NIST SPECIAL PUBLICATION 1800-4B

Mobile Device Security

Cloud and Hybrid Builds

Volume B:
Approach, Architecture, and Security Characteristics

Joshua Franklin
National Institute of Standards and Technology
Information Technology Laboratory

Kevin Bowler
Christopher Brown
Spike E. Dog
Sallie Edwards
Neil McNab
Matthew Steele
The MITRE Corporation
McLean, VA

February 2019

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-4

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

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor 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 1800-4B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-4B, 61 pages, February 2019, 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.

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 IT security — the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily 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

This document proposes a reference design on how to architect enterprise-class protection for mobile devices accessing corporate resources. The example solutions presented here can be used by any organization implementing an enterprise mobility management solution. This project contains two distinct builds: cloud and hybrid. The cloud build makes use of cloud-based services and solutions, while the hybrid build achieves the same functionality but hosts the data and services within an enterprise's own infrastructure. The example solutions and architectures presented here are based upon standards-based, commercially available products.

KEYWORDS

mobile; mobile device; mobile device management; mobility management; mobile security

ACKNOWLEDGMENTS

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

Name	Organization
Rick Engle	Microsoft
Kevin Fiftel	Intel
Paul Fox	Microsoft
Steve Kruse	Symantec
Tim LeMaster	Lookout
Nate Lesser	NIST National Cybersecurity Center of Excellence
Adam Madlin	Symantec
Kevin McPeak	Symantec
Rene Peralta	Microsoft
Atul Shah	Microsoft
Steve Taylor	Intel

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 the example solutions. We worked with:

Technology Partner/Collaborator	Build Involvement
Intel	Lenovo Miix 2.8 Mobile Device
Lookout	Enterprise Mobility Management Application
Microsoft	Microsoft Cloud Service, Company Portal, Intune, Office 365 Enterprise E3, Outlook & Community Portal Mobile Applications, System Center 2012 R2 Configuration Manager SP1, Windows Phone OS
Symantec	X.509 Certificate

Contents

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-4.

List of Figures

List of Tables

1 Summary

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide addresses the challenge of securely deploying and managing mobile devices in an enterprise. In many organizations, mobile devices are adopted on an ad hoc basis, possibly without the appropriate policies and infrastructure to manage and secure the enterprise data they process and store. Introducing devices in this fashion increases the attack surface of an enterprise, requiring that additional controls be implemented to reduce the risk of intrusion.

The NIST SP 1800-4 series of documents contains…

- descriptions of a mobile device deployment alongside an associated enterprise mobility management (EMM) system to implement a set of security characteristics and capabilities, along with a rationale for doing so
- a series of How-To Guides — including installation and configuration of the necessary services — showing system administrators and security engineers how to achieve similar outcomes

The solutions and architectures presented are built upon standards-based, commercially available products and can be used by any organization deploying mobile devices in the enterprise that is willing to have at least part of the solution hosted within a public cloud. This project contains two distinct builds: cloud and hybrid. The cloud build uses cloud-based data storage and management services for mobile devices, while the hybrid build achieves the same functionality as the cloud build but hosts a portion of the data, services, and physical equipment within an enterprise's own infrastructure.

1.1 The Challenge

Mobile devices allow an organization's users to access information resources wherever they are and whenever they need. This presents both opportunities and challenges. The constant internet access available via a mobile device's cellular and Wi-Fi connections has the potential to make business practices more efficient and effective, but it can be challenging to ensure the confidentiality, integrity, and availability of the information that a mobile device accesses, stores, and processes. As mobile technologies mature, users increasingly want to use both organization-issued and personally owned mobile devices to access enterprise services, data, and other resources to perform work-related activities. Despite the increased security risks posed by the coexistence of enterprise data with personally owned devices, organizations are under pressure to accept them due to several factors, including anticipated cost savings, increased productivity, and users' demand for more convenience.

1.2 The Solution

This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can enable secure access to the organization's sensitive email, contacts, and calendar information from users' mobile devices. In our lab at the National Cybersecurity Center of Excellence (NCCoE) at NIST, we built an environment to simulate a lightweight enterprise architecture, including common components present in most organizations such as directory services.

Our approach to mobile device security (MDS) includes…

- determining the security characteristics required to mitigate in large part the risks of storing enterprise data on mobile devices and transmitting enterprise data to and from mobile devices
- mapping security characteristics to standards and best practices from NIST and other organizations recognized for promulgating security information, such as the National Security Agency (NSA) and the Defense Information Systems Agency
- architecting a design for our example solutions
- selecting mobile devices and EMM systems that provide the necessary controls
- evaluating our example solutions

Although corporately owned, personally enabled (COPE) and bring your own device (BYOD) scenarios are not specifically addressed by this project, the necessary features to enable a secure demonstration of either scenario are available. Those making information technology (IT) policy and infrastructure decisions within an organization will need to use their own judgment to decide where on the device management spectrum they choose to exist. To make these security controls available, organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, operating system (OS), management agent, and the applications used to accomplish business objectives. This document provides but one method of accomplishing this task.

1.3 Benefits

Our proposed solutions provide the following value to organizations:

- reduce risk so that employees are able to access the necessary enterprise data from nearly any location, over any network, when using a wide variety of mobile devices
- enable the use of BYOD, COPE, and other mobile device deployment models, which may provide cost savings and increased flexibility for organizations
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement industry standard mobile security controls, reducing long-term costs and decreasing the risk of vendor lock-in

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to mobile security. This reference design is modular and can be deployed in whole or in part. Before implementing this guide, readers may also want to review other mobile security efforts such as those from the National Information Assurance Partnership (NIAP), the U.S. Government Chief Information Officer (CIO) Council, and the Open Web Application Security Project.

This guide contains three volumes:

- NIST SP 1800-4A: *Executive Summary*
- NIST SP 1800-4B: *Approach, Architecture, and Security Characteristics* — what we built and why **(you are here)**
- NIST SP 1800-4C: *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 1800-4A, which describes the following topics:

- challenges enterprises face in implementing and using mobile devices
- example solutions built at the NCCoE
- benefits of adopting the example solutions

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 1800-4B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.3, Risk, which provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map, which maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary,* NIST SP 1800-4A, with your leadership team to help them understand the importance of adopting standards-based access management approaches to protect your organization's mobile and digital assets.

IT professionals who want to implement an approach like this will find the entire practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-4C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solutions. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. Although we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a mobile device management solution. 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 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by the reference solutions.

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.**
`Monospace`	command-line input, on-screen 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://nccoe.nist.gov/.

3 Approach

Enterprises traditionally established boundaries to separate their trusted internal IT network(s) from untrusted external networks. When enterprise users consume and generate enterprise data on mobile devices, this traditional boundary erodes. Due to the rapid changes in today's mobile platforms, enterprises have the challenge of ensuring that mobile devices connected to their networks can be trusted to protect sensitive data as it is stored, processed, and transmitted while still giving users the features they have come to expect from mobile devices. Additionally, some enterprises host enterprise data in a public cloud infrastructure, which also needs to be protected.

This guide proposes a system of commercially available technologies that provides enterprise-class protection for mobile platforms accessing and interacting with enterprise resources. The implementations presented here can be used by any organization interested in implementing an EMM solution.

This project contains two distinct builds: one focuses on cloud-based data, management, and services; the other leverages the same EMM infrastructure in-house. The cloud build may be useful to smaller organizations wanting to rapidly deploy a mobile solution or offload services hosted in-house to the cloud. The hybrid build uses the same services as the cloud build but hosts services and data on site within an organization's premises.

When conceptualizing the project, the project team looked to EMM systems deployed by industry. Users were sometimes frustrated with policies pushed from enterprises, and system administrators were confused about the most appropriate policies to push to mobile devices. This information was the impetus for creating the scenarios included in the building block definition document [1].

A number of security characteristics and capabilities are documented within the building block definition. We analyzed the content and concepts from multiple standards to generate the necessary security characteristics. These include NIST Special Publication (SP) 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [2]; NIST SP 800-164 (DRAFT), *Guidelines on Hardware-Rooted Security in Mobile Devices* [3]; NSA mobile access capability package [4] and the appropriate NIAP protection profiles [5], [6], [7].

3.1 Audience

The cloud build is geared toward organizations wanting to operate and maintain systems external to their enterprise environment to lower operational expenses. These organizations elect to leverage a software as a service cloud provider for services such as office productivity tools for workstations. The addition of mobile devices into this environment adds complexity because the organization requires protection of its sensitive data, but this data is not under its direct control.

The hybrid build is meant for organizations that are concerned with the risks associated with storing and processing confidential enterprise information in the cloud. These organizations have the willingness and technical expertise to implement and manage the necessary infrastructure to host the services on premises and may need to prevent cloud-based authentication and not wish to expose their existing identity repository to the cloud. The hybrid build includes a combination of enterprise assets likely to be present in an organization's existing network and adds cloud services for EMM, making it a starting point for an organization that has significant investment in or dependence on an internal Active Directory (AD) server.

3.2 Scope

This publication seeks to assist organizations in developing and implementing sound EMM deployments for securely accessing email, contacts, and calendaring. It provides practical, real-world guidance on developing, implementing, and maintaining secure, effective mobile devices, mobile applications, and EMM solutions in an enterprise. The publication presents EMM technologies from a high-level viewpoint and then provides a step-by-step guide to implementing a specific solution. The OSes and applications storing and transmitting the data must be securely configured and implemented. The EMM used within this build accomplishes this by sending policies to the mobile device and enforcing these policies by leveraging the device's OS protections.

The problem statement for this building block [1] describes a large number of security and functional characteristics and capabilities. It is important to note that this document does not employ each and every one of them. For instance, topics such as mobile application vetting, privacy, continuous monitoring, and comprehensive security testing of our build are important complementary steps to securing devices in an enterprise but are out of scope for this phase of the building block.

The specific security characteristics and capabilities used in the cloud and hybrid builds are noted later in Section 4.3. The scope of these two builds demonstrates the following objectives:

- secure implementation of email, contacts, and calendaring
- installation, implementation, and configuration of an EMM system
- hardened mobile devices securely accessing enterprise data for which the user and device are authorized

Privacy issues can be complex and difficult to implement, particularly since these issues often span a broad range of topics, from law and policy to technology. Although privacy protections are listed within our desired capabilities, these goals are out of scope for this publication and will be addressed in subsequent efforts. In the meantime, organizations may want to follow a more comprehensive privacy engineering effort to satisfy these goals, such as National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [8].

Finally, the breadth of technologies in this building block was intentionally limited to organizations that have entered into a National Cybersecurity Excellence Partnership (NCEP) with the NCCoE, meaning that only NCEP partners of the NCCoE were allowed to participate in the build phase of this project. We anticipate significantly expanding on the technologies used within the next phase of this MDS project by leveraging Cooperative Research and Development Agreements (CRADAs) with other interested collaborators. Organizations wishing to participate in future efforts should visit the NCCoE's website for more information about participating.

3.3 Assumptions

The following assumptions exist for this project:

- Both the cloud and hybrid builds are highly dependent on Microsoft's cloud platform, including Microsoft Office 365 and Microsoft Intune. Organizations trust these services to function properly and to appropriately handle sensitive information
- Organizations manage their own domains with the ability to alter Domain Name System (DNS) information on an ad hoc basis to prove ownership of a DNS name space so it can be associated to Office 365 services, email authority, mail exchanger records, and establishment of federation services
- Within the hybrid build, organizations place a system outside a perimeter firewall that proxies the connection between their Active Directory Domain Services and Microsoft's cloud services
- Organizations trust the mobile OSes within this build (e.g., Android, iOS, Windows) to store and process sensitive information

3.4 Risk Assessment

NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and

(ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST 800-39, *Managing Information Security Risk* [9], which is freely available to the public. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* [10], proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

The nature of mobile devices creates a set of unique risks in the modern enterprise. Future phases of this guide will include a NIST SP 800-30 based risk assessment, but it is currently out of scope for this effort. However, it is useful to highlight broad categories of threats and vulnerabilities.

We have used NIST SP 800-124 [2]; NIST SP 800-163 [11]; and the United States Computer Emergency Readiness Team (US-CERT) Technical Information Paper-TIP-10-105-01, *Cyber Threats to Mobile Devices* [12], as sources for this section, which is not an exhaustive list of threats to mobile devices. Although this practice guide focuses only on the threats and vulnerabilities related to the mobile device, readers should also consider broader threats to services that provide mobile device management (MDM) capabilities while assessing risk. Additional consideration should be given to threats posed from cloud services and the mobile ecosystem supporting the device. Cloud MDM services that leverage the Federal Risk and Authorization Management Program (FedRAMP), for example, can increase confidence in the security of these solutions with consistent security authorizations using a baseline set of agreed-upon standards [13].

To further address comments received in the public comment period of 1800-4*, Mobile Device Security: Cloud and Hybrid Builds* draft publication, the NCCoE Mobile Device Security Project team has produced National Institute of Standards and Technology Interagency Report 8144, *Assessing Threats to Mobile Devices & Infrastructure*. This publication accompanies the Mobile Threat Catalogue, which describes, identifies, and structures the threats posed to mobile information systems. We received many comments with a common theme that the example architectures in 1800-4 did not address the entire mobile security ecosystem. We encourage readers to review National Institute of Standards and Technology Interagency Report 8144 and the Mobile Threat Catalogue to assist in developing risk assessments, building threat models, enumerating the attack surface of their mobile infrastructure, and identifying mitigations for their mobile deployments.

3.4.1 Threats

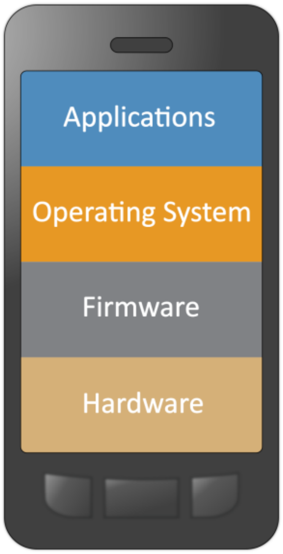
Below are common threats to mobile devices:

- mobile malware
- social engineers
- stolen data due to loss, theft, or disposal
- unauthorized access
- electronic eavesdropping
- electronic tracking
- access to data by legitimate third-party applications

3.4.2 Vulnerabilities

Vulnerabilities are commonly associated with applications that are installed on mobile devices. However, it is important to recognize that vulnerabilities can be exploited at all levels in the mobile device stack, which is outlined below in Figure 3-1.

Figure 3-1 Mobile Technology Stack



Applications that can be exploited can come from various sources — they may be installed by the device owner, preinstalled by a mobile network operator (i.e., carrier), or natively bundled with the OS. Although carrier and bundled applications can add valuable functionality to the device, the attack surface is also broadened. Further, carrier-installed applications can be particularly troublesome because they can be difficult to remove. Applications may be intentionally malicious, particularly those installed by the device owner. Mobile applications specifically developed to do harm to a device are categorized as mobile malware and often exploit design flaws or vulnerabilities in the mobile OS to achieve malicious design goals.

Note that on mobile devices, the firmware and hardware levels are not as clearly defined as Figure 3-1 depicts. Mobile devices with access to a cellular network contain a baseband processor comprising a distinct telephony subsystem used solely for telephony services (e.g., voice calls, texts, data transfer via the cellular network) [14]. This processor and the associated software/firmware on which it operates are separated from the mobile OS running on the application processor. Furthermore, some mobile devices contain additional security-specific hardware and firmware used to assist with making security decisions and storing important information, such as encryption keys, certificates, and credentials [15], [16], [17].

For up-to-date information regarding vulnerabilities, we recommend that security professionals leverage the National Vulnerability Database (NVD). The NVD is the U.S. government repository of standards-based vulnerability management data [18].

3.4.3 Risk

Using the common threats identified previously as a guide, we identified risks that an organization might face when deploying mobile devices. In general, these risks focus on data leakage and compromise. Because modern mobile devices process many types of information (e.g., personal, enterprise, financial, medical), there are many types of data leakages, each with its own level of severity in a given context. The following are potential reasons for data leakage and/or compromise:

- lack of mobile access control (e.g., loss of the mobile device, lock screen protection, enabling smudge attacks)
- lack of confidentiality protection (e.g., encryption of data in transit) of information due to operating on unsafe or untrusted networks (e.g., Wi-Fi, cellular)
- unpatched firmware, OS, or application software bypassing the OS security architecture (e.g., rooted/jailbroken device)
- users running malicious mobile applications which may glean information via misuse of inter-process communication or other access control mechanisms
- device interaction with cloud services outside corporate control
- misuse or misconfiguration of location services, such as global positioning system
- acceptance of fake mobility management profiles, providing malicious actors with a high degree of device control
- social engineering via voice, short message service /multimedia messaging service, third-party text communication, or email communication

3.4.4 Security Control Map

Using this risk information, NCCoE engineers identified the security characteristics of the solution. Table 3-1 through Table 3-6 map these characteristics to the Subcategories from the NIST Cybersecurity Framework [19], NIST SP 800-53 Revision 4 [20], International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27002 [21], and the Council on CyberSecurity’s Critical Security Controls for Effective Cyber Defense [22]. Note: Before transfer to the Council on Cybersecurity, [22] was informally known as the Sysadmin, Audit, Networking, and Security Consensus Audit Guidelines (CAG) 20.

The following tables identify security characteristic standards mappings for data protection, data isolation, device integrity, monitoring, identity and authorization, and privacy. For more information on each of these, reference Section 6.

Table 3-1 Security Characteristic Standards Mapping (Data Protection)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
device encryption	PR.AC-3, PR.DS-1, PR.DS-5, PR.PT-2	AC-19(5), MP-5(4), SC-13, SC-28(1)	6.2.1, 8.3.1, 10.1.1, 11.2.7, 18.1.5	CSC 17-1, CSC 17-2
application-level encryption	PR.DS-1	SC-28(1)	6.2.1, 8.3.1, 10.1.1, 18.1.5	CSC 17-1, CSC 17-2, CSC 17-3
secure containers	ID.AM-3, PR.AC-4, PR.DS-1, PR.DS-3, PR.DS-5	AC-3, AC-3(8), AC-4, MP-6(8), SC-13, SC-28(1)	6.2.1, 8.3.1, 9.4.1, 10.1.1, 18.1.5	CSC 15-4, CSC 15-5, CSC 17-1, CSC 17-2, CSC 17-3
trusted key storage	PR.DS-5, PR.PT-3	AC-3(5), SC-12, SC-13, SC-3, SC-3(1)	10.1.1, 10.1.2, 14.1.3	CSC 12-13, CSC 16-15, CSC 16-17
hardware security modules	PR.DS-1, PR.DS-5, PR.PT-3	IA-7, SC-3, SC-3(1), SC-34	10.1.1, 10.1.2, 18.1.5	CSC 17-15
remote wipe	PR.DS-1, PR.DS-3, PR.IP-6	MP-6(8), SC-28(1)	6.2.1, 8.1.2, 8.1.4, 8.3.2, 11.2.7	
selective wipe	PR.DS-1, PR.DS-3, PR.IP-6	MP-6(8), SC-28(1)	6.2.1, 8.1.2, 8.1.4, 8.3.2, 11.2.7	
automatic wipe	DE.AE-2, PR.DS-1, PR.DS-3, PR.IP-6	AC-7, AC-7(2), MP-6(8), SC-28(1)	6.2.1, 8.1.2, 8.3.2, 11.2.7, 11.2.8	
encrypted memory	PR.DS-1, PR.DS-5	SC-13, SC-28(1)	10.1.1	CSC 17-3
protected communications	PR.DS-2, PR.DS-5	SC-8, SC-8(1), SC-13	9.1.2, 9.4.2, 10.1.1, 13.1.1, 13.2.1, 13.2.3, 14.1.3	CSC 3-7, CSC 7-6, CSC 15-4, CSC 16-15, CSC 16-16, CSC 17-7
protected execution environments	PR.AC-4, PR.DS-5	AC-6(4), SC-11, SC-3, SC-39, SC-39(1)	14.1.3	

Table 3-2 Security Characteristic Standards Mapping (Data Isolation)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
virtualization	PR.AC-3, PR.AC-4, PR.AC-5	AC-20(3), AC-6(4), SC-7(21)	6.2.2	CSC 2-8

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
sandboxing	PR.AC-5, PR.DS-5	SC-39, SC-7(21)		
memory isolation	PR.DS-5	SC-39		
trusted execution	PR.DS-5	SA-13, SC-3, SC-11	14.1.3	
device resource management	PR.AC-3, PR.AC-5, PR.DS-5, PR.IP-1	AC-4, AC-19, CM-2, SC-7(21)	6.1.2, 6.2.1, 9.1.2, 11.1.5, 13.2.1	CSC 3-1, CSC 7-5, CSC 7-8, CSC 7-9, CSC 11-1, CSC 17-8
data flow control	PR.DS-5	AC-4	6.2.1, 8.2.1, 8.2.3, 9.1.1, 9.4.1, 13.2.1	CSC 15-5
data tagging	ID.AM-3, PR.AC-4	AC-4(1), AC-16	8.2.1, 8.2.2	CSC 15-5
baseband isolation	PR.DS-5	SC-39, SC-39(1)		

Table 3-3 Security Characteristic Standards Mapping (Device Integrity)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
baseband integrity checks	PR.DS-6	SI-7, SI-7(1), SI-7(9)	12.2.1	
application whitelisting/ blacklisting	DE.CM-3, PR.IP-1	CM-7(4), CM-7(5), CM-11	6.2.1, 12.2.1, 12.6.2	CSC 2-1, CSC 2-2, CSC 6-1
boot validation	PR.DS-6	SI-7, SI-7(6), SI-7(9), SI-7(10), SI-7(12)	12.2.1	
application verification	PR.DS-6	SI-7, SI-7(1), SI-7(6)	12.2.1	CSC 3-8
verified application and OS updates	PR.DS-6	SI-7, SI-7(1), SI-7(6)	12.2.1	CSC 3-8
mobile malware detection	DE.AE-2, DE.CM-4, PR.PT-2	MP-7, SI-3, SI-3(2), SI-3(7), SI-4(7)	6.2.1, 12.2.1, 13.2.1	CSC 5-1, CSC 5-2, CSC 5-8
trusted integrity reports	PR.PT-1, PR.DS-6	AU-9, AU-9(3), IA-3(4), SA-13, SI-7, SI-7(1)	18.2.3	CSC 3-8, CSC 13-8
policy integrity verification	PR.DS-6	SI-7, SI-7(1), SI-7(6)	18.2.3	CSC 3-8

Table 3-4 Security Characteristic Standards Mapping (Monitoring)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
inventory of mobile device hardware, firmware, and software	ID.AM-1, ID.AM-2	CM-8, CM-8(2)	8.1.1, 8.3.1, 12.2.1, 12.6.1, 18.1.2	CSC 1-1, CSC 1-3, CSC 1-4, CSC 2-4, CSC 2-5
asset management	ID.RA-1, PR.AC-3, PR.IP-1	AC-19, CM-2, CM-6, SC-43, SI-2	6.2.1, 8.1.1, 9.1.2, 11.2.8, 11.2.9, 12.1.1, 12.1.2, 12.5.1, 12.6.1, 12.6.2, 18.1.2	CSC 3-1, CSC 3-3, CSC 3-7, CSC 3-10, CSC 16-5, CSC 16-6, CSC 16-8, CSC 16-9
compliance checks	DE.CM-3, ID.AM-3, ID.AM-4, PR.AC-3, PR.IP-1	AC-19, AC-20, AC-20(1), CA-9, CA-9(1), CM-6(1), CM-6(2), CM-11(1)	12.1.2, 12.2.1, 18.2.3	CSC 2-3, CSC 3-1, CSC 7-1, CSC 13-8d
root and jailbreak detection	PR.DS-6	SI-7, SI-7(1), SI-7(2), SI-7(6), SI-7(9)	12.2.1	CSC 7-1, CSC 13-8
anomalous behavior detection	DE.AE-2, DE.CM-4	IA-10, SI-4, SI-4(5), SI-4(11), SI-4(24), SI-15	9.4.2, 12.2.1	CSC 5-8
auditing and logging	PR.PT-1, RS.AN-1	AU-2, AU-3, AU-8, AU-9, AU-12, IR-5	12.1.1, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.7.1, 16.1.1	CSC 14-1, CSC 14-2
canned reports and ad hoc queries	PR.PT-1	AU-7, AU-7(1), AU-7(2)		
geofencing	DE.CM-7, ID.AM-3, PR.AC-4, PR.AC-5, PR.PT-1	AC-4AC-4(3), AC-4(8), AC-6, CM-8(8)	9.1.2	

Table 3-5 Security Characteristic Standards Mapping (Identity and Authorization)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG 20
local authentication of user to device	PR.AC-4, PR.DS-5	AC-3, IA-6	6.2.1, 9.3.1, 9.4.1, 9.4.2, 10.1.1	CSC 16-8
local user authentication to applications	PR.AC-4, PR.DS-5	AC-3, IA-6	6.2.1, 9.1.1, 9.3.1, 9.4.1, 9.4.2, 10.1.1	CSC 16-8
remote user authentication	PR.AC-1, PR.AC-4, PR.DS-5	AC-3, AC-17, IA-2, IA-2(2), IA-2(11), IA-6	6.2.1, 9.1.1, 9.1.2, 9.3.1, 9.4.1, 9.4.2, 10.1.1, 13.1.1, 14.1.3	CSC 7-1, CSC 12-8, CSC 13-7, CSC 16-8, CSC 16-14
remote device authentication	PR.AC-1, PR.AC-3, PR.AC-4	AC-3, AC-17, AC-19, IA-3, IA-3(1), IA-3(4)	6.2.1, 9.1.1, 9.4.1, 10.1.1, 13.1.1, 14.1.3	CSC 1-7, CSC 7-1, CSC 7-7, CSC 13-8
implementation of user and device roles for authorization	PR.AC-4	AC-3, AC-3(7), AC-6	6.2.1, 9.1.1	
device provisioning and enrollment	ID.AM-1, PR.AC-3, PR.PT-1, PR.PT-2, PR.PT-3	AC-19, CM-7(3), CM-8(4), MP-5(3), MP-7(1)	6.2.1, 8.1.2, 8.1.4, 8.2.3, 8.3.1, 8.3.2, 9.2.2, 11.2.5	CSC 5-7, CSC 7-1, CSC 13-8
credential and token storage and use	PR.AC-1	IA-2, IA-2(10), IA-2(11), IA-2(12), IA-5, IA-5(1), IA-5(2), IA-5(4), IA-5(6), IA-5(9), IA-5(10), IA-5(11), IA-5(12), IA-5(13)	9.2.3, 9.2.4, 9.3.1, 9.4.2, 10.1.1, 10.1.2, 14.1.3	CSC 1-7, CSC 12-13, CSC 12-12, CSC 16-8, CSC 16-14, CSC 16-15, CSC 16-16

Table 3-6 Security Characteristic Standards Mapping (Privacy)

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002
informed consent of user	ID.GV-3	AC-8, PS-6	8.1.3, 9.4.2

Security Characteristic	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002
data monitoring minimization	ID.GV-3	DM-1	
custom privacy statement	ID.GV-3	TR-1	

3.5 Technologies

Following the draft publication of NIST SP 800-164 [2], NIST began looking for additional ways to foster mobile security in the enterprise. The three primary mobility security principles of NIST SP 800-164 (i.e., device integrity, isolation, and protected storage) were used as a baseline. Moving forward, NCCoE engineers used other standards and guidance relating to mobility to build upon these principles to create the full list of security characteristics and capabilities in Section 4.3.

The initial document describing this project's security challenge was released in 2014 [1]. After incorporating public comments and revising the document, the NCCoE MDS team consulted with the NCCoE's NCEP partners to understand which technologies would be applicable to this project. The technologies used in this project are listed in Table 3-7. Note that this represents a best effort in reflecting how key security functions of each product can support an organization's standards-based approach to cybersecurity risk management. These products may have additional security functions not represented here.

Table 3-7 Technology Security Characteristic Mapping

Technology	Use	Product	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev4 Controls
EMM	Web service used to define and send policies to mobile devices	Microsoft Intune	DE.CM-3, ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID-RA-1, PR.AC-3, PR.AC-4, PR.DS-3, PR.DS-6, PR.IP-1, PR.IP-6, PR.PT-1, PR.PT-2, PR.PT-3, RS.AN-1	AC-3, AC-6(1), AC-6(3), AC-17(2), AC-19, AU-2, AU-3, AU-7, AU-7(1), AU-7(2), AU-8, AU-9, AU-12, AC-20, AC-20(1), CA-9, CA-9(1), CM-2, CM-6, CM-6(1), CM-6(2), CM-7, CM-7(3), CM-7(4), CM-7(5), CM-8, CM-8(2), CM-8(4), CM-11, CM-11(1), IR-5, MP-5(3), MP-6(8), MP-7(1), SC-8, SC-8(1), SI-2, SI-7(1), SI-7(2), SI-7(5)

Technology	Use	Product	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev4 Controls
		Microsoft Office 365 MDM	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.RA-1, PR.AC-3, PR.AC-4, PR.DS-3, PR.DS-6, PR.IP-1, PR.IP-6, PR.PT-1, PR.PT-2, PR.PT-3, RS.AN-1	AC-2, AC-3, AC-6(1), AC-6(3), AC-17(2), AC-19, AC-20, AC-20(1), AU-2, AU-3, AU-7, AU-7(1), AU-8, AU-9, CA-9, CA-9(1), CM-2, CM-6, CM-6(1), CM-6(2), CM-7, CM-7(3), CM-8, CM-8(2), CM-8(4), IR-5, MP-5(3), MP-6(8), MP-7(1), SC-8, SC-8(1), SI-2, SI-7(1), SI-7(2), SI-7(5)
Cloud Platform	Provides directory services and web-based productivity applications	Microsoft Office 365 Enterprise E3	PR.AC-1, PR.AC-4, PR.DS-2, PR.DS-5	AC-2, AC-3, AC-17, IA-2, IA-2(10), IA-5, IA-6, SC-8, SC-8(1)
Federation Services	Allows service providers to authenticate users who are managed by a trusted identity provider	Microsoft Active Directory Federation Services	ID.GV-3, PR.AC-4, PR.DS-2	AC-17, AC-24(1), SC-8, SC-8(1), TR-1
Inventory and Configuration Management	Provides centralized IT asset inventory, configuration, and management	Microsoft System Center 2012 R2 Configuration Manager	DE.CM-3, ID.AM-1, ID.AM-2, ID.AM-4, ID.RA-1, PR.AC-3, PR.PT-1, PR.IP-1, RS.AN-1	AU-2, AU-3, AU-6, AU-7, AU-7(1), AU-7(2), AU-8, AU-9, AU-12, AC-19, AC-20, AC-20(1), CM-2, CM-5, CM-6, CM-6(1), CM-6(2), CM-7(4), CM-7(5), CM-8, CM-8(2), CM-8(4), CM-8(7), CM-11, CM-11(1), IR-5, SI-2
Mobile Device End Point Protection	Mobile malware detection and OS integrity verification	Lookout Mobile Threat Protection (MTP)	DE.CM-4, PR.AC-1, PR.DS-6, PR.IP-1, PR.PT-1, PR.PT-2, PR.PT-3	AU-2, AU-3, AU-6, AU-7(2), AU-12, CM-6(2), CM-7(3), IA-2(13), MP-7, SI-3(2), SI-3, SI-3(7), SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(6)

Technology	Use	Product	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev4 Controls
Mobile Device	Provides remote access to organizational services and data	iPhone 6 (iOS 8.3), Motorola Nexus 6 (Android 5.1), Nokia Lumia 830 (Windows Phone 8.1)	DE.AE-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-5, PR.DS-6, PR.IP-1, PR.IP-6, PR.PT-2, PR.PT-3	AC-3, AC-3(5), AC-6(4), AC-7, AC-7(2), AC-19(5), CM-2, CM-5(3), IA-5, IA-6, MP-5(4), MP-6, MP-6(8), SA-13, SC-3, SC-7(21), SC-3(1), SC-8, SC-8(1), SC-11, SC-12, SC-13, SC-17, SC-28, SC-28(1), SC-3(1), SC-39, SC-39(1), SC-8(1), SI-7, SI-7(1), SI-7(6), SI-7(9), SI-7(10), SI-7(12)
Secure communications protocol	Protects the confidentiality and integrity of data communicated between end points	Transport Layer Security (TLS)	PR.DS-2, PR.DS-5	SC-8, SC-8(1), SC-13
E-mail, contacts, and calendar application	Provides core business productivity	Microsoft Outlook Application	PR.AC-1, PR.DS-2, PR.DS-5	IA-6, SC-8, SC-8(1), SC-13
MDM Agent	Client application with administrative control that enforces MDM policies on the device	Microsoft Company Portal Application	DE.CM-3, ID.GV-3, PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.IP-1, PR.IP-6	AC-3, AC-4, AC-19, CM-2, CM-5, CM-6, CM-7(4), CM-7(5), CM-11, CM-11(1), IA-6, SC-7(21), SC-8, SC-8(1), SI-7(1), SI-7(2), SI-7(6)
Digital Certificate	Used for authentication of end points in federated services	Symantec Digital Certificate	PR.DS-5	SC-13

The following mobile devices were used throughout this project:

- Dell Venue 8 Pro (Intel)
- Lenovo Miix 2 (Intel)
- Nexus 6
- Nokia Lumina 830
- iPhone 6
- Samsung Galaxy S5

4 Architecture

This section documents the functional and network architectures of both the cloud and hybrid builds. Before continuing, it is useful to describe a notional EMM deployment. An EMM can consist of multiple services, including MDM, mobile application management (MAM), and other mobile computing services. Enterprises use EMMs to define a set of policies, push those policies to a mobile device, and then enforce these policies on a mobile device via an enforcement mechanism on the device (e.g., OS, mobile application). Before policies can be pushed to a given device, an enterprise must enroll that device into the management services. Once enrolled, policies, such as the requirement to use an eight-digit passcode, are defined and then pushed to the device via a secure communications channel. These processes and technologies enable users to work inside and outside the enterprise network with a securely configured mobile device with the following functional and security capabilities:

- **Device encryption:** cryptographic protection of all or portions of a device's data storage locations to prevent unauthorized disclosure of enterprise data
- **Application-level encryption:** an alternative or additional layer of cryptographic protection applied only to application data to prevent unauthorized disclosure when device encryption is either undesirable or has been defeated
- **Trusted key storage:** protected locations in software, firmware, or hardware in which long-term cryptographic keys or secrets are safeguarded from unauthorized disclosure or modification
- **Protected communications:** strong cryptographic protection of data transmitted over untrusted networks to mitigate unauthorized disclosure or modification
- **Remote wipe:** action that prevents the unauthorized access of data stored on a lost or stolen device by rendering data recovery techniques infeasible
- **Selective wipe:** remote wipe that affects only enterprise data, leaving personal data intact; also occurs automatically as a consequence of a device user unenrolling their device from enterprise management
- **Automatic wipe:** action that reactively wipes all device data in response to multiple subsequent failed attempts to unlock a locked device, which may occur before the loss or theft of a mobile device is discovered
- **Hardware security modules:** embedded or removable tamper-resistant hardware used to perform cryptographic operations and provide secure storage to protect security operations or data from unauthorized access or modification

- **Sandboxing:** OS or application-level virtualization, isolation, and integrity mechanisms utilizing multiple protection, isolation, and integrity capabilities to achieve higher levels of overall process isolation
- **Memory isolation:** OS-enforced separation of memory spaces allocated to running processes to protect their integrity, which secondarily protects the confidentiality, integrity, and availability of data in process
- **Trusted execution:** protection of security processes within an isolated and trustworthy environment using distinct memory spaces and controlled interfaces to provide higher levels of isolation than memory isolation alone
- **Device resource management:** ability to selectively disable unused or unnecessary peripherals to prevent their abuse and preserve other resources (e.g., battery life, data limits)
- **Application whitelisting/blacklisting:** allowing or disallowing the use of applications based on a prespecified list to prevent the execution of malicious, vulnerable, or flawed applications
- **Boot validation:** integrity checks on the content of boot files and the execution of boot processes to verify the OS has been launched into a known-good and trustworthy state
- **Application verification:** integrity checks on application installation packages and validation of the digital signature to verify that applications come from a trusted source and have not been modified prior to installation
- **Verified application and OS updates:** application verification techniques, as above, are applied to application and OS update packages prior to execution
- **Mobile malware detection:** identification of malicious software on mobile platforms to facilitate remediation and limit their potential to cause harm
- **Inventory of mobile device hardware and software:** maintain version information for the hardware, firmware, OS, and installed applications on devices in order to respond effectively to discovered vulnerabilities
- **Asset management:** identify, configure, and maintain the security configuration of devices, components, software, and services residing on a network to reduce the potential for compromise
- **Compliance checks:** determine a device's level of compliance with mandated security policies to prevent granting access to improperly configured and vulnerable devices
- **Root and jailbreak detection:** verification that the security architecture for a mobile device has not been compromised to prevent granting access to untrustworthy devices
- **Auditing and logging:** capture and store security events for devices, including enrollment, failed compliance checks, administrative actions, and unenrollment
- **Canned reports and ad hoc queries:** use preconfigured reports or active searches or filters on security logs to manage incidents and audit compliance
- **Local authentication of user to device:** require a user to provide a personal identification number (PIN), password, cryptographic token, or other authentication mechanism to prevent granting unauthorized access to sensitive device functionality or accessible data
- **Local user authentication to applications:** as above, but specific to an application

- **Remote user authentication:** as above, but for networked applications that require successful authentication to a remote service before granting full access to its functionality and data
- **Device provisioning and enrollment:** identification and association of specific mobile devices with organizational user accounts to ensure that remote access is granted only to authorized users using approved devices
- **Custom privacy statement:** inform users about the implications to privacy or changes to device functionality as a result of accepting organizational management of their personal device or remotely accessing enterprise resources

This project installs, configures, and integrates two distinct MDMs from Microsoft: Office 365 (included in most Office 365 deployments) and Microsoft Intune. These MDMs offer varying levels of functionality — security and otherwise.

The integration of the various technologies within these builds would be extremely difficult without the use of standards and best practices. The following standards are crucial to a successful implementation:

- NIST SP 800-124 Rev 1*: Guidelines for Managing the Security of Mobile Devices in the Enterprise* [2]
- NIST SP 800-164 (Draft): *Guidelines on Hardware-Rooted Security in Mobile Devices* [3]
- NIST SP 800-147: *BIOS Protection Guidelines* [23]
- NIST SP 800-155: *BIOS Integrity Measurement Guidelines* [24]
- NIST SP 800-88 Rev 1: *Guidelines for Media Sanitization* [25]
- NIST SP 800-163: *Vetting the Security of Mobile Applications* [11]
- NSA: *Mobility Capability Package 2.3* [4]
- *Department of Defense Commercial Mobile Device Implementation Plan* [26]
- CIO Council: *Government Mobile and Wireless Security Baseline* [27]
- GSA Managed Mobility Program Request for Technical Capabilities [28]
- NIAP: *Protection Profile for Mobile Device Management Version* 1.1 [29]
- NIAP: *Protection Profile for Mobile Device Fundamentals Version 2.0* [6]
- NIAP: *Extended Package for Mobile Device Management Agents Version 2.0* [7]
- GlobalPlatform: specifications for Secure Element and Trusted Execution Environment [15], [16]
- Trusted Computing Group: specifications for Trusted Platform Module [17]

Section 4.1, Cloud Build: Architecture Description and Section 4.2, Hybrid Build: Architecture Description describe the cloud and hybrid architectures, respectively, as well as their benefits and security features.

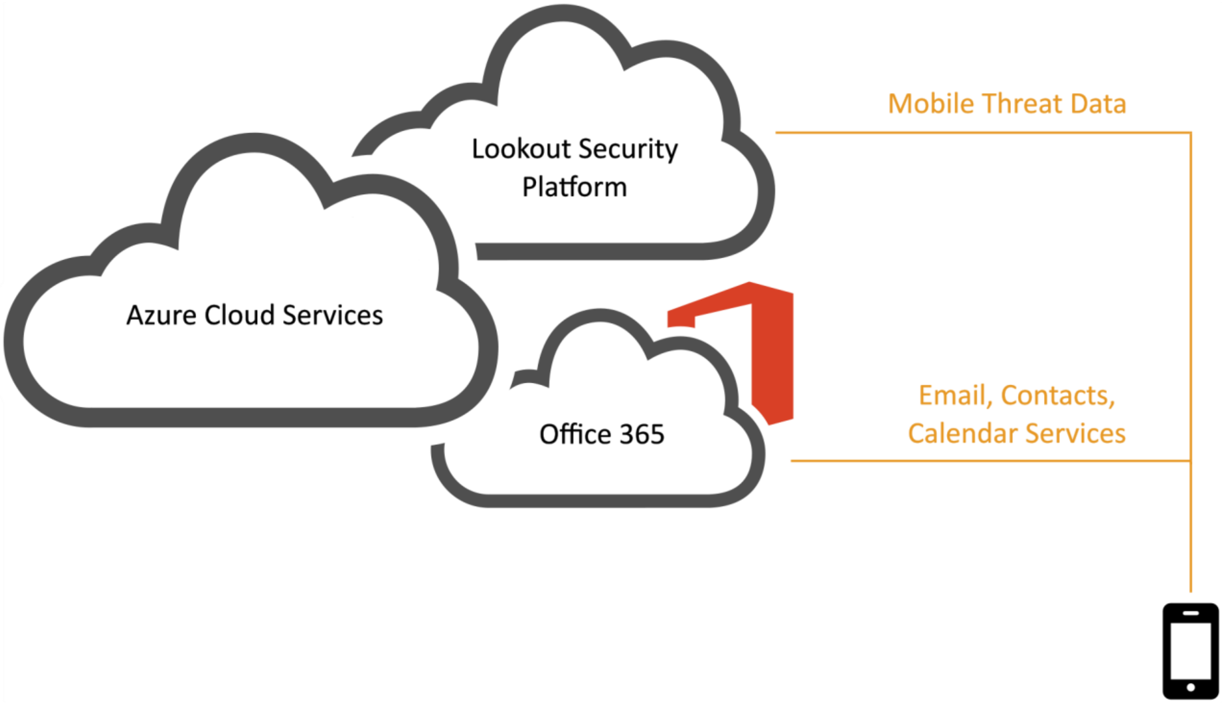
4.1 Cloud Build: Architecture Description

The cloud build is intended to assist organizations wanting to leverage mobile devices and manage these devices via the cloud. These organizations may include entities needing to stand up mobile deployments with minimal effort and entities with established enterprise mobile deployments wanting to leverage the benefits of cloud computing. This build can be quickly deployed within enterprises without an internal AD server. Although this build uses the MDM system included with Office 365, an organization could choose to leverage Intune instead in this instance. Office 365 was chosen to diversify the MDMs used within this project.

This solution can be easily configured and operated as a cloud service to onboard personally or enterprise-owned mobile devices into the EMM, allowing users to access enterprise resources and enterprise managers to push policies to mobile devices. Office 365 allows for a variety of policies to be pushed to the device (detailed in Appendix C) but offers a significantly reduced feature set when compared with Microsoft Intune.

Figure 4-1 provides the overall architecture of the cloud build.

Figure 4-1 Cloud Build Architecture



Mobile devices communicate with Office 365 over a public communications network, which then accesses Microsoft's mobile applications such as Word and Excel. System administrators manage devices via the Office 365 admin center. In order to make full use of cloud services, a globally recognized commercial domain is required. For test purposes, the NCCoE acquired cmdsbb.org (CMDSBB is an acronym for cloud mobile device security building block) from a commercial domain registrar and used it throughout this guide. The exact method for DNS acquisition and management is unique for each registrar and enterprise and is therefore unable to be addressed by this guide.

4.1.1 Cloud Architecture Benefits

The security benefits of a cloud architecture will depend heavily on the service provider that is chosen. NIST SP 800-146 states that in a public cloud scenario, "the details of provider system operation are usually considered proprietary information and are not divulged to consumers. … Consequently, consumers do not (at the time of this writing) have a guaranteed way to monitor or authorize access to their resources in the cloud" [30]. However, organizations that lack security subject matter experts can realize a benefit because "clouds may be able to improve on some security update and response issues." We recommend that readers consider the recommendations in Section 9.3 of NIST SP 800-146 [30] before choosing a cloud service provider.

Functionally, the cloud architecture benefits from the rapid development of features — a trait found in modern web-based services. The MDM service used within the cloud build is able to keep pace with the quick-changing landscape of mobile devices. For example, mobile device vendors can add device management features as they iterate through OS versions. These features can be immediately available through the cloud service rather than delayed by a traditional on-premises software upgrade cycle.

Another benefit of the cloud architecture is the ability to manage mobile devices from any physical location. Our cloud MDM portal is available to administrators through a web interface; the only requirements are a modern web browser and an internet connection. This allows administrators to take action while outside the boundaries of the enterprise network. Further, it reduces reliance on desktop applications that may not be available on all workstations.

4.1.2 Cloud Build Security Characteristics

Much of the security of the cloud build relies on the protections provided by the mobile device, the policies implemented by the MDM, and the Microsoft Outlook mobile application installed on the device. The initial selection of the mobile device makes a large difference in the security features available due to low-level boot firmware and/or OS integrity checks. Some mobile devices provide some form of secure boot rooted in hardware or firmware by default, while other devices offer no boot integrity at all. Another feature available only on certain mobile devices is secure key storage, which may or may not be rooted in hardware. Organizations may wish to ensure that the devices they support include these desirable hardware/firmware capabilities.

An individual who decides to participate in a managed scenario must download the Microsoft Community Portal application and input the required information. Then the device is provisioned into the EMM, and the default set of policies listed in Appendix C is applied to the device. This includes local authentication to the mobile OS via a lock screen and the encryption capabilities provided by the mobile OS to protect data on the device. The Outlook application provides an additional layer of application-level encryption to email and Outlook application-related data via the Microsoft managed application policies [31].

The Outlook application uses a TLS 1.2 tunnel to communicate with the Office 365 email, calendaring, and contact services, and does the same for the cloud-based AD service offered by Office 365. The management interface to access the Office 365 EMM and other administrative functions is also protected via a TLS 1.2 tunnel over the internet. Further, if a user is not in compliance with the policies specified in Appendix C, the system administrator is notified. As an additional layer of protection, inclusion of the Lookout for Enterprise application also provides anti-malware protection alongside jailbreak/root detection.

4.2 Hybrid Build: Architecture Description

The hybrid build leverages the same cloud-based services from the cloud build but integrates them into the network in a different manner. It includes a combination of enterprise assets likely to be present within an organization's existing network, including EMM capabilities, and adds cloud services for MDM. This build might be a starting point for an organization that has significant investment in or dependence on an internal AD server. The cornerstone of the hybrid build is the existing AD server housing user data and associated credentials. Figure 4-2 depicts the high-level hybrid build architecture.

Figure 4-2 Hybrid Build Architecture

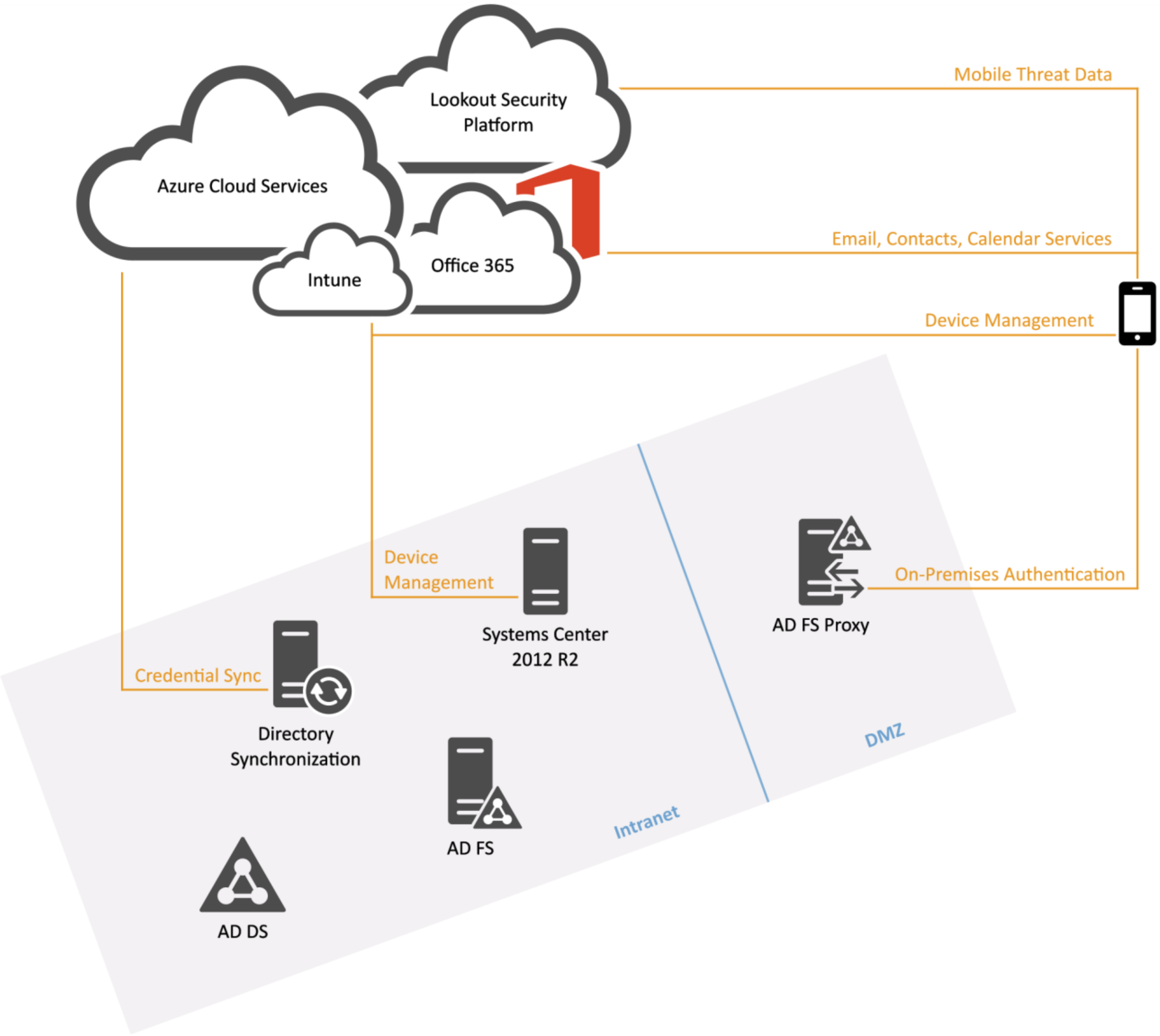


Table 4-1 Legend for Hybrid Build Architecture Diagram

Acronym	Term
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
DMZ	Demilitarized Zone

Microsoft Intune functions as the EMM for this solution, which can be easily configured and operated as a cloud service to onboard personally or enterprise-owned mobile devices into the EMM. This allows users to access enterprise resources and allows those involved with enterprise management to push policies to mobile devices.

The hybrid build contains the following elements:

- In the cloud:
  - Intune provides MDM, MAM, and end point management capabilities. Devices outside the enterprise firewall can connect to Intune for configuration management and monitoring
  - Office 365 synchronizes with AD Domain Services (DS) 2012R2 to provide email, contacts, and calendaring services. It also has its own user database, which can be selectively synced with AD DS via the Azure AD Sync Tool
  - The Lookout Security Platform provides the back end to the threat protection mobile application to identify risks on the device
- In the enterprise intranet:
  - AD DS stores directory data and manages communication between users and domains, including user log-on processes, authentication, and directory searches. It is used to centrally manage servers and users, and information is synchronized with cloud services https://technet.microsoft.com/en-us/library/Cc770946(v=WS.10).aspx
  - AD Federation Services (FS) 2012R2 is a standards-based service that allows the secure sharing of AD DS identity information between trusted business partners across an extranet. https://msdn.microsoft.com/en-us/library/Bb897402.aspx
  - Azure AD Sync Services is used to mirror Azure AD and Office 365 with a single-forest or multiforest on-premises AD. It does not require access to the Azure AD tenant that is created with the associated Office 365 subscription. Systems Center Configuration Manager (SCCM) provides unified management across on-premises, service provider, and Azure environments for both Windows computers and mobile devices. http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/
- In the enterprise demilitarized zone:
  - The Web Application Proxy (WAP) provides reverse proxy functionality for AD FS to allow access to users on any device from outside the enterprise network. It acts as a security

    - barrier by not allowing direct access into the AD environment from the internet and is not joined to the domain itself

- From the internet:
    - Mobile applications (Lookout MTP, Intune MDM client, Outlook) deployed to the device that support the functional and security characteristics of this build

Additional components not pictured:

Making full use of cloud services requires a globally recognized commercial domain. For our test purposes, we acquired hmdsbb.org from a commercial domain registrar and used it throughout this practice guide. The exact method for DNS management will be unique for each registrar and organization and is therefore unable to be addressed by this guide.

The build team generated a certificate from the Symantec Secure Site Pro Secure Sockets Layer Certificates service to fulfill prerequisite requirements from AD FS to federate with Office 365.

A router/firewall is used to simulate various network and security domains within an organization.

4.2.1 Hybrid Architecture Benefits

The hybrid architecture leverages the flexibility of cloud services discussed in Section 4.1 while benefiting from security enhancements by using on-premises services. First, we made the architectural decision to use identity federation services that are realized through AD FS and Microsoft's AD Authentication Library (ADAL) service. This build leverages federation when the device owner is required to authenticate to Intune and Office 365 cloud services. This allows an organization to act as an identity provider — device owner passwords are shared only with on-premises systems and never with third-party cloud services.

The NCCoE made the architectural decision in this build to use a WAP. The WAP serves as a front end for requests to the on-premises AD FS system. This setup has the security benefit of adding a layer of defense by isolating front-end requests from the corresponding back-end requests to the protected federation service. This is important because the AD FS holds sensitive cryptographic keys such as the token-signing and service identity key. In this way, the AD FS system is protected within the enterprise network boundaries and not exposed to internet-facing networks [32].

Functionally, the architecture provides the benefit of managing enterprise identities within the traditional workflow of an on-premises AD system. Many organizations utilize identity management systems that require on-premises AD services but would also like to leverage cloud services without having two disparate identity systems. To solve this issue, we made the architectural decision to add an on-premises system dedicated to syncing identities between the on-premises AD and the cloud-based Office 365 environment.

SCCM is another instance of how our hybrid architecture benefits from on-premises and cloud services. This build could leverage traditional workstation configuration capabilities while enjoying the benefits of using a cloud MDM service. This is possible because the on-premises SCCM system is integrated with the Intune cloud service. Therefore, administrators can continue their normal workflow from the SCCM console and have a complete picture of enterprise assets from a single view.

4.2.2 Hybrid Build Security Characteristics

The security characteristics of the hybrid build closely resemble the characteristics in Section 4.1.2, Cloud Build Security Characteristics. The Outlook mobile application uses a TLS tunnel to communicate with the Office 365 email, calendaring, and contact services that live in the cloud. However, in the hybrid build, mobile traffic is directed through a proxy before communicating with internal enterprise services when interacting with the enterprise for authentication services. Additionally, on-premises systems communicate with Microsoft cloud services via a TLS tunnel. This includes the SCCM system and the AD Sync systems.

4.3 Security Characteristics and Capabilities

The security characteristics and capabilities presented in Appendix C are based on the principles identified in NIST SP 800-164 and NIST SP 800-124. Security characteristics are the goals that this build is trying to achieve, while security capabilities are the individual mechanisms to accomplish these goals. A goal would be to implement the identified characteristics and capabilities with verifiable integrity via continued assertions that the device has not been compromised. This would ensure that key firmware or OS files have not been tampered with, that the device has not been rooted or jailbroken, and that the device’s security policies are verified as those being issued by the enterprise. Therefore, these characteristics and capabilities should be implemented at the lowest possible level; for instance, firmware is preferred to an application layer service.

The original problem definition document [1] defines a superset of security characteristics and capabilities. This project does not implement every item within that document. What is specifically achieved in the context of this project is detailed in Appendix C, along with implementation notes for the build. Finally, note that many of the terms used below are not standardized throughout industry. Therefore, the descriptions provided alongside the capabilities reflect the term’s meaning in the context of this project.

4.3.1 Default Policies

Multiple standards espouse management policies that should be applied to user devices. Specifically, NIST SP 800-124 Revision 1 and the NIAP protection profile for MDMs suggest desirable features and functionality for an enterprise MDM policy. Table 4-2 shows the default policy used in this project and pushed to devices within this building block, fulfilling our goals of a reasonable balance between security and user functionality. Suggested policies such as turning off Bluetooth and Wi-Fi, while reducing the threat surface to which a mobile device is exposed, remove important functionality desired by users. Some of these policies may be accomplished by the underlying mobile OS (e.g., Android, iOS, Windows Phone) while others require application-level features, and still others are accomplished via the MDM. Although the following policies were used for the building block, organizations need to perform their own assessments to understand the risks associated with their systems. Guidance for performing this assessment and selecting appropriate policies can be found within NIST 800-124 r1 [2].

Table 4-2 SP 800-124 Mapping to Security Characteristic

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Automatically monitor device configuration and detect policy violations	• Intune and Office 365 MDM periodically query the Company Portal MDM agent for a device's current level of compliance • The Company Portal MDM agent monitors the device for policy compliance and enforces policy settings on local device functionality (e.g., access to location services or removable media)	Compliance checks	Company Portal, Intune, and Office 365 MDM automatically monitor managed devices for policy compliance
Automatically report when policy violations occur, such as changes from the approved security configuration baseline	SCCM can log the policy violations for subsequent reporting and review, which can be optionally sent to Event Viewer to enable additional monitoring and reporting functionality	Auditing and logging	When configuring an MDM policy in SCCM, setting noncompliance severity for reports to the least information will log violations of any included settings in Configuration Manager. [33]
Automatically take action in response to policy violations when possible and appropriate	Intune and SCCM offer policy settings that authorize the Company Portal MDM agent to attempt to restore non-compliance settings back to a compliant state	Asset management	Most MDM policy sections configurable by Intune/SCCM have a remediate noncompliant settings option. Note that automatic remediation for any given policy setting may not be supported on all OS versions

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Limit or prevent access to enterprise services based on whether the device has been rooted/jailbroken	• Intune and Office 365 MDM can block access to enterprise resources when the device is detected as being jailbroken or rooted • Intune and SCCM via Intune have MAM policy settings that block user access to managed applications when the device is not compliant with MDM policy • The Conditional Access Extension for SCCM enables blocking access to an on-premises Exchange server, Exchange Online, and SharePoint online for noncompliant devices	Root and jailbreak detection	Conditional access is set through SCCM Exchange connector. Mobile users are not allowed to access enterprise email services until the target device is compliant (i.e., phone is encrypted and not rooted/jailbroken)
Limit or prevent access to enterprise services based on the mobile device's OS version	Intune/SCCM must be explicitly configured to allow enrollment of iOS and Android devices. Each MDM policy created using Intune/SCCM can apply to a different set of specific OS versions	Device provisioning and enrollment	When creating an MDM policy using SCCM, the Platform Applicability step of the Create Configuration Item Wizard will list policy settings that are not supported by selected OS versions
Limit or prevent access to enterprise services based on the mobile device's vendor/brand or model	Intune enables a device enrollment manager to enroll users' devices on their behalf, allowing an organization to manually control which models of mobile devices will be enrolled	Device provisioning and enrollment	
Limit or prevent access to enterprise services based on the MDM software client version (if applicable)	N/A	N/A	

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Strongly encrypt data communications between the mobile device and the organization	Each of the mobile devices and OSes used in the build are capable of secure communications that use TLS	Protected communications	The Company Portal and Microsoft Outlook applications initiate secure communications with Microsoft Intune and Office 365 using TLS by default
Strongly encrypt stored data on built-in storage.	• Intune/SCCM and Office 365 MDM offer a policy setting requiring that built-in device storage be encrypted • Intune/SCCM offer a MAM policy setting enforcing encryption of application data	Device encryption	Device encryption implementation varies among device manufacturers. Encrypting the application data setting may not provide additional cryptographic protection over full-device encryption. However, when device encryption is undesirable, this setting is an alternative
Strongly encrypt stored data on removable storage	Intune/SCCM offer a policy setting to force encryption of removable media, which is advertised to work with Windows Phone 8.1	N/A	If removable storage is not a necessary feature and encryption of removable storage is not supported, consider disabling the use of removable storage media
Wipe the device (to scrub its stored data) before reissuing it to another user, retiring the device, etc.	Intune/SCCM and Office 365 MDM can trigger a full or selective wipe of data remotely	Remote wipe	Administrators are able to fully wipe devices by selecting the device from the SCCM console

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or has otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party.	Intune/SCCM and Office 365 MDM can trigger a full or selective wipe of data remotely	Remote wipe	Administrators are able to selectively or fully wipe devices by choosing the device from the SCCM console
A device often can also be configured to wipe itself after a certain number of incorrect authentication attempts	Intune/SCCM and Office 365 offer a policy setting that activates this feature and sets the number of allowed unlock attempts	Device wipe after unsuccessful unlock attempts	
Require a device unlock code be set before authorizing access to the organization's resources	Intune/SCCM and Office 365 offer a policy setting that requires a managed device to have a device unlock code set	Local authentication of user to device	This setting is a prerequisite for device encryption
Require basic parameters for password strength	• Intune/SCCM and Office 365 have a policy setting that requires that a device unlock code possesses a minimum length • Intune/SCCM and Office 365 have a policy setting that requires that the device unlock code meets certain complexity requirements	N/A	Longer or more complex device unlock codes increase the cryptographic strength of derived device encryption key and are more resistant to discovery (e.g., shoulder surfing attacks)

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Optionally require other authentication (e.g., token-based authentication, network-based device authentication, domain authentication) before accessing the organization’s resources	Intune/SCCM offer a MAM policy setting that forces a four-digit PIN or corporate credentials to be entered before Company Portal will allow managed applications to be accessed locally by the device user	Local authentication of user to applications	
Require a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device)	Intune/SCCM offer a MAM policy setting that sets a limit on the maximum number of managed application authentication attempts (via PIN or corporate credentials) before the PIN will be reset.	N/A	
If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device	Intune/SCCM have a policy setting that allows a password reset PIN to be synchronized with a Microsoft Exchange server; advertised for Windows devices only	N/A	
Have the device automatically lock itself after it is idle for a period (e.g., five minutes)	Intune/SCCM and Office 365 have a policy setting that requires that the device automatically locks after a specified number of minutes of inactivity	N/A	If an attacker has access to an unlocked device, they likewise will have access to any data not protected by additional authentication

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Under the direction of an administrator, remotely lock the device if it is suspected that the device has been left in an unlocked state in an unsecured location	Intune/SCCM can issue a remote lock instruction to managed devices	N/A	Administrators are able to remotely lock devices from the SCCM console
Restrict the use of OS and application synchronization services (e.g., local device synchronization, remote synchronization services, and websites)	Intune/SCCM offer a series of policy settings applicable to iOS and Samsung Android with KNOX that block synchronization of various kinds of content (photos, files, application backups) with either locally connected computers or cloud services	Device resource management	As support for this feature varies across OS versions, and restriction of synchronization can significantly impact device functionality, we did not choose to block synchronization. Consider using MAM policies to restrict the data-sharing functions accessible to managed applications
Verify digital signatures on applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified	Intune/SCCM offer MDM policy settings that block installation of unsigned applications or files	Application verification, verified application, and OS updates	Each of the mobile device OSes used supports verification of digital signatures for applications and application and OS updates
Query the current version of the hardware model of the device	Intune/SCCM and Office 365 MDM automatically query and record device hardware and OS versions for enrolled devices. Additionally, SCCM incorporates this information with its centralized asset inventory	Inventory of mobile device hardware, firmware, and software	

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Alert the administrator to security events	Intune/SCCM offer alert-level settings for each category of policy settings (e.g., encryption or cloud); detected violations of any setting within that group. Additionally, by default, deployment of a configuration baseline is configured to automatically send alerts to when overall policy compliance falls below a specified compliance threshold (90% by default)	Auditing and logging, compliance checks	When configuring an MDM policy in SCCM, if the noncompliance severity for reports setting for a given policy section is set to critical with event, then in addition to logging by Configuration Manager, a Windows event will be generated, enabling additional notification features by using Event Viewer
Import keys/secrets into the secure key storage locations	• Intune/SCCM allow digital certificates to be automatically installed onto mobile devices upon enrollment • iOS 8.3, Android 5.3, and Windows Phone 8.1 allow application to store cryptographic keys/secrets in OS-managed secure key storage locations (e.g., Android Keychain)	Trusted key storage	This is accomplished at the OS level of iOS, Android, and Windows Phone 8.1. Note: Use of OS-managed secure key storage by any given application is optional
Restrict which application stores may be used	Intune and SCCM offer a policy setting that restricts enrolled devices to installing applications from the official application store for its OS. Additionally, Intune/SCCM can block user access to the official application store	Whitelisting/ blacklisting	Note that blocking the installation of third-party applications is currently incompatible with the use of an organization-managed application store
Restrict which applications may be installed through whitelisting (preferable) or blacklisting	Intune/SCCM offer policy settings to establish both whitelists and blacklists of applications; lists are specific to each mobile OS	Whitelisting/ blacklisting	

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Restrict the permissions (e.g., camera access, location access) assigned to each application	• Intune/SCCM offer policy settings that can block use of certain specific device peripherals or OS functionality for all applications (e.g., camera, location services) • Intune/SCCM offer MAM policy settings that can block access to specific OS-provided functions (e.g., cut-and-paste, data transfer between applications, or screen capture) for managed iOS or Android applications	Device resource management, data protection	
Install, update, and remove applications	Intune has MAM functionality that allows it to automatically install, update (may require manual deployment), and remove applications from managed devices	N/A	
Safeguard the mechanisms used to install, update, or remove applications	Access to the policies and software functions that will install, upgrade, or remove applications from managed devices is managed by a role-based access management scheme using AD groups	N/A	The SCCM built-in role of Application Deployment Manager can be used to manage which administrators can install and remove applications from managed devices
Keep a current inventory of all applications installed on each device	Intune and SCCM receive application information from Company Portal; the installed applications with version information are inventoried for each device	Inventory of mobile device hardware, firmware, and software	

NIST SP 800-124 rev1 EMM/MDM Security Services	Related Technical Functions	NIST SP 1800-4 Security Characteristic	Note
Distribute the organization’s applications from a dedicated mobile application store	Intune and SCCM have MAM functionality that allows an organization to upload internally developed and publicly available applications to a private application store accessible only to managed devices	N/A	At the time of this document, no mobile OS differentiates between an organization’s private application store and any other third-party (unofficial) application store. If a private application store is used without an explicit whitelist of applications, those from unofficial application stores could also be downloaded

5 Outcome

This section discusses the building block from the perspective of the user and the system administrator. We define system administrator as a person within the organization who has elevated privileges on the management systems in the build.

5.1 The User’s Experience

When users access enterprise services on their device, their devices will be enrolled into an EMM. Access to email, contacts, and calendaring services occurs via the Microsoft Outlook mobile application. Device enrollment is accomplished by downloading and installing the Microsoft Company Portal application, available in the iOS and Android application store. Windows Phone devices have some management capability built into the OS, but they also require the Company Portal application to relay information to the enterprise. The Company Portal application can be downloaded directly onto the device from the Windows Application Store.

In general, the specific hardware of a mobile device will make little difference in how information is presented to the user. Accordingly, boot integrity has little impact on the workflow unless a user needs the capability to modify the mobile OS (e.g., jailbreaking, rooting) or if boot integrity is compromised. Enrolling a mobile device into the EMM causes a number of policies to be applied to it. One of the items most affecting a user’s experience is the case in which a user does not have local authentication on the device because the default EMM policies espoused within Appendix C require authentication to the OS lock screen. The exact complexity of the authentication solution (e.g., PIN, passcode, gesture) is subject to the needs of the enterprise, although NIST SP 800-63-3 [34] provides enterprises with guidance on this topic.

The user’s enrollment authentication experience remains largely the same between the cloud and hybrid builds, even though the hybrid build supports identity federation between the enterprise and

Microsoft cloud services. The hybrid build leverages ADAL-based sign-in — which uses a Security Assertion Markup Language-based AD FS identity provider. This allows the user to keep a familiar workflow with the added security benefit of keeping passwords within the enterprise boundary.

To receive the Lookout security services, which provide mobile malware protection, users should download the Lookout application from their device's application store in one of two ways. First, during the EMM enrollment process, users are presented with a direct link to the device's application store in the Company Portal. Second, the user is sent an invitation to enroll with Lookout through email. There is no technical control in this build, however, to require the installation of the Lookout application. Implementers of this build may wish to implement a MAM policy as a means to enforce the installation of the Lookout application.

To enroll in the Lookout service, a user will have to supply the application with his or her email address and a unique code received via email. The Lookout application generally interacts with users only if there is a security violation on the device.

Figure 5-1, Figure 5-2, and Figure 5-3 present the high-level workflow of device owner enrollment on the Android, iOS, and Windows Phone platforms, respectively.

Figure 5-1 Android Workflow

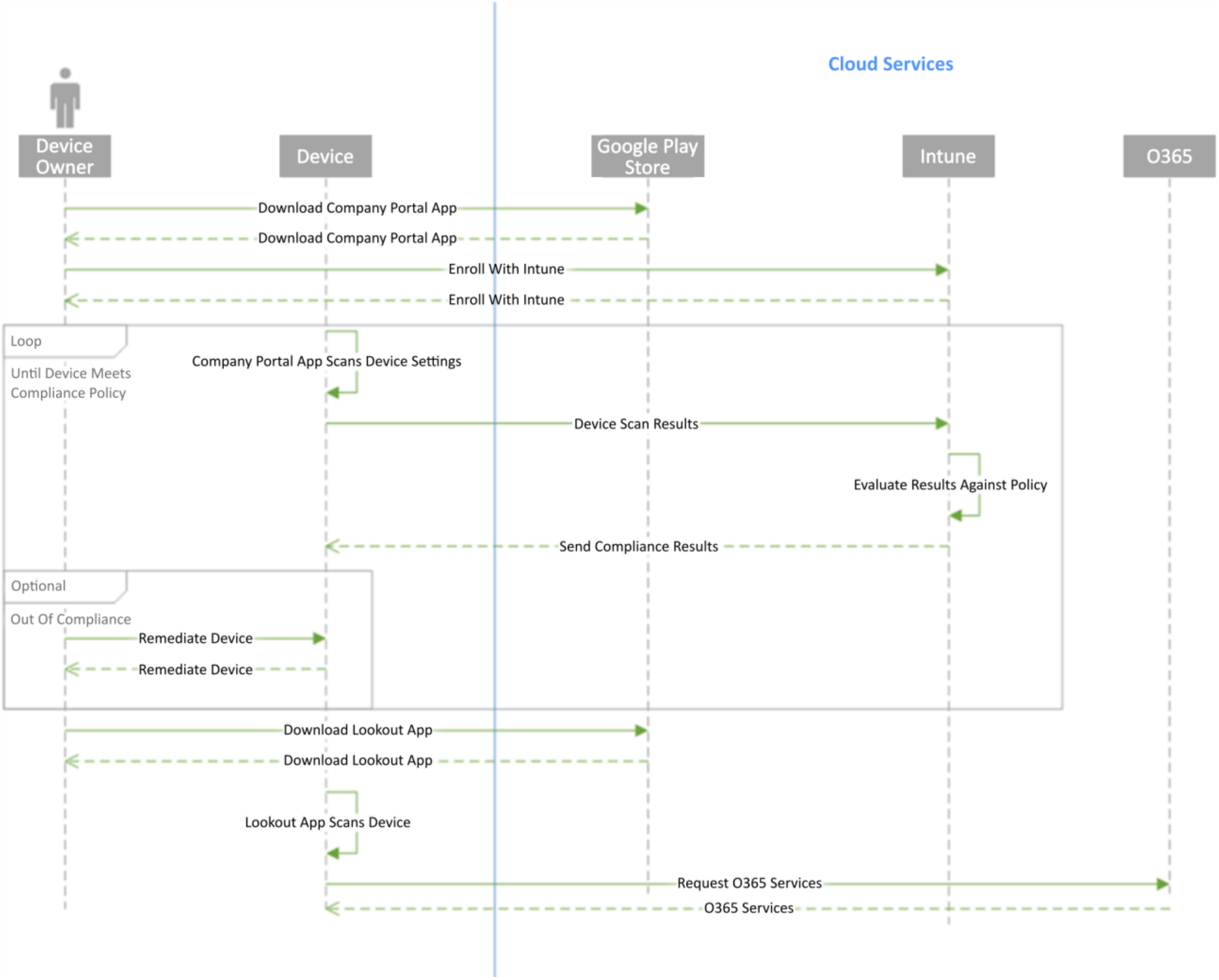


Figure 5-2 iOS Workflow

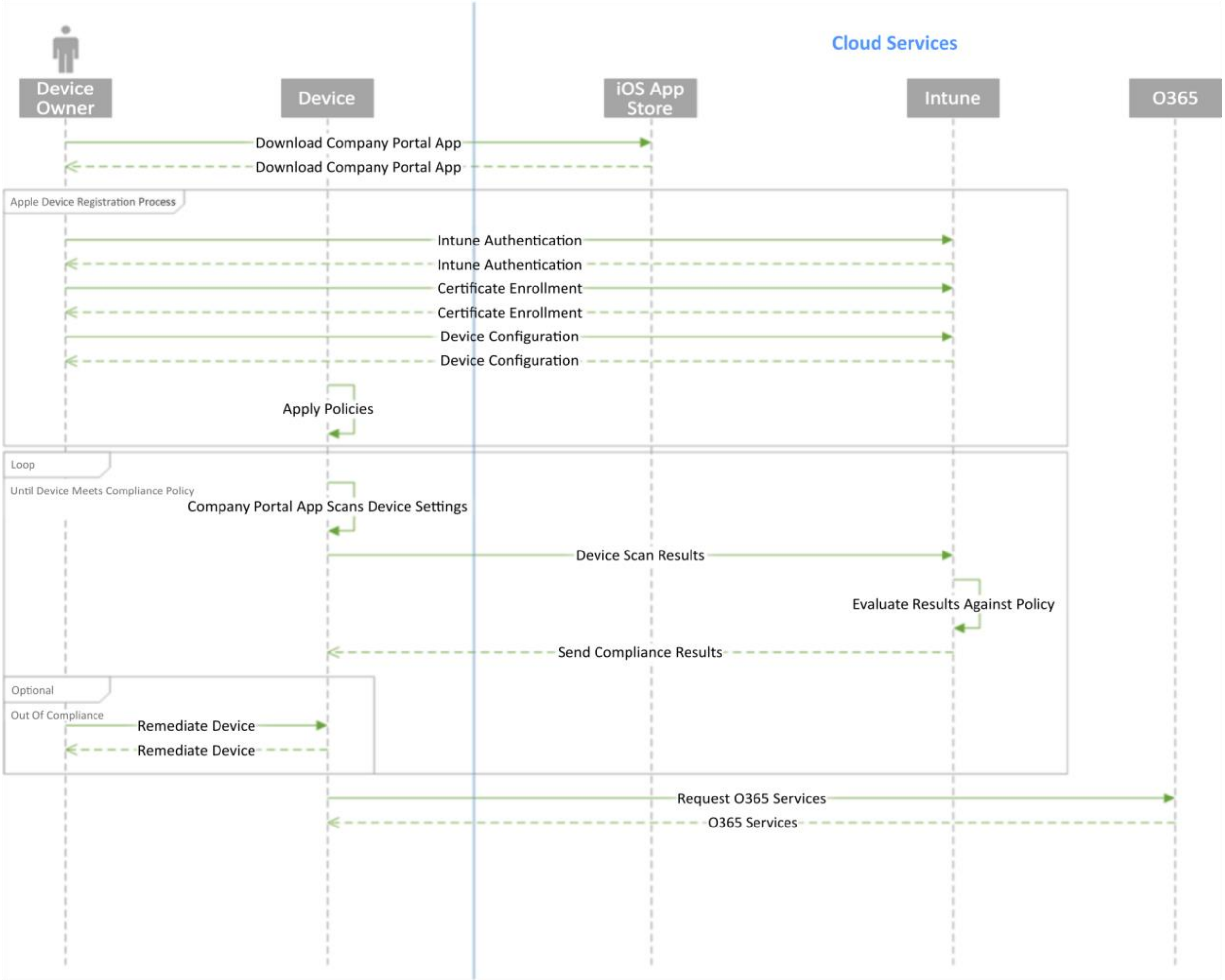
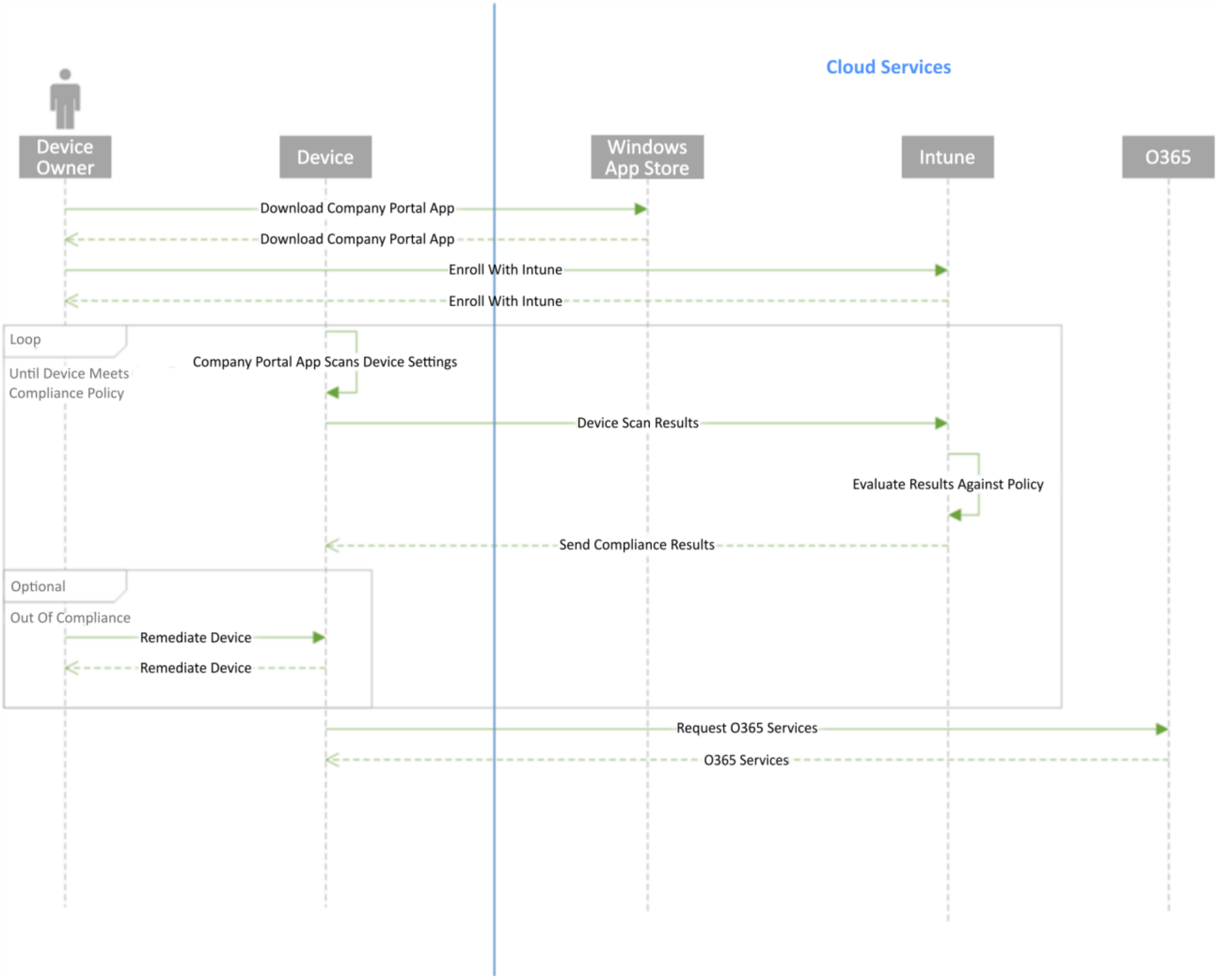


Figure 5-3 Windows Phone Workflow



5.2 The System Administrator’s Experience

The experience of the system administrator will be different based on whether they are using the hybrid or cloud builds, mostly due to the type and granularity of policies available via the EMM interfaces. Installation, configuration, and deployment of the management systems are relatively simple if an organization decides to adopt the cloud-based EMM services, where setup can be accomplished in less than a few hours. The installation of the EMM and associated services on premises is significantly more complex, with installation time estimated in hours at least. Defining EMM policies within the web interface of the EMMs is relatively simple, as is distribution to mobile devices.

Provisioning and de-provisioning email, contacts, and calendaring services on mobile devices is an important capability of this build. The process by which provisioning occurs will differ for the system administrator in the cloud and hybrid scenarios. Because the MDM functions are embedded within Office 365, provisioning mobile devices is quite simple in the cloud scenario. While creating a new user within the Office 365 administrative console, the system administrator has the option to allow the user mobile access.

The complex nature of the hybrid architecture, however, necessitates a slightly more intricate process. The high-level process is as follows:

1. A new enterprise user is created in the on-premises AD. The means by which this happens is outside the scope of this building block; however, many organizations choose to use a third-party identity management system
2. The user is placed within a specific group within AD that is configured to sync identities. The user is synchronized by the on-premises Azure AD Sync system to the cloud Azure AD service
3. The on-premises SCCM system detects the new user, who is automatically added to the Intune collection. A collection represents a group of users who have mobile devices to be managed
4. The Windows Intune Connector extension installed on the SCCM system syncs the new user to the Intune cloud service
5. The new user can now enroll in the Intune service by using the Company Portal application

De-provisioning is a simple task for the system administrator in both the cloud and hybrid builds. In the cloud build, de-provisioning a user can be as simple as disabling or deleting the user from the Office 365 administrative console. In the hybrid build, the user is removed from the Intune collection on the SCCM system. Implementers should note that de-provisioning actions may not be immediate. They will depend on the syncing periodicity configured in the Intune extension.

While Lookout services offer direct integration with selected EMM providers, this build did not use a compatible EMM. As a result, the system operator would not receive predefined alerts (e.g., malware on a device) through the SCCM workflow. The system operator must configure the Lookout administrative console to send email alerts to designated personnel when threats are present on user devices. In practice, the operator would receive an email with a warning of malware on a user’s device. The operator would then find the user within SCCM and take appropriate action on the device. Further, in this build there is no technical mechanism to enforce the installation and use of Lookout technologies. An administrator could, however, periodically compare the list of enrolled users in Lookout and the EMM. Users who were absent from the Lookout enrollment could be encouraged to download and install the application through an out-of-band means.

A step-by-step description of setup, installation, and configuration is available in NIST SP 1800-4C.

6 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating a method of protecting organizational data while permitting users the freedom to access and process data via mobile devices. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

6.1 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 that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture

6.2 Build Testing

The evaluation included an analysis of the project to identify weaknesses and discuss mitigations. The focus of this portion of the evaluation was hands-on testing of the laboratory build and examination of product manuals and documentation. Our objective was to evaluate the example solution and not specific products. However, the presence of three primary OSes for mobile devices (Android, iOS, and Windows) made complete product independent hands-on testing unrealistic.

Table 6-1 describes the goals of each test case.

Table 6-1 Cybersecurity Framework Subcategory Evaluation

Test ID	Cybersecurity Framework Subcategory	Related NIST SP 800-53 Controls	Evaluation Objective
Data Protection			
1	PR.DS-1: Data at rest is protected	SC-28 Protection of Information at Rest	Data is accessible only to authorized users and services. Data is protected during storage and processing
2	PR.DS-2: Data in transit is protected	SC-8 Transmission Confidentiality and Integrity SC-13 Cryptographic Protection	The confidentiality and integrity of information is protected while in transit (SC-8) by using a cryptographic mechanism. A Federal Information Processing Standard (FIPS) 140-2-compliant mechanism is used to secure data in transit
Data Isolation			
14	PR.DS-5: Protections against data leaks are implemented	SC-7 Boundary Protection	Monitor and control communications at the external boundary of the system and at key internal boundaries within the system
Device Integrity			
16	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity	SI-7 Software, Firmware, and Information Integrity	Integrity mechanisms are running to check the integrity of software and information files
17	DE.CM-4: Malicious code is detected	SI-3 Malicious Code Protection	Malicious code protection is installed on mobile devices. Anti-malware software (e.g., anti-virus software) is installed
18	DE.CM-5: Unauthorized mobile code is detected	SC-18 Mobile Code	Only mission-appropriate content may be uploaded within the application. The application should employ functionality to restrict upload of file types to those expressly required for operations (e.g., TIFF, JPEG, and PDF)
Monitoring			

Test ID	Cybersecurity Framework Subcategory	Related NIST SP 800-53 Controls	Evaluation Objective
20	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8 Information System Component Inventory	Mobile devices are inventoried within the SCCM database
21	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8 Information System Component Inventory	Software and licensing are inventoried within the SCCM database
28	DE.AE-5: Incident-alert thresholds are established	IR-5 Incident Monitoring	When alerts exceed the established threshold, the administrator is notified
37	DE.CM-8: Vulnerability scans are performed	RA-5 Vulnerability Scanning	Scanning mechanisms are implemented and effective. Vulnerability scanners provide comprehensive coverage and employ best practices
Identity and Authorization			
41	PR.AC-1: Identities and credentials are managed for authorized devices and users	IA Controls	The architecture accounts for multiple user roles with access privileges assigned to each role. Access controls are documented.
42	PR.AC-1	AC-2 Account Management; Identification and Authentication Controls	Only enrolled/managed devices can access email, contacts, and calendaring. Information is available only to authorized devices

6.3 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 NIST 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.

The remainder of this subsection discusses how the reference architecture solution addresses the six desired security characteristics that are listed in Table 3-1 through Table 3-6.

6.3.1 Data Protection

We chose to examine the capability of protecting data at rest. The primary means used by this building block to accomplish data protection is encryption. Android, iOS, and Windows Phone devices used as part of this build deployed device encryption. The Android devices used dm-crypt, a disk encryption subsystem that calls a number of cryptographic libraries. The Android implementation of this has not been FIPS 140-2 validated, although it uses the same crypto library as the Red Hat Enterprise Linux validation. For environments where FIPS 140-2 validation is necessary, organizations could consider using a third-party data and application isolation solution, such as a secure container providing application-level encryption.

Our Apple devices use Apple OS X CoreCrypto Kernel Module v5.0. As of 2015, it has received FIPS 140-2 level 1 validation on iOS 8.x devices. The Windows phones used in this exercise are FIPS 140-2 compliant. The Microsoft Kernel Mode Cryptographic Primitives Library has met FIPS 140-2 compliance at level 1 by using a Qualcomm Snapdragon 800 system on a chip.

Finally, the Outlook application provides an additional level of encryption. Microsoft protects the Outlook data via AES-128 encryption in cipher block chaining mode utilizing Android's cryptography libraries. The iOS application-level encryption was not evaluated as Microsoft indicated that information is encrypted via the OS cryptographic engine.

6.3.2 Data Isolation

When a device is utilized for organizational and personal activities, the ability to isolate data is essential. We inspected the sandboxing capability of devices and found that each of the OSes in use offers native isolation functions. Android, iOS, and Windows run applications in a sandbox that prevents a third-party application from accessing, gathering, or modifying information from other applications. While this is a valuable security feature, it does not replace the need to educate device users on the potential dangers of downloading unknown and untrusted applications.

6.3.3 Device Integrity

Each of the mobile platforms has integrity-checking mechanisms. We examined the native file integrity mechanisms as well as malicious code protection. Each platform requires application authors to digitally sign applications before the applications are available for users. The integrity-checking mechanism does not ensure that the application itself is secure or free of malware. To protect devices from malware, the MDS building block specifies that anti-virus software be installed on mobile devices and that the configuration "allow unknown sources" is not enabled. The build restricts the ability to download file types via email by enabling the file attachment filter in Office 365. We verified this by disallowing PDF file types. A user then attempted to send an email with a PDF file attached. The intended recipient was notified that an email addressed to them was blocked according to policy.

6.3.4 Monitoring

Our examination of security monitoring provided evidence of basic monitoring and scanning being performed. Devices enrolled in the MDM tool were displayed within the configuration management system console. This can be used for hardware inventory reporting as the MDM tools have customizable reports. We were able to use software reporting to only a limited degree. Intune provided software reporting only for applications published under the organization's application store. It did not monitor and conduct an inventory of applications downloaded from other sources such as Google Play.

The MDM provides the capability to tailor compliance policy for devices. When a device exceeds the organization-defined threshold for compliance, the administrator receives an alert showing which device is out of compliance. As an additional precaution, an organization may desire to restrict devices from downloading outside its own organizational application store if the potential for unknown applications exceeds the organization's risk appetite.

Finally, the Lookout MTP service provides monitoring of enrolled devices for malware risks on Android devices. In this build, the administrator periodically reviewed the status of enrolled devices in the enterprise through the MTP web console. More sophisticated notification systems, however, could be developed for larger deployments.

6.3.5 Identity and Authorization

Identity and authorization are integrated within the enterprise. The NCCoE needed to verify that only users with authorized access via mobile devices were able to exercise that access. Because the lab was built as a Microsoft environment, access control was implemented via AD. Test users were members of a domain users' group synchronized through AD FS. We had users who were not members of the appropriate group attempt to access their email on an enrolled mobile device, and those attempts failed.

We also sought to verify device authorization. We wanted to ensure that only currently enrolled devices could access organizational resources. Our verification included devices never enrolled and devices previously enrolled.

Access attempts for devices not enrolled produced the following results:

- iOS redirected the user to the organization portal, then directed the user to enroll his or her device. Email was not accessible until the device was enrolled and compliant with the organization's mobile device policy.
- Android attempted to enroll the device with the active sync policy when not managed by Intune. Android would not retrieve email until the device was enrolled in SCCM and compliant with policy.
- When attempting to access Office 365 services from out-of-compliance devices, users could activate the email client on the device but were unable to retrieve email.

7 Future Build Considerations

As we expand this work to future builds, our objective is to solicit feedback from the user community toward prioritization of additional capabilities and to solicit suggestions from the EMM vendor community on commercial products that provide those capabilities.

There is potential for the development and implementation of new MDS architectures under this build. To explore these various architectures, the NCCoE would like to engage with any individual or company with commercially or publicly available technology relevant to MDS. The NCCoE published a Federal Register notice (https://www.federalregister.gov/articles/2015/08/14/2015-20040/national-cybersecurity-center-of-excellence-mobile-device-security-building-block) inviting parties to submit a Letter of Interest to express their desire and ability to contribute to this effort. Interested parties would be required to enter into a consortium CRADA partnership.

Some topics of interest for future builds include…

- sector-specific MDM policy configurations
- mobile application vetting
- baseband integrity
- containerization technology
- rogue wireless access point detection
- enhanced identity services, such as two-factor authentication, derived personal identity verification (PIV) as demonstrated in NIST Interagency Report 8055, or use of the FIDO Alliance's technology

All interested parties are encouraged to engage the NCCoE with additional ideas and system requirements by reaching out to mobile-nccoe@nist.gov.

Appendix A Acronyms

AD	Active Directory
ADAL	Active Directory Authentication Library
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
BYOD	Bring Your Own Device
CAG	Consensus Audit Guidelines
CIO	Chief Information Officer
DNS	Domain Name System
DoD	Department of Defense
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
MAM	Mobile Application Management
MDM	Mobile Device Management
MDS	Mobile Device Security
MTP	Mobile Threat Protection
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OS	Operating System
PHA	Potentially Harmful Application
PIV	Personal Identity Verification
SCCM	Systems Center Configuration Manager

SP	Special Publication
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
US-CERT	United States Computer Emergency Readiness Team
WAP	Web Application Proxy

Appendix B References

[1] National Cybersecurity Center of Excellence, *Mobile Device Security for Enterprises*, Sept. 2014. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise.

[2] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 1, Gaithersburg, Md., June 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[3] L. Chen et al., *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*, NIST SP 800-164 (Draft), Gaithersburg, Md., Oct. 2012. Available: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[4] National Security Agency, *Mobile Access Capability Package 2.0*, Aug. 2017. Available: https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/capability-packages/mobile-access-cp.pdf.

[5] National Information Assurance Partnership (NIAP), *Protection Profile for Mobile Device Management Version 1.1*, March 2014. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_v1.1.pdf.

[6] NIAP, *Protection Profile for Mobile Device Fundamentals Version 2.0*, September 2014. https://www.niap-ccevs.org/MMO/PP/pp_md_v2.0.pdf.

[7] NIAP, *Extended Package for Mobile Device Management Agents Version 2.0*, Dec. 2014. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf.

[8] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, National Institute of Standards and Technology Internal Report 8062, NIST, Gaithersburg, Md., Jan. 2017. Available: https://doi.org/10.6028/NIST.IR.8062.

[9] NIST, *Managing Information Security Risk*, NIST SP 800-39 Revision 1, Gaithersburg, Md., Mar. 2011. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[10] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37 Revision 1, Gaithersburg, Md., Feb. 2010. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

[11] S. Quirolgico et al., *Vetting the Security of Mobile Applications*, NIST SP 800-163, Gaithersburg, Md., Jan. 2015. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf.

[12] United States Computer Emergency Readiness Team (US-CERT), *Cyber Threats to Mobile Devices*, Technical Information Paper-TIP-10-105-01, US-CERT, Apr. 2010. Available: https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf.

[13] Federal Risk and Authorization Management Program, *Program Overview*. Available: https://www.fedramp.gov/about/.

[14] G. Delugré, *Reverse engineering a Qualcomm baseband*, Sogeti/ESEC R&D, 2011. Available: https://events.ccc.de/congress/2011/Fahrplan/attachments/2022_11-ccc-qcombbdbg.pdf.

[15] Global Platform, Introduction to Secure Element. May 2018. Available: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf.

[16] Global Platform, Introduction to Trusted Execution Environment (TEE) Guide. May 2018. Available: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf.

[17] Trusted Computing Group, TPM Main Specification. Available: http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

[18] NIST, *National Vulnerability Database*, Gaithersburg, Md., 2015. Available: http://nvd.nist.gov.

[19] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, Gaithersburg, Md., Apr. 16, 2018. Available: https://www.nist.gov/cyberframework.

[20] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, Gaithersburg, Md., Apr. 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[21] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Information technology — Security techniques — Code of practice for information security management, ISO/IEC 27002, 2013.

[22] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense*, Version 6.0, May 2016. Available: https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

[23] D. Cooper et.al., *BIOS Protection Guidelines*, NIST SP 800-147, Gaithersburg, Md., Apr. 2011. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf.

[24] A. Regenscheid and K. Scarfone, *BIOS Integrity Measurement Guidelines (Draft)*, NIST SP 800-155 (Draft), Gaithersburg, Md., Dec. 2011. Available: http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf.

[25] R. Kissel et al., *Guidelines for Media Sanitization*, NIST SP 800-88 Revision 1, Gaithersburg, Md., Dec. 2014. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[26] Department of Defense (DoD), *DoD Commercial Mobile Device Implementation Plan*, Feb. 15, 2013. Available: http://archive.defense.gov/news/DoDCMDImplementationPlan.pdf.

[27] U.S. Government Chief Information Officer Council, *Government Mobile and Wireless Security Baseline*, May 23, 2013. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf.

[28] General Services Administration (GSA), *GSA Managed Mobility Program Request for Technical Capabilities,* Available: https://www.gsa.gov/cdnstatic/Managed_Mobility_ML%26EM_RFTC_-_FINAL.pdf.

[29] National Information Assurance Partnership (NIAP), *Protection Profile for Mobile Device Management Version 2.0*, Dec. 2014. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_v2.0.pdf.

[30] L. Badger et al., *Cloud Computing Synopsis and Recommendations*, NIST SP 800-146, Gaithersburg, Md., May 2012. Available: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

[31] Microsoft, *How to create and assign app protection policies*, Microsoft Technet, Nov. 30, 2018. Available: https://technet.microsoft.com/en-us/library/dn878026.aspx.

[32] Microsoft, "Office 365 Single Sign-On with AD FS 2.0 whitepaper," June 2012. Available: https://www.microsoft.com/en-us/download/details.aspx?id=28971.

[33] Microsoft, *Compliance Policies in Configuration Manager,* Microsoft Technet, Apr. 7, 2016. Available: https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/mt131417(v=technet.10).

[34] NIST, *Digital Identity Guidelines*, NIST SP 800-63-3, Gaithersburg, Md., June 2017. Available: https://pages.nist.gov/800-63-3.

[35] Microsoft, *Windows Phone 8.1 Security Overview*, Apr. 2014. Available: http://download.microsoft.com/download/B/9/A/B9A00269-28D5-4ACA-9E8E-E2E722B35A7D/Windows-Phone-8-1-Security-Overview.pdf.

[36] Lookout, *Change to sideloading apps in iOS 9 is a security win*. Available: https://blog.lookout.com/blog/2015/09/10/ios-9-sideloading/.

[37] The White House, *Bring Your Own Device — A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*, Aug. 23, 2012. Available: https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device.

[38] Google, *Help protect against harmful apps with Google Play Protect*. Available: https://support.google.com/accounts/answer/2812853?hl=en.

[39] Microsoft, *Windows Phone Library*, Apr. 2014. Available: https://technet.microsoft.com/en-us/windows/dn771706.aspx.

[40] NIST, *Best Practices for Privileged User PIV Authentication*, NIST Cybersecurity White Paper, Gaithersburg, Md., Apr. 2016. Available: http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf.

Appendix C Security Characteristics and Capabilities

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
Data Protection	Device encryption: cryptographic protection of all or portions of a device's data storage locations — primarily flash memory locations	Operating system (OS)-level capability provided by each mobile OS, often a combination of full disk encryption and file-level encryption	Unauthorized access to corporate data stored on a locked lost/stolen mobile device
Data Protection	Application-level encryption: potential additional layer of cryptographic protection on managed application data	Due to variations in implementation of encryption on mobile devices, per-application encryption may only provide additional protection over device encryption for certain devices in certain states (e.g., encrypted application data not in use and device locked)	Unauthorized access to corporate data stored on a lost/stolen device, particularly when device-level encryption is not in use or has been bypassed
Data Protection	Trusted key storage: protected locations in software, firmware, or hardware in which long-term cryptographic keys can be held	• Android not in use: Android Keystore. The underlying implementation is device-specific but is typically backed by firmware or hardware capabilities to securely store keys and perform cryptographic operations • iOS: provided by Secure Enclave • Windows Phone: has a Trusted Platform Module (TPM) capable of trusted key storage [27]	Cryptographic key theft when keys are stored in unprotected memory locations

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
Data Protection	Protected communications: The confidentiality of data transmitted over untrusted networks is protected by strong encryption	Communication between mobile devices, cloud services, and on-premises components are protected by Transport Layer Security	Eavesdropping or manipulation of unencrypted data transmitted over untrusted networks
Data Protection	Remote wipe: renders access to both personal and enterprise data stored on lost/stolen devices infeasible, but may wipe only a portion of flash memory	• Android: Device Policy Manager application program interface which is used by enterprise mobility management / mobile device management (EMM/MDM) agents, Google's Android Device Manager, and numerous third-party applications • iOS: provided by iCloud and can additionally be provided by an EMM/MDM system when the device is enrolled into enterprise management • Windows Phone: provided by windowsphone.com • Microsoft Intune and Office 365 MDM: can trigger a full wipe of enrolled devices remotely • Due to variations in implementation of wipe operations on mobile devices, the inability to recover data may be contingent on device- or application-level	Unauthorized access to personal and corporate data when an attacker is suspected of having physical access to a lost or stolen device

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
		encryption to achieve a cryptographic wipe by destroying the decryption key	
Data Protection	Selective wipe: Render access to enterprise data stored on a device infeasible without affecting personal data	• Microsoft Intune/ Systems Center Configuration Manager (SCCM) and Office 365 MDM: An administrator can wipe only organizational data from an enrolled device, leaving personal data intact • Android: Disabling the device administrator associated with Company Portal performs a selective wipe and unenrolls the device from Intune/Office 365 MDM • iOS: Removing the device management profile created during enrollment performs a selective wipe and unenrolls the device from Intune/Office 365 MDM • Windows Phone: Deleting the workplace created during the enrollment process performs a selective wipe and unenrolls the device from Intune/Office 365 MDM	• Unauthorized access to enterprise data when a managed device is under the control of an untrusted user, but destruction of personal data is undesirable • Accidental disclosure of corporate data that may be accessible to personal applications once the user has opted to unenroll their personal device from enterprise management
Data Protection	Automatic wipe: Multiple failed unlock attempts of lost/stolen devices can render access to both personal and enterprise data infeasible	• OS-level capability provided by each mobile OS • Microsoft Intune/SCCM and Office 365 MDM: Offer a policy setting to enforce activation of automatic wipe functionality	Unauthorized access to personal and corporate data when an attacker attempts brute-force attacks against the unlock mechanism for a lost or stolen device

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
Data Protection	Hardware security modules: tamper-resistant hardware used to perform cryptographic operations and secure storage that may be removable or physically part of the device	• Android: Device implementation specific, may be discrete hardware, or may be implemented in firmware (e.g., by using ARM TrustZone) • iOS: provided by Secure Enclave • Windows Phone: has a Trusted Platform Module capable of common cryptographic operations, which may be discrete hardware or may be implemented in firmware	Cryptographic key theft when keys are stored in memory locations accessible to untrusted code
Data Isolation	Sandboxing: OS or application-level mechanisms utilizing multiple protection, isolation, and integrity capabilities to achieve higher levels of overall isolation	OS-level capability provided by each mobile OS	• Exploitation of vulnerabilities in standard-process isolation mechanisms that would allow a process to access the instructions or data stored in the memory space or storage locations of another process • Exploitation of vulnerabilities in the OS by compromised or malicious mobile applications • Loss of availability of some OS functionality by flawed mobile applications that enter an unrecoverable execution state (e.g., application crashes)
Data Isolation	Memory isolation: Processes should be unable to access or	OS-level capability provided by each mobile OS	Unauthorized access by a running process to the data in use by another running process, or manipulation of the

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
	modify another process's memory		instructions loaded into another process's memory space
Data Isolation	Trusted execution: A process is created and runs in a trustworthy and isolated execution environment leveraging distinct memory spaces and controlled interfaces	OS-level capability provided by each mobile OS	Exploitation of vulnerabilities in standard-process isolation mechanisms in which the attacking and target processes run in the same security context
Data Isolation	Device resource management: ability to enable/disable device peripherals and certain OS-provided functionality	Microsoft Intune/SCCM and Office 365 MDM: Offer policy settings to restrict or disable peripherals and functions, which are applied and enforced on a mobile device by the Company Portal mobile application	• Compromise of the mobile OS via exploits delivered over unused wireless communications protocols (e.g., Bluetooth or near field communication (NFC) • Exfiltration of personal or enterprise data by malware or compromised mobile applications using unsecured and often unmonitored wireless communications protocols (e.g., Bluetooth or NFC) • Tracking the physical location of a mobile device using unused wireless communications protocols • Loss of availability of mobile device functionality resulting from an increase of power consumption by unused device peripherals (e.g., Bluetooth, NFC, Wi-Fi, location services)

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
			• Behavior tracking by malware or potentially harmful applications (PHAs) leveraging data obtained from device peripherals (e.g., Wi-Fi, location services, accelerometer) • Compromise of enterprise data, which can be recorded inconspicuously by Trojan or other malicious applications using accessible device peripherals (camera, microphone, location services)
Data Isolation	Data flow control: application-level access policies on OS-provided functionality that would transfer data into or out of its control	Microsoft Intune/SCCM: MDM and MAM policies can restrict how data is permitted to flow in or out of managed applications	Loss of confidentiality of and enterprise control over enterprise data that can be shared between mobile applications
Device Integrity	Application whitelisting/ blacklisting: allowing or disallowing installation of applications based on a prespecified list	Microsoft Intune/SCCM and Office 365 MDM: can create device policies that deny installation of applications from unofficial application stores	• Installation of mobile malware or PHAs, particularly repackaged versions of legitimate applications • Exploitation of vulnerabilities in a third-party library (e.g., advertisement library) embedded in an application
Device Integrity	Application whitelisting/blacklisting	Microsoft Intune/SCCM: can additionally specify a whitelist or blacklist of specific applications and prohibit unsigned applications from being installed	• Installation of vulnerable applications, which increases the probability of application and device compromise

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
			• Installation of untrusted applications, which handle sensitive data in an insecure manner
Device Integrity	Boot validation: validation that the device is in a known working state and unmodified at boot (e.g., basic input-output system integrity checks)	• Android: optional Verified Boot capability with device-specific availability. Additionally, other optional device-specific boot-loader protections may be present • iOS: provide by Secure Boot Chain • Windows Phone: provide by Secure Boot	Compromise of the mobile OS via modification of code executed during the boot process
Device Integrity	Application verification: ensures that applications being installed come from a valid source	• OS-level capability provided by each mobile OS to verify the digital signature of applications • Android: ability in device settings to enable/disable installation of applications from untrusted sources (typically meaning the Google Play Store) • iOS: For applications side-loaded in iOS 9, the user must explicitly trust the application developer before the application can be used [36] unless the application is installed through an MDM system that the device is enrolled in	Installation of applications that contain malicious code introduced after submission from the developer or, for applications downloaded from an official application store, after review by the application store authority (e.g., Google, Apple, Microsoft)
Device Integrity	Verified application and OS updates: Ensure that application and OS	OS-level capability provided by each mobile OS to verify the digital signature of applications and OS updates	• Introduction of malicious code into an installed (and thus trusted) application

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
	updates being installed come from a valid source		via an update that was modified since submission or review • Exploitation of publicly known vulnerabilities on unpatched devices • Introduction of malicious code into the OS via an update that was modified since submission
Device Integrity	Mobile malware detection: identification of malicious software on mobile platforms	Lookout Mobile Threat Protection (MTP) performs signature and non-signature-based analysis of installed mobile applications	Installation of mobile malware, PHAs, particularly repackaged versions of legitimate applications
Monitoring	Inventory of mobile device hardware and software: Provide version information for the hardware, firmware, OS, and installed applications for enrolled mobile devices	Microsoft Intune/SCCM and Office 365 MDM inventory enrolled devices, including hardware, firmware, and OS versions	Compromise of mobile devices through known and unpatched vulnerabilities in device firmware or the mobile OS
Monitoring	Inventory of mobile device hardware and software	Intune/SCCM inventory installed applications on enrolled mobile devices	• Compromise of mobile devices or data through known and unpatched vulnerabilities in installed applications • Data compromise through flawed applications known to handle sensitive data insecurely (e.g., store it unencrypted in areas normally accessible to other applications)

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
			• Data compromise through applications that are known to harvest sensitive or user behavior data unnecessary for their advertised purposes
Monitoring	Asset management: identifies, configures, and tracks devices, components, software, and services residing on a network	Provided by SCCM for hybrid build and Office 365 Enterprise E3 for cloud build	Lower the likelihood of device or application compromise by configuring the device to restrict or disable the use of vulnerable components or applications
Monitoring	Compliance checks: Provide information about whether a device is compliant with a mandated set of policies	Microsoft Intune/SCCM and Office 365 MDM: Periodically audit and log device policy compliance via Company Portal	Mobile devices with unapproved configurations of hardware, firmware, OS, applications, and device settings are used to access, store, or process enterprise data
Monitoring	Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised	• Microsoft Intune/SCCM and Office 365 MDM: can create device policies that enforce jailbreak detection on enrolled mobile devices • Company Portal: performs jailbreak and root detection on devices running iOS, Android, and Windows Phone 8.1 • Lookout MTP: performs jailbreak and root detection on device running iOS and Android	• Loss of confidentiality, integrity, or availability of personal or enterprise data accessed, stored, or processed on a mobile device running a compromised OS • For Lookout MTP, include losses on devices in which compromise of the OS may not be detected by the MDM agent
Monitoring	Auditing and logging: Capture and store security events for	Microsoft Intune/SCCM and Office 365 MDM: Routinely audit enrolled devices for compliance	Repeated compromise via exploits that could be mitigated following review of audit logs

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
	devices, including enrollment, failed compliance checks, administrative actions, and unenrollment		
Monitoring	Canned reports and ad hoc queries: produces preconfigured reports from audit logs and the ability to actively search or filter logs for specific data	• Provided by Intune/SCCM and Lookout MTP components • Microsoft Intune/SCCM: additionally, maintains a log of administrative actions and compliance check results to support reporting and alerting functions • Lookout MTP: routinely scans devices and logs any detected malware or indicators of OS compromise via rooting or jailbreaking	Repeated compromise via exploits that could be mitigated following review of audit logs
Identity and Authorization	Local authentication of user to device: requirement of a personal identification number (PIN), password, gesture, token, or other mechanism before the device can be fully used	OS-level capability provided by each mobile OS	Unauthorized access to or modification of enterprise or personal data accessible to applications that do not require authentication when an attacker has physical access to a mobile device
Identity and Authorization	Local user authentication to applications: application requires a PIN, password, token, or other authentication	Application-specific functionality that prevents usage of the application until the user successfully authenticates. May be contingent on remote authentication, as with Company Portal	Unauthorized access to or modification of enterprise data locally accessible to the application when an attacker has physical access to an unlocked mobile device

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
	mechanism to be fully used		
Identity and Authorization	Local user authentication to applications	Microsoft Intune/SCCM: Offer a MAM policy setting that requires entry of a PIN to use the application, which is enforced by Company Portal	Unauthorized access to or modification of enterprise data locally accessible to a managed application when an attacker has physical access to an unlocked mobile device
Identity and Authorization	Remote user authentication: Networked managed applications require authentication to a remote service to be fully used	Outlook and Company Portal: Require successful authentication to Office 365 Enterprise E3 for full functionality	Unauthorized remote access to enterprise resources when an attacker has access to a networked application for which application- or device-level authentication does not exist or has been bypassed
Identity and Authorization	Device provisioning and enrollment: restricts access to organization resources to provisioned mobile devices	Company Portal: provisions mobile devices into Microsoft Intune or Office 365 MDM	• Remote access to enterprise resources from untrusted mobile devices • Compromise of enterprise systems by malware executed on untrusted mobile devices
Privacy	Custom privacy statement: notification provided to users about the implications to privacy by the use of organizational resources and to privacy and device and application functionality for enrolled devices	Microsoft ADFS: allows the organization to customize the authentication portal, including a privacy statement	Violation of an employee's expectation of privacy as a result of monitoring an employee's personal mobile device during remote access sessions of enterprise resources

Security Characteristic	Security Capability and Capability Description	Implementation Note	Example Mitigated Threats
Privacy	Custom privacy statement	Company Portal: notifies the user of the implications of enrolling their device into an MDM	Violation of an employee's expectation of privacy as a result of monitoring an employee's personal mobile device following enrollment in an enterprise MDM