operating system (OS), or device firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: Employees have access to download any applications at any time. If an employee requires an application that provides a desired function, the employee can download that application from any available source (trusted or untrusted). If an application performs an employee's desired function, they may download an application from an untrusted source whose app then requires privacy-intrusive permissions.

Level of Impact: High

Justification: Orvilia's mobile devices currently have the ability to download an application from an untrusted source whose apps require privacy-intrusive permissions. This poses a threat for sensitive corporate data, as some applications may include features that access corporate data, unbeknownst to the user.

3.4.2.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email Phishing Campaign

Summary: Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over SMS or email. Effective use of social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutiny of the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: Phishing campaigns are a common threat that occurs almost daily.

Level of Impact: High

Justification: A successful phishing campaign could provide the malicious actor with corporate credentials, allowing access to sensitive corporate data, or personal credentials that could lead to compromise of corporate data or infrastructure via other means.

3.4.2.3 Threat Event 3—Malicious Applications Installed via Uniform Resource Locators (URLs) in SMS or Email Messages

Summary: Malicious actors may send users SMS or email messages that contain a URL where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood they access the URL using their mobile device. If they do, it will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions

requested by the application. Granting the former facilitates the installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Installation of malicious applications via URLs is less common than other phishing attempts. The process for sideloading applications requires much more user input and consideration (e.g., trusting the developer certificate) than standard phishing, which solely requests a username and password. A user may proceed through the process of sideloading an application to acquire a desired capability from an application.

Level of Impact: High

Justification: Once a user installs a malicious sideloaded application, this could provide a malicious actor with full access to a mobile device, and therefore, access to corporate data and credentials, without the user's knowledge.

3.4.2.4 Threat Event 4—Confidentiality and Integrity Loss Due to Exploitation of Known Vulnerability in the OS or Firmware

Summary: When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and then issues commands in the context of the root user or the OS kernel. These commands may be enough for some to accomplish their goal, but advanced malicious actors will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the malicious actor will be able to launch further attacks against the user, the device, or any other systems connected to the device. As a result, any data stored on, generated by, or accessible to the device at that time—or in the future—may be compromised.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Many public vulnerabilities specific to mobile devices have been seen over the years, such as Stagefright. Users jailbreak iOS devices and root Android devices to download third-party applications and apply unique settings/configurations that the device would not typically be able to apply/access.

Level of Impact: High

Justification: Exploiting a vulnerability allows circumventing security controls and modifying protected device data that should not be modified. Jailbroken and rooted devices may exploit kernel vulnerabilities

and allow third-party applications/services root access that can also be used to bypass security controls built-in or applied to a mobile device.

3.4.2.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

Summary: Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System [GPS] receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as when recording any nearby sounds. Captured sensor data may be immediately useful to a malicious actor, such as a recording of an executive meeting. Alternatively, the data may be analyzed in isolation or in combination with other data to yield sensitive information. For example, audio recordings of on-device or proximate activity can be used to probabilistically determine user inputs to touchscreens and keyboards–essentially turning the device into a remote key logger.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: This has been seen on public application stores in the past, with applications allegedly being used for data collection [18]. As mentioned in Threat Event 1, unbeknownst to the user, a downloaded application may be granted privacy-intrusive permissions that allow access to device sensors.

Level of Impact: High

Justification: When the sensors are being misused, the user may not be aware. This allows collection of sensitive enterprise data, such as location, without knowledge of the user.

3.4.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Summary: Malicious actors who successfully install an Enterprise Mobility Management/Mobile Device Management (EMM/MDM), network, or VPN profile or certificate onto a device will gain a measure of additional control over the device or its communications. Presence of a malicious EMM/MDM profile will allow an attacker to misuse existing OS application programming interfaces (APIs) to send the device a wide variety of commands. This may allow a malicious actor to obtain device information; install or restrict applications; or remotely locate, lock, or wipe the device. Malicious network profiles may allow a malicious actor to automatically compel the device to connect to access points under their control to achieve a person-in-the-middle attack on all outbound connections. Alternatively, malicious VPN profiles assist in the undetected exfiltration of sensitive data by encrypting it, thus hiding it from network scanning tools. Additionally, malicious certificates may allow the malicious actor to compel the device to

automatically trust connections to malicious web servers, wireless access points, or installation of applications under the attacker's control.

Risk Assessment Analysis:

Overall Likelihood: Moderate

Justification: Unlike installation of an application, installation of EMM/MDM, network, VPN profiles, and certificates requires additional effort and understanding from the user to properly implement.

Level of Impact: Very High

Justification: If a malicious actor were able to install malicious configuration profiles or certificates, they would be able to perform actions such as decrypt network traffic and possibly even control the device.

3.4.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Summary: Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, a malicious actor would gain unauthorized access to any data sent or received by the device for any session not already protected by encryption at either the transport or application layers. Even if the transmitted data were encrypted, an attacker may be privy to the domains, internet protocol (IP) addresses, and services (as indicated by port numbers) to which the device connects; such information could be used in future watering hole attacks or person-in-the-middle attacks against the device user.

Additionally, visibility into network layer traffic enables a malicious actor to conduct side-channel attacks against its encrypted messages, which can still result in a loss of confidentiality. Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session with another host or endpoint may facilitate attacks that ultimately compromise security of the session.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Users require network access to retrieve email and access cloud services and other necessary data on the internet. Users can connect to readily available free internet access in public venues such as coffee shops, hotels, and airports.

Level of Impact: High

Justification: Users may connect to unencrypted wireless networks, and many applications do not properly encrypt network communications. Improper use of encryption, or lack thereof, allows a malicious actor to eavesdrop on network traffic.

3.4.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

Summary: A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, side-channel attacks that infer the unlock code by detecting taps and swipes to the screen can be attempted by applications with access to any peripherals that detect sound or motion (microphone, gyroscope, or accelerometer). Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the attacker may further gain unauthorized access to those systems.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Unlike shoulder-surfing to observe a user's passcode, brute-force attacks are not as common or successful due to the built-in deterrent mechanisms. These mechanisms include exponential back-off/lockout period and device wipes after a certain number of failed unlock attempts.

Level of Impact: High

Justification: If a malicious actor can successfully unlock a device without the user's permission, they could have full control over the user's corporate account and thus gain unauthorized access to corporate data.

3.4.2.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

Summary: If a malicious actor gains unauthorized access to a mobile device, the attacker also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: Often applications include hard-coded credentials for the default password of the administrator account. Default passwords are readily available online. These passwords may not be changed to allow for ease of access and to eliminate the pressure of remembering a password.

Level of Impact: High

Justification: Successful extraction of the credentials allows an attacker to gain unauthorized access to enterprise data.

3.4.2.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

Summary: An employee who accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by a malicious actor. Therefore, users who violate security policies to gain unauthorized access to enterprise resources from such devices risk providing attackers with access to sensitive organizational data, services, and systems.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: This may occur accidentally when an employee attempts to access their email.

Level of Impact: High

Justification: Unmanaged devices pose a sizable security risk because the enterprise has no visibility into their security or risk posture. Due to this lack of visibility, a compromised device may allow an attacker to attempt to exfiltrate sensitive enterprise data.

3.4.2.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device

Summary: Due to the nature of the small form factor of mobile devices, they can be misplaced or stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: Mobile devices are small and can be misplaced. Enterprise devices may be lost or stolen at the same frequency as personally owned devices.

Level of Impact: High

Justification: Similar to Threat Event 9, if a malicious actor can gain access to the device, they could potentially have access to sensitive corporate data.

3.4.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its Unauthorized Storage in Non-Organizationally Managed Services

Summary: If employees violate data management policies by using unmanaged services to store sensitive organizational data, this data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from the public disclosure of trade secrets.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: This could occur either intentionally or accidentally (e.g., taking a screenshot and backup pictures to an unmanaged cloud service).

Level of Impact: High

Justification: Storage in unmanaged services presents a risk to the confidentiality and availability of corporate data because the corporation would no longer control it.

3.4.3 Identification of Vulnerabilities and Predisposing Conditions

In Section 3.4, we identified vulnerabilities and predisposing conditions that increase the likelihood that identified threat events will result in adverse impacts for Orvilia Development. Each vulnerability or predisposing condition is listed in Table 3-2 along with the corresponding threat events and ratings of threat pervasiveness. More details on the use of threat event ratings can be found in Appendix F.

Table 3-2 Identify Vulnerabilities and Predisposing Conditions

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-10, TE-11	Very High

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their corporate mobile devices.	TE-7	Very High
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on corporate mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Very High

3.4.4 Summary of Risk Assessment Findings

Table 3-3 summarizes the risk assessment findings. More detail about the methodology used to rate overall likelihood, level of impact, and risk can be found in Appendix F.

Table 3-3 Summary of Risk Assessment Findings

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	Very High	High	High
TE-2: Theft of credentials through an SMS or email phishing campaign	VULN-1	Very High	High	High
TE-3: Malicious applications installed via URLs in SMS or email messages	VULN-3	High	High	High
TE-4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	High	High	High
TE-5: Violation of privacy via misuse of device sensors	VULN-3	Very High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	VULN-3	Moderate	Very High	High
TE-7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2, VULN-3	High	High	High
TE-8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	High	High	High
TE-9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	Very High	High	High
TE-10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1	Very High	High	High
TE-11: Loss of organizational data due to a lost or stolen device	VULN-1, VULN-3	Very High	High	High
TE-12: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	High	High	High

Note 1: Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST Special Publication 800-30 Revision 1 [12].

Note 2: The risk rating itself is derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST Special Publication 800-30 Revision 1 [12]. Because these scales are not true

interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two variables. This is demonstrated in the table above where levels of moderate weigh more heavily than other ratings.

Note 3: Ratings of risk relate to the probability and level of adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1, adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e., very high).

3.4.5 Privacy Risk Assessment

This section describes the privacy risk assessment conducted on Orvilia's enterprise security architecture. To perform the privacy risk assessment, the NIST Privacy Risk Assessment Methodology (PRAM) was used. The PRAM is a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. The PRAM can also serve as a useful communication tool to convey privacy risks within an organization. A blank version of the PRAM is available for download on NIST's website [19].

The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal Report (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [20], to analyze for problematic data actions. Data actions are any system operations that process PII. Processing can include collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of PII. A problematic data action is one that could cause an adverse effect for individuals. The PRAM activities identified the following potential problems for individuals.

3.4.5.1 Potential Problems for Individuals

Three data actions were identified in the PRAM that have the potential to create problems for individuals. Those three data actions, along with their risk assessment analysis, follow:

- blocking access and wiping devices
- employee monitoring
- data sharing across parties

3.4.5.1.1 Data Action 1: Blocking Access and Wiping Devices

Employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data. This is a potential problem for individuals because employee use of work devices for both personal and work-related purposes is common.

Devices that might pose a risk to the organization's security posture can be blocked from accessing enterprise resources or wiped and reset to factory setting defaults, which could result in loss of information contained on the device. Potential options for minimizing the impact to the employee include:

- blocking the device's access to enterprise resources until it is granted access permission again
- selectively wiping elements of the device without removing all data on the device. Within the example solution, this option is available for iOS devices.
- advising employees to back up the personal data maintained on devices
- limiting staff with the ability to perform wipes or block access

3.4.5.1.2 Data Action 2: Employee Monitoring

Employees may not be aware of the monitoring of their interactions with the system and may not want this monitoring to occur. Employer-owned or -controlled networks like Orvilia's often can monitor activities, and many do on a regular basis.

The assessed infrastructure offers Orvilia a number of security capabilities, including reliance on comprehensive monitoring capabilities. A significant amount of data relating to employees, their devices, and their activities is collected and analyzed by multiple parties. Potential options for minimizing the impact to the employee include:

- limit staff with ability to review data about employees and their devices
- develop organization policies and techniques to limit collection of specific data elements
- develop organization policies and techniques regarding disposal of PII

3.4.5.1.3 Data Action 3: Data Sharing Across Parties

Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them.

The infrastructure involves several parties that serve different purposes supporting Orvilia's security objectives. As a result, a significant flow of data about individuals and their devices occurs across various parties.

If a wide audience of administrators and co-workers know which of their colleagues are conducting activity on their devices that triggers security alerts, it could lead to undesired outcomes such as employee embarrassment. Potential options for minimizing the impact to the employee include:

- developing organization policies and techniques for the de-identification of data
- using encryption
- limiting or disabling access to data

- developing organization policies and techniques to limit the collection of specific data elements
- using contracts to limit third-party data processing

Additional information regarding these potential problems for individuals and potential options for minimizing the impact to the employees is provided in Appendix G.

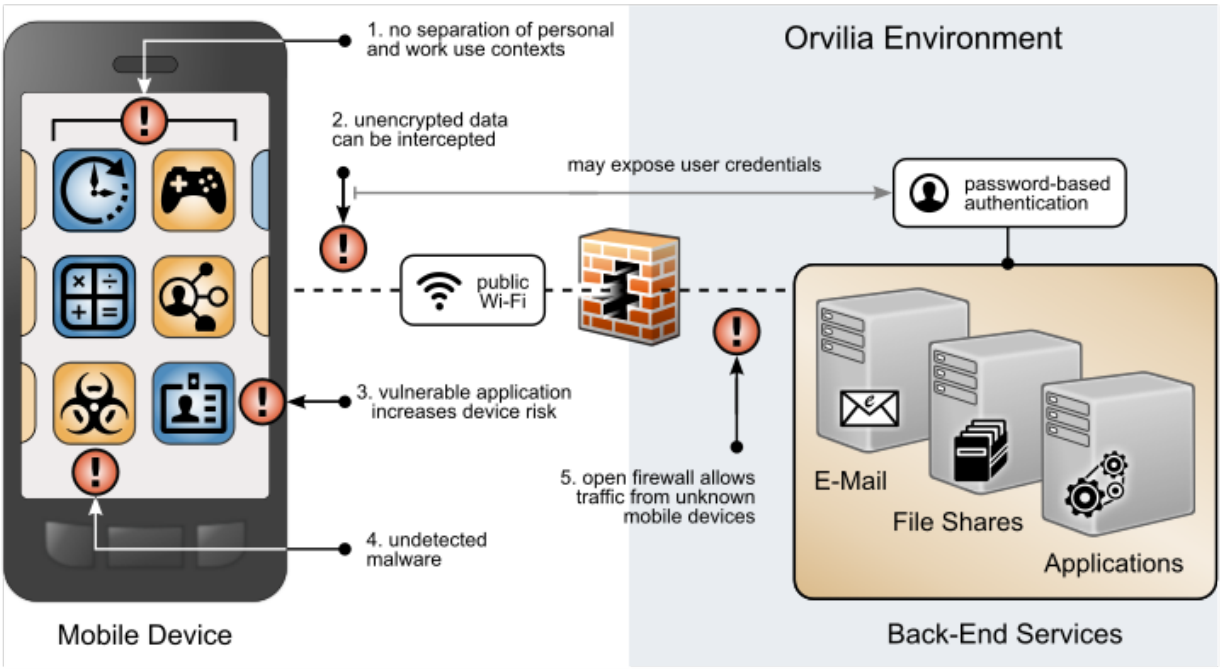
3.5 Solution Goals

This section describes the solution goals for revising Orvilia's mobile security architecture. Here is an overview of the security issues identified within Orvilia's original (also known as current) mobile device infrastructure architecture. To address these issues, a list of security goals was developed to provide a high-level overview of factors that could be applied to improve the security of Orvilia's mobile architecture.

3.5.1 Current Architecture

Prior to investing in security improvements to their mobile infrastructure—as identified based on the aforementioned risk assessment—Orvilia Development had not implemented a mobile security strategy. Several weaknesses were identified based on their use of mobile devices. A subset of these weaknesses is presented in Figure 3-4.

Figure 3-4 Orvilia's Mobile Deployment Before Security Enhancements



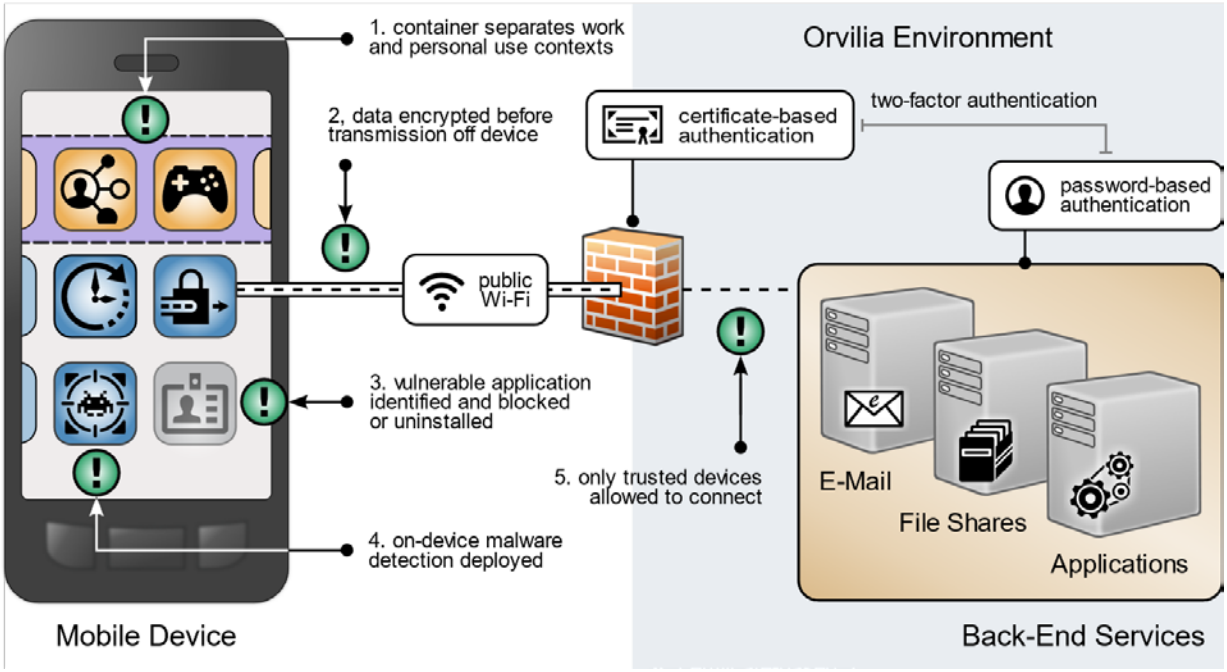
The following issues are highlighted in Figure 3-4 with a red exclamation mark:

1. Organizational and personal data can become commingled if either the same application is used in both contexts or if multiple applications access shared device resources (e.g., contacts or calendar).
2. Mobile devices are connecting to Orvilia from unencrypted public Wi-Fi hotspots; data transmitted prior to a secure connection is subject to eavesdropping, including passwords.
3. Applications for work or personal use may contain unidentified vulnerabilities or weaknesses that increase the risk of device compromise.
4. Applications may be obtained outside official application stores, increasing the risk that they are malware in disguise.
5. Because mobile devices can connect from unknown locations, firewall rules must allow inbound connections from unrecognized, potentially malicious IP addresses.

3.5.2 Security Goals

In considering improvement to the security of their current deployment, Orvilia was able to identify high-level security goals to correct these shortcomings, as illustrated in Figure 3-5.

Figure 3-5 Orvilia's Security Goals



The following strategies are highlighted in Figure 3-5 with a green exclamation mark:

1. Organizational and personal information can be separated by restricting data flow between organizationally managed and unmanaged applications. Sensitive data is protected from crossing between work and personal contexts.
2. Mobile devices can connect to Orvilia over a VPN or similar solution to encrypt all data before it is transmitted from the device, protecting otherwise unencrypted data from interception.
3. Identifying applications with significant vulnerabilities or weaknesses facilitates blocking or uninstalling those applications from managed devices, reducing their risk to the organization.
4. Malware detection could be deployed to devices to identify malicious applications and facilitate remediation.

5. Mobile devices can be provisioned with a security certificate that allows them to be identified and authenticated at the connection point, which combines with user credentials to create two-factor authentication from mobile devices.

These high-level goals, obtained from a review of their current mobile security posture, provide examples of why a thorough risk assessment process is beneficial to organizations implementing mobile device security capabilities.

3.6 Technologies

This section describes the mobile-specific technology components used within this example solution. These technologies were selected to address the security goals and threat events identified in the risk assessment. This section provides a brief description of each technology and discusses the security capabilities that each component provides to address Orvilia's security issues. For additional information, Appendix I provides the technologies used in this project and provides a mapping between the specific product used and the cybersecurity standards and best practices that the product provides in the example solution discussed in this guide.

3.6.1 Architecture Components

The security components in this section are combined into a cohesive enterprise security architecture to enable enterprises to address mobile security threats and provide secure access to enterprise resources from mobile devices. The security components described in this section provide protection for the following enterprise architecture components that are accessed by Orvilia's users with their mobile devices.

- email/Outlook Web Access–contacts
- private chat server
- travel support
- organization intranet (e.g., internal announcements, organizational charts, policies)
- time reporting

3.6.1.1 Trusted Execution Environment

A trusted execution environment (TEE) is "a tamper-resistant processing environment that runs on a separation kernel. It guarantees the authenticity of the executed code, the integrity of the runtime states (e.g., central processing unit registers, memory and sensitive I/O), and the confidentiality of its code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide remote attestation that proves its trustworthiness for third-parties [21]."

3.6.1.2 Enterprise Mobility Management

Organizations use Enterprise Mobility Management solutions to secure the mobile devices of users who are authorized to access organizational resources. Such solutions generally have two main components. The first is a backend service that mobile administrators use to manage the policies, configurations, and security actions applied to registered mobile devices. The second is an on-device agent, usually in the form of a mobile application, that integrates between the mobile OS and solution's backend service. Alternatively, iOS supports a web-based EMM enrollment use case.

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

EMM solutions commonly include any of the following: mobile application management, mobile content management, and implementations of or integrations with device- or mobile OS-specific containerization solutions, such as Samsung Knox (please refer to Appendix E for more information). These capabilities can be used to manage installation and usage of applications based on the applications' trustworthiness and work relevance. Additionally, they can control how managed applications access and use organizational data and possibly strengthen the separation between a user's personal and professional usage of the device.

Further, EMM solutions often have integrations with a diverse set of additional tools and security technologies that enhance their capabilities. An example is an EMM embedded with a mobile threat defense tool that serves to perform on-device, behavioral-based threat detection and to trigger policy remediation without the need to communicate to any server or service outside the device. This type of integration allows one application, the EMM agent, to manage, detect, and remediate device, network, application, malware, and spear phishing attacks. Additionally, because the remediation is autonomous at the device (does not require reaching a policy server), it has the advantage in addressing network-based threat vectors such as Pineapple or Stingray impersonation of valid Wi-Fi or cellular networks [22].

For further reading, NIST SP 800-124 Revision 2 Draft, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [13], provides additional information on mobile device management with EMM solutions. Additionally, NIAP's *Protection Profile for Mobile Device Management Version 4.0* [23] describe important capabilities and security requirements to look for in EMM systems.

3.6.1.3 Virtual Private Network

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

VPN connections apply an additional layer of encryption to the communication between remote devices and the internal network, and VPN gateways can enforce access control decisions by limiting which devices or applications can connect to it. Integration with other security mechanisms allows a VPN gateway to base access control decisions on more risk factors than it may be able to collect on its own; examples include a device's level of compliance with mobile security policies or the list of installed applications that are not allowed by the organization as reported by an integrated EMM.

NIAP's *Extended Package for VPN Gateways* [24], in combination with the internationally and collaboratively developed *Protection Profile for Network Devices* [25], describes important capabilities and security requirements to expect from VPN gateways.

3.6.1.4 Mobile Application Vetting Service

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

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

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

NIAP does not provide a Protection Profile for application vetting services themselves. However, NIAP's *Protection Profile for Application Software* [26] describes security requirements to be expected from mobile applications. Many mobile application vetting vendors provide capabilities to automate evaluation of applications against NIAP's requirements.

3.6.1.5 Mobile Threat Defense

MTD generally takes the form of an application that is installed on the device, which provides the widest and most timely access to information about what activity is taking place. Ideally, the MTD solution will be able to detect unwanted activity and properly inform the user so they can act to prevent or limit the harm an attacker could cause. Additionally, MTD solutions may integrate with EMM solutions to leverage the EMM agent's on-device capabilities, such as blocking a malicious application from being launched until the user can remove it.

MTD products typically analyze device-based, application-based, and network-based attacks. Device-based threats include outdated operating system versions and insecure configuration settings. Application-based threats include the issues discussed above regarding the mobile application vetting service, though sometimes without the same breadth or depth found in services dedicated to application vetting. Network-based attacks include use of unencrypted or public Wi-Fi networks and attacks such as active attempts to intercept and decrypt network traffic.

3.6.1.6 Mobile Threat Intelligence

In this guide, we describe mobile threat intelligence as actionable information that mobile administrators can use to make changes to their security configuration to improve their posture relative to recent discoveries. Intelligence data include malicious URLs, IP addresses, domain names, and application names or package/bundle IDs, as well as malware signatures or vulnerabilities in applications, mobile devices, device platform services, or mobile security products. This list is not all-encompassing, as any recent information that could inform rapid changes to enable an enterprise to better secure a mobile deployment against novel or newly enhanced threats is equally applicable to the term. This capability may be found in various other types of technology, such as MTD and other network analysis tools.

3.6.1.7 Mobile Operating System Capabilities

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

3.6.1.7.1 Secure Boot

Secure boot is a general term that refers to a system architecture designed to prevent and detect any unauthorized modification to the boot process. A system that successfully completes a secure boot has loaded its start-up sequence information into a trusted operating system. A common mechanism is for the first program executed (a boot loader) to be immutable (stored on read-only memory or implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified prior to execution by either immutable or verified code. This process establishes a chain of trust that can be traced back to immutable, implicitly trustworthy code. Use of an integrated TEE as part of a secure boot process is preferable to an implementation that uses software alone [27].

3.6.1.7.2 Device Attestation

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

Device attestation requires cryptographic operations using an immutable private key that can be verified by a trusted third party, which is typically the original equipment manufacturer of the TEE (e.g., Qualcomm or Samsung) or device platform vendor (e.g., Google, Apple, or Microsoft). Proof of possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique device identifiers, metadata, and the results of integrity checks on mutable software, and possibly metrics from the boot or attestation process itself [27].

3.6.1.7.3 Device Management and MDM API

Mobile operating systems and platform-integrated firmware (e.g., Samsung Knox) provide a number of built-in security features that are generally active by default. Examples include disk and file-level encryption, verification of digital signatures for installed software and updates, a device unlock code, remote device lock, and automatic device wipe following a series of failed device unlock attempts. Some of these features are directly configurable by the user via a built-in application or through a service provided by the device platform vendor (e.g., Google, Apple, or Microsoft).

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

4 Architecture

This section helps familiarize the reader with the example solution's:

- architecture description
- enterprise security architecture privacy data map
- security control map

This example solution consists of the six mobile security technologies described in Section 3.6: trusted execution environment, enterprise mobility management, virtual private network, mobile application vetting service, mobile threat defense, and mobile threat intelligence. Table 4-1, identifies the commercially available products used in this example solution and how they aligned with the six mobile security technologies.

Table 4-1 Commercially Available Products Used

Commercially Available Product	Mobile Security Technology
Appthority Cloud Service	Mobile threat intelligence
Kryptowire Cloud Service	Mobile application vetting service
Lookout Cloud Service/Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android)	Mobile threat defense
MobileIron Core Version 9.7.0.1 MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android)	Enterprise mobility management
Palo Alto Networks, PA-220 Version 8.1.1	Virtual private network
Qualcomm, (version is mobile device dependent)	Trusted execution environment

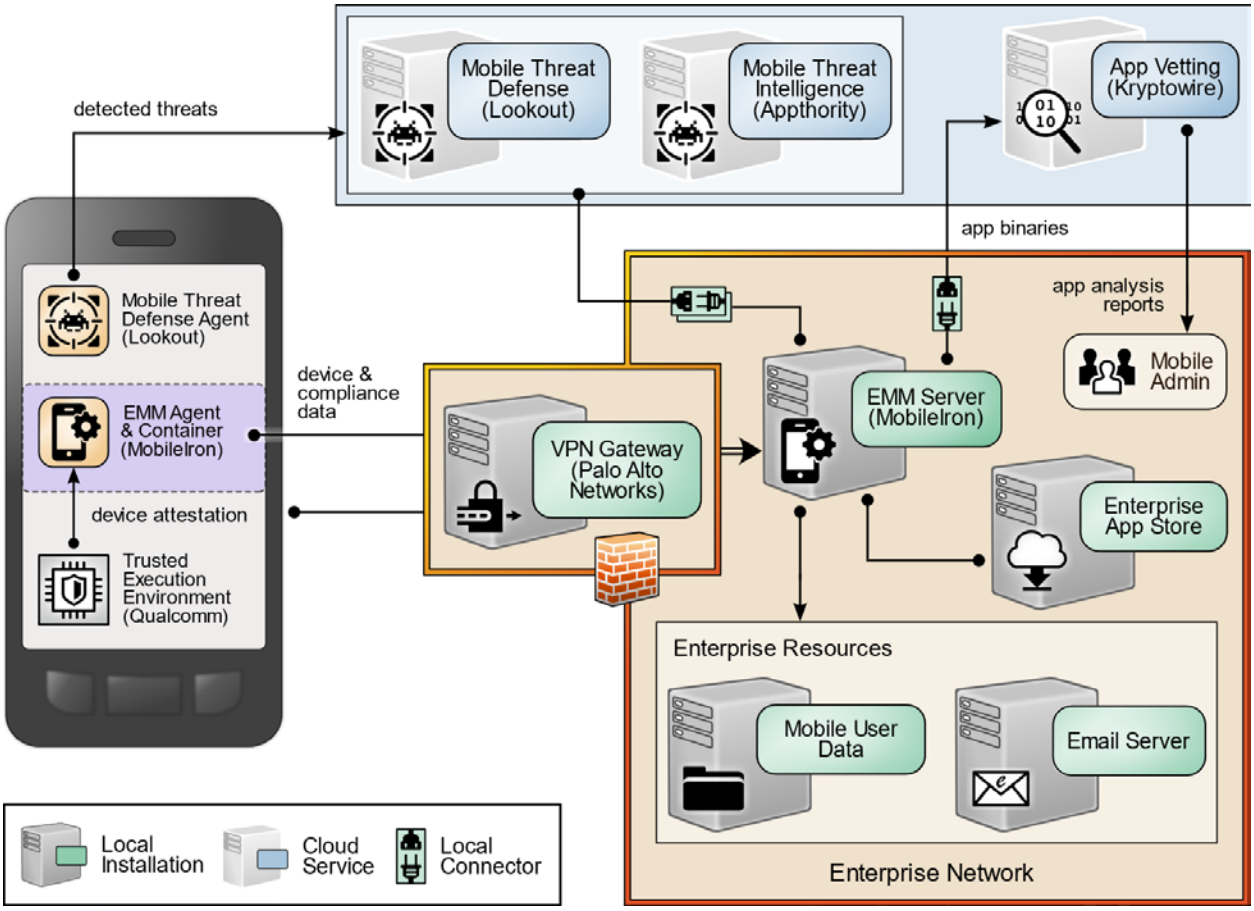
These components are further integrated with broader on-premises security mechanisms and a VPN gateway as shown in Figure 4-1. This integrated solution provides a broad range of capabilities to help

securely provision and manage devices, protect against and detect device compromise, and help provide security-enhanced access to enterprise resources by only authorized mobile users and devices.

Organizations exploring the use of on-premises EMM technology should be aware they will be responsible for installing and configuring the on-premises instances of the EMM technology. This will include the software licenses that must be paid for directly by the organization for any underlying platforms or components. Pre-built software images and containers may be available that can help ease installation and configuration work. As a recommended best practice, if prebuilt containers and images are used, it is recommended that they be checked for common software vulnerabilities.

On-premises mobile device management solutions offer the benefit that enterprise data resides within the organization. Allowed devices may still send and receive information from the mobile device solution that they are authorized to obtain. Organizations that are interested can explore monitoring data flows from the EMM to other devices. Additionally, on-premises mobile device management solutions provide the organization with the capability to maintain physical security of the EMM.

Figure 4-1 Example Solution Architecture



4.1 Architecture Description

The NCCoE worked with industry subject matter experts to develop an open, standards-based, commercially available architecture that addresses the risks identified during the risk assessment process in Section 3.4.

Where possible, the architecture uses components that are present on NIAP's Product Compliant List [28], meaning the product has been successfully evaluated against a NIAP-approved Protection Profile [26]. NIAP collaborates with a broad community, including industry, government, and international partners, to publish technology-specific security requirements and tests in the form of Protection Profiles. The requirements and tests in these Protection Profiles are intended to ensure that evaluated products address identified security threats.

The example solution architecture supports its desired security characteristics as a result of the following integrations.

4.1.1 Enterprise Integration

This example solution extends central identity and access management to mobile devices via an integration between both MobileIron Core and Palo Alto Networks GlobalProtect with Microsoft Active Directory Domain Services (ADDS). The integrity of identification and authentication by mobile devices to the enterprise is further enhanced by using device certificates issued by local Microsoft Active Directory Certificate Services (ADCS).

By integrating with AD, MobileIron Core allows administrators to authorize select groups of users to register a mobile device, limiting mobile access to only those users who require it. Additionally, different security policies, device configurations, and authorized applications can be deployed to different AD groups, allowing administrators to centrally manage distinct mobile use cases. MobileIron Core queries AD using the lightweight directory access protocol.

Through its integration with ADCS, MobileIron Core automatically configures devices to obtain locally managed device certificates by using the Simple Certificate Enrollment Protocol (SCEP). Our example solution mitigates the potential of remote exploitation of SCEP by restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network that allows devices to access only MobileIron Core and the Network Device Enrollment Service server. Further, this example solution uses a dynamic SCEP scheme, in which MobileIron Core supplies a registered mobile device with a onetime password to include in its SCEP request, thus helping prevent unknown and untrusted devices that gain unauthorized access to the dedicated Wi-Fi network from obtaining a trusted device certificate.

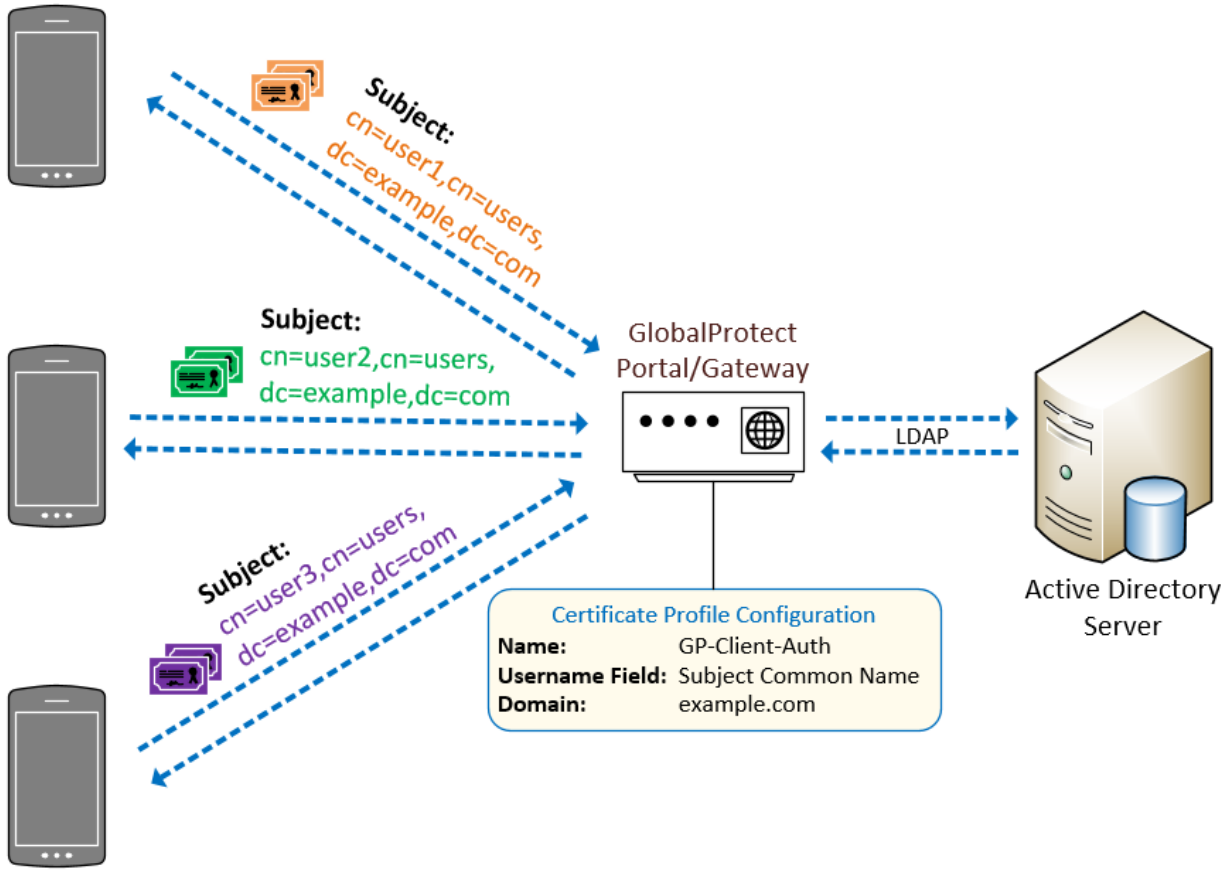
The example solution's chosen certificate enrollment configuration includes the mobile user's User Principal Name (UPN) in the device certificate's Subject Alternative Name field, which the Palo Alto

Networks GlobalProtect VPN gateway uses to perform chain validation and enforce access control for the unique combination of mobile user and device.

MobileIron Core-registered devices also utilize the device certificate indirectly to enhance the security of remote connections to the enterprise in two ways. First, communication with MobileIron Core (which must be accessible from the internet in the demilitarized zone) is secured using two-way Transport Layer Security (TLS). This protects MobileIron Core from establishing secure connections with untrusted mobile devices. Second, the device certificate is used in the GlobalProtect VPN configuration, which restricts access to the VPN to only trusted devices. Further, GlobalProtect uses the device user's UPN to grant appropriate access to enterprise resources based on the device user's UPN through its integration with ADDS.

As shown in Figure 4-2 [29], devices present the certificates to the VPN and EMM authentication services after the certificates have been successfully issued. The GlobalProtect VPN authenticates the device user. On successful authentication, the GlobalProtect application prompts the user to authenticate using a second factor–their Active Directory domain password. Once this is verified, GlobalProtect establishes a tunnel with the gateway and is assigned an IP address from the IP pool in the gateway's tunnel configuration.

Figure 4-2 Example Solution Gateway Architecture



4.1.2 Mobile Component Integration

This section describes how the various mobile technology components integrate with one another. The majority of these components integrate with the EMM, MobileIron. MobileIron supports the integration of third-party cloud services through a defined API. MobileIron Core authenticates external systems by using basic authentication, so TLS protects the confidentiality of API account credentials and MobileIron's responses to clients' Representational State Transfer calls. MobileIron API client accounts for Kryptowire, Lookout Mobile Endpoint Security, and Appthority Mobile Threat Protection (MTP) are each assigned administrative roles that grant the minimum set of permissions necessary to achieve integration [30], [31].

4.1.2.1 Appthority–MobileIron

The Appthority application reputation service provides an integration with MobileIron Core systems through implementation of connector software provided by Appthority. The connector provides the

code that exercises the APIs provided by MobileIron Core and the Appthority cloud service. In this integration, an API user was created within the MobileIron Core system and assigned specific roles required for successful operation of the application vetting service.

Automatic syncing between the Appthority service and MobileIron Core system can occur on a configurable basis. Specifically, the application and device inventory data are synced between the two systems. In this integration, syncing occurs every hour, but this value should be adjusted to fit the needs of the organization.

In this example solution, the integration provides the primary security benefit of compliance enforcement and remediation escalation. In the initial step of the process, the application inventory is gathered from the MobileIron Core system, and each application is assigned a threat measurement score. If an application is installed on a device that is not compliant with the configured policy, Appthority MTP communicates with the MobileIron Core system to identify those devices, which triggers MobileIron compliance enforcement actions.

4.1.2.2 Lookout–MobileIron

The Lookout mobile threat defense service provides integration with MobileIron Core systems through implementation of connector software provided by Lookout. The connector provides the code that exercises the APIs provided by MobileIron Core and the Lookout cloud service. This integration allows Lookout to retrieve device details as well as application inventory information and to apply labels to devices as necessary.

Following analysis, Lookout uses the API to apply specific labels to devices to categorize them based on risk posture, which is calculated based on the severity of issues detected on the device. MobileIron can then automatically respond to application of specific labels based on built-in compliance actions. This allows administrators to configure exactly how MobileIron will respond to devices in the following categories:

- Pending–Lookout not yet activated
- Secured–Lookout active
- Threats Present–Lookout has detected threats
- Deactivated–Lookout has been deactivated
- Low Risk–devices with a low risk score in Lookout
- Moderate Risk–devices with a moderate risk score in Lookout
- High Risk–devices with a high-risk score in Lookout

4.1.2.3 Kryptowire–MobileIron

Kryptowire obtains device details, such as device platform, OS version, and the universally unique identifiers assigned to each registered device by MobileIron Core to enable clear identification of a particular device across systems. Kryptowire obtains the inventory of applications from all of the devices enrolled in MobileIron.

Kryptowire performs static, dynamic, and behavioral binary code analysis on mobile applications against government (NIAP) and industry (The Open Web Application Security Project, or OWASP) [32] standards. Kryptowire provides both a detailed security analysis, provides pass/fail evidence down to the line of code, and provides a summary weighted risk score for each application.

Mobile application administrators can use these detailed reports to inform decisions on which applications are trusted and compliant with enterprise security and privacy policies and which are restricted for enterprise or personal use.

4.1.2.4 Palo Alto Networks–MobileIron

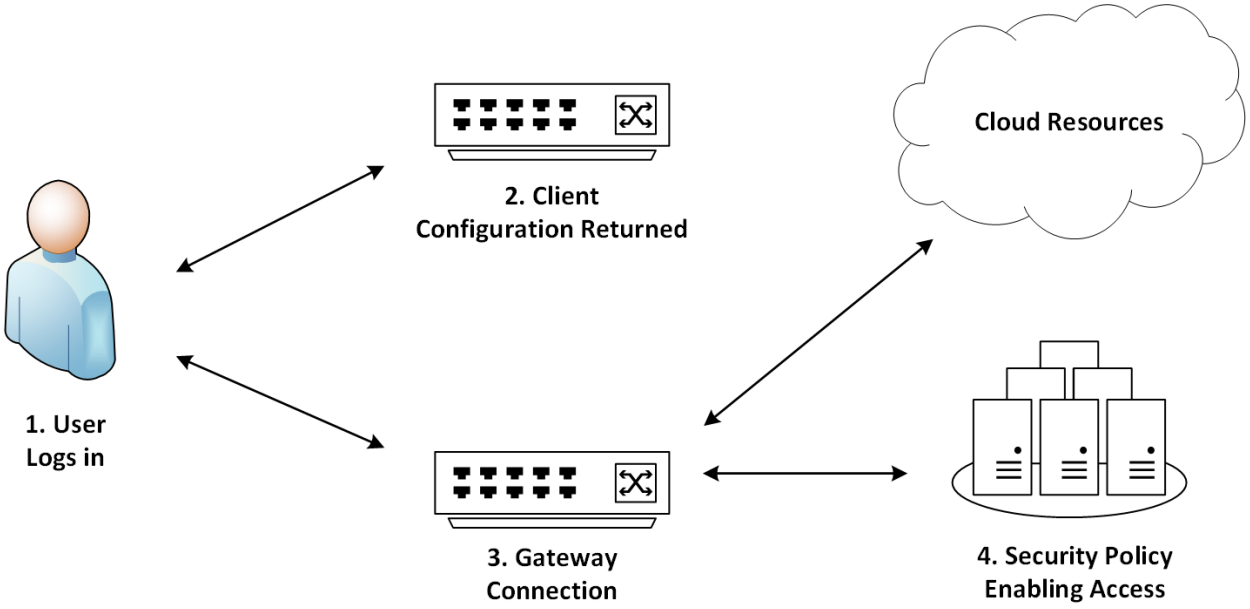
Palo Alto Networks' GlobalProtect VPN is used to secure remote connections from mobile devices. MobileIron Core offers specific configuration options for the GlobalProtect client available on Android and iOS that facilitates secure deployment of VPN clients and enablement of VPN access using certificate-based authentication to the GlobalProtect gateway. Details of the certificate enrollment process are provided in Section 4.1.1

The VPN architecture used in this example solution is composed of two components of the Palo Alto Networks next-generation firewall–a GlobalProtect portal and a GlobalProtect gateway. The portal provides the management functions for VPN infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s).

The gateway provides security enforcement for traffic from GlobalProtect applications. It is configured to provide access to specific enterprise resources only to mobile device users after a successful authentication and authorization decision.

The VPN tunnel negotiation between the VPN endpoint/mobile device and the VPN gateway is presented in Figure 4-3 [33]. It demonstrates a user logging into the system (1), the portal returning the client configuration (2), the agent automatically connecting to the gateway and establishing a VPN tunnel (3), and the gateway's security policy enabling access to internal and external applications (4).

Figure 4-3 Example Solution VPN Architecture



For our example solution, we chose to enforce an always-on VPN configuration. This configuration causes registered devices to establish a VPN connection to the GlobalProtect gateway whenever they have network connectivity–this occurs over cellular or Wi-Fi and is persistent across device reboot. This configuration affords devices with the greatest degree of protection, as additional Palo Alto Networks services can be extended to GlobalProtect. This example solution uses URL filtering, which blocks mobile devices from accessing prohibited internet domains or any domain that Palo Alto Networks associates with active exploits (e.g., phishing campaigns, watering hole attacks, botnet command and control). NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and BYOD Security* [34], describes the most common VPN options used for remote workers.

4.1.2.4.1 FIPS Compliance

Any sensitive information passing over the internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through cryptography [34]. While federal agencies are required to use cryptographic algorithms that are NIST-approved and contained in Federal Information Processing Standards (FIPS)-validated modules, adoption of these standards is available to private and commercial organizations [35]. This example solution uses these best practices in the following ways:

- *FIPS-CC* mode in the GlobalProtect VPN appliance is enabled, which requires TLS 1.1 (or above) and limits the public key use to FIPS-approved algorithms. This example solution's implementation uses the highest version of TLS available, with TLS 1.2 being the minimum

acceptable version. A full list of security functions can be found on the Palo Alto Networks FIPS-CC Security Functions documentation site [36].

- As described in Section 4.1.1, dynamic SCEP challenges are enabled.

To align our example solution with guidance in NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [37], this example solution implements the following configuration:

- The GlobalProtect portal and gateway restrict the list of cipher suites available to the client application by using a TLS service profile. The minimum version of TLS is set to 1.2 as recommended by NIST SP 800-52.
- The GlobalProtect portal and gateway server certificates use 2048-bit RSA key modulus signed with *sha256WithRSAEncryption* algorithm.

4.1.2.5 iOS and Android EMM Integration

iOS and Android-based devices both integrate directly with EMM solutions, providing enterprise-level management of security controls based on policy.

iOS Integration

iOS devices are managed by configuration profiles. Configuration profiles can force security policies such as VPN usage, enterprise Kerberos support, and access to cloud services. iOS further incorporates a set of additional security controls in what is termed *supervised* mode, which denotes a corporately owned device. Typically, organizations choose to use the Apple Business Manager (formerly Device Enrollment Program) [38] for large-scale deployments of iOS devices in *supervised* mode due to the reduction of labor involved in manually configuring each device. However, due to the small number of devices in our reference design, we have configured *supervised* mode using the Apple Configurator 2 tool [39]. A description of iOS security capabilities can be found in Apple Platform Security [40].

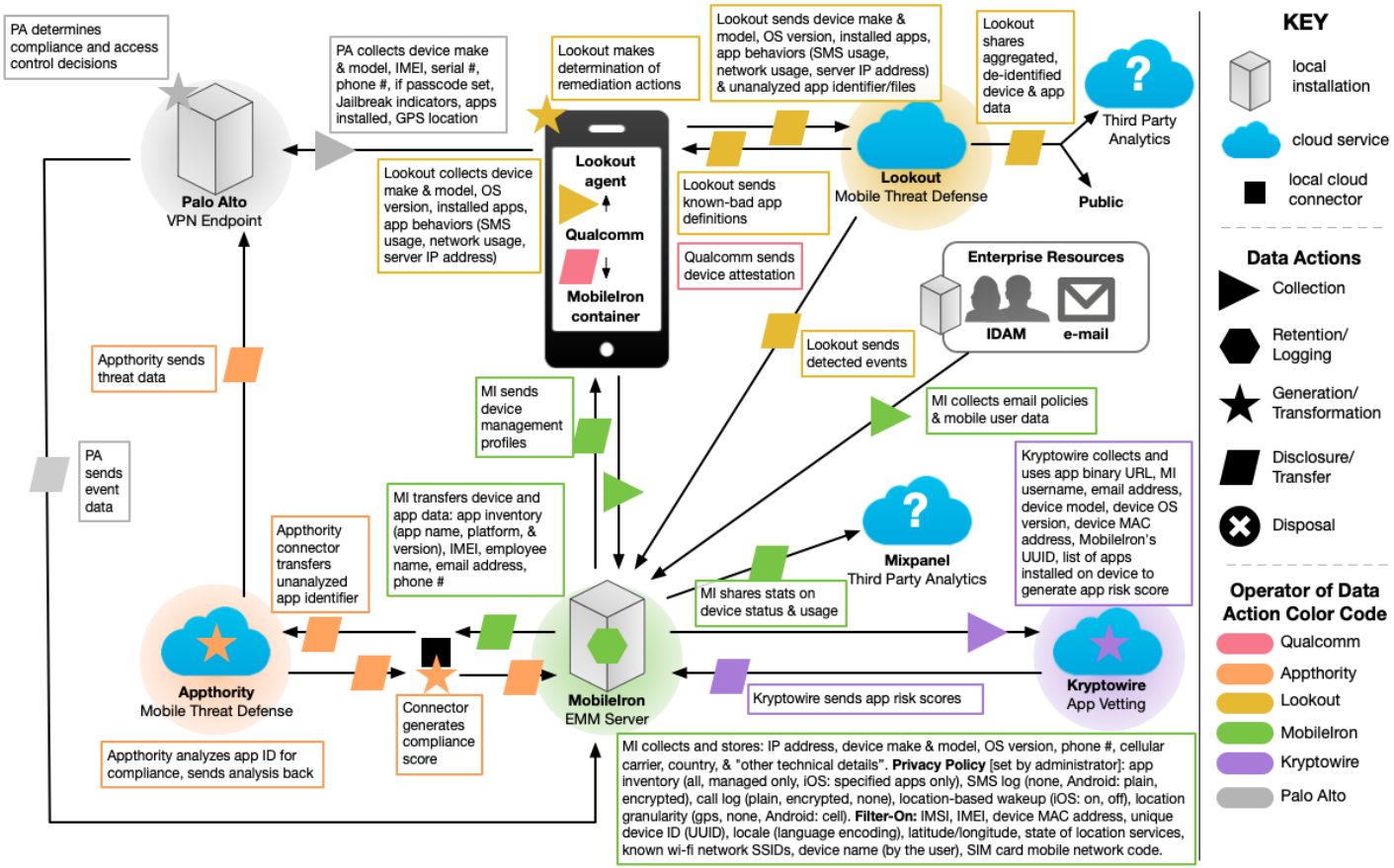
Android Integration

Similarly, Android-based devices offer security controls that an EMM can leverage for enterprise deployments. The Android Enterprise program by Google is available on devices with Android 5.0 (Lollipop) and higher. An EMM deploys a device policy controller [41] as part of its on-device agent that controls local device policies and system applications on devices. A newer mode introduced in Android 8.0 supports fully-managed devices with a work profile, intended for COPE deployments [42], [43], [44]. In this scenario, the device is corporately owned. Device level controls such as device wipe and reset to factory default settings are available. A work profile is also created to keep enterprise applications and data separate from any personal data. This scenario allows for some flexibility of the device owner to permit personal use of the device while retaining device controls and is the chosen deployment of this reference implementation.

4.2 Enterprise Security Architecture Privacy Data Map

Orvilia performed a privacy analysis using both the information gathered in the initial PRAM effort and the identified mobile security technologies included in the revised architecture. The output from the PRAM activities, including data flows between the components, along with their on-premises or cloud-based location, resulted in the information contained in Figure 4-4. Note: The Key within this figure includes all data action types, but this particular example solution does not cover the Disposal of data in the Privacy Data Mapping exercise. For additional information on the PRAM activities, see Appendix G.

Figure 4-4 NIST Privacy Risk Assessment Methodology Data Map for Orvilia's Enterprise Security Architecture



4.3 Security Control Map

Using the developed risk information as input, the security characteristics of the solution were identified. A security control map was developed documenting the example solution's capabilities with applicable Subcategories from the NIST Cybersecurity Framework Version 1.1 [5]; NIST SP 800-53 Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* [11]; International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, *Information technology–Security techniques–Information security management systems – Requirements* [45]; the Center for Internet Security's Control set [46] Version 6; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [7].

The security control map identifies the security characteristic standards mapping for the products as they were used in the example solution. The products may be capable of additional capabilities not used in this example solution. For that reason, it is recommended the mapping not be used as a reference for all of the security capabilities these products may be able to address. The security control map can be found in Table I-1.

5 Security Characteristic Analysis

This section helps familiarize the reader with:

- assumptions and limitations
- build testing
- scenarios and findings

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating how to increase the security of mobile devices within an enterprise by deploying EMM, MTD, MTI, application vetting, secure boot/image authentication, and VPN services.

5.1 Analysis Assumptions and Limitations

The security characteristic analysis has the following limitations:

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

5.2 Build Testing

Functional testing was used to confirm the example solution's capabilities. We use the test activities to demonstrate Orvilia's susceptibility to the threat before implementing the architecture detailed in this practice guide. We use the test activities again after implementing the architecture to demonstrate that the threats have been appropriately addressed.

5.2.1 Threat Event 1 —Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

Summary: Unauthorized access to sensitive information via a malicious or privacy-intrusive application is tested. We tested this threat by placing a mock sensitive enterprise contact list and calendar entries on devices, then attempted to install and use applications on the Apple App Store and Google Play Store [47] that access and back up those entries. Ideally, the enterprise's security architecture would either detect or prevent use of these applications, or it would block the applications from accessing enterprise-controlled contact list and calendar entries.

Test Activity: Install an iOS or Android application that accesses the contact and calendar entries and backs them up to a cloud service. We have no reason to believe these applications are malicious. However, the behavior of accessing and backing up enterprise-controlled data (contacts and calendar entries) without authorization presents an activity that should be mitigated by this example solution's security architecture.

Desired Outcome: The enterprise's security architecture should identify the presence of the applications and the fact that they access contact and calendar entries. The security architecture should block these applications from installing, block them from running, or detect their presence and cause another appropriate response to occur, such as blocking the mobile device from accessing enterprise resources until the applications are removed.

Alternatively, built-in device mechanisms such as Apple's managed applications functionality and Google's Android enterprise work profile functionality could be used to separate the contact and calendar entries associated with enterprise email accounts, so they can be accessed only by enterprise applications (applications authorized and managed by the EMM), not applications manually installed by the user. The user should not have the ability to manually provision their enterprise email account. The account should be able to be provisioned only by the EMM, enabling enterprise controls on the enterprise contact list and calendar data. However, in this practice guide build, we chose to make the devices fully managed, not divided into separate enterprise and personal areas.

Observed Outcome: Appthority identified the presence of applications that have access to sensitive data and updated the device labels in MobileIron Core.

5.2.2 Threat Event 2 —Theft of Credentials Through an SMS or Email Phishing Campaign

Summary: A fictitious phishing event was created where protection against theft of credentials through an SMS or email phishing campaign was tested.

Test Activity:

- Establish a web page with a form that impersonates an enterprise login prompt.
- Send the web page's URL via SMS or email and attempt to collect and use enterprise login credentials.

Desired Outcome: The enterprise's security architecture should block the user from browsing to known malicious websites. Additionally, the enterprise should use multifactor authentication or phishing-resistant authentication methods, such as those based on public key cryptography, so that either there is no password for a malicious actor to capture, or capturing the password is insufficient to obtain access to enterprise resources.

Observed Outcome: The example solution used Palo Alto Networks' next-generation firewall. The firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The URL filtering database is updated regularly to help protect users from malicious URLs. The next-generation firewall blocked the attempt to visit the phishing site because the malicious URL was present in PAN-DB. This kept the user from accessing the phishing site.

5.2.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

Summary: Unauthorized applications, not present on the official Apple App Store or Google Play Store, are installed via URL links in SMS, email messages, or third-party websites.

Test Activity (Android):

- Send an email to the user containing a link to a file with a message urging the user to click on the link to install the application.
- On the device, if not already enabled, attempt to enable the Unknown Sources toggle setting in the device security settings to allow installing applications from sources other than the Google Play Store.
- On the device, read the received email, click on the link, and attempt to install the F-Droid application.
- Observe whether the F-Droid application could be successfully installed. If so, observe whether the enterprise detected and responded to installation of the unauthorized application.

Test Activity (iOS):

- Send an email to the user containing a link to an iOS application available for installation from a website, along with a message urging the user to click on the link to install the application.
- On the device, read the received email, click on the link, and attempt to install the application.
- On the device, attempt to explicitly trust the developer's signing certificate. Then attempt to run the application.
- Observe whether the application could run. If so, observe whether the enterprise detected and responded to installation of the unauthorized application.

Desired Outcome: The device does not allow the user to install the unauthorized application. If the application is somehow installed, its presence should be detected, and an appropriate response should occur, such as blocking the device from accessing enterprise resources until the application is removed.

Observed Outcome: On iOS devices, Lookout detected that an application had been sideloaded, and it applied a label to the device. MobileIron then quarantined the device (removed the device's access to enterprise resources) until the threat was resolved.

On iOS devices, MobileIron has a configuration option that prohibited the user from trusting the developer certificate.

On Android devices, MobileIron has a configuration option that prohibited the user from enabling Unknown Sources on the device.

5.2.4 Threat Event 4 —Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the OS or Firmware

Summary: When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of the root user or the OS kernel.

Test Activity: Attempt to access enterprise resources from a mobile device with known vulnerabilities (e.g., running an older, unpatched version of iOS or Android).

Desired Outcome: The enterprise's security architecture should identify the presence of devices that are running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be possible, when warranted by the risks, to block devices from accessing enterprise resources until system updates are installed.

Observed Outcome: Lookout identified that devices were running outdated operating systems. This information was communicated to MobileIron, which subsequently automatically quarantined the devices until the operating system was updated.

5.2.5 Threat Event 5 —Violation of Privacy via Misuse of Device Sensors

Summary: There is collection of location, camera, or microphone data by an application that has no need to access this data.

Note: Not all applications that have access to location, camera, or microphone data are malicious. However, when an application is found to be collecting this information, additional vetting or testing may be required to determine the intent of its use and to then determine if the application is malicious.

Test Activity: Upload the application to Kryptowire; observe the output report.

Desired Outcome: Output report identifies the use of location, camera, or microphone use by the application.

Observed Outcome: The Kryptowire report identified the use of location sensor, camera, or microphone by the application. An administrator could then perform further testing on the application, and if necessary, identify the application as prohibited within the EMM.

5.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Summary: There is compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates using a person-in-the-middle approach.

Test Activity:

- Install mitmproxy (https://mitmproxy.org/) on a computer (we used a Mac) connected to the same Wi-Fi network as the mobile devices.
- Install mitmproxy's CA certificate (stored at *~/.mitmproxy/mitmproxy-ca-cert.cer* on our Mac) onto the mobile devices being tested. iOS- and Android-specific instructions are found below.
- Configure the computer as necessary to run mitmproxy in transparent mode, as described in https://docs.mitmproxy.org/stable/howto-transparent/.
- To illustrate a malicious actor's ability to manipulate network traffic, we downloaded the mitmproxy *internet_in_mirror* script from https://docs.mitmproxy.org/stable/addons-examples/#internet-in-mirror. It performs a mirror reflection of the content of all websites.
- Run mitmproxy in transparent mode and using the *internet_in_mirror* script: `mitmproxy –mode transparent –ssl-insecure –showhost -s internet_in_mirror.py`
- Rather than perform an intrusive attack such as address resolution protocol spoofing, we manually configured each mobile device's Wi-Fi network settings to change the default gateway's (sometimes referred to as router in the network settings) IP address to the

computer's IP address rather than the router's IP address. This configuration change forced all the network traffic from each device through the computer.

Test Activity (Android):

- Place mitmproxy's CA certificate as an attachment within an email message.
- Open the email message on the Android device and click on the attachment to attempt to install the CA certificate.
- Modify the device's Wi-Fi network settings to manually change the default gateway's IP address to the address of the computer running mitmproxy.
- Browse to a hypertext transfer protocol secure (https) website (e.g., https://www.nccoe.nist.gov), and observe whether the content has been reversed, illustrating that the person-in-the-middle attack on a TLS-protected connection was successful.

Test Activity (iOS):

- Use Apple Configurator 2 on a Mac, or another tool, to create an iOS configuration profile containing mitmproxy's CA certificate. The configuration profile used in testing was named Enterprise Access. The configuration profile was signed using a key associated with an Apple free developer account certificate. The signature was optional (Configuration profiles do not have to be signed).
- Send the configuration profile as an attachment within an email message.
- Open the email message and attempt to click on the attachment to install the configuration profile. Attempt to follow the prompts to complete the profile installation.
- Attempt to enable the CA certificate in the iOS device's Certificate Trust Settings.

Desired Outcome: The enterprise's security architecture should block installation of unauthorized configuration profiles (iOS) or CA certificates (Android). Alternatively, the security architecture may detect the presence of unauthorized configuration profiles or CA certificates and perform another appropriate action, such as blocking the device from accessing enterprise resources until the configuration profile or CA certificate is removed. The architecture should also detect attempted person-in-the-middle attacks.

Observed Outcome: Lookout detected a person-in-the-middle attack on both iOS and Android devices. Lookout also detected the unknown configuration profile on iOS.

5.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Summary: Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, a malicious actor would gain unauthorized access to any

data sent or received by the device for any session not already protected by encryption at either the transport or application layers.

Test Activity: Test if applications will attempt to establish an http or unencrypted connection.

Desired Outcome: Be alerted when applications attempt to make an unencrypted connection or prevent the application from being able to do so.

Appthority can determine if applications will attempt to establish an http or unencrypted connection.

iOS and Android also can require a secure connection for an application. (When it tries to connect to the server if it is unencrypted, it will just drop the connection).

Observed Outcome: On both iOS and Android, Appthority detected a "sends data unencrypted" threat for an application. Transferring data over unencrypted connections could result in the loss of confidentiality of information being transmitted by that application.

5.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced device Unlock Code

Summary: A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks.

Test Activity:

- Attempt to completely remove the device unlock code. Observe whether the attempt succeeds.
- Attempt to set the device unlock code to "1234," a weak four-digit personal identification number (PIN). Observe whether the attempt succeeds.
- Attempt to continuously unlock the device, confirming the device is factory reset after 10 failed attempts.

Desired Outcome: Policies set on the device by the EMM (MobileIron) should require a device unlock code to be set, prevent the device unlock code from being removed, require a minimum complexity for the device unlock code, and factory reset the device after 10 failed unlock attempts.

Additionally, Lookout can identify and report devices that have the lock screen disabled.

Observed Outcome: MobileIron applied a policy to the devices that enforced a mandatory PIN and device wipe capability after 10 failed unlock attempts. Further, Lookout reports when the device has the lock screen disabled. For both devices, all data was erased after 10 failed unlock attempts.

The option to remove the unlock PIN/passcode had been disabled. Upon attempting to set the PIN to one with repetitious or consecutive characters, an error was displayed, informing the user they cannot use the PIN they entered.

5.2.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

Summary: If a malicious actor gains unauthorized access to a mobile device, the attacker also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services.

Test Activity: Application was submitted to Appthority for analysis of credential weaknesses.

Desired Outcome: Discover and report credential weaknesses.

Observed Outcome: Appthority recognized within an application that it uses hard-coded credentials. The application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded credentials were used for access to enterprise resources by unauthorized entities. If the hard-coded credentials result was applied to an application policy, that policy would be applied as a label in MobileIron to all devices with that application installed.

5.2.10 Threat Event 10 —Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

Summary: An employee that accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by an attacker.

Test Activity: Attempt to directly access enterprise services, e.g., Exchange email server or corporate VPN, on a mobile device that is not enrolled into the EMM system.

Desired Outcome: Enterprise services should not be accessible from devices that are not enrolled into the EMM system. Otherwise, the enterprise is not able to effectively manage devices to prevent threats.

Observed Outcome: Devices that were not enrolled in MobileIron were unable to access enterprise resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper client certificates. The client certificates are obtainable only by enrolling in the EMM.

5.2.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device

Summary: Due to the nature of the small form factor of mobile devices, they can be misplaced or stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Test Activity: Attempt to download enterprise data onto a mobile device that is not enrolled into the EMM system (may be performed in conjunction with TE-10). Attempt to remove (in conjunction with TE-8) the device unlock code or demonstrate that the device does not have a device unlock code in place. Attempt to locate and wipe the device through the EMM console (it will fail if the device is not enrolled in the EMM).

Desired Outcome: It should be possible to locate or wipe EMM-enrolled devices in response to a report that they have been lost or stolen. As demonstrated by TE-10, only EMM-enrolled devices should be able to access enterprise resources. As demonstrated by TE-8, EMM-enrolled devices can be forced to have a screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of organizational data) if the device has been lost or stolen.

Should the device be unreachable by the EMM (e.g., disconnected from all networking), EMM control and corporate data will be removed after 10 failed unlock attempts.

Observed Outcome (Enrolled Devices): Enrolled devices are protected. An enterprise policy requiring a personal identification number/lock screen is present, and therefore, the enterprise data on the device could not be accessed. After 10 attempts to access the device, the device was wiped. Additionally, the device was remotely wiped after it was reported as lost to enterprise mobile device service management.

Observed Outcome (Unenrolled Devices): As shown in Threat Event 10, only enrolled devices can access enterprise services. When the device attempted to access enterprise data, no connection to the enterprise services was available. Because the device cannot access the enterprise, enterprise information would not be located on the device.

5.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its Unauthorized Storage in Non-Organizationally Managed Services

Summary: If employees violate data management policies by using unmanaged services to store sensitive organizational data, this data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Test Activity: Connect to the enterprise VPN. Open an enterprise website or application. Attempt to extract enterprise data by taking a screenshot, or copy/paste and send it via an unmanaged e-mail account.

Desired Outcome: Screenshots and other data-sharing actions will be prohibited by the EMM while using managed applications.

Observed Outcome: Through MobileIron restriction and lockdown policies, an administrator prevented the following actions on devices:

Android

- copy/paste
- screen capture
- data transfer over near-field communication
- data transfer over Universal Serial Bus
- Bluetooth

iOS

- screen capture and recording (iOS 9+)
- AirDrop
- iCloud Backup
- iCloud Documents and data access
- managed applications storing data in iCloud
- data flow between managed and unmanaged applications
- hand-off

These restrictions prohibited the user from executing common data leakage methods.

5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory.

The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

This section provides the scenarios and findings for the security and privacy characteristics the example solution was intended to support. They include:

- development of the Cybersecurity Framework and NICE Framework mappings
- threat event scenarios and example solution architecture mitigations
- data action scenarios and potential mitigations that organizations could employ

5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings

While the example solution was being developed, the Cybersecurity Framework Subcategory mappings were developed into a table mapping for organizations implementing the example solution's capabilities.

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

This mapping became an important resource to the example solution contained in this practice guide because it provides the ability to communicate with the organization's stakeholders about the security controls that the example solution can help mitigate, and the workforce requirements that the example solution will require.

The example solution's products, security control, and workforce mapping can be found in Table I-1.

5.3.2 Threat Event Scenarios and Findings

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

Note: While not demonstrated in the table, TEE provided tamper-resistant processing environment capabilities that helped mitigate mobile device runtime and memory threats in the example solution.

Table 5-1 Threat Event Scenarios and Findings Summary

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	Ensured administrators have insight into what corporate data applications can access.	MTI
Threat Event 2: Theft of credentials through an SMS or email phishing campaign	Utilized PAN-DB to block known malicious websites.	Firewall

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 3: Malicious applications installed via URLs in SMS or email messages	Disabled installing applications from unknown sources.	EMM
Threat Event 4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Quarantined noncompliant device until its operating system was updated.	EMM
Threat Event 5: Violation of privacy via misuse of device sensors	Application vetting reports indicated the sensors to which an application requested access.	MTI
Threat Event 6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	Detected a person-in-the-middle attack and an unauthorized configuration profile on iOS.	MTD
Threat Event 7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	Application vetting reports indicated if an application sent data without proper encryption.	Application Vetting
Threat Event 8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	Enforced mandatory device wipe capabilities after 10 failed unlock attempts.	EMM
Threat Event 9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	Application vetting reports indicated if an application used credentials improperly.	MTI
Threat Event 10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	Devices not enrolled in the EMM system were not able to connect to the corporate VPN.	VPN

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 11: Loss of organizational data due to a lost or stolen device	Enterprise data was protected by enforced passcode policies and device wipe capabilities.	EMM
Threat Event 12: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	Policies that enforce data loss prevention were pushed to devices.	EMM

5.3.3 Data Action Scenarios and Findings

The results of the PRAM found that three data actions were especially relevant to the build. Potential mitigations that could be used by an organization to lessen their impact were identified by the PRAM as shown below. Further details on the PRAM's findings can be found in Appendix G.

Table 5-2 Data Action Scenarios and Findings Summary

Data Action	Data Action Description	How the Data Action Could Be Mitigated
Data Action 1: Blocking access and wiping devices	Employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data.	Block the device's access to enterprise resources until it is granted access permission again. Selectively wipe elements of the device without removing all data on the device. Advise employees to back up the personal data maintained on devices. Limit staff with the ability to perform wipes or block access.
Data Action 2: Employee monitoring	Employer-owned or controlled networks monitor activities on a	Limit staff with ability to review data about employees and their devices.

Data Action	Data Action Description	How the Data Action Could Be Mitigated
	regular basis. Employees may not be aware of the monitoring of their interactions with the system and may not want this monitoring to occur.	Develop organizational policies and techniques to limit collection of specific data elements. Develop organizational policies and techniques regarding disposal of PII.
Data Action 3: Data sharing across parties	Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them.	Develop organizational policies and techniques for de-identification of data. Use encryption. Limit or disable access to data. Develop organizational policies and techniques to limit collection of specific data elements. Use contracts to limit third-party data processing.

6 Conclusion

This document provides an overview of the Risk Management Framework and the Privacy Risk Assessment Methodology, an explanation of mobile device security concepts, and an example solution for organizations implementing a COPE deployment.

Our fictitious Orvilia Development organization started with a mobile device infrastructure that was lacking mobile device security architecture concepts. It employed security risk management and privacy risk assessment methodologies to understand the current gaps in its architecture and methods to enhance the security and privacy of its systems.

After identifying the core threat events from the risk assessment, the appropriate mobile device security technologies were applied. These included an on-premises EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities in support of a usage scenario.

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

The example solution of our reference design uses standards-based, commercially available products. It can be used directly by any organization with a COPE usage scenario by implementing a security infrastructure that supports an integration of on-premises with cloud-hosted mobile security technologies. The practice guide provides a reference design and example solution that an organization may use in whole or in parts as the basis for a custom solution that realizes the security and privacy characteristics that best support its unique mobile device usage scenario.

7 Future Build Considerations

A topic of interest for a future build is a bring your own device (BYOD) scenario. This entails protecting corporate data on personally owned devices that employees will use for work as well as personal activity. Another area of interest is a thin client deployed to mobile devices allowing the employee to access a virtual device contained within the corporate infrastructure.

Further, examination of emerging 5G technologies as they relate to mobile device security is a new field that presents a wide breadth of research opportunities.

Appendix A List of Acronyms

AD	Active Directory
ADCS	Active Directory Certificate Services
ADDS	Active Directory Domain Services
API	Application Programming Interface
ATARC	Advanced Technology Academic Research Center
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CIS	Center for Internet Security
COMSEC	Communications Security
COPE	Corporate-Owned Personally-Enabled
CSP	Credential Service Provider
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
EMM	Enterprise Mobility Management
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IR	Interagency Report
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
MSCT	Mobile Services Category Team

MTC	Mobile Threat Catalogue
MTD	Mobile Threat Defense
MTI	Mobile Threat Intelligence
MTP	Mobile Threat Protection
NCCoE	National Cybersecurity Center of Excellence
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OS	Operating System
PA	Palo Alto Networks
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
ROM	Read-only Memory
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Information and Event Management
SMS	Short Message Service
SP	Special Publication
TE	Threat Event
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UPN	User Principal Name
URL	Uniform Resource Locator
VPN	Virtual Private Network

Appendix B Glossary

Access Management	Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [48].
Agent	A host-based intrusion prevention system program that monitors and analyzes activity and performs preventive actions; OR a program or plug-in that enables an SSL VPN to access non-Web-based applications and services [49].
Application Layer	Layer of the TCP/IP protocol stack that sends and receives data for particular applications such as DNS, HTTP, and SMTP [49].
App-Vetting Process	The process of verifying that an app meets an organization's security requirements. An app vetting process comprises app testing and app approval/rejection activities [50].
Brute-Force Attack	In cryptography, an attack that involves trying all possible combinations to find a match [51].
Chief Information Officers (CIO) Council	The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources [52].
Common Vulnerabilities and Exposures	A dictionary of common names for publicly known information system vulnerabilities [53].
Corporate-Owned Personally-Enabled (COPE)	A device owned by an enterprise and issued to an employee. Both the enterprise and the employee can install applications onto the device.
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output [54].
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification [55].

Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification [54].
Data Action	System operations that process PII [20].
De-identification	General term for any process of removing the association between a set of identifying data and the data subject [51].
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks [56].
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [20].
Encryption	The cryptographic transformation of data to produce ciphertext [54].
Enterprise Mobility Management	Enterprise Mobility Management (EMM) systems are a common way of managing mobile devices in the enterprise. Although not a security technology by itself, EMMs can help to deploy policies to an enterprise's device pool and to monitor device state [9].
Identity Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). Adapted from Verification [54].
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system [11].

Key Logger	A remote program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures [57].
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code [11].
Manageability	Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure [20].
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [11].
Mobile Device Management (MDM)	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices [50].
Network Layer	Layer of the TCP/IP protocol stack that is responsible for routing packets across networks [49].
Person (Man)-in-the-Middle Attack	An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrollment, or between subscriber and CSP during authenticator binding [55].

Phishing	An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP [55].
Predictability	Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service [20].
Predisposing Conditions	A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation [12].
Privacy Risk Assessment Methodology (PRAM)	The PRAM is a tool that applies the risk model from NISTIR 8062 and helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions. The PRAM can help drive collaboration and communication between various components of an organization, including privacy, cybersecurity, business, and IT personnel [58].
Read-Only Memory	ROM is a pre-recorded storage medium that can only be read from and not written to [59].
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization [11].
Replay Resistance	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access [60].
Risk	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 [12].

Risk Assessment	The process of identifying 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. Synonymous with risk analysis [11].
Risk Management Framework	The Risk Management Framework (RMF) provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of systems into the mission and business processes of the organization [61].
Sandbox	A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized (Under Sandboxing) [54].
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements [11].
Side-Channel Attacks	An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions [55].
Social Engineering	The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust [55].
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [12].
Threat Events	An event or situation that has the potential for causing undesirable consequences or impact [12].

Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes [62].
Threat Sources	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent [11].
Transport Layer	Layer of the TCP/IP protocol stack that is responsible for reliable connection-oriented or connectionless end-to-end communications [49].
Transport Layer Security (TLS)	A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol [54].
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor" [63].
Unmanaged Device	A device inside the assessment boundary that is either unauthorized or, if authorized, not assigned to a person to administer [64].
Virtual Private Network	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line [54].
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [12].
Watering Hole	Watering hole attacks involve attackers compromising one or more legitimate Web sites with malware in an attempt to target and infect visitors to those sites [65].

Appendix C References

[1] National Institute of Standards and Technology (NIST), "NIST Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/publications/sp800.

[2] National Information Assurance Partnership (NIAP), "NIAP Home Page," [Online]. Available: https://www.niap-ccevs.org/.

[3] Department of Homeland Security, "Home Page," [Online]. Available: https://www.dhs.gov/.

[4] Federal Chief Information Officers (CIO) Council, "Federal CIO Home Page," [Online]. Available: https://www.cio.gov/.

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

[6] National Institute of Standards and Technology (NIST), "NIST Privacy Engineering Program," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[7] National Institute of Standards and Technology (NIST), "NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final.

[8] National Institute of Standards and Technology (NIST), "Risk Management Framework (RMF) Overview," [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

[9] National Institute of Standards and Technology (NIST), "Mobile Threat Catalogue," [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/.

[10] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Mobile Device Security for Enterprises Building Block Version 2 Final Draft," 12 September 2014. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/mds-project-description-final.pdf.

[11] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," 22 January 2015. [Online]. Available: https://csrc.nist.gov/publications/sp.

[12] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[13] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 2 Draft, Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.

[14] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-4, Mobile Device Security: Cloud and Hybrid Builds," 21 February 2019. [Online]. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid.

[15] International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE), "International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering – System life cycle processes," 2015. [Online]. Available: https://www.iso.org/standard/63711.html.

[16] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," November 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

[17] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[18] Tech Times, "Flashlight apps are spying on users Android, iOS, Windows Phone smartphones, is yours on the list?," 26 October 2014. [Online]. Available: https://www.techtimes.com/articles/18762/20141026/flashlight-apps-are-spying-on-users-android-ios-windows-phone-smartphones-is-yours-on-the-list.htm.

[19] National Institute of Standards and Technology (NIST), "NIST Privacy Framework," [Online]. Available: https://www.nist.gov/privacy-framework.

[20] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems," January 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[21] M. A. A. B. Mohamed Sabt, "Trusted Execution Environment: What It is, and What It is Not. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland," August 2015. [Online]. Copy and paste link into browser to access. Available: https://hal.archives-ouvertes.fr/hal-01246364/file/trustcom_2015_tee_what_it_is_what_it_is_not.pdf.

[22] Zimperium, "MobileIron Threat Defense, Mobile Device Security & MDM," [Online]. Available: https://www.zimperium.com/partners/mobileiron.

[23] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Management Version 4.0," 25 April 2019. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[24] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Extended Package for VPN Gateways Version 2.1," 8 March 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[25] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314," 14 March 2018. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[26] National Information Assurance Partnership, "Approved Protection Profiles," [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

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

[28] National Information Assurance Partnership (NIAP), "Product Compliant List," [Online]. Available: https://www.niap-ccevs.org/Product/.

[29] Palo Alto Networks, "Remote Access VPN (Certificate Profile)," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile.

[30] MobileIron, "Admin Google Android Google Apps API," [Online]. Available: http://mi.extendedhelp.mobileiron.com/45/all/en/desktop/Google_Apps_API.htm.

[31] MobileIron, "MobileIron unified endpoint security platform," [Online]. Available: https://www.mobileiron.com/en/unified-endpoint-management/platform.

[32] Open Web Application Security Project (OWASP), [Online]. Available: https://www.owasp.org/index.php/Main_Page.

[33] Palo Alto Networks, "Always On VPN Configuration," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/7-1/globalprotect-admin/globalprotect-quick-configs/always-on-vpn-configuration.

[34] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[35] National Institute of Standards and Technology (NIST), "Cryptographic Module Validation Program," [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program.

[36] Palo Alto Networks, "FIPS-CC Security Functions documentation site," [Online]. Available: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certifications/fips-cc-security-functions.

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

[38] Apple Computer, "Apple at Work," [Online]. Available: https://www.apple.com/business/it/.

[39] Apple Computer, "Apple Configurator 2," [Online]. Available: https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?mt=12.

[40] Apple Computer, "Apple Platform Security," [Online]. Available: https://support.apple.com/guide/security/welcome/web.

[41] Android.com, "Build a device policy controller," [Online]. Available: https://developer.android.com/work/dpc/build-dpc.

[42] Android.com, "Work profiles on fully managed devices," [Online]. Available: https://developers.google.com/android/work/requirements/work-profile.

[43] Google.com, "Android Enterprise Fully managed device," [Online]. Available: https://developers.google.com/android/work/requirements/fully-managed-device.

[44] Google.com, "Android Enterprise Work profile," [Online]. Available: https://www.android.com/enterprise/.

[45] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements," October 2013. [Online]. Available: https://www.iso.org/standard/54534.html.

[46] Center for Internet Security, "Center for Internet Security Home Page," [Online]. Available: https://www.cisecurity.org/.

[47] Google.com, "Google Play Store," [Online]. Available: https://play.google.com/store/apps.

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

[49] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-113 Guide to SSL VPNs," July 2008. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-113/final.

[50] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-163 Revision 1, Vetting the Security of Mobile Applications," April 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf.

[51] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8053, De-Identification of Personal Information," October 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[52] General Services Administration, "Chief Information Officers Council (CIOC)," [Online]. Available: https://www.gsa.gov/about-us/organization/office-of-governmentwide-policy/office-of-shared-solutions-and-performance-improvement/chief-information-officers-council-cioc.

[53] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126 Revision 3, The Technical Specification for the Security Content Automation Protocol (SCAP)," February 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf.

[54] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary, Publication 4009," 6 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

[55] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines," 2 March 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[56] National Institute of Standards and Technology (NIST), "NISTIR 7711 Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf.

[57] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security," May 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[58] National Institute of Standards and Technology (NIST), "Risk Assessment Tools," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools.

[59] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1, Guidelines for Media Sanitization," December 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[60] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," February 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[61] National Institute of Standards and Technology (NIST), "Risk Management Framework: Quick Start Guide," [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides.

[62] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing," October 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[63] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.

[64] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8011 Volume 1, Automation Support for Security Control Assessments," June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf.

[65] United States Department of Homeland Security, "ICS-CERT Monitor," October, November, December 2013. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.

[66] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines," 2 March 2020. [Online]. Available: https://csrc.nist.gov/publications/sp.

[67] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final.

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

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

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

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

[72] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobility Strategy Development Guidelines Working Group Document," June 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12997/Agency_Mobility_Strategy_Deliverable.pdf.

[73] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobile Threat Protection App Vetting and App Security Working Group Document," July 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12996/Mobile_Threat_Protection_Deliverable.pdf.

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

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

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

[77] National Information Assurance Partnership (NIAP), "NIAP U.S. Government Approved Protection Profile - Extended Package for Mobile Device Management Agents Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=403&id=403.

[78] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals Version 3.1," 16 June 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[79] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Management Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=392&id=392.

[80] United States Office of Management and Budget (OMB), "Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services," 4 August 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_20.pdf.

[81] National Institute of Standards and Technology (NIST), "United States Government Configuration Baseline (In Development)," [Online]. Available: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline.

[82] Department of Homeland Security (DHS), "DHS Study on Mobile Device Security," April 2017. [Online]. Available: https://www.dhs.gov/publication/csd-mobile-device-security-study.

[83] Android, "Android zero-touch enrollment," [Online]. Available: https://www.android.com/enterprise/management/zero-touch/.

[84] Google, "Android's enterprise requirements," [Online]. Available: https://support.google.com/work/android/answer/6174145?hl=en.

[85] Apple, "Business Support," [Online]. Available: https://support.apple.com/business.

[86] Apple, "Configuration Profile," 3 May 2019. [Online]. Available: https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf.

[87] Samsung, "Knox Mobile Enrollment," [Online]. Available: https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment.

[88] Samsung, "Secured by Knox," [Online]. Available: https://www.samsungknox.com/en/secured-by-knox.

[89] Samsung, "Devices built on Knox," [Online]. Available: https://www.samsungknox.com/en/knox-platform/supported-devices.

[90] Samsung, "Knox features on Android," [Online]. Available: https://www.samsungknox.com/en/knox-features/android/kme.

[91] The MITRE Corporation, "ATT&CK," [Online]. Available: https://attack.mitre.org/.

[92] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8144 (Draft), Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue," [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8144/draft.

[93] The MITRE Corporation, "ATT&CK for Mobile," [Online]. Available: https://attack.mitre.org/resources/mobile-introduction/.

[94] The MITRE Corporation, "Common Vulnerabilities and Exposures (CVEs)," [Online]. Available: http://cve.mitre.org/.

[95] FedRAMP, "FedRAMP Home Page," [Online]. Available: https://www.fedramp.gov/.

[96] National Institute of Standards and Technology (NIST), "NIST Information Technlogy Laboratory National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/.

[97] Android Open Source Project, "Pixel / Nexus Security Bulletins," [Online]. Available: https://source.android.com/security/bulletin/pixel/.

[98] Apple Computers, "Apple Security Updates," [Online]. Available: https://support.apple.com/en-us/HT201222.

[99] Apple, "Managing Devices & Corporate Data on iOS," July 2018. [Online]. Available: https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf.

[100] Samsung, "Android Security Updates," [Online]. Available: https://security.samsungmobile.com/securityUpdate.smsb.

Appendix D Standards and Guidance

- National Institute of Standards and Technology (NIST) *Cybersecurity Framework Version 1.1* [5]
- NIST *Mobile Threat Catalogue* [9]
- NIST *Risk Management Framework* [8]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [14]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [17]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [34]
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [37]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [11]
- NIST SP 800-63, *Digital Identity Guidelines* [66]
- NIST SP 800-113, *Guide to SSL VPNs* [49]
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [67]
- NIST SP 800-124 Revision 2 Draft, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [13]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [50]
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [60]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [7]
- Center for Internet Security [46]
- Executive Office of the President, Bring Your Own Device Toolkit [68]
- Federal Chief Information Officers (CIO) Council and Department of Homeland Security (DHS) Mobile Security Reference Architecture, Version 1.0 [69]
- Digital Services Advisory Group and Federal Chief Information Officers Council, Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis [70]

- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, *Information technology–Security techniques–Information security management systems–Requirements* [45]
- Mobile Computing Decision Example Case Study [71]
- Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), Mobility Strategy Development Guidelines Working Group Document [72]
- MSCT ATARC, Mobile Threat Protection App Vetting and App Security Working Group Document [73]
- MSCT, Device Procurement and Management Guidance [74]
- MSCT, Mobile Device Management (MDM), MDM Working Group Document [75]
- MSCT, Mobile Services Roadmap, MSCT Strategic Approach [76]
- NIAP U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 3.0 [77]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Fundamentals Version 3.1 [78]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Management Version 3.0 [79]
- NIAP Product Compliant List [28]
- United States Office of Management and Budget (OMB), Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services [80]
- The United States Government Configuration Baseline (USGCB) [81]
- United State Department of Homeland Security (DHS) Study on Mobile Device Security [82]

Appendix E Android, Apple, and Samsung Knox Mobile Enrollment

Device enrollment and management capabilities are available when deploying mobile devices in bulk. Certain settings can be preloaded, and devices can ship preconfigured for enterprise management. iOS-, Android-, and Samsung Knox-based devices integrate directly with Enterprise Mobility Management (EMM) solutions, providing enterprise-level management of security controls based on policy.

E.1 Android Devices

For Android devices, zero-touch enrollment provides an option different from the manual setup of Android devices. Android-based devices offer security controls that an EMM can leverage for enterprise deployments. The Android Enterprise program by Google is available on devices with Android 5.0 (Lollipop) and higher. An EMM deploys a device policy controller as part of its on-device agent that controls local device policies and system applications on devices. Android Enterprise supports corporate-owned personally-enabled and bring your own device deployment scenarios through work-managed and work-profile device solutions [83], [84].

E.2 iOS Devices

For iOS devices, Apple Configurator supports Volume Purchase and Device Enrollment Program scenarios. Apple Business Manager provides a mobile device management solution to assist organizations in deploying iOS devices. iOS devices are managed by configuration profiles. Configuration profiles can force security policies such as virtual private network usage, enterprise Kerberos support, and access to cloud services. iOS further incorporates a set of additional security controls in what is termed supervised mode, which denotes a corporately owned device.

Typically, organizations choose to use the Device Enrollment Program for large-scale deployments of iOS devices in supervised mode due to the reduction of labor involved in manually configuring each device. However, due to the small number of devices in our reference design, we have configured supervised mode using the Apple Configurator 2 tool. A more detailed description of iOS capabilities can be found in the iOS Security Guide [85], [86].

E.3 Samsung Knox Devices

Samsung Knox Mobile Enrollment provides the ability to add Samsung devices to the enterprise without manually enrolling each device. Samsung Knox Mobile Enrollment works on Samsung Galaxy devices running Android Lollipop or higher. It allows remote provisioning of devices when they connect to Wi-Fi or cellular networks. Samsung Knox Mobile Enrollment works with a number of EMM solutions, including cloud-based options [87], [88], [89], [90].

Appendix F Risk Assessment

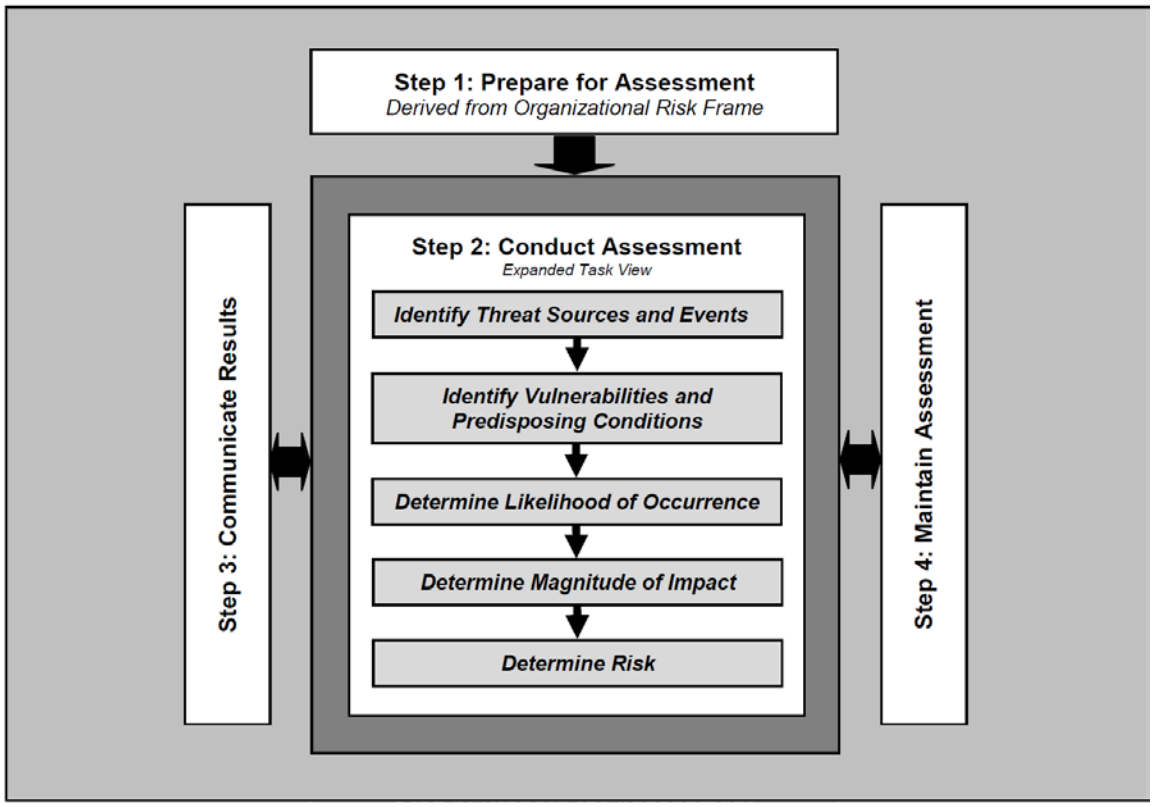
F.1 Risk Assessment

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments,* [12] 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.

This section details the risk assessment undertaken to improve the mobile security posture of the fictional organization Orvilia Development. Typically, a NIST SP 800-30 Revision 1-based risk assessment follows a four-step process as shown in Figure F-1: Prepare for assessment, conduct assessment, communicate results, and maintain assessment.

Figure F-1 Risk Assessment Process



To provide the most value in this exercise:

- We focused on the preparation, which established the context of the risk assessment.
- We conducted the risk assessment, which produced a list of information security risks that were prioritized by risk level and used to inform risk response decisions.
- We followed the process detailed in Section 3 of NIST SP 800-30 Revision 1 [12] to perform a risk assessment of the current mobile infrastructure.

We recommend that organizations performing a risk assessment communicate results and perform maintenance of the risk assessment, but these activities were deemed out of scope for this project. The following tasks were used during the assessment process.

F.1.1 Task 1-1: Risk Assessment Purpose

Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

The purpose of the risk assessment of Orvilia Development was to identify and document new risks to its mission resulting from addition of a mobility program.

The results of the risk assessment informed decisions to Orvilia's mobility deployment that included:

- implementation of new security mechanisms
- configuration changes to existing infrastructure
- updates to security and appropriate-use policies relevant to their mobility program

F.1.2 Task 1-2: Risk Assessment Scope

Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.

Organizational Applicability:

The scope of this risk assessment was limited to systems impacted by inclusion of a mobility program; it did not include existing information technology (IT) infrastructure to which no impact was anticipated. With their original architecture, Orvilia deployed corporate-owned personally-enabled (COPE) devices. Orvilia employees utilized mobile devices for local and remote work activities and limited personal activities (e.g., phone calls, messaging, social applications, and personal emails).

With Orvilia's new government contract, this risk assessment also evaluated Orvilia's mobile deployment regarding its ability to access and store government data while meeting applicable information security and privacy requirements.

While not directly associated with risk assessment activities, Orvilia will be required to demonstrate compliance with government standards and policies established to improve data security. Therefore, Orvilia needed to determine how compliance with government policy and application of its standards would best align with its strategy to identify, protect again, detect, respond to, and recover from threats related to its mobility program.

Time Frame Supported:

Because this was the first risk assessment performed by Orvilia, the process was more time-intensive than it will be in future risk management cycles. Orvilia completed the initial risk assessment within six months.

Architectural and Technology Considerations:

This risk assessment was scoped to Orvilia's mobile deployment, which constitutes mobile devices used to access Orvilia enterprise resources along with any backend IT components used to manage or provide services to those mobile devices.

The following provide an overview of the mobile deployment components involved in the original (current) Orvilia architecture.

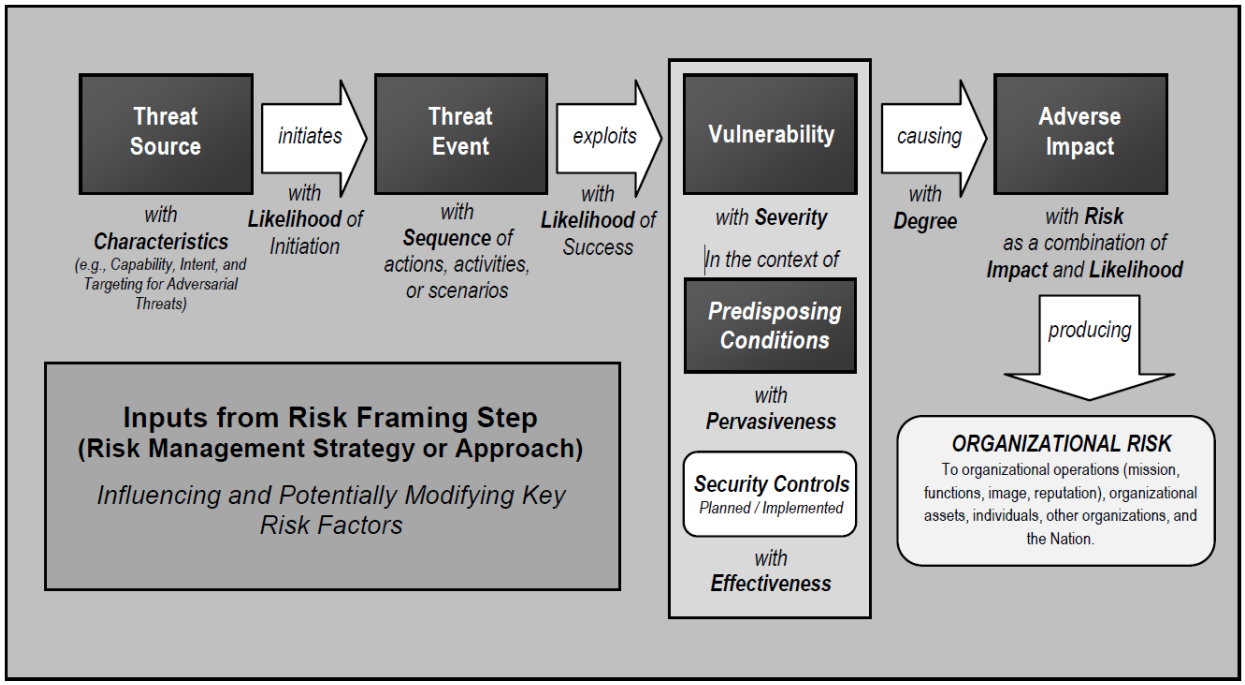
- **Mobile Device:** A mobile device is a small form factor device with a rich operating system, at least one wireless network interface, and the ability to run applications. These features are considered essential for Orvilia to have portable and efficient access to enterprise data.
- **Communication Networks and Data Transmission:** Mobile devices will establish connections to the internet by using their cellular or Wi-Fi adapters. As connections may be made to unsecured access points or may traverse untrusted networks, consideration will be given to the risks associated with the security of those connections and the data transmitted over them. Additionally, the organization will need to consider risks arising from permitting inbound connections by mobile devices via the internet.
- **Public Application Stores:** With a COPE deployment strategy, employees will have the option to download any mobile application available from official platform application stores (e.g., Google Play Store). While those platforms analyze applications for malicious behaviors, it is still possible for such applications to exceed Orvilia's needs for user privacy or pose a risk to the devices or data. Therefore, risks from such applications should be included in this assessment.
- **Device and Operating System (OS) Vendor Infrastructure:** The hardware, firmware, and software that compose each model of mobile device can vary, particularly those from different manufacturers and vendors, which may incorporate technology that is exclusive to their products. It will be important to select devices that demonstrate security mechanisms that align with the organization's risk mitigation strategy. However, risks that are specific to given device components (e.g., chipsets or driver versions) will be out of scope for this assessment.
- **Enterprise Systems:** If a potentially compromised mobile device can connect to the enterprise, it poses direct risks to any systems it can reach or data it can access. Such systems will reasonably include on-premises mobile application stores, mobile management technologies, email servers, file servers, and intranet web servers. Subsequent compromise of any of these systems may cascade to others not directly reachable by the mobile device. Risks to all such systems by a mobile device should be included in this assessment.

F.1.3 Task 1-3: Risk Assessment Assumptions and Constraints

Identify the specific assumptions and constraints under which the risk assessment is conducted.

Risk assessment assumptions and constraints were developed using a NIST SP 800-30 Revision 1 Generic Risk Model as shown in Figure F-2.

Figure F-2 NIST 800-30 Generic Risk Model



F.1.3.1 Risk Assessment Assumptions

Some of the threats and their resulting risks and impacts span several levels. In cases where these risks and impacts have several possible levels, it was assumed that Orvilia would document these using a high-water mark methodology. This assumption of greatest risk then provided the basis for risk mitigation activities. For example, where the threat risk could pose a moderate, high, or very high outcome, the very high outcome was selected, and these very high risks were prioritized for mitigation.

F.1.3.2 Risk Assessment Constraints

Information regarding the following were used as input for the constraints for the risk assessment.

- threat sources
- threat events
- vulnerabilities and predisposing conditions
- likelihood
- impacts
- risk assessment and analysis approaches
- resources available for the assessment

- skills and expertise

Threat Sources

Orvilia's executives and managers identified two threat sources as possible concerns. Orvilia's technical staff were provided security control mappings identified within this guide to help them understand the additional security that the example solution could provide to Orvilia as they implemented the example solution.

Additionally, due to the cybersecurity-focused scope of the risk assessment, non-adversarial threat sources (e.g., unintentional hardware, software, or system design and architecture shortcoming threats) were not considered.

As identified in Section F.1.6, Task 2-1: Identify and Characterize Threat Sources of Concern, the risk assessment identified the following threat sources of concern:

- Orvilia's competitors
- nation-state actors

Threat Events

- Threat events were described at a high level and in general terms within the risk assessment. Similar threat events were combined into a single, broader threat.
- Only those threat events that have been previously observed by an authoritative source were considered (e.g., reported as already having occurred by other organizations), drawing primarily from the NIST National Cybersecurity Center of Excellence Mobile Threat Catalogue [9].
- Threat events involving exploitation of vulnerabilities within the cellular network, including a mobile device's cellular baseband, reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.
- Threat events involving exploitation of vulnerabilities in low-level hardware, firmware, and device controllers reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.
- Threat events involving exploitation of vulnerabilities in the supply chain reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.

Vulnerabilities and Predisposing Conditions

- Mobile device vulnerabilities considered during this risk assessment included those in mobile operating systems and mobile applications, including third-party software libraries.
- Vulnerabilities in commonly used noncellular network protocols such as Bluetooth and Wi-Fi were considered.

- Vulnerabilities related to a potential Enterprise Mobility Management (EMM) system were considered.
- Additional information and determinations were made via Appendix F of NIST SP 800-30 Revision 1.

Likelihood

- Likelihood determinations were made via Appendix G of NIST SP 800-30 Revision 1.

Note: The rating of overall likelihood is derived from the Likelihood of Initiation and Likelihood that Threat Events Result from Adverse Impacts using Table G-5 of Appendix G in NIST SP 800-30 Revision 1 [12]. Ratings of the latter two variables relied heavily on the subjective judgment of Orvilia employees.

Impacts

- Impact determinations were made via Appendix H of NIST SP 800-30 Revision 1.

Note: Ratings of impact relied heavily on the subjective judgment of Orvilia employees.

Risk Assessment and Analysis Approaches

- This risk assessment focused on identifying an initial set of threats to Orvilia's mobile deployment.
- Approaches for describing threats and their impact were informed by the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework [91].
- The rating of Risk was derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [12].

Resources Available for the Assessment

- Orvilia ensured the appropriate staff with the requisite expertise were available to conduct the assessment within the time allotted.
- Orvilia provided funding for the risk analysis staff.
- Orvilia staff who conducted the risk assessment had the necessary information systems and software.

Skills and Expertise

- Risk assessments were conducted by experts leveraging industry best practices and NIST risk assessment frameworks.

F.1.4 Task 1-4: Risk Assessment Threat, Vulnerability, and Impact Sources

Identify the sources of descriptive threat, vulnerability, and impact information to be used in the risk assessment.

Orvilia used the following methods to identify mobile infrastructure threats, vulnerabilities, and impacts.

F.1.4.1 Sources of Threats

This risk assessment identified NIST's Mobile Threat Catalogue (MTC) [9], along with its associated NIST Interagency Report 8144, *Assessing Threats to Mobile Devices & Infrastructure* [92], and MITRE's ATT&CK Mobile Profile [93] as credible sources for threat information. Each entry in the MTC contains several pieces of information: an identifier, a category, a high-level description, details on its origin, exploit examples, Common Vulnerabilities and Exposures [94] examples, possible countermeasures, and academic references.

MITRE's ATT&CK is a curated knowledge base and model for cyber-adversary behavior. ATT&CK details specific techniques that can be used by cyber adversaries. Each technique entry typically includes a detailed technical description, mitigations, detection analytics, examples of use by malicious actors, and references. The ATT&CK model organizes these techniques into high-level malicious actor tactical objectives, referred to as tactics. A primary use case for ATT&CK is use by organizations to assess the state of their cybersecurity defenses and prioritize deployment of defensive capabilities. The ATT&CK Mobile Profile describes tactics and techniques specific to the mobile environment.

Due to Orvilia's current use of cloud services, it identified the outputs of the Federal Risk and Authorization Management Program [95] and associated NIST SP 800-53 security controls as being in scope for this risk assessment.

F.1.4.2 Sources of Vulnerabilities

Vulnerabilities are commonly associated with mobile operating systems, device drivers, mobile applications, and third-party libraries. However, vulnerabilities can be present in any level of the mobile technology stack. For up-to-date information regarding vulnerabilities, this risk assessment identified the National Vulnerability Database (NVD) [96] as a credible source of information. The NVD is the U.S. government repository of standards-based vulnerability management data. Use of NVD was supplemented by review of individual vendor vulnerability disclosures such as those published in the Pixel/Nexus Security Bulletins [97] for Android, Apple security updates [98] for iOS, Managing Devices & Corporate Data on iOS [99], and Android Security Updates [100] for Android-based Samsung devices.

F.1.4.3 Sources of Impacts

This risk assessment identified the scenario described in Section F.1.2 as the primary source of impact determination information. The scenario identified the following systems as being critical to the organization's mission:

- Microsoft Active Directory domain
- Microsoft Exchange email server

- timekeeping web application
- travel support web application
- corporately owned mobile devices

An example of a successful attack against a mobile device is one that could be used to glean the credentials for the travel support web application and use them to penetrate the application server. While Orvilia can absorb minimal downtime to the web application, the attacker could use this position to gain a foothold in the Orvilia infrastructure to laterally move to more critical systems in the environment, such as the email server. Compromise of the email server would have high impact, possibly causing serious harm to the organization.

F.1.5 Task 1-5: Risk Assessment Risk Model and Analytic Approach Identification

Identify the risk model and analytic approach to be used in the risk assessment.

In this risk assessment, the analytic approach used qualitative (i.e., subjective) ratings of risk (i.e., very low, low, moderate, high, and very high). The approach was primarily threat oriented, as described in Section F.1.6.

F.1.6 Task 2-1: Identify and Characterize Threat Sources of Concern

Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.

Orvilia examined NIST SP 800-30 Revision 1's Table D-2: Taxonomy of Threat Sources [12] and identified the following threat sources of concern:

Table F-1 Threat Sources of Concern

Identifier	Threat Source	Description	Characteristic
TS-1	Adversarial, Organization, Competitor	Orvilia's competitors seek to exploit dependence on cyber resources, specifically the data entrusted by its customers to increase market share.	Capability, Intent, Targeting
TS-2	Adversarial, Nation-State	Nation-state actors stealing sensitive government data from unsecured devices and infrastructure	Capability, Intent, Targeting

Orvilia produced the following table as output of Task 2-1 to provide relevant inputs to the risk tables. It identifies the threat sources identified in NIST SP 800-30 Revision 1 with the associated risk rating of

capability, intent, and targeting score (using the previously mentioned five-point scale: very low, low, moderate, high, and very high).

Orvilia's assessment found that all threat events could be initiated by both threat sources (Organization/Competitor and Nation-State).

Capability refers to the level of expertise of the malicious actor. Intent refers to the malicious actor's goal. Targeting refers to the reconnaissance and selection methods performed by the malicious actor.

Table F-2 Threat Sources Qualitative Scale

Identifier	Threat Events Relevant to Threat Sources	In Scope	Capability	Intent	Targeting
TS-1	All threat events (Threat Events 1-12)	Yes	High	High	High
TS-2	All threat events (Threat Events 1-12)	Yes	Very High	Very High	Very High

F.1.7 Task 2-2: Identify Potential Threat Events

Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.

The threat events used for the example solution are described below. These threat events describe how the mobile devices in Orvilia might be compromised by malicious activities. All of the threat events map to both threat sources identified in Section F.1.6.

Orvilia examined the sample tables in NIST SP 800-30 Revision 1—Tables E-1, E-2, E-3, E-4, and E-5—and analyzed the sources of mobile threats identified in Task 1-4. Using this process, Orvilia leadership identified the following threat events.

F.1.7.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, camera roll), and general device data available to any application (e.g., International Mobile Equipment Identity, device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the OS, or device

firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

F.1.7.2 Threat Event 2—Theft of Credentials Through an SMS or Email Phishing Campaign

Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over short message service (SMS) or email. Effective use of social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutiny of the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

F.1.7.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

Malicious actors may send users SMS or email messages that contain a uniform resource locator (URL) where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood they access the URL by using their mobile device. If the URL is accessed, the device will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions requested by the application. Granting the former facilitates installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

F.1.7.4 Threat Event 4—Confidentiality and Integrity Loss Due to Exploitation of Known Vulnerability in the OS or Firmware

When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of the root user or the OS kernel. This may be enough for some to accomplish their goal, but advanced malicious actors will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the attacker will be able to launch further attacks against the user, the device, or any other systems to which the device connects. As a result, any data stored on, generated by, or accessible to the device at that time—or in the future—may be compromised.

F.1.7.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as

when recording any nearby sounds. Captured sensor data, such as a recording of an executive meeting, may be immediately useful to a malicious actor. Alternatively, the data may be analyzed in isolation or in combination with other data to yield sensitive information. For example, audio recordings of on-device or proximate activity can be used to probabilistically determine user inputs to touchscreens and keyboards—essentially turning the device into a remote key logger.

F.1.7.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Malicious actors who successfully install an EMM/mobile device management (MDM), network, or virtual private network (VPN) profile or certificate onto a device will gain a measure of additional control over the device or its communications. Presence of an EMM/MDM profile will allow an attacker to misuse existing OS application programming interfaces to send the device a wide variety of commands. This may allow a malicious actor to obtain device information, install or restrict applications, or remotely locate, lock, or wipe the device. Malicious network profiles may allow a malicious actor to automatically compel the device to connect to access points under their control to achieve a person-in-the-middle attack on all outbound connections. Alternatively, VPN profiles assist in the undetected exfiltration of sensitive data by encrypting it, thus hiding it from network scanning tools. Additionally, malicious certificates may allow the malicious actor to compel the device to automatically trust connections to malicious web servers, wireless access points, or installation of applications under their control.

F.1.7.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, an attacker would gain unauthorized access to any data sent or received by the device for any session not already protected by encryption at either the transport or application layers. Even if the transmitted data were encrypted, an attacker would be privy to the domains, internet protocol addresses, and services (as indicated by port numbers) to which the device connects; such information could be used in future watering hole attacks or person-in-the-middle attacks against the device user. Additionally, visibility into network layer traffic enables a malicious actor to conduct side-channel attacks against its encrypted messages, which can still result in a loss of confidentiality. Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session with another host or endpoint may facilitate attacks that ultimately compromise the security of the session.

F.1.7.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, side-channel attacks that infer the unlock code by detecting taps and swipes to the screen can be attempted by applications with access to any peripherals that detect sound or motion (e.g., microphone, gyroscope, or accelerometer). Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the malicious actor may further gain unauthorized access to those systems.

F.1.7.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

If a malicious actor gains unauthorized access to a mobile device, the malicious actor also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

F.1.7.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

An employee who accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by a malicious actor. Therefore, users who violate security policies to gain unauthorized access to enterprise resources from such devices risk providing malicious actors with access to sensitive organizational data, services, and systems.

F.1.7.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device

Due to the nature of the small form factor of mobile devices, they can be misplaced or stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

F.1.7.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its Unauthorized Storage to Non-Organizationally Managed Services

If employees violate data management policies by using unmanaged services to store sensitive organizational data, the data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from the public disclosure of trade secrets.

F.1.8 Task 2-3: Identify Vulnerabilities and Predisposing Conditions

Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

Drawing on the scenario described in Section 3.4.3, there existed vulnerabilities and predisposing conditions that increased the likelihood that identified threat events would result in adverse impacts for Orvilia. Each vulnerability or predisposing condition is listed in the table below along with the corresponding threat events.

The methodology used to rate the level of pervasiveness was qualitative (i.e., subjective) and used a five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table F-3 Identify Vulnerabilities and Predisposing Conditions

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-10, TE-11	Very High
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their corporate mobile devices.	TE-7	Very High
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on corporate mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Very High

Note 1: Ratings of the level of pervasiveness were based on the qualitative scale found in Table F-5 of Appendix F in NIST SP 800-30 Revision 1 [12].

Note 2: Ratings of pervasiveness indicate that the vulnerabilities apply few (i.e., very low), some (i.e., low), many (i.e., moderate), most (i.e., high), or all (i.e., very high) organizational missions/business functions and processes, or information systems.

F.1.9 Task 2-4: Determine Likelihood of a Threat and the Likelihood of the Threat Having Adverse Impacts

Determine the likelihood that threat events of concern result in adverse impacts, considering (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those presumed to have a foreseeably high likelihood of occurrence.

The methodology used to identify the likelihood of threats of concern was qualitative (i.e., subjective) and used the following five-point scale.

- Very High

- High
- Moderate
- Low
- Very Low

Table F-4 Likelihood of Threat Events of Concern

Threat ID	Likelihood of Threat Event Initiation	Likelihood of Threat Event Resulting in Adverse Impacts	Overall Likelihood
TE-1	High	Very High	Very High
TE-2	Very High	High	Very High
TE-3	High	High	High
TE-4	Moderate	Very High	High
TE-5	High	Very High	Very High
TE-6	Moderate	High	Moderate
TE-7	High	High	High
TE-8	Moderate	High	High
TE-9	Moderate	High	Very High
TE-10	High	Very High	Very High
TE-11	Very High	Very High	Very High
TE-12	High	High	High

Note 1: For the Likelihood of Threat Event Initiation, the ratings translate as follows: Moderate = malicious actor is somewhat likely to initiate; High = malicious actor is highly likely to initiate; Very high = malicious actor is almost certain to initiate.

Note 2: For the Likelihood of Threat Event Resulting in Adverse Impacts, the ratings translate as follows: Moderate = if the threat is initiated, it is somewhat likely to have adverse impacts; High = if the threat is

initiated, it is highly likely to have adverse impacts; Very high = if the threat is initiated, it is almost certain to have adverse impacts.

Note 3: Overall likelihood was calculated based on the qualitative scale found in Table G-3 of Appendix G in NIST SP 800-30 Revision 1 [12]. It is derived from both the Likelihood of Threat Event Initiation and Likelihood of Threat Event Resulting in Adverse Impacts. Because these scales are not true interval scales, the combined overall ratings do not always reflect a strict mathematical average of the two ratings.

F.1.10 Task 2-5: Determine the Extent of Adverse Impacts

Determine the adverse impacts from threat events of concern considering (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Threat events with a high potential for adverse impacts were then identified in our specific scenario.

The methodology used to determine the extent of adverse impacts was qualitative (i.e., subjective) and used the following five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table F-5 Potential Adverse Impacts

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
TE-1	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-2	Harm to Operations, Other Organizations	Inability, or limited ability, to perform missions/business functions in the future	High

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
TE-3	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-4	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-5	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Loss of personally identifiable information	High
TE-6	Harm to Operations, Assets, Other Organizations	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Damage to reputation (and hence future or potential trust relationships)	Very High
TE-7	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-8	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
TE-9	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-10	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-11	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Damage to reputation (and hence future or potential trust relationships) Loss of personally identifiable information	High
TE-12	Harm to Operations, Assets, Other Organizations, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Loss of personally identifiable information Damage to reputation (and hence future or potential trust relationships)	High

Note 1: Ratings of maximum impact were based on the qualitative scale found in Appendix H, Table H-3 in NIST SP 800-30 Revision 1 [12].

Note 2: Ratings of maximum impact indicate the threat event could be expected to have negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), or multiple severe or catastrophic effects (i.e., very high).

Note 3: For specific examples of types of impact, see Appendix H of NIST SP 800-30, Revision 1 [12].

F.1.11 Task 2-6: Determine Risk to Organization

Determine the risk to the organization from threat events of concern considering (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.

In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those presumed to have a foreseeably high likelihood of occurrence and high potential for adverse impact in Orvilia's specific scenario.

Threat Source Characteristics

This table summarizes the risk assessment findings.

The methodology used to identify risk to organization was qualitative (i.e., subjective) and used the following five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table F-6 Summary of Risk Assessment Findings

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	Very High	High	High
TE-2: Theft of credentials through an SMS or email phishing campaign	VULN-1	Very High	High	High
TE-3: Malicious applications installed via URLs in SMS or email messages	VULN-3	High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	High	High	High
TE-5: Violation of privacy via misuse of device sensors	VULN-3	Very High	High	High
TE-6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	VULN-3	Moderate	Very High	High
TE-7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2	High	High	High
TE-8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	High	High	High
TE-9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	Very High	High	High
TE-10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1	Very High	High	High
TE-11: Loss of organizational data due to a lost or stolen device	VULN-3	Very High	High	High
TE-12: Loss of confidentiality of organizational data due to its	VULN-3	High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
unauthorized storage in non-organizationally managed services				

Note 1: Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [12].

Note 2: The risk rating itself is derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [12]. Because these scales are not true interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two variables. This is demonstrated in the table above in which levels of Moderate weigh more heavily than other ratings.

Note 3: Ratings of risk relate to the probability and level of adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1, adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e., very high).

Appendix G Privacy Risk Assessment

This section describes the privacy risk assessment conducted on Orvilia's enterprise security architecture. To perform the privacy risk assessment, the National Institute of Standards and Technology (NIST) Privacy Risk Assessment Methodology (PRAM) was used, a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. The PRAM can also serve as a useful communication tool to convey privacy risks within an organization. A blank version of the PRAM is available for download on NIST's website [19].

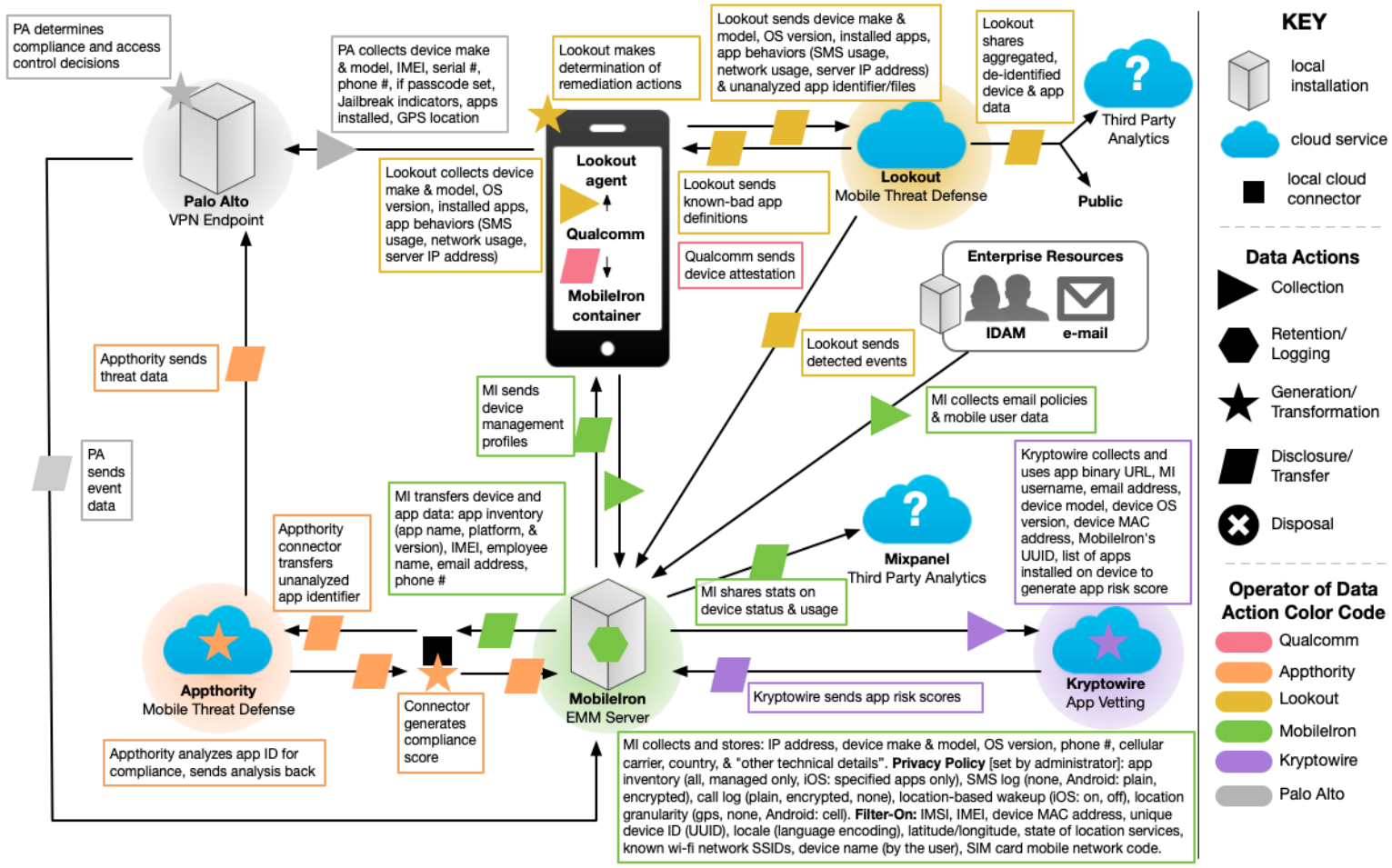
The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [20], to analyze potential problematic data actions. Data actions are any system operations that process personally identifiable information (PII). Processing can include collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of PII. A problematic data action is one that could cause an adverse effect for individuals.

The PRAM begins with framing the business objectives for the system, including the organizational needs served, and framing organizational privacy governance, including identification of privacy-related legal obligations and commitments to principles or other organizational policies. Next, create a data map to illustrate the data actions performed by the system and the PII processed by the data actions. These data actions, the PII being processed, and the contextual factors that describe the circumstances surrounding the system's processing of PII serve as inputs to the risk analysis.

Then, assess the probability that a data action will become problematic for individuals, assess the secondary costs absorbed by the organization from a data action creating a problem for individuals, and use likelihood and impact calculations to determine the total estimated risk per data action. Finally, list potential mitigating technical and policy controls for the identified risks. The output from the PRAM activities resulted in the information contained in Figure G-1.

Note: The Key within Figure G-1 includes all data action types (Collection, Retention/Logging, Generation/Transformation, Disclosure/Transfer, and Disposal), but this particular example solution does not cover the Disposal of data in the Privacy Data Mapping exercise.

Figure G-1 PRAM Data Map for Orvilia's Enterprise Security Architecture



As an output of the Orvilia PRAM, we identified three broad data actions with the potential to create problems for individuals and relevant mitigations. Some mitigations listed under a particular data action may provide privacy benefits to individuals beyond the scope of that data action. We also identified overarching training and support controls that can help mitigate risks associated with all three of these data actions.

While a security information and event management (SIEM) capability was not used in the reference implementation, SIEMs, as discussed here, can be extremely beneficial in understanding the privacy implications of the mobile device security data being logged, aggregated, and stored.

G.1 Data Action 1: Blocking Access and Wiping Devices

Devices that might pose a risk to the organization's security posture can be blocked from accessing enterprise resources or wiped and reset to factory setting defaults. Options are outlined in the following sections for how this might be accomplished.

G.1.1 Potential Problem for Individuals

In a corporate-owned personally-enabled or bring your own device environment, employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data—and employees may not even expect this possibility. A hypothetical example would be that an Orvilia employee stores personal pictures on the mobile device issued to them by Orvilia, but these photos are lost when their device is wiped after anomalous activity is detected.

G.1.2 Mitigations

Block access instead of wiping devices.

As an alternative to wiping data entirely, devices can be blocked from accessing enterprise resources, for example, until an unapproved application is removed. This temporary blocking of access helps ensure an individual will not lose personal data through a full wipe of a device. Taking this approach may help bring the system's capabilities into alignment with employees' expectations about what can happen to their devices, especially if they are unaware that devices can be wiped by administrators—providing for greater *predictability* in the system.

- Related mitigation: If this approach is taken, remediation processes should also be established and communicated to employees. It is important to have a clear remediation process in place to help employees regain access to resources on their devices at the appropriate time. It is equally important to clearly convey this remediation process to employees. A remediation process provides greater manageability in the system supporting employees' ability to access resources. If well communicated to employees, this also provides greater predictability, as employees will know the steps involved in regaining access.

Enable only selective wiping.

An alternative mitigation option for wiping is to specify the information to be wiped. Performing a selective wipe is an option that only removes enterprise data from the device instead of being a full factory reset. When configured this way, a wipe preserves employees' personal configurations, applications, and data while removing only the corporate configurations, applications, and data. Within the example solution, this option is available for iOS devices.

Advise employees to back up the personal data maintained on devices.

If device wiping remains an option for administrators, encourage employees to perform regular backups of their personal data to ensure it remains accessible in case of a wipe.

Limit staff with the ability to perform wipes or block access.

Limit staff with the ability to perform a wipe to only those with that responsibility by using role-based access controls. This can help decrease the chances of accidentally removing employee data or blocking access to resources.

G.2 Data Action 2: Employee Monitoring

The assessed infrastructure offers Orvilia a number of security capabilities, including reliance on comprehensive monitoring capabilities, as noted in Section 4, Architecture. A significant amount of data relating to employees, their devices, and their activities is collected and analyzed by multiple parties.

G.2.1 Potential Problem for Individuals

Employees may not be aware that their interactions with the system are being monitored and may not want this monitoring to occur. Collection and analysis of information might enable Orvilia or other parties to craft a narrative about an employee based on their interactions with the system, which could lead to a power imbalance between Orvilia and the employee and loss of trust in the employer if the employee discovers unanticipated monitoring.

G.2.2 Mitigations

Limit staff with ability to review data about employees and their devices.

This may be achieved using role-based access controls and by developing organizational policies to limit how employee data can be used by staff with access to that data. Access can be limited to any dashboard in the system containing data about employees and their devices but is most sensitive within the mobile management dashboard, which is the hub for data about employees, their devices, and threats. Minimizing access to sensitive information can enhance *disassociability* for employees using the system.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. Consider the configuration options for intrusive device features, such as location services, application inventory collection, and location-based wake-ups. When collecting application inventory data, ensure that information is gathered only from applications installed from the organization's corporate application store. While these administrative configurations may help provide for disassociability in the system, there are also some opportunities for employees to limit the data collected.

Organizations may allow their employees to manage certain aspects and configurations of their device. For example, employees may be able to disable location services in their device OS to prevent collection of location data. Each of these controls contributes to reducing the number of attributes collected regarding employees and their mobile devices. This reduction of collected data limits administrators' ability to associate information with specific individuals.

Dispose of PII.

Disposal of PII after an appropriate retention period can help reduce the risk of entities building profiles of individuals. Disposal can also help bring the system's data processing into alignment with employees' expectations and reduce the security risk associated with storing a large volume of PII. Disposal may be particularly important for certain parties in the system that collect a larger volume of data or more sensitive data. Disposal may be achieved using a combination of policy and technical controls. Parties in the system may identify what happens to data, when, and how frequently.

G.3 Data Action 3: Data Sharing Across Parties

The infrastructure involves several parties that serve different purposes supporting Orvilia's security objectives. As a result, there is a significant flow of data about individuals and their devices occurring across various parties. This includes sharing device and application data publicly and with third-party analytics services, and includes sharing device status and usage with third-party analytics.

G.3.1 Potential Problems for Individuals

Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them. If administrators and co-workers know what colleague is conducting activity on his or her device that triggers security alerts, it could cause employee embarrassment or emotional distress. This information being revealed and associated with specific employees could also lead to stigmatization and even impact Orvilia upper management in their decision-making regarding the employee. Further, clear text transmissions could leave information vulnerable to attackers and the unanticipated release of employee information.

G.3.2 Mitigations

Use de-identification techniques.

De-identification of data helps decrease the chances that a third party is aggregating information pertaining to one specific individual. While de-identification can help reduce privacy risk, there are residual risks of reidentification. De-identification techniques may be applied to aggregated data before sharing it with third-party analytics and publicly.

Use encryption.

Encryption decreases the chances of insecure information being transmitted between parties. Organizations should keep this in mind when considering how their enterprise data is transmitted and stored. Mobile security systems share mobile device and application data with one another to optimize efficiency and leverage data to perform security functions. This data may include application inventory and employee name, email address, and phone number. Some systems offer multiple encryption options that allow an organization to choose the encryption level necessary for the type of data that is stored or transmitted.

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with individuals, is important in preventing association of specific events with particular employees, which could cause embarrassment. Products used by the organization may offer options for restricting the amount of employee information that an administrator can access. These options may include hiding an employee's username and email address from the administrator console. Mobile application information may also include employee information. Organizations should consider how their mobile and other security systems hide application names, application binary analysis details, network names service set identifier, and network analysis details from administrators.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. Identifying the employee information collected and determining what data elements are stored assist in assessing the privacy risk of mobile security systems. Organizations should consider the mobile security system's ability to limit or reduce collection and storage of employee information, such as username, email address, Global Positioning System location, and application data.

Use contracts to limit third-party data processing.

Establish contractual policies to limit data processing by third parties to only the processing that facilitates delivery of security services, and no data processing beyond those explicit purposes.

G.4 Mitigations Applicable Across Various Data Actions

Several mitigations provide benefits to employees pertaining to all three data actions identified in the privacy risk assessment. These training and support mitigations can help Orvilia appropriately inform employees about the system and its data processing.

Mitigations:

Provide training to employees about the system, parties involved, data processing, and administrative actions that can be taken.

Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to third parties. Training should include confirmation from employees that they understand the actions that can be taken on their devices and the consequences—whether this involves blocking access or wiping data. Employees may also be informed of data retention periods and when their data will be disposed of. This can be more effective than sharing a privacy notice, which research has shown that individuals are unlikely to read.

Provide ongoing notifications or reminders about system activity.

This can be achieved using push notifications, similar to those pictured in screenshots in Appendix H, Threat Event 6, to help directly link administrative actions on devices to relevant threats and help employees understand why an action is being taken. Notifications of changes to policies can help increase system predictability by setting employee expectations appropriately with the way the system processes data and the resulting actions.

Provide a support point of contact.

By providing employees with a point of contact in the organization who can respond to inquiries and concerns regarding the system, employees can gain a better understanding of the system's processing of their data, which enhances predictability.

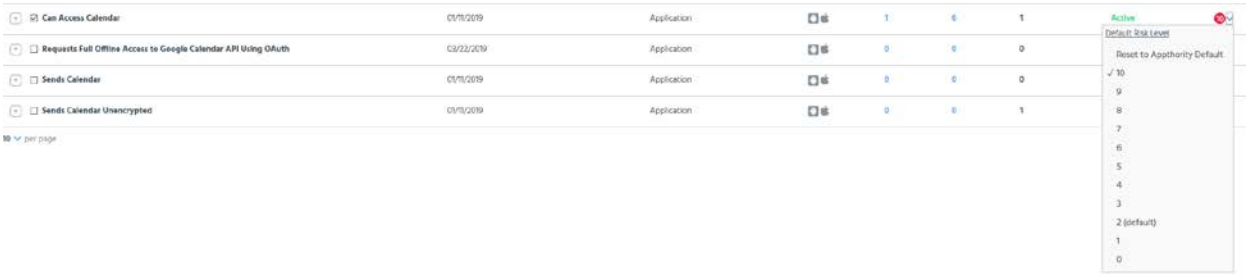
Appendix H Threat Event Test Information

Detailed information and screenshots for some of this practice guide's threat events and their testing results are provided below.

H.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

A part of Threat Event 1's testing conclusions is shown in the following screen capture, where the calendar access permission is being set to a risk score of 10. This allows MobileIron to automatically apply the mobile threat protection high-risk label to the device and quarantine the device until the privacy-intrusive application is removed.

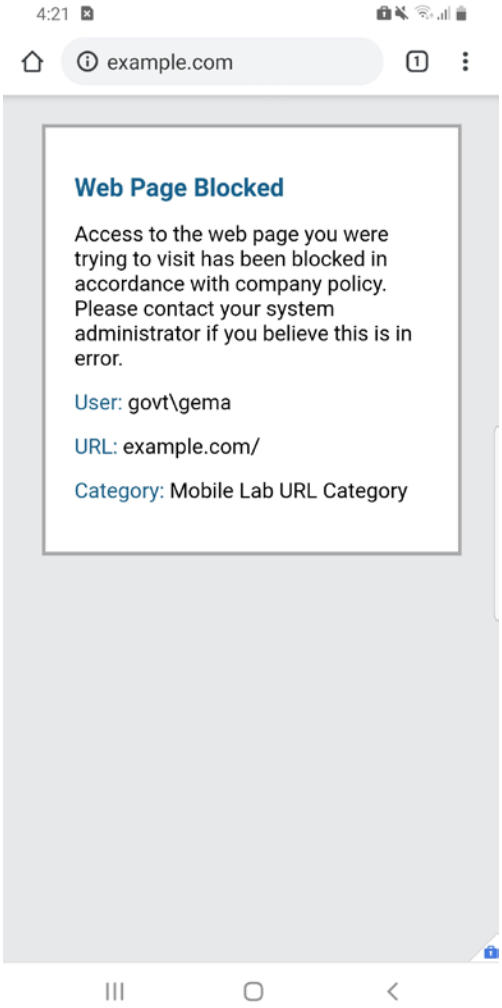
Figure H-1 Setting a Custom Risk Level in Appthority



H.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email Phishing Campaign

Threat Event 2's outcome is shown in the following screen capture, where PAN-DB is blocking a website manually added to the malicious uniform resource locator (URL) database.

Figure H-2 PAN-DB Blocked Website



H.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

The following screenshots demonstrate enabling the Unknown Sources toggle and installing an application through a link in an email message.

Figure H-3 Lock Screen and Security

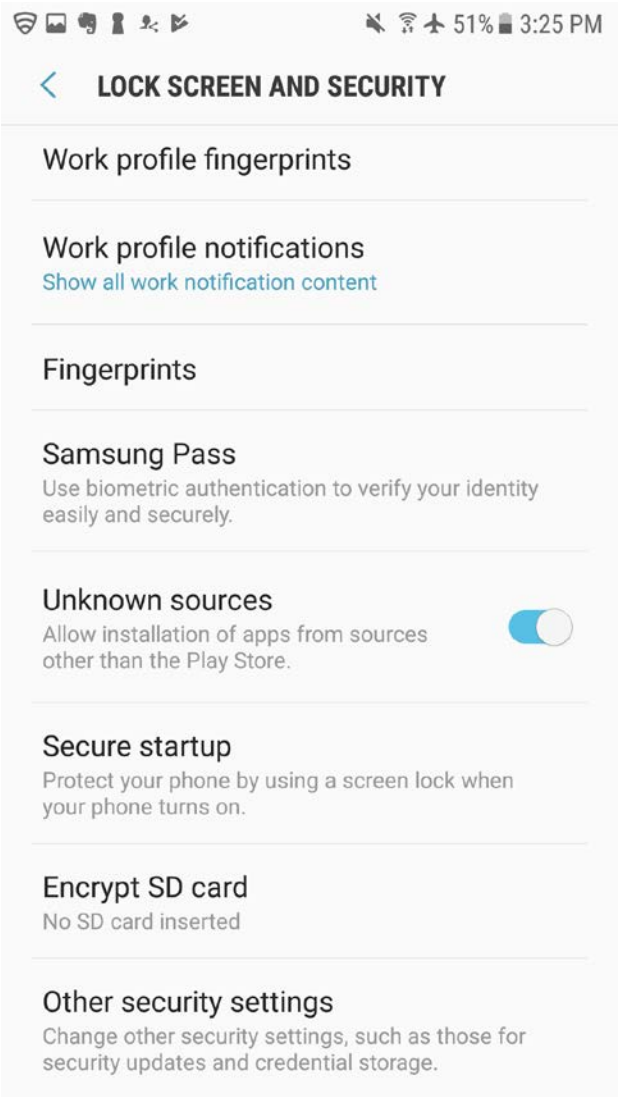


Figure H-4 Phishing Email on Android

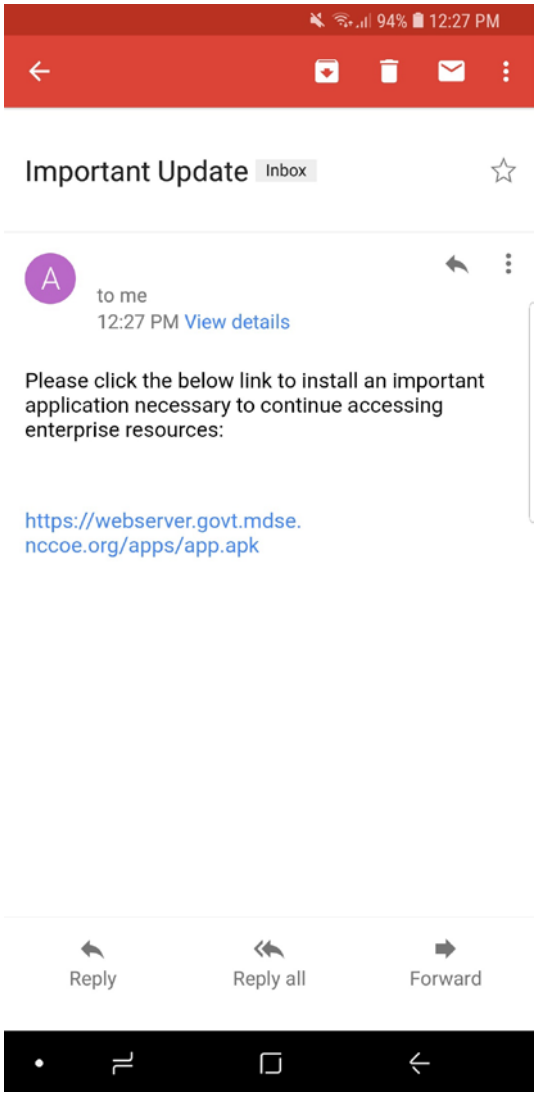


Figure H-5 depicts the iOS test activity of receiving an email containing a link to an application from a non-Apple App Store source.

Figure H-5 Phishing Email on iOS

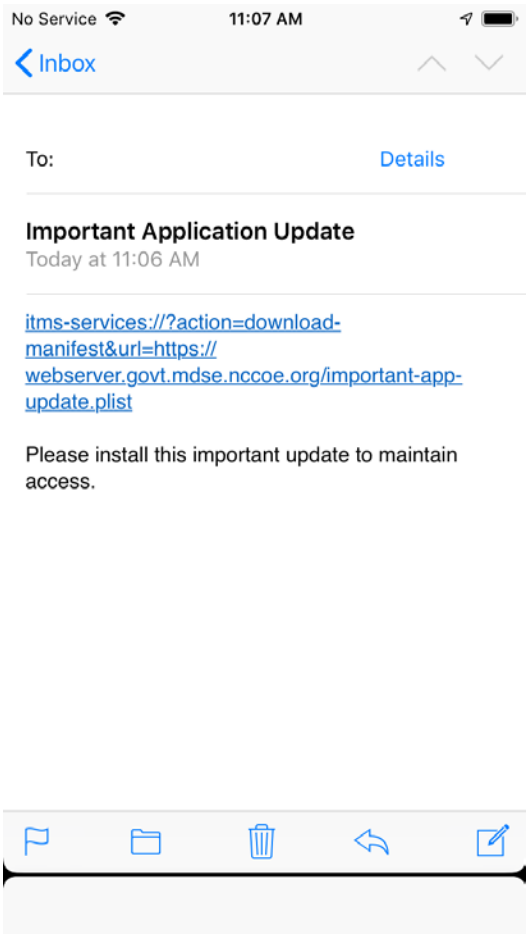
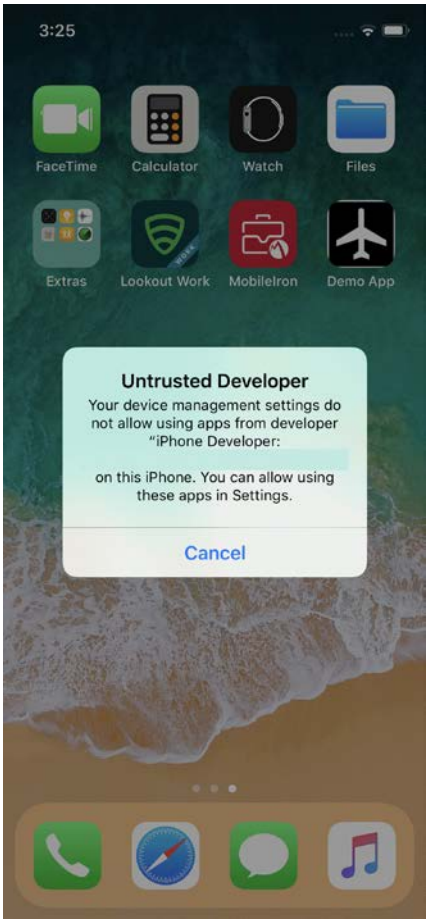


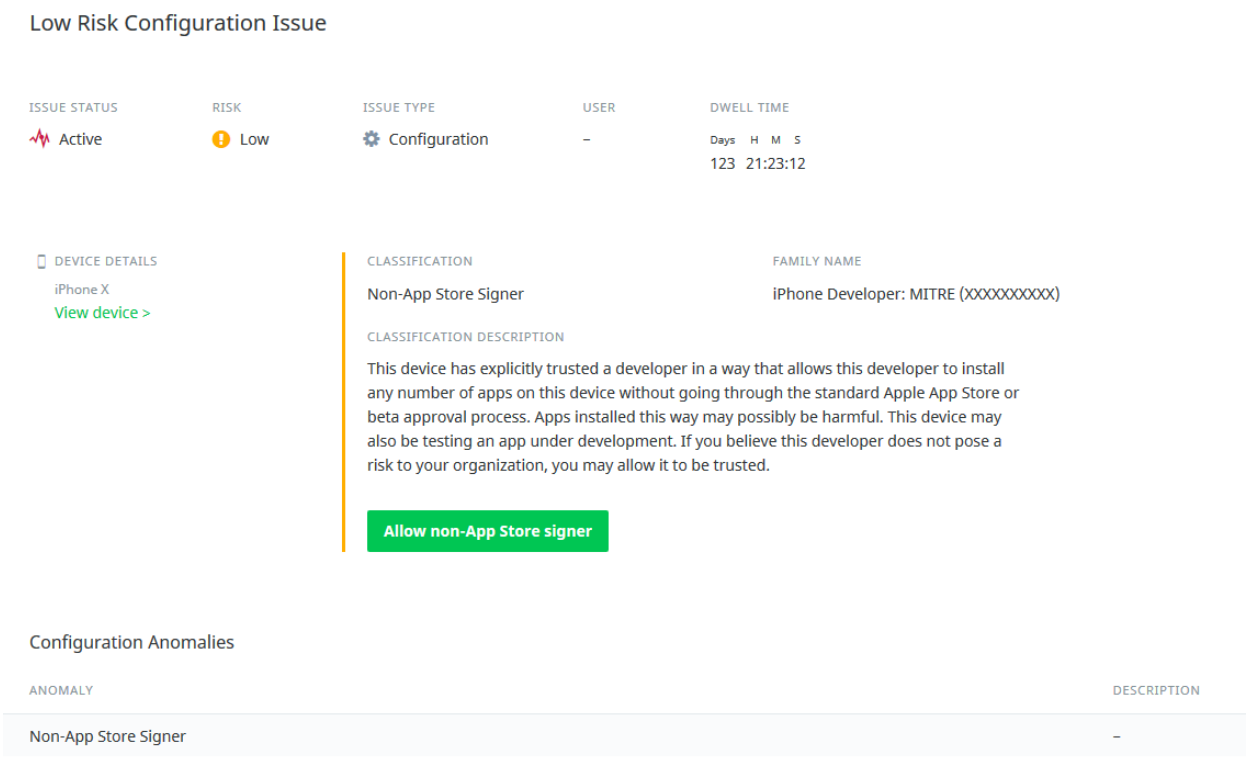
Figure H-6 Untrusted Developer Warning



After the application is installed, an untrusted developer notice appears as shown in Figure H-6 when the user attempts to launch the application.

Figure H-7 shows Lookout's ability to detect application signing certificates that have been trusted on a device by the user to execute applications from sources other than Apple's App Store.

Figure H-7 Application Signing Certificates



The following screenshots depict an attempt to install and run the unauthorized demo application on an iOS device with the `allowEnterpriseAppTrust` policy restriction set to false by an Enterprise Mobility Management (EMM) system. The user is not able to trust the developer when the policy restriction is active, and hence the application will not run.

Figure H-8 Restriction Setting Modification Screen

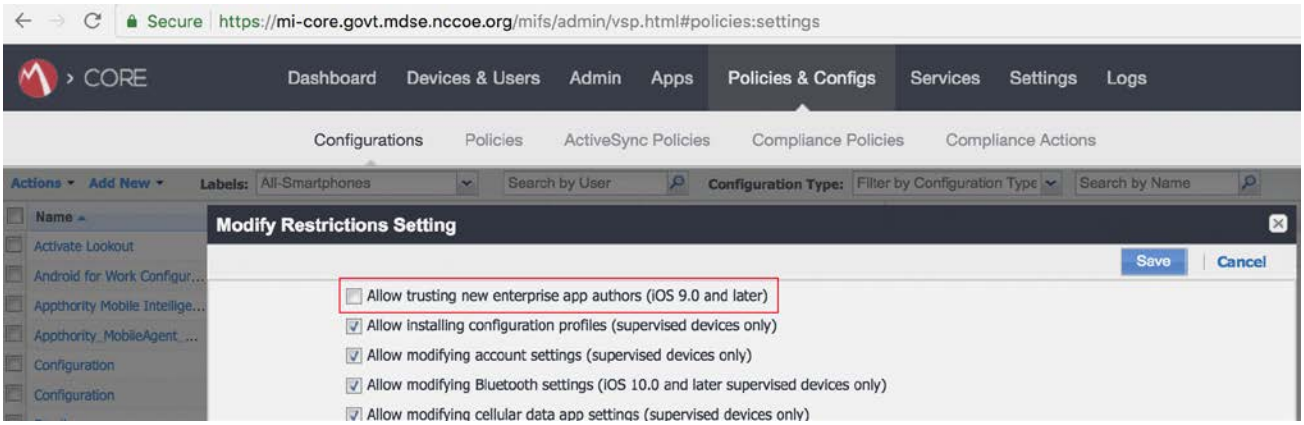
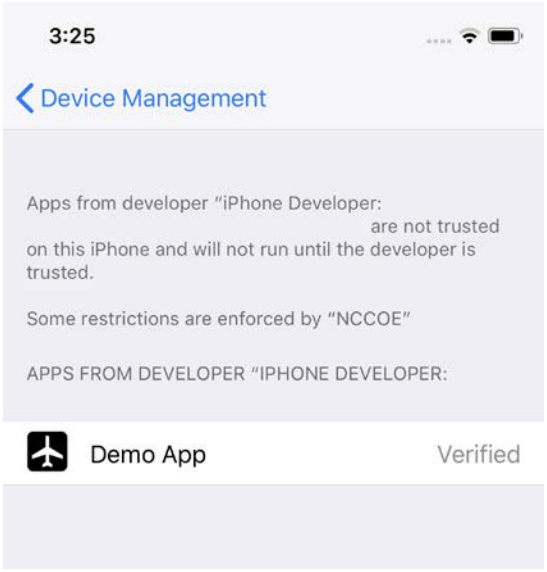


Figure H-9 Unable to Trust Developer

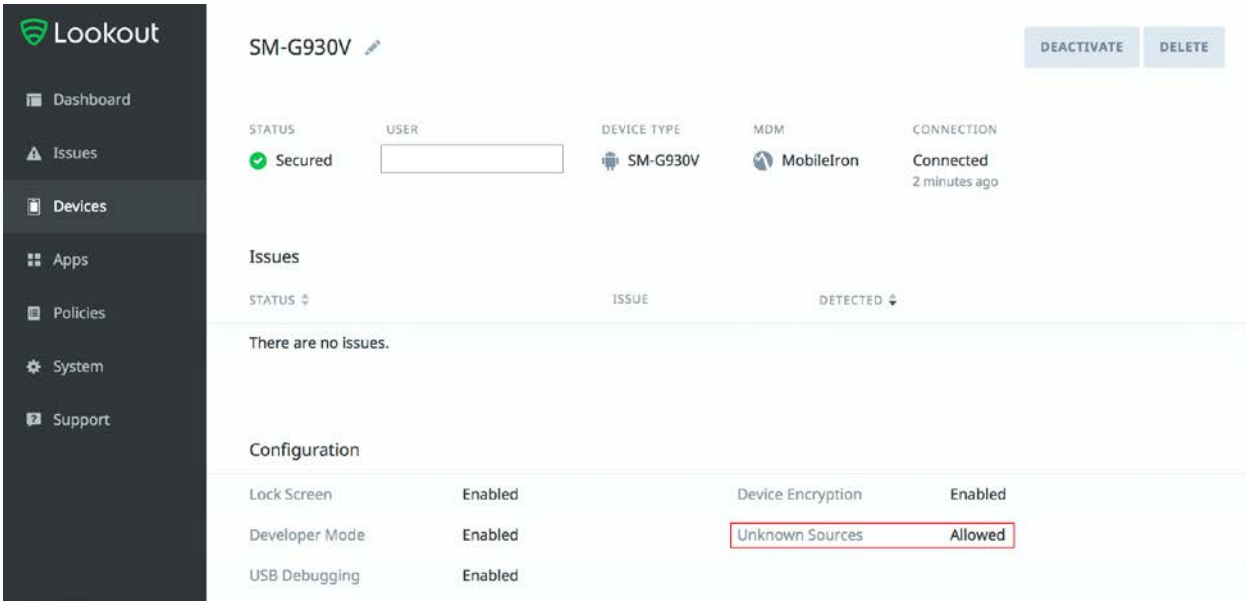


Android Device Testing

On Android devices, applications cannot be installed from sources other than the Google Play Store unless the Unknown Sources setting is enabled in the device's security settings. Lookout can identify when the Unknown Sources setting has been enabled and can communicate this information to MobileIron to enable automated response actions, such as blocking device access to enterprise resources until the situation is resolved. However, even if Unknown Sources is disabled, it is possible that the setting was previously enabled and that unauthorized applications were installed at that time.

Figure H-10 shows Lookout's ability to detect Android devices with Unknown Sources enabled.

Figure H-10 Unknown Sources Detection



H.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the Operating System or Firmware

Figure H-11 demonstrates Lookout's ability to identify known vulnerabilities to which unpatched iOS and Android devices are susceptible. Figure H-12 shows the patch level of the device.

Figure H-11 Vulnerability Identification

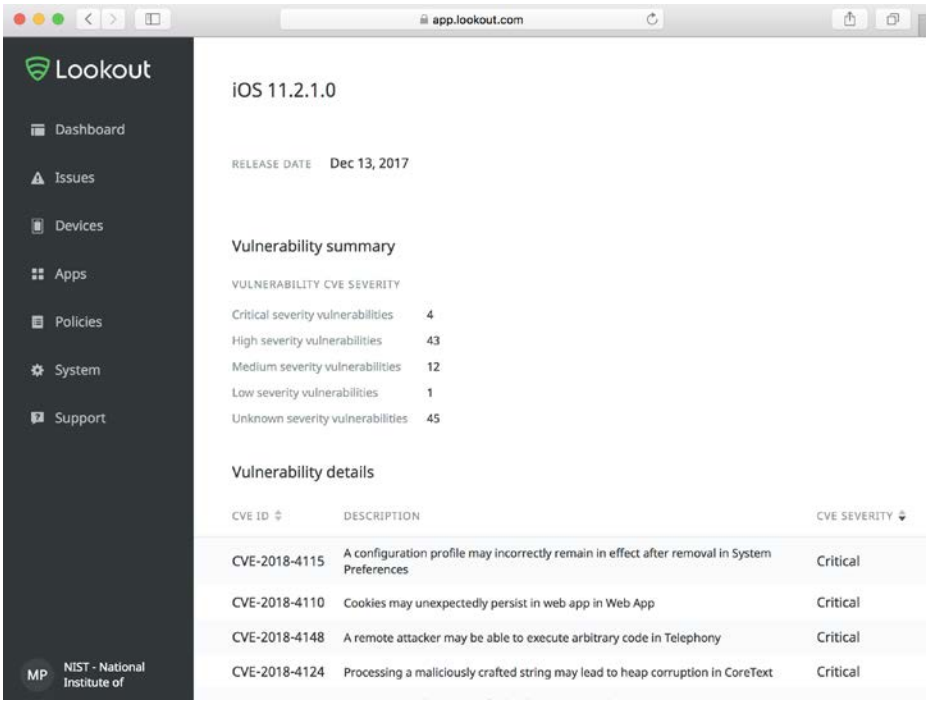
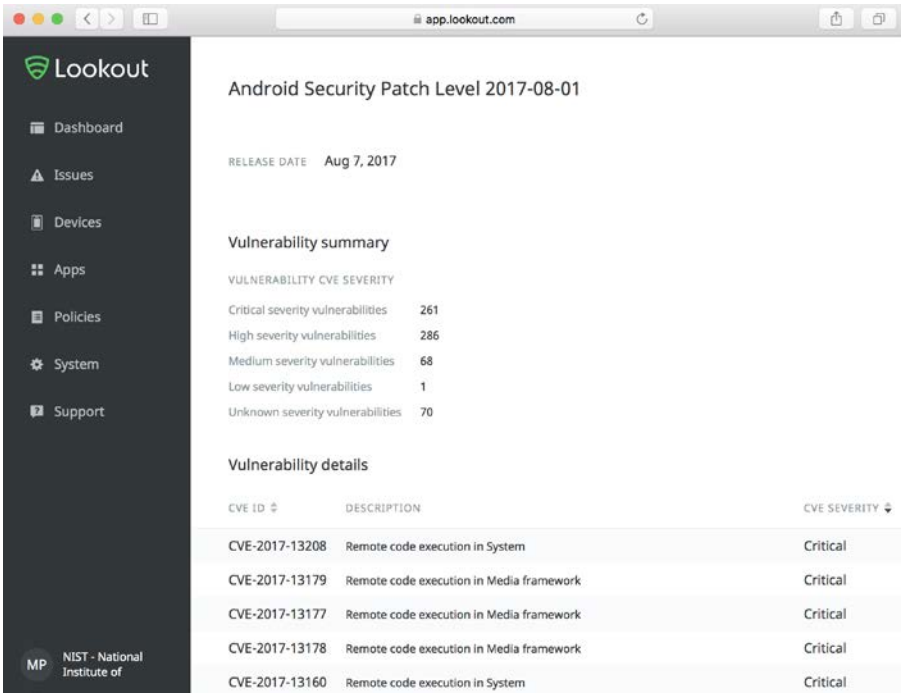


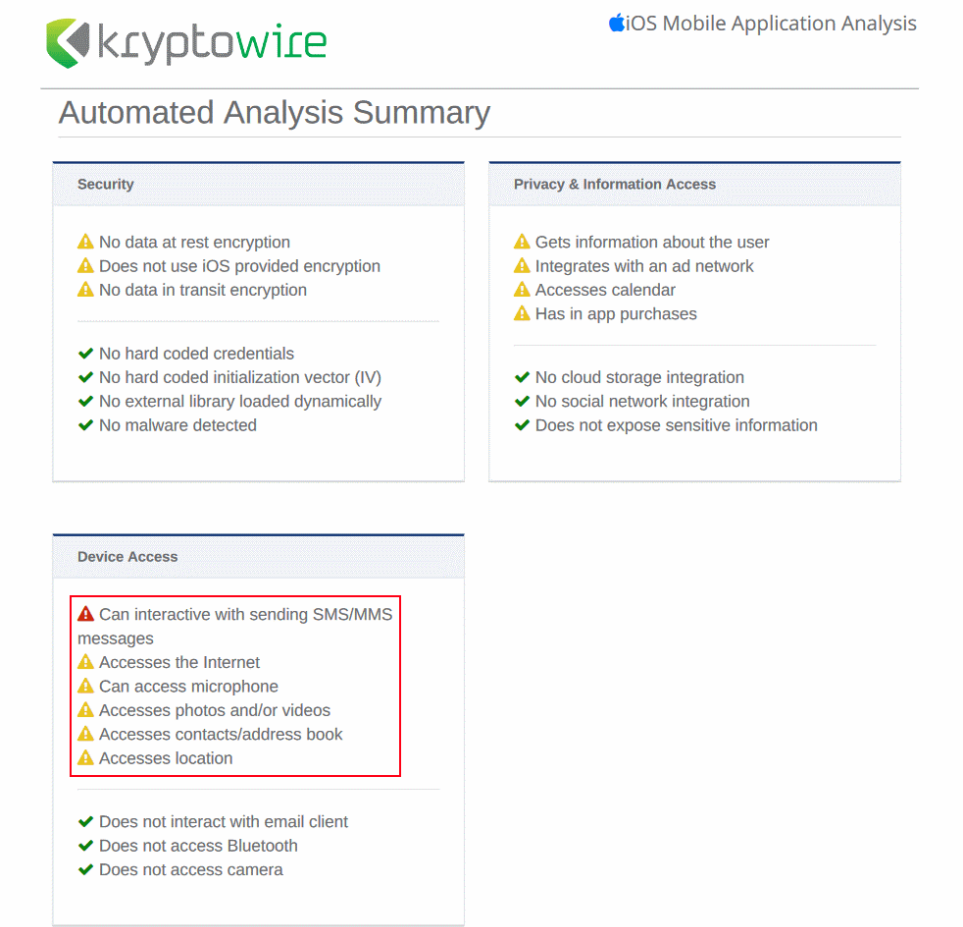
Figure H-12 Patch Level Display



H.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

The following screenshot depicts a Kryptowire application analysis report and the reported permissions that this application was requesting.

Figure H-13 Kryptowire Analysis Report



H.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/Mobile Device Management, Network, Virtual Private Network (VPN) Profiles, or Certificates

The configuration profile used for configuring and testing Threat Event 6 is shown in Figure H-14.

Figure H-14 Configuration Profile Example

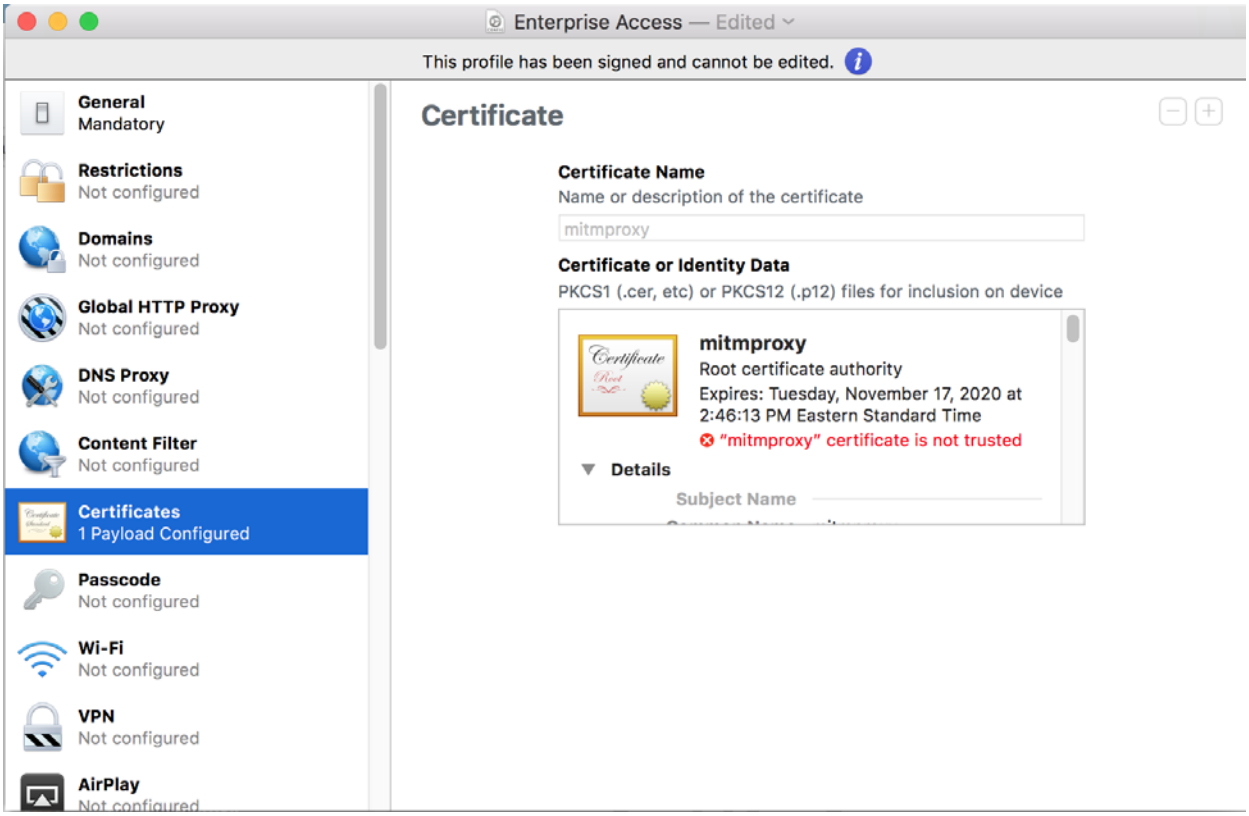


Figure H-15 shows the email containing a malicious device configuration profile, and Figure H-16 shows the warning displayed to the user when attempting to mark the malicious certificate as a trusted root.

Figure H-15 Configuration Profile Phishing Email

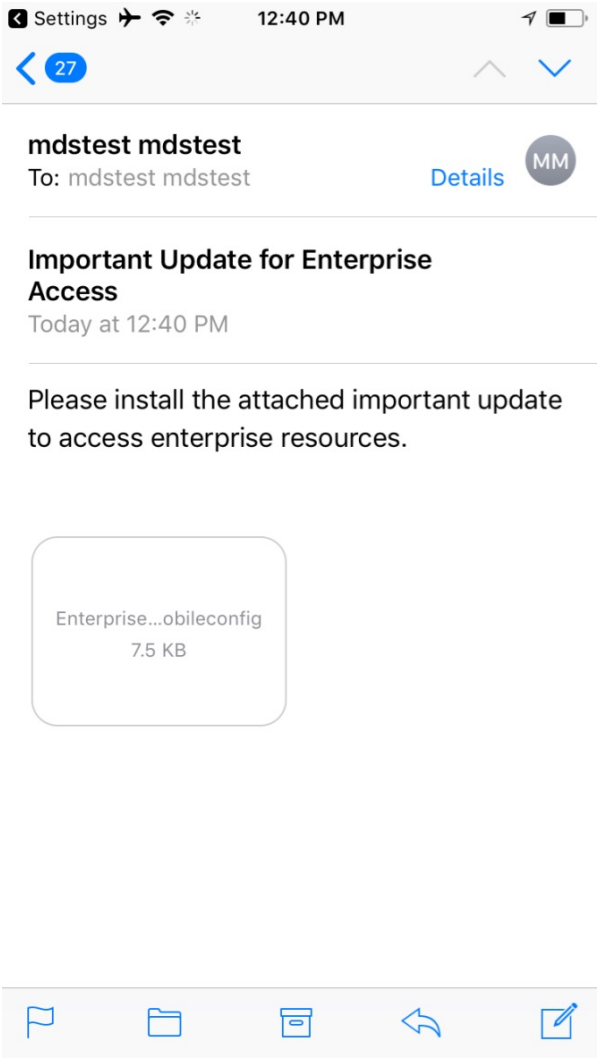


Figure H-16 Root Certificate Authority Enablement Warning

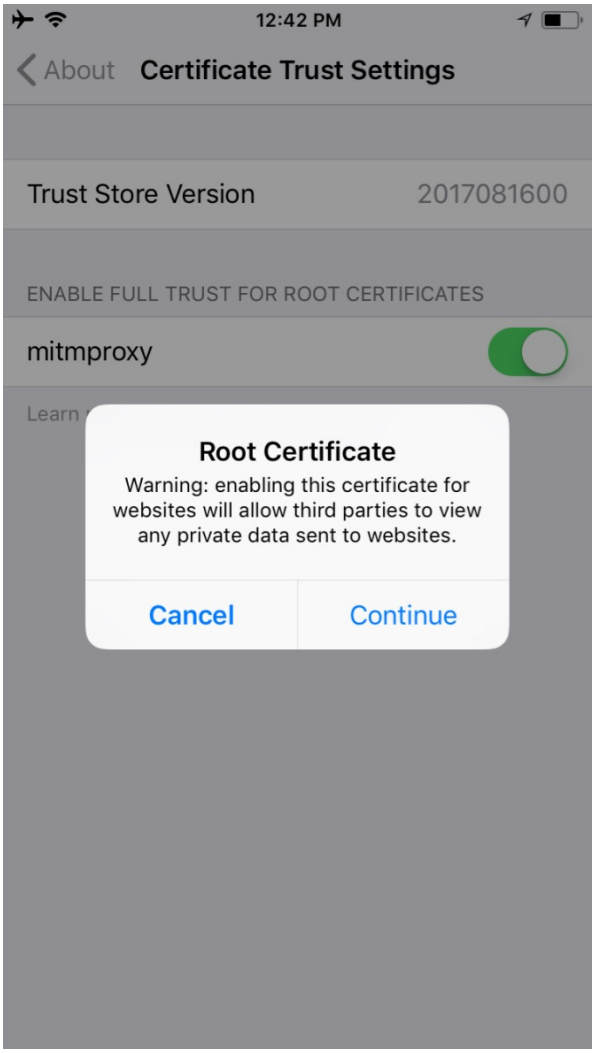
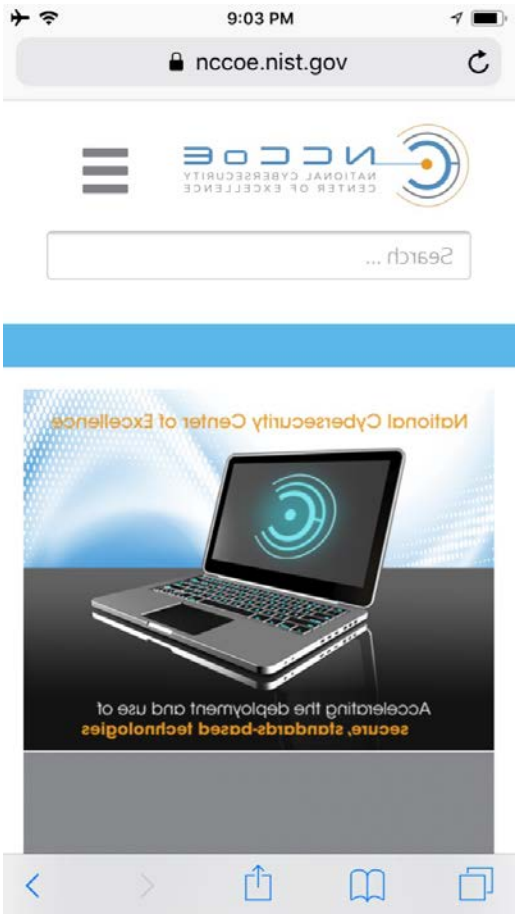


Figure H-17 Reversed Web Page



Browse to a hypertext transfer protocol secure (https) website from the mobile device and observe whether the content has been reversed. Figure H-17 illustrates that the person-in-the-middle attack on a Transport Layer Security-protected connection was successful.

The following screenshots demonstrate a person-in-the-middle attack on Android.

Figure H-18 Certificate Phishing Email

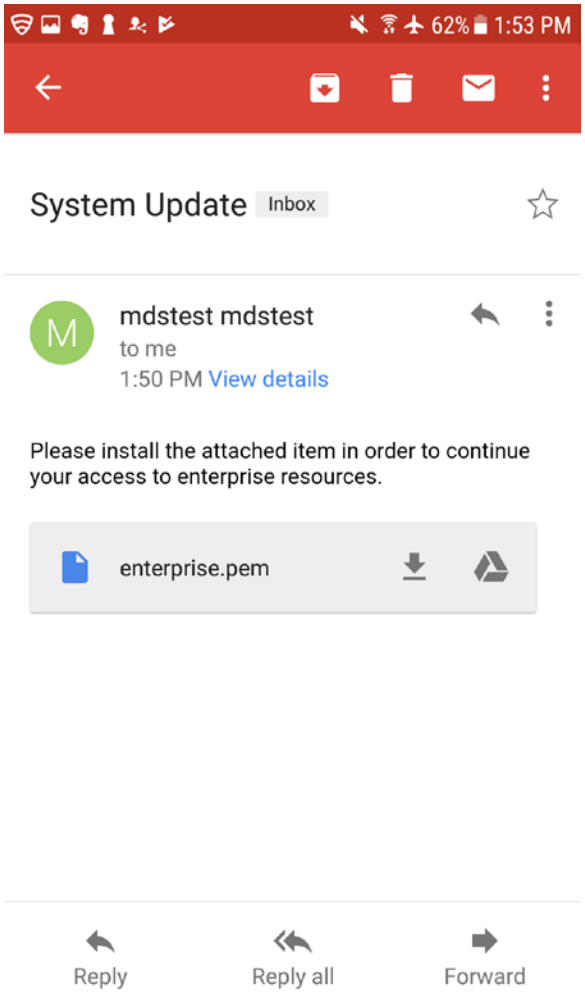
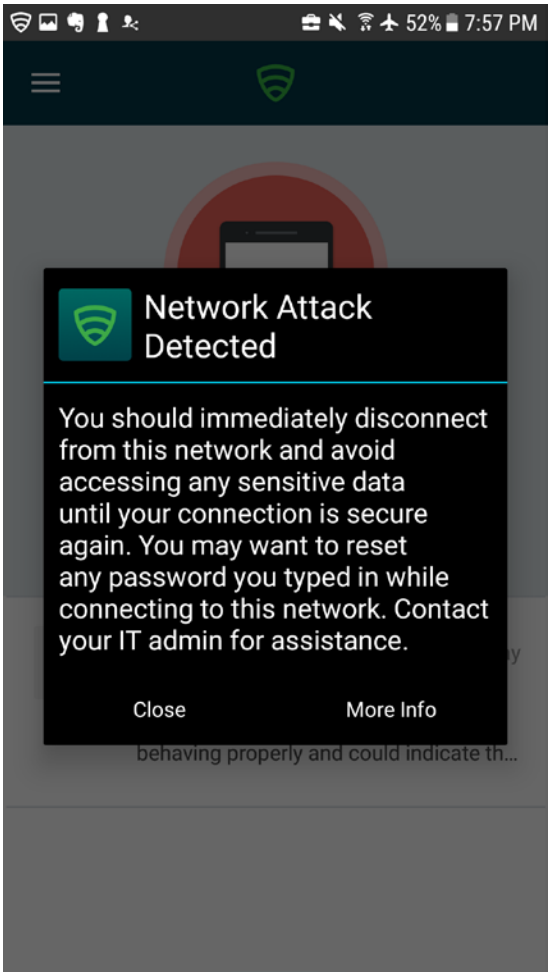


Figure H-19 Reversed Web Page

Person-in-the-middle attack is detected by Lookout as shown in Figure H-20.

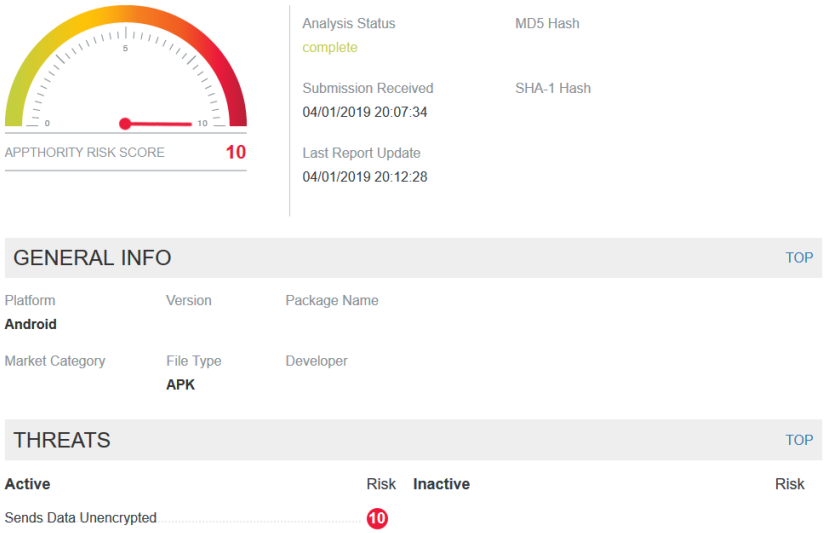
Figure H-20 Network Attack Detected



H.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

The following screenshot shows Appthority detecting an application sending data unencrypted.

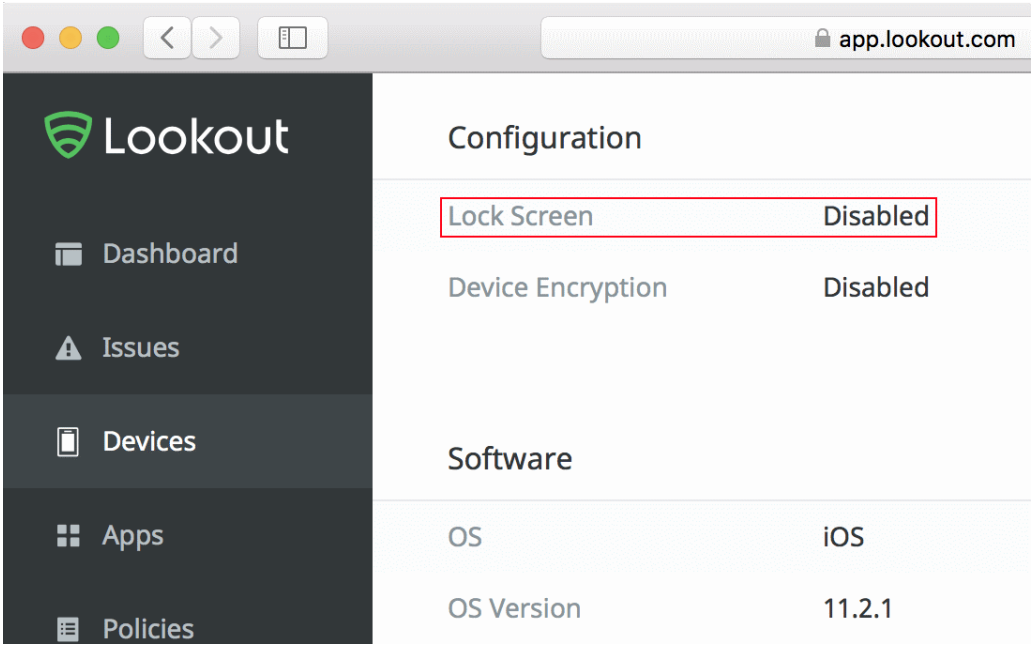
Figure H-21 Unencrypted Data Transfer



H.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

MobileIron applies a policy to the devices to enforce a mandatory personal identification number and device-wipe capability. Lookout reports devices that have the lock screen disabled.

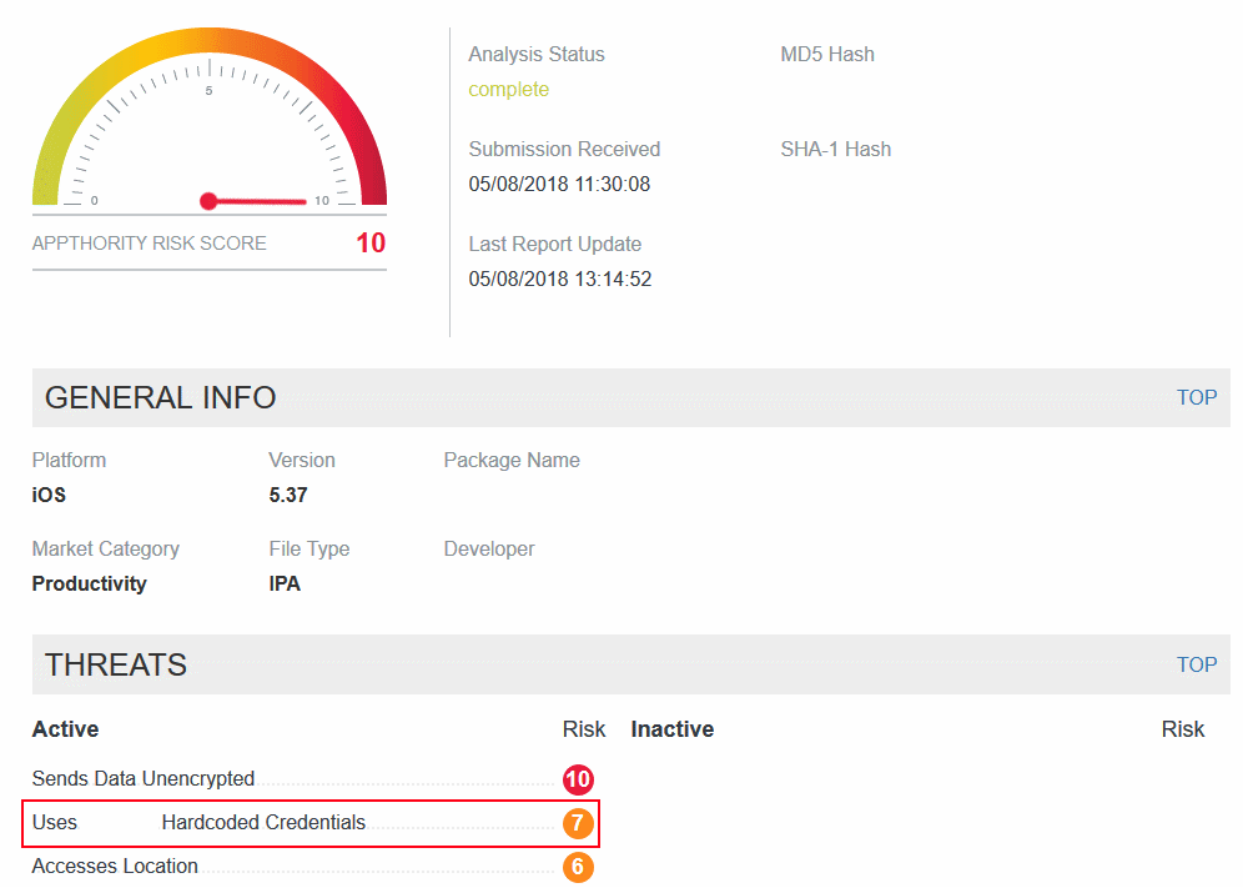
Figure H-22 Lock Screen Disabled Detection Notice



H.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

As shown in Figure H-23, Appthority recognized that an application used hard-coded credentials. The application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded credentials were used for access to enterprise resources by unauthorized entities or for unauthorized actions.

Figure H-23 Hard-Coded Credentials



H.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

The following two screenshots depict the inability to connect to the GlobalProtect VPN without the proper client certificates, obtainable only through enrolling the device in MobileIron.

Figure H-24 No Certificates Found on Android

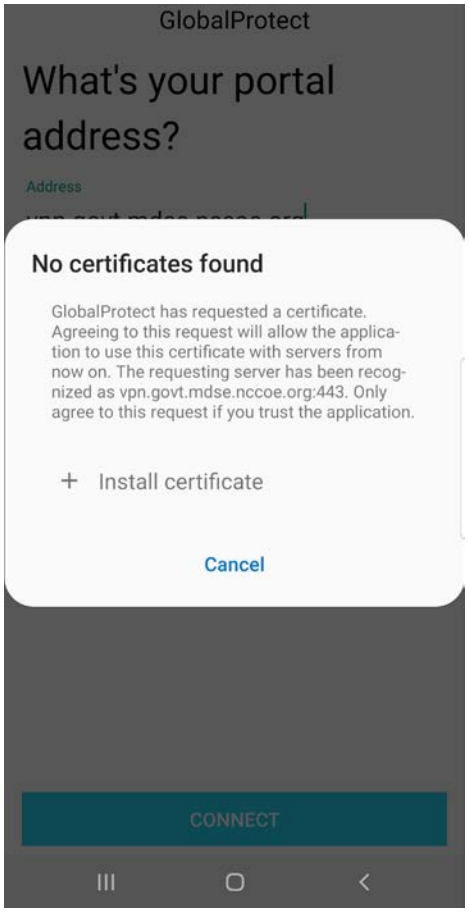
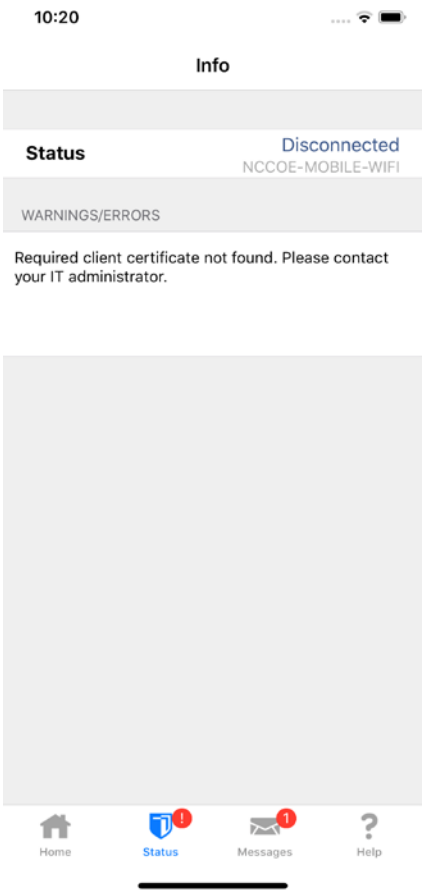


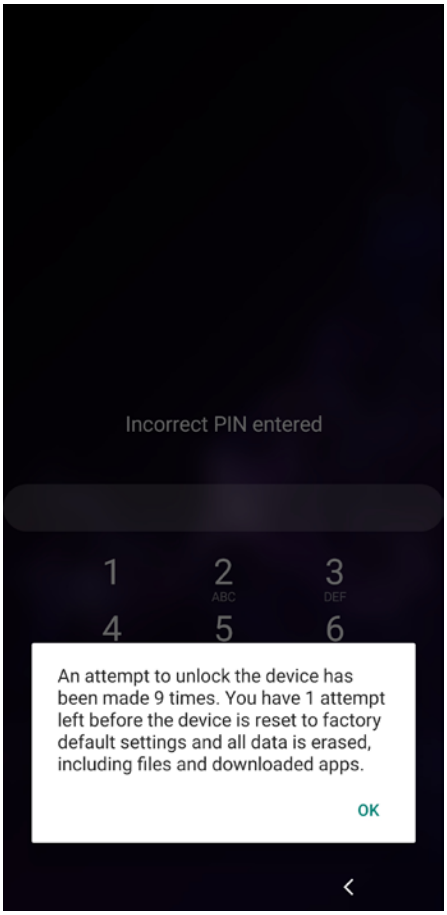
Figure H-25 No Certificates Found on iOS



H.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device

This screenshot depicts the final warning before Android factory-resets the device. In the event the device was stolen, all corporate data would be removed from the device after one more failed unlock attempt, thwarting the malicious actor's goal.

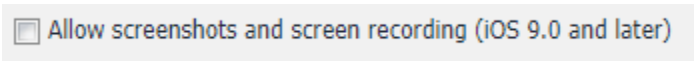
Figure H-26 Android Device Wipe Warning



H.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its Unauthorized Storage in Non-Organizationally Managed Services

The following screenshot shows one of the data loss prevention configuration options in MobileIron for iOS.

Figure H-27 Disallowing Screenshots and Screen Recording



Appendix I Example Security Control Map

Table I-1 lists the technologies used in this project and provides a mapping among the generic application term, the specific product used, the security control(s) the product provides, and a mapping to the relevant National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Work Roles*. From left to right, the columns in the table describe:

- **Specific product used:** vendor product used by the example solution
- **How the component functions in the build:** capability the component provides in the example solution. This is mapped to the general mobile technology component term.
- **Applicable Cybersecurity Framework Subcategories:** applicable Cybersecurity Framework Subcategory(s) that the component is providing in the example solution
- **Applicable NIST controls:** the NIST SP 800-53 Revision 4 controls that the component provided in the example solution
- **ISO/IEC 27001:2013:** International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013 mapping that the component provides in the example solution
- **CIS 6:** Center for Internet Security (CIS) version 6 controls mapping that the component provides in the example solution
- **NIST SP 800-181, *NICE Framework Work Roles:*** NICE Framework work role(s) that could be used to manage this component's use in the example solution. This mapping provides information on the workforce members who would be engaged in this part of the example solution's support.

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

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Mobile Threat Intelligence						
Appthority Cloud Service	Mobile Threat Intelligence	ID.RA-1—Asset vulnerabilities are identified and documented	Security Assessment and Authorization CA-2, CA-7, CA-8 Risk Assessment RA-3, RA-5 System and Services Acquisition SA-5, SA-11 System and Information Integrity SI-2, SI-4, SI-5	A.12.6.1 Control of Technical vulnerabilities A.18.2.3 Technical Compliance Review	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor SP-ARC-002 Security Architect OM-ANA-001 Systems Security Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager
		ID.RA-3—Threats, both internal and external, are	Risk Assessment RA-3	Clause 6.1.2 Information Risk Assessment Process	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor PR-CDA-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		identified and documented	System and Information Integrity SI-5 Insider Threat Program PM-12, PM-16			Cyber Defense Analyst OV-SPP-001 Cyber Workforce Developer and Manager OV-TEA-001 Cyber Instructional Curriculum Developer AN-TWA-001 Threat/Warning Analyst PR-VAM-001 Vulnerability Assessment Analyst OV-MGT-001 Information Systems Security Manager
		DE.CM-4—Malicious code is detected	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 4 Continuous Vulnerability Assessment and Remediation	PR-VAM-001 Vulnerability Assessment Analyst PR-CIR-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
					CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses CSC 12 Boundary Defense	Cyber Defense Incident Responder PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
		DE.CM-5—Unauthorized mobile code is detected	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
Mobile Application Vetting Service						
Kryptowire Cloud Service	Application Vetting	ID.RA-1—Asset vulnerabilities are identified and documented	Security Assessment and Authorization CA-2, CA-7, CA-8 Risk Assessment RA-3, RA-5	A.12.6.1 Control of Technical vulnerabilities A.18.2.3 Technical	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor SP-ARC-002 Security Architect

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
			System and Services Acquisition SA-5, SA-11 System and Information Integrity SI-2, SI-4, SI-5	Compliance Review		OM-ANA-001 Systems Security Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager
		ID.RA-3—Threats, both internal and external, are identified and documented	Risk Assessment RA-3 System and Information Integrity SI-5 Insider Threat Program PM-12, PM-16	Clause 6.1.2 Information Risk Assessment Process	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor OM-ANA-001 Systems Security Analyst OV-SPP-001 Cyber Workforce Developer and Manager OV-TEA-001 Cyber Instructional Curriculum Developer

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						AN-TWA-001 Threat/Warning Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager
		DE.CM-4—Malicious code is detected	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 4 Continuous Vulnerability Assessment and Remediation CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses CSC 12 Boundary Defense	PR-CIR-001 Cyber Defense Incident Responder PR-CDA-001 Cyber Defense Analyst PR-VAM-001 Vulnerability Assessment Analyst OM-NET-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						Network Operations Specialist
		DE.CM-5—Unauthorized mobile code is detected	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
Mobile Threat Defense						
Lookout Cloud Service/ Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android)	Mobile Threat Defense/Endpoint Security	PR.AC-5—Network integrity is protected (e.g., network segregation, network segmentation)	Access Control AC-4, AC-10 System and Communications Protection SC-7	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.13.2.1 Information Transfer Policies and Procedures	CSC 9 Imitation and Control of Network Ports, Protocols, and Services CSC 14 Controlled Access Based on the Need to Know CSC 15 Wireless Access Control	OM-ADM-001 System Administrator OV-SPP-002 Cyber Policy and Strategy Planner PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions	CSC 18 Application Software Security	
		PR.PT-4—Communications and control networks are protected	Access Control AC-4, AC-17, AC-18 Contingency Planning Policy and Procedures CP-8 System and Communications Protection SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.14.1.3 Protecting Application Services Transactions	CSC 8 Malware Defenses CSC 12 Boundary Defense CSC 15 Wireless Access Control	OM-ADM-001 System Administrator OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager SP-ARC-0001 Enterprise Architect PR-CDA-001 Cyber Defense Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
			39, SC-40, SC-41, SC-43			SP-ARC-002 Security Architect OM-NET-001 Network Operations Specialist
		DE.CM-5—Unauthorized mobile code is detected	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
Enterprise Mobility Management						
MobileIron Core Version 9.7.0.1	Enterprise Mobility Management	ID.AM-1—Physical devices and systems within the organization are inventoried	Information System Component Inventory CM-8 Information System Inventory PM-5	A.8.1.1 Inventory of Assets A.8.1.2 Ownership of Assets	CSC 1 Inventory of Authorized and Unauthorized Devices	OM-STS-001 Technical Support Specialist OM-ADM-001 System Administrator

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.AC-1—Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Access Control AC-1, AC-2 Identification and Authentication IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.3 Management of Privileged Access Rights A.9.2.4 Management of Secret Authentication Information of Users A.9.2.6 Removal or Adjustment of Access Rights A.9.3.1 Use of Secret Authentication Information	CSC 1 Inventory of Authorized and Unauthorized Devices CSC 5 Controlled Use of Administrative Privileges CSC 15 Wireless Access Control CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OM-ADM-001 System Administrator OV-MGT-002 Communications Security (COMSEC) Manager OM-STS-001 Technical Support Specialist OM-ANA-001 Systems Security Analyst PR-CDA-001 Cyber Defense Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				A.9.4.2 Secure Log-On Procedures A.9.4.3 Password Management System		
		PR.AC-6—Identities are proofed and bound to credentials and asserted in interactions	Access Control AC-1, AC-2, AC-3, AC-16, AC-19, AC-24 Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8 Physical and Environmental Protection PE-2 Personnel Security PS-3	A.7.1.1 Screening A.9.2.1 User Registration and De-Registration	CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OM-ADM-001 System Administrator
		PR.IP-1—A baseline configuration of	Information System Component	A.12.1.2 Change Management	CSC 3 Secure Configurations for Hardware and	SP-ARC-002 Security Architect

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality)	Inventory CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9 System and Services Acquisition SA-10	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation A.14.2.2 System Change Control Procedures A.14.2.3 Technical Review of Applications After Operating Platform Changes A.14.2.4 Restrictions on Changes to Software Packages	Software on Mobile Devices, Laptops, Workstations, and Servers CSC 9 Limitation and Control of Network Ports, Protocols, and Services CSC 11 Secure Configurations for Network Devices Such as Firewalls, Routers, and Switches	OV-SPP-002 Cyber Policy and Strategy Planner SP-SYS-001 Information Systems Security Developer OM-ADM-001 System Administrator PR-VAM-001 Vulnerability Assessment Analyst OM-NET-001 Network Operations Specialist OV-MGT-001 Information Systems Security Manager OM-STS-001 Technical Support Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android)	EMM/Endpoint Agent	PR.DS-6—Integrity-checking mechanisms are used to verify software, firmware, and information integrity	System and Communications Protection SC-1 System and Information Integrity SI-7	A.12.2.1 Controls Against Malware A.12.5.1 Installation of Software on Operational Systems A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions A.14.2.4 Restrictions on Changes to Software Packages	CSC 2 Inventory of Authorized and Unauthorized Software CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	OV-SPP-002 Cyber Policy and Strategy Planner SP-ARC-0001 Enterprise Architect OV-MGT-001 Information Systems Security Manager OM-ADM-001 System Administrator OM-STS-001 Technical Support Specialist
Trusted Execution Environment						

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Qualcomm (Version is mobile device dependent)	Trusted Execution Environment	PR.DS-1—Data at rest is protected	Media Downgrading MP-8 System and Communications Protection SC-12, SC-28	A.8.2.3 Handling of Assets	CSC 13 Data Protection CSC 14 Controlled Access Based on the Need to Know	OV-SPP-002 Cyber Policy and Strategy Planner PR-INF-001 Cyber Defense Infrastructure Support Specialist OV-LGA-002 Privacy Officer/Privacy Compliance Manager OV-MGT-002 COMSEC Manager OM-NET-001 Network Operations Specialist OM-ANA-001 Systems Security Analyst
		PR.DS-6—Integrity-checking mechanisms are used to verify	System and Communications Protection SC-16	A.12.2.1 Controls Against Malware	CSC 2 Inventory of Authorized and	OV-SPP-002 Cyber Policy and Strategy Planner

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		software, firmware, and information integrity	System and Information Integrity SI-7	A.12.5.1 Installation of Software on Operational Systems A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions A.14.2.4 Restrictions on Changes to Software Packages	Unauthorized Software CSC 3 Secure Configurations for Hardware and Software on Mobile	PR-CDA-001 Cyber Defense Analyst SP-ARC-0001 Enterprise Architect OV-MGT-001 Information Systems Security Manager OM-STS-001 Technical Support Specialist OM-ADM-001 System Administrator
		PR.DS-8—Integrity-checking mechanisms are used to verify	Developer Configuration Management SA-10	A.11.2.4 Equipment Maintenance	Not applicable	OM-ADM-001 System Administrator SP-ARC-0001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		hardware integrity	System and Information Integrity SI-7			Enterprise Architect
		DE.CM-4—Malicious code is detected	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 5 Controlled Use of Administrative Privileges CSC 7 Email and Web Browser Protections CSC 14 Controlled Access Based on the Need to Know CSC 16 Account Monitoring and Control	PR-CDA-001 Cyber Defense Analyst PR-INF-001 Cyber Defense Infrastructure Support Specialist PR-VAM-001 Vulnerability Assessment Analyst OM-NET-001 Network Operations Specialist PR-CDA-001 Cyber Defense Analyst
Virtual Private Network						
Palo Alto Networks, PA-220	Virtual Private Network	PR.AC-3—Remote access is managed	Access Control AC-1, AC-17, AC-19, AC-20	A.6.2.1 Mobile Device Policy	CSC 12 Boundary Defense	OV-SPP-002 Cyber Policy and Strategy Planner

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Version 8.1.1			System and Communications Protection SC-15	A.6.2.2 Teleworking A.11.2.6 Security of Equipment and Assets Off-Premises A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures		OV-MGT-002 Communications Security (COMSEC) Manager OM-NET-001 Network Operations Specialist
		PR.AC-5—Network integrity is protected (e.g., network segregation, network segmentation)	Access Control AC-4, AC-10 System and Communications Protection SC-7	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.13.2.1 Information	CSC 9 Limitation and Control of Network Ports, Protocols, and Services CSC 14 Controlled Access Based on the Need to Know	PR-CDA-001 Cyber Defense Analyst OM-ADM-001 System Administrator OM-NET-001 Network Operations Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				Transfer Policies and Procedures A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions	CSC 15 Wireless Access Control CSC 18 Application Software Security	
		PR.AC-6—Identities are proofed and bound to credentials and asserted in interactions	Access Control AC-1, AC-2, AC-3, AC-16, AC-19, AC-24 Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8 Physical and Environmental Protection PE-2, PS-3	A.7.1.1 Screening A.9.2.1 User Registration and De-Registration	CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OM-ADM-001 System Administrator

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.DS-2—Data in transit is protected	System and Communications Protection SC-8, SC-11, SC-12	A.8.2.3 Handling of Assets A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures A.13.2.3 Electronic Messaging A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions	CSC 13 Data Protection CSC 14 Controlled Access Based on the Need to Know	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OV-LGA-002 Privacy Officer/Privacy Compliance Manager OM-NET-001 Network Operations Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.PT-4—Communications and control networks are protected	Access Control AC-4, AC-17, AC-18 Contingency Planning CP-8 System and Communications Protection SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures A.14.1.3 Protecting Application Services Transactions	CSC 8 Malware Defenses CSC 12 Boundary Defense CSC 15 Wireless Access Control	PR-INF-001 Cyber Defense Infrastructure Support Specialist OV-SPP-002 Cyber Policy and Strategy Planner PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist