## NIST SPECIAL PUBLICATION 1800-22B

# Mobile Device Security:

## Bring Your Own Device (BYOD)

**Volume B:**
**Approach, Architecture, and Security Characteristics**

**Kaitlin Boeckl**
**Nakia Grayson**
**Gema Howell**
**Naomi Lefkovitz**

Applied Cybersecurity Division
Information Technology Laboratory

**Jason G. Ajmo**
**Milissa McGinnis***
**Kenneth F. Sandlin**
**Oksana Slivina**
**Julie Snyder**
**Paul Ward**

The MITRE Corporation
McLean, VA

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

March 2021

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device

# DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol. Spec. Publ. 1800-22B, 121 pages, (March 2021), CODEN: NSPUE2

# FEEDBACK

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

Comments on this publication may be submitted to: mobile-nccoe@nist.gov.

Public comment period: March 18, 2021 through May 03, 2021

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

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

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

However, some of the features that make BYOD mobile devices increasingly flexible and functional also present unique security and privacy challenges to both work organizations and device owners. The unique nature of these challenges is driven by the diverse range of devices available that vary in type, age, operating system (OS), and the level of risk posed.

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

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

| Name | Organization |
|---|---|
| Donna Dodson* | NIST |
| Joshua M. Franklin* | NIST |
| Jeff Greene | NIST |
| Natalia Martin | NIST |
| William Newhouse | NIST |
| Murugiah Souppaya | NIST |
| Kevin Stine | NIST |
| Chris Brown | The MITRE Corporation |

| Name | Organization |
|---|---|
| Nancy Correll | The MITRE Corporation |
| Spike E. Dog | The MITRE Corporation |
| Sallie Edwards | The MITRE Corporation |
| Parisa Grayeli | The MITRE Corporation |
| Marisa Harriston | The MITRE Corporation |
| Karri Meldorf | The MITRE Corporation |
| Erin Wheeler | The MITRE Corporation |
| Dr. Behnam Shariati | University of Maryland, Baltimore County |
| Jeffrey Ward | IBM |
| Cesare Coscia | IBM |
| Chris Gogoel | Kryptowire |
| Tom Karygiannis | Kryptowire |
| Jeff Lamoureaux | Palo Alto Networks |
| Sean Morgan | Palo Alto Networks |
| Kabir Kasargod | Qualcomm |
| Viji Raveendran | Qualcomm |
| Mikel Draghici | Zimperium |

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

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

| Technology Partner/Collaborator | Build Involvement |
|---|---|
| IBM | Mobile Device Management |
| Kryptowire | Application Vetting |
| Palo Alto Networks | Firewall; Virtual Private Network |
| Qualcomm | Trusted Execution Environment |
| Zimperium | Mobile Threat Defense |

## DOCUMENT CONVENTIONS

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

## CALL FOR PATENT CLAIMS

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

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

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

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

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

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

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

Such statements should be addressed to: mobile-nccoe@nist.gov

# Contents

1 Summary ........................................ 1

1.1 Challenge ........................................ 1

1.2 Solution ........................................ 3

1.2.1 Standards and Guidance ........................................ 4

1.3 Benefits ........................................ 4

2 How to Use This Guide ........................................ 5

2.1 Typographic Conventions ........................................ 6

3 Approach ........................................ 7

3.1 Audience ........................................ 7

3.2 Scope ........................................ 8

3.3 Assumptions ........................................ 8

3.4 Risk Assessment ........................................ 9

4 Architecture ........................................ 10

4.1 Understanding Common BYOD Architecture Threats and the Example Solution's Goals to Remediate Those Threats ........................................ 11

4.1.1 Threat Events ........................................ 11

4.1.2 Privacy Problematic Data Actions ........................................ 12

4.1.3 Security and Privacy Goals ........................................ 13

4.2 Example Scenario: Putting Guidance into Practice ........................................ 15

4.3 Technologies that Support the Security and Privacy Goals of the Example Solution ........................................ 15

4.3.1 Trusted Execution Environment ........................................ 16

4.3.2 Enterprise Mobility Management ........................................ 16

4.3.3 Virtual Private Network ........................................ 17

4.3.4 Mobile Application Vetting Service ........................................ 17

4.3.5 Mobile Threat Defense ........................................ 18

4.3.6 Mobile Operating System Capabilities ........................................ 19

4.4 Architecture Description ........................................ 21

4.5 Enterprise Integration of the Employees’ Personally Owned Mobile Devices ........... 22
4.5.1 Microsoft Active Directory Integration ........................................................24
4.5.2 Mobile Device Enrollment ..........................................................................25
4.6 Mobile Components Integration ........................................................................ 26
4.6.1 Zimperium–MaaS360..................................................................................27
4.6.2 Kryptowire–MaaS360 .................................................................................28
4.6.3 Palo Alto Networks–MaaS360 ....................................................................28
4.6.4 iOS and Android MDM Integration .............................................................29
4.7 Privacy Settings: Mobile Device Data Processing.............................................. 29
4.7.1 EMM: MaaS360...........................................................................................29
4.7.2 MTD: Zimperium .........................................................................................31
4.7.3 VPN: Palo Alto Networks ............................................................................34
5 Security and Privacy Analysis ........................................................... 34
5.1 Analysis Assumptions and Limitations ............................................................. 34
5.2 Build Testing ..................................................................................................... 34
5.3 Scenarios and Findings ..................................................................................... 35
5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings...................35
5.3.2 Threat Events and Findings..........................................................................35
5.3.3 Privacy Problematic Data Actions and Findings.........................................37
5.4 Security and Privacy Control Mappings ............................................................ 38
6 Example Scenario: Putting Guidance into Practice .............................. 39
7 Conclusion........................................................................................ 39
8 Future Build Considerations .............................................................. 41
Appendix A List of Acronyms ............................................................. 42
Appendix B Glossary .......................................................................... 44
Appendix C References ....................................................................... 46
Appendix D Standards and Guidance.................................................... 52
Appendix E Example Solution Lab Build Testing Details ......................... 54
E.1 Threat Event 1 ................................................................................................... 54

E.2 Threat Event 2 ........ 54

E.3 Threat Event 3 ........ 55

E.4 Threat Event 4 ........ 56

E.5 Threat Event 5 ........ 56

E.6 Threat Event 6 ........ 56

E.7 Threat Event 7 ........ 57

E.8 Threat Event 8 ........ 57

E.9 Threat Event 9 ........ 58

E.10 Threat Event 10 ........ 58

E.11 Threat Event 11 ........ 59

E.12 Threat Event 12 ........ 60

E.13 Problematic Data Action 1 ........ 60

E.14 Problematic Data Action 2 ........ 60

E.15 Problematic Data Action 3 ........ 61

**Appendix F Threat Event Test Information ........ 62**

F.1 Threat Event 1 ........ 62

F.2 Threat Event 2 ........ 64

F.3 Threat Event 3 ........ 65

F.4 Threat Event 4 ........ 68

F.5 Threat Event 5 ........ 72

F.6 Threat Event 6 ........ 73

F.7 Threat Event 7 ........ 74

F.8 Threat Event 8 ........ 76

F.9 Threat Event 9 ........ 77

F.10 Threat Event 10 ........ 80

F.11 Threat Event 11 ........ 82

F.12 Threat Event 12 ........ 84

F.13 Problematic Data Action 1 ........ 85

F.14 Problematic Data Action 2 ........ 86

F.15 Problematic Data Action 3 ........ 87

Appendix G Example Security Subcategory and Control Map ................. 89
Appendix H Example Privacy Subcategory and Control Map ................ 109

## List of Figures

Figure 3-1 Cybersecurity and Privacy Risk Relationship.......................................................... 10
Figure 4-1 Security and Privacy Goals............................................................................................ 14
Figure 4-2 iOS App Transport Security............................................................................................ 20
Figure 4-3 Example Solution Architecture ...................................................................................... 21
Figure 4-4 iOS Application Management and Benefits .................................................................. 23
Figure 4-5 Android Application Management and Benefits .......................................................... 24
Figure 4-6 Example Solution VPN Authentication Architecture ..................................................... 26
Figure 4-7 Data Collected by Example Solution Mobile Device Management................................ 30
Figure 4-8 Example Solution Mobile Device Management Privacy Settings ................................... 31
Figure 7-1 Example Solution Architecture ...................................................................................... 40
Figure F-1 Policy Violation Notification ........................................................................................... 62
Figure F-2 Policy Violation Email...................................................................................................... 63
Figure F-3 Policy Violation Alert Details Email .................................................................................. 63
Figure F-4 Enterprise Mobility Management Removal Alert............................................................ 64
Figure F-5 PAN-DB Blocked Website ............................................................................................... 65
Figure F-6 Zimperium Threat Detected............................................................................................ 66
Figure F-7 Zimperium Sideloaded Application Alert........................................................................ 67
Figure F-8 Zimperium Threat Log with Sideloaded Application Alert ............................................. 67
Figure F-9 Email Regarding MaaS360 Policy Violation Alert ........................................................... 68
Figure F-10 MaaS360 Policy Violation Alert...................................................................................... 69
Figure F-11 Zimperium Risk Detected.............................................................................................. 70
Figure F-12 Zimperium OS Risk ....................................................................................................... 71
Figure F-13 MaaS360 Compliance Rule Violation............................................................................. 71
Figure F-14 MaaS360 Policy Violation Email .................................................................................... 72
Figure F-15 Kryptowire iOS Application Report .............................................................................. 73

Figure F-16 Kryptowire Android Application Report ....................74
Figure F-17 MaaS360 Applying Mandatory PIN Policy....................75
Figure F-18 Zimperium Reporting Devices with a Disabled Lock Screen ....................76
Figure F-19 Application Report with Hardcoded Credentials ....................77
Figure F-20 Attempting to Access the Virtual Private Network (VPN) on an Unmanaged Device ....................78
Figure F-21 Android: Attempting to Access the VPN on an Unmanaged Device ....................79
Figure F-22 Android: Attempting to Access the VPN on a Managed Device....................80
Figure F-23 Selectively Wiping an iOS Device ....................81
Figure F-24 Selective-Wipe Completed....................81
Figure F-25 No Corporate Data Left on Device....................82
Figure F-26 MaaS360 DLP Configuration ....................83
Figure F-27 Attempting to Paste Text on iOS ....................84
Figure F-28 GlobalProtect Requires the User’s Password ....................85
Figure F-29 Initiating a Selective Wipe ....................86
Figure F-30 Application Inventory Information....................86
Figure F-31 Location Information Restricted....................87
Figure F-32 Non-Administrator Failed Portal Login ....................88

# List of Tables

Table 4-1 Examples of BYOD Deployment Threats....................12
Table 4-2 Examples of BYOD Potential Privacy Events and Problematic Data Actions ....................12
Table 4-3 Commercially Available Products Used ....................27
Table 4-4 Data Collected by Zimperium....................32
Table 5-1 Threat Events and Findings Summary ....................36
Table 5-2 Summary of Privacy Problematic Data Actions and Findings....................37
Table G-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping....................89
Table H-1 Example Solution’s Privacy Standards and Best Practices Mapping....................109

# 1 Summary

This section familiarizes the reader with

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

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

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

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

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

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

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

## 1.1 Challenge

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

BYOD deployment challenges can include:

**Supporting a broad ecosystem of mobile devices**

- with diverse technologies that rapidly evolve and vary in manufacturer, operating system (OS), and age of the device
- where each device has unique security and privacy requirements and capabilities
- whose variety can present interoperability issues that might affect organizational integration

**Reducing organizational risk and threats to the enterprise's sensitive information**

- posed by applications like games that may not usually be installed on devices issued by an organization
- that result from lost, stolen, or sold mobile devices that still contain or have access to organizational data
- created by a user who shares their personally owned device with friends and family members when that personally owned device may also be used for work activities
- due to personally owned mobile devices being taken to places that increase the risk of loss of control for the device
- that result from malicious applications compromising the device and subsequently the data to which the device has access
- produced by network-based attacks that can traverse a device's always-on connection to the internet
- caused by phishing attempts that try to collect user credentials or entice a user to install malicious software

**Protecting the privacy of employees**

- by helping to keep their personal photos, documents, and other data private and inaccessible to others (including the organization)
- by helping to ensure separation between their work and personal data while simultaneously meeting the organization's objectives for business functions, usability, security, and employee privacy
- by providing them with concise and understandable information about what data is collected and what actions are allowed and disallowed on their devices

**Clearly communicating BYOD concepts**

- among an organization's information technology team so it can develop the architecture to address BYOD's unique security and privacy concerns while using a repeatable, standardized, and clearly communicated risk framework language
- to organizational leadership and employees to obtain support in deploying BYOD

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

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

## 1.2 Solution

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

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

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

**The example solution in this practice guide helps**

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

- vet the security of mobile applications used for work-related activities
- organizations implement settings to protect employee privacy
- an organization deploy its own BYOD solution by providing a series of how-to guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture—to help security and privacy engineers rapidly deploy and evaluate a mobile device solution in their test environment

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

### 1.2.1 Standards and Guidance

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

## 1.3 Benefits

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

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

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

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

- safeguards to help protect their privacy
- better protected personal devices by screening work applications for malicious capability before installing them

- enhanced understanding about how their personal device will integrate with their organization through a standardized BYOD deployment

# 2 How to Use This Guide

This section familiarizes the reader with

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

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

This guide contains four volumes:

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

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

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

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

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

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

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

**IT professionals** who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of this guide's example solution for BYOD security management. Your organization's security experts should identify the products that will effectively address the BYOD risks identified for your organization and best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 4.3, Technologies that Support the Security and Privacy Goals of the Example Solution, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

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

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

Acronyms used in figures can be found in the Acronyms Appendix.

## 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

# 3 Approach

This section familiarizes the reader with

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

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

Two broad and significant themes emerged from this research:

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

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

## 3.1 Audience

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

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

## 3.2 Scope

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

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

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

## 3.3 Assumptions

This project is guided by the following assumptions:

- The example solution was developed in a lab environment. While the environment is based on a typical organization's IT enterprise, the example solution does not reflect the complexity of a production environment.
- The organization has access to the skills and resources required to implement a mobile device security and privacy solution.
- The example security and privacy control mappings provided as part of this practice guide are focused on mobile device needs, and do not include general control mappings that would also typically be used in an enterprise. Those general control mappings that do not specifically apply to this guide's mobile device security example solution are outside the scope of this guide's example solution.
- Because the organizational environment in which this build could be implemented represents a greater level of complexity than is captured in the current guide, we assume that organizations

will first examine the implications for their current environment before implementing any part of the proposed example solution.

- The organization has either already invested or is willing to invest in the security of mobile devices used within it and in the privacy of participating employees, and in the organization's IT systems more broadly. As such, we assume that the organization either has the technology in place to support this implementation or has access to the off-the shelf technology used in this build, which we assume will perform as described by the respective product vendor.
- The organization has familiarized itself with existing standards and any associated guidelines (e.g., NIST Cybersecurity Framework [1]; *NIST Privacy Framework* [2]; NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]; NIST SP 1800-4 *Mobile Device Security: Cloud and Hybrid Builds* [7]) relevant to implementation of the example solution proposed in this practice guide. We also assume that any existing technology used in the example solution has been implemented in a manner consistent with these standards.
- The organization has instituted relevant mobile device security and privacy policies, and these will be updated based on implementation of this example solution.
- The organization will provide guidance and training to its employees regarding BYOD usage and how to report device loss or suspected security issues in which their devices are involved. This guidance will be periodically reviewed and updated, and employees will be regularly trained on BYOD usage.

## 3.4 Risk Assessment

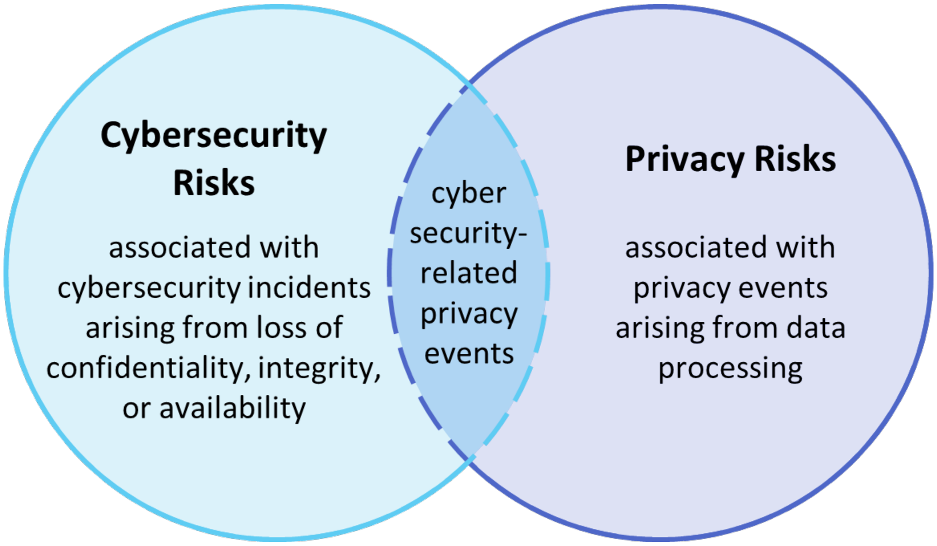
NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the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

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

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

An example of a security risk that may also be considered a privacy risk is an employer having increased access to an employee's personal use applications such as personal contacts and personal calendars on their device. An example of a privacy risk that is not driven by a security risk is a BYOD implementation being used to track employee location, which may reveal information about the places they visit.

**Figure 3-1 Cybersecurity and Privacy Risk Relationship**


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

The security capabilities in this build help address some of the privacy risks that arise for employees. This build also uses the *NIST Privacy Framework* [2] and Privacy Risk Assessment Methodology (PRAM) [8] to identify and address privacy risks that are beyond the scope of security risks. Regardless of whether cybersecurity and privacy are situated in the same part of the organization or in different parts, the two capabilities must work closely together to address BYOD risks.

A risk assessment can include additional analysis areas. For more information on the example solution's:

- **Security and privacy threats**, and **goals to remediate those threats**, see Section 4.1
- **Vulnerabilities** that influenced the reference architecture, see Appendix Section F-5 of the Supplement
- **Risks** that influenced the architecture development, see Appendix Section F-6 of the Supplement
- **Security Control Mapping** to cybersecurity and privacy standards and best practices, see Appendix G and Appendix H

# 4 Architecture

This section helps familiarize the reader with

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

## 4.1 Understanding Common BYOD Architecture Threats and the Example Solution's Goals to Remediate Those Threats

This section contains examples of common security and privacy concerns in BYOD architectures. We provide a list of goals to address those challenges. Once completed, the architecture provides organizations with a security and privacy-enhanced design for their mobile devices. The example solution's challenges and goals are highlighted below, followed by the architecture that supports those goals.

### 4.1.1 Threat Events

Leveraging a system life cycle approach [9], this build considered threats relating to BYOD deployments. Information from the Open Web Application Security Project Mobile Top 10 [10], which provides a consolidated list of mobile application risks, and information from the NIST Mobile Threat Catalogue [5], which examines the mobile information system threats in the broader mobile ecosystem were used to develop applicable threats. Table 4-1 gives each threat an identifier for the purposes of this build, a description of each threat event (TE), and the related NIST Mobile Threat Catalogue Threat identifiers (IDs).

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

Table 4-1 Examples of BYOD Deployment Threats

| Threat Event ID | Threat Event Description | NIST Mobile Threat Catalogue Threat ID |
|---|---|---|
| **TE-1** | privacy-intrusive applications | APP-2, APP-12 |
| **TE-2** | account credential theft through phishing | AUT-9 |
| **TE-3** | malicious applications | APP-2, APP-5, APP-31, APP-40, APP-32, AUT-10 |
| **TE-4** | outdated phones | APP-4, APP-26, STA-0, STA-9, STA-16 |
| **TE-5** | camera and microphone remote access | APP-32, APP-36 |
| **TE-6** | sensitive data transmissions | APP-0, CEL-18, LPN-2 |
| **TE-7** | brute-force attacks to unlock a phone | AUT-2, AUT-4 |
| **TE-8** | weak password practices protection | APP-9, AUT-0 |
| **TE-9** | unmanaged device protection | EMM-5 |
| **TE-10** | lost or stolen data protection | PHY-0 |
| **TE-11** | protecting data from being inadvertently backed up to a cloud service | EMM-9 |
| **TE-12** | personal identification number (PIN) or password-sharing protection | AUT-0, AUT-2, AUT-4, AUT-5 |

### 4.1.2 Privacy Problematic Data Actions

This build also considered operational activities of the example solution that interact with employee data during BYOD processes (“data actions”). Additionally, it identified those that potentially cause privacy-related problems for individuals (“problematic data actions”). Problematic data actions (PDAs) are those actions that may cause an adverse effect for individuals.

The NIST PRAM [8] and accompanying Catalog of Problematic Data Actions and Problems [11] were used to conduct this analysis. Table 4-2 provides the results of this analysis. See Appendix G of the Supplement for an example of determining the privacy risks based on these data actions.

Table 4-2 Examples of BYOD Potential Privacy Events and Problematic Data Actions

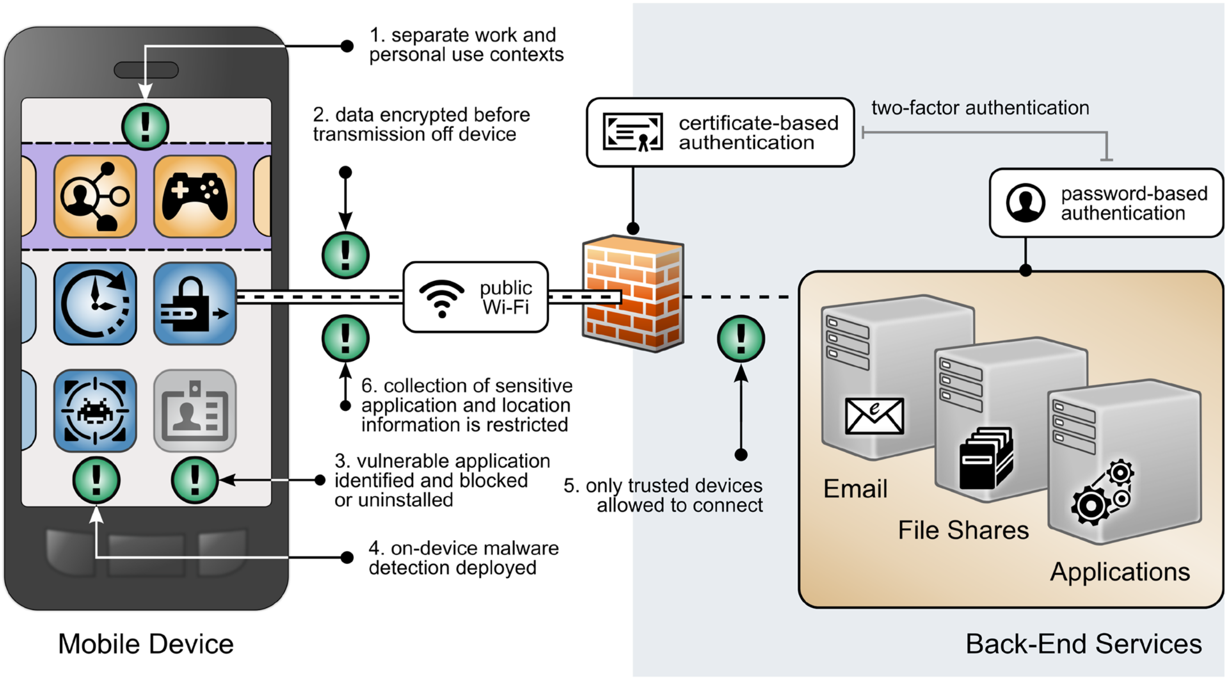
| Problematic Data Action ID | Mobile Data Actions | Problematic Data Actions |
|---|---|---|
| **PDA-1** | Devices can be wiped and reset to factory settings based on inputs regarding anomalous activity and untrusted applications. | Unwarranted restriction:<br>Blocking device access or wiping devices entirely may result in loss of personal data, which can cause employee loss of autonomy in their interactions with their device, economic loss to recover personal data, or loss of trust in the organization’s BYOD implementation. |

| Problematic Data Action ID | Mobile Data Actions | Problematic Data Actions |
|---|---|---|
| **PDA-2** | The BYOD infrastructure comprehensively monitors device interactions related to enterprise connectivity and data processing. | Surveillance:<br>Monitoring BYOD resources on personal devices provides a degree of visibility into personal devices that employers would not otherwise have, which in turn can result in the employer creating an incomplete narrative about employees that could lead to issues such as discrimination or employee loss of trust in the employer if the employee discovers unanticipated monitoring. Additionally, employees who connect their personal mobile device to the organization's network may not be aware of the degree of visibility into their personal activities and data and may not want this to occur. For example, employers may be able to collect location information or application data that provides insights into employee health. Employees may feel as though they are being surveilled. |
| **PDA-3** | Data about individuals and their devices flows between various applications and analytical tools, some of which may be shared with third parties and publicly. | Unanticipated revelation:<br>Transmission of employee device information and personal data to the employer and third parties beyond the employer may occur through monitoring, data sharing across parties for analytics, and other operational purposes. Administrator and co-worker awareness of otherwise private activities on devices may reveal information about employees that results in dignity losses, such as embarrassment or emotional distress.<br><br>Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to information about them. This transmission could reveal personal information about the employee to parties they would not expect to have such information. This lack of employee visibility and awareness of data-sharing practices may also cause employee loss of trust in the employer. |

### 4.1.3 Security and Privacy Goals

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

Figure 4-1 Security and Privacy Goals


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

The following goals were highlighted above in Figure 4-1 Security and Privacy Goals, with a green exclamation mark:

1. **Separate organization and personal information.** BYOD deployments can place organizational data at risk by allowing it to travel outside internal networks and systems when it is accessed on a personal device. BYOD deployments can also place personal data at risk by capturing information from employee devices. To help mitigate this, organizational and personal information can be separated by restricting data flow between organizationally managed and unmanaged applications. The goals include helping to prevent sensitive data from crossing between work and personal contexts.
2. **Encrypt data in transit.** Devices deployed in BYOD scenarios can leverage nonsecure networks, putting data at risk of interception. To help mitigate this, mobile devices can connect to the organization over a VPN or similar solution to encrypt all data before it is transmitted from the device, protecting otherwise unencrypted data from interception. A user would not be able to access the organization’s resources without an active VPN connection and required certificates.
3. **Identify vulnerable applications.** Employees may install a wide range of applications on their personally owned devices, some of which may have security weaknesses. When vulnerable personal applications are identified, an organization can remove the employee’s work profile or configuration file from the device rather than uninstalling the employee’s personal applications.

4. **Detect malware.** On personally owned devices without restriction policies in place, users may obtain applications outside official application stores, increasing the risk of installing malware in disguise. To help protect from this risk, an organization could deploy malware detection to devices to identify malicious applications and facilitate remediation.
5. **Trusted device access.** Because mobile devices can connect from unknown locations, an organization can provision mobile devices with a security certificate that allows identifying and authenticating them at the connection point, which combines with user credentials to create two-factor authentication from mobile devices. An employee would not be able to access the organization's resources without the required certificates.
6. **Restrict information collection.** Mobile device management tools can track application inventory and location information, including physical address, geographic coordinates, location history, internet protocol (IP) address, and Secure Set Identifier (SSID). These capabilities may reveal sensitive information about employees, such as frequently visited locations or habits. Device management tools can be configured to exclude application and location information. Excluding the collection of information further protects employee privacy when device and application data is shared outside the organization for monitoring and analytics.

## 4.2 Example Scenario: Putting Guidance into Practice

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

The example scenario supplement shows how a fictional organization used the guidance in NIST's Cybersecurity Framework [1], Privacy Framework [2], Risk Management Framework [9], and PRAM [8] to identify and address their BYOD security and privacy goals.

## 4.3 Technologies that Support the Security and Privacy Goals of the Example Solution

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

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

### 4.3.1 Trusted Execution Environment

A trusted execution environment (TEE) is “a tamper-resistant processing environment that runs on a ‘separation kernel’. It guarantees the authenticity of the executed code, the integrity of the runtime states (e.g., central processing unit (CPU) registers, memory and sensitive I/O), and the confidentiality of its code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide remote attestation that proves its trustworthiness for third-parties” [12]. The TEE helps protect the mobile devices from executed code with integrity issues. This is important in BYOD environments due to an enterprise’s limited control over an employee’s personally owned device. Users can install and run many types of applications on personally owned devices without restriction from the enterprise.

### 4.3.2 Enterprise Mobility Management

Organizations use EMM solutions to secure the mobile devices of users who are authorized to access organizational resources. Such solutions generally have two main components. The first is a backend service that mobile administrators use to manage the policies, configurations, and security actions applied to registered mobile devices. The second is an on-device agent, usually in the form of a mobile application, that integrates between the mobile OS and the solution’s backend service. iOS also supports a web-based EMM enrollment use case, which we do not discuss in this document.

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

EMM solutions commonly include any of the following capabilities: mobile application management, mobile content management, and implementations of or integrations with device- or mobile-OS-specific containerization solutions, such as Samsung Knox. These capabilities can be used in the following ways:

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

For further reading on this topic, NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6] provides additional information on mobile device management with EMM solutions. The National Information Assurance Partnership’s (NIAP’s) *Protection*

*Profile for Mobile Device Management Servers and Extended Package for Mobile Device Management Agents* [13] describes important capabilities and security requirements to look for in EMM systems.

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

### 4.3.3 Virtual Private Network

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

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

NIAP's *Module for Virtual Private Network (VPN) Gateways 1.0* [14], in combination with *Protection Profile for Network Devices* [15], describes important capabilities and security requirements to expect from VPN gateways.

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

### 4.3.4 Mobile Application Vetting Service

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

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

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

While NIAP does not provide a protection profile for application vetting services, their *Protection Profile for Application Software* [16] describes security requirements to be expected from mobile applications. Many mobile application vetting vendors provide capabilities to automate evaluation of applications against NIAP's requirements.

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

### 4.3.5 Mobile Threat Defense

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

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

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

### 4.3.6 Mobile Operating System Capabilities

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

#### *4.3.6.1 Secure Boot*

Secure boot is a general term that refers to a system architecture that is designed to prevent and detect any unauthorized modification to the boot process. A system that successfully completes a secure boot has loaded its start-up sequence information into a trusted OS. A common mechanism is for the first program executed (a boot loader) to be immutable (stored on read-only memory or implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified by either immutable or verified code prior to execution. This process establishes a chain of trust that can be traced back to immutable, implicitly trustworthy code. Using an integrated TEE as part of a secure boot process is preferable to an implementation that uses software alone [17].

#### *4.3.6.2 Device Attestation*

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

Device attestation requires cryptographic operations using an immutable private key that can be verified by a trusted third party, which is typically the original equipment manufacturer of the TEE or device platform vendor. Proof of possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique device identifiers, metadata, the results of integrity checks on mutable software, and possibly metrics from the boot or attestation process itself [17].

#### *4.3.6.3 Mobile Device Management Application Programming Interfaces*

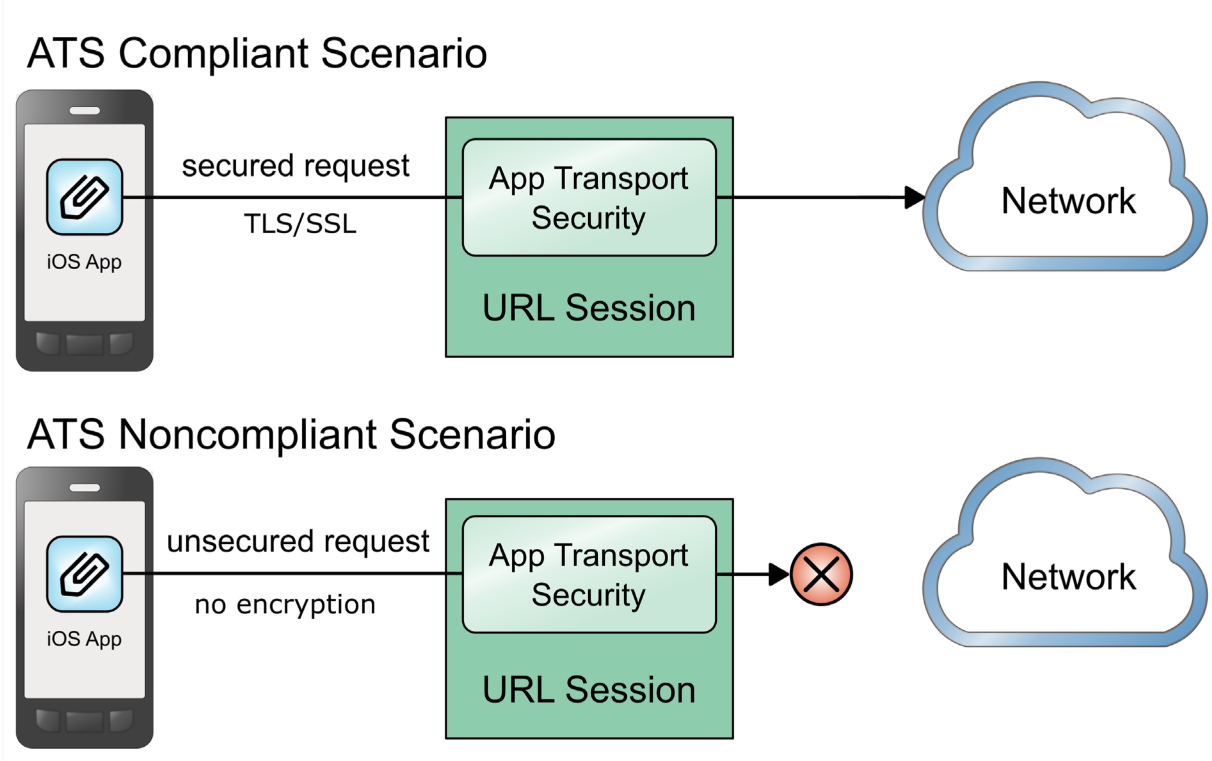
Mobile OS and platform-integrated firmware can provide a number of built-in security features that are generally active by default. Examples include disk- and file-level encryption, verification of digital signatures for installed software and updates, a device unlock code, remote device lock, and automatic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

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

#### 4.3.6.4 iOS App Transport Security

App Transport Security (ATS) is a networking security feature on Apple iOS devices that increases data integrity and privacy for applications and extensions [18], [19]. ATS requires that the network connections made by applications are secured through the Transport Layer Security protocol, which uses reliable cipher suites and certificates. In addition, ATS blocks any connection that does not meet minimum security requirements. For applications linked to iOS 9.0 and later, ATS is enabled by default. Figure 4-2 shows how ATS compliant and noncompliant applications function. As demonstrated in the figure, secured application requests are allowed, and nonsecure requests are blocked.

**Figure 4-2 iOS App Transport Security**



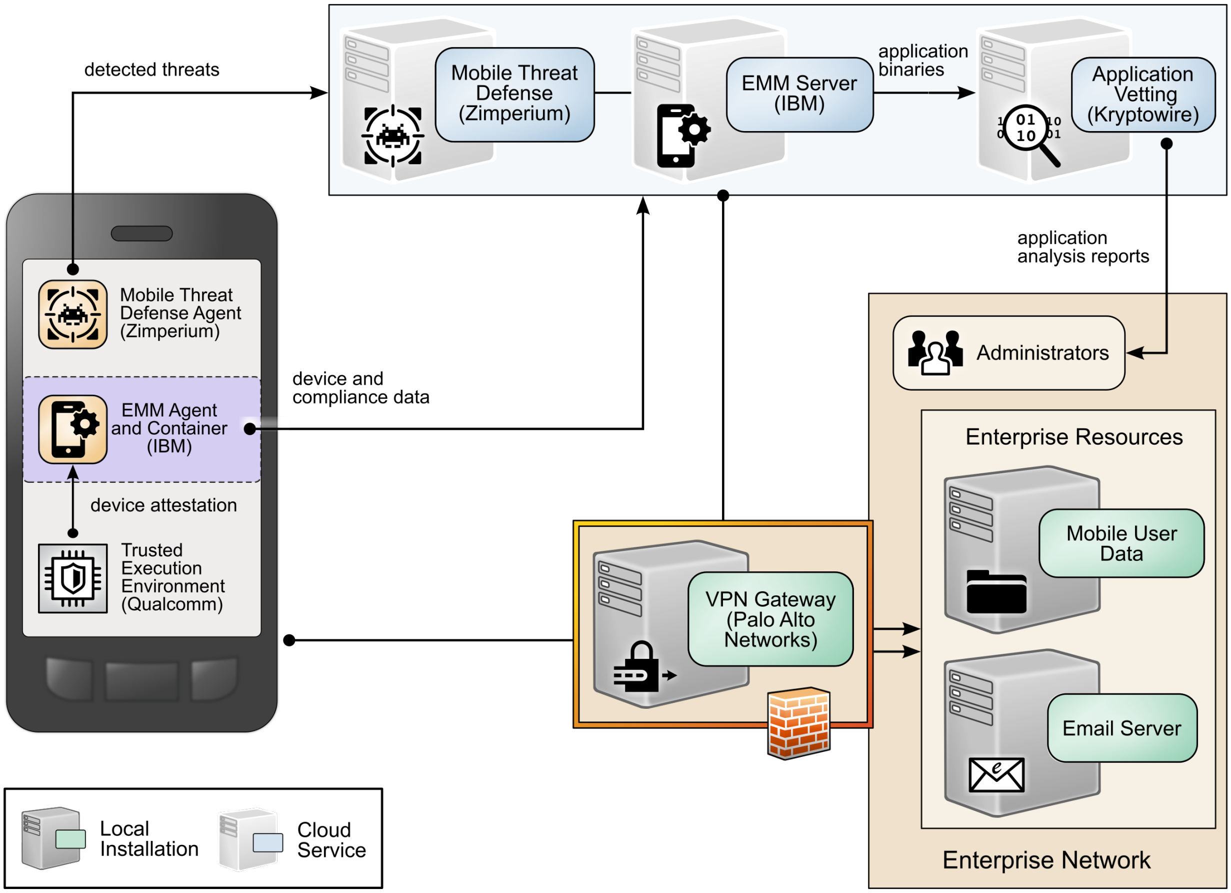
#### 4.3.6.5 Android Network Security Configuration

With data privacy becoming even more important, Google released mobile OS enhancements to protect data that traverses Android devices and endpoints [20], [21]. The Android Network Security Configuration prevents applications from transmitting sensitive data unintentionally in unencrypted cleartext. By default, `cleartextTrafficPermitted` is set to `false`. Through the Android Network Security Configuration feature, developers can designate what certification authorities are trusted to ensure secure communications and issue certificates.

## 4.4 Architecture Description

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

**Figure 4-3 Example Solution Architecture**


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
01 10
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Local Installation
Cloud Service
Enterprise Network

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

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

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

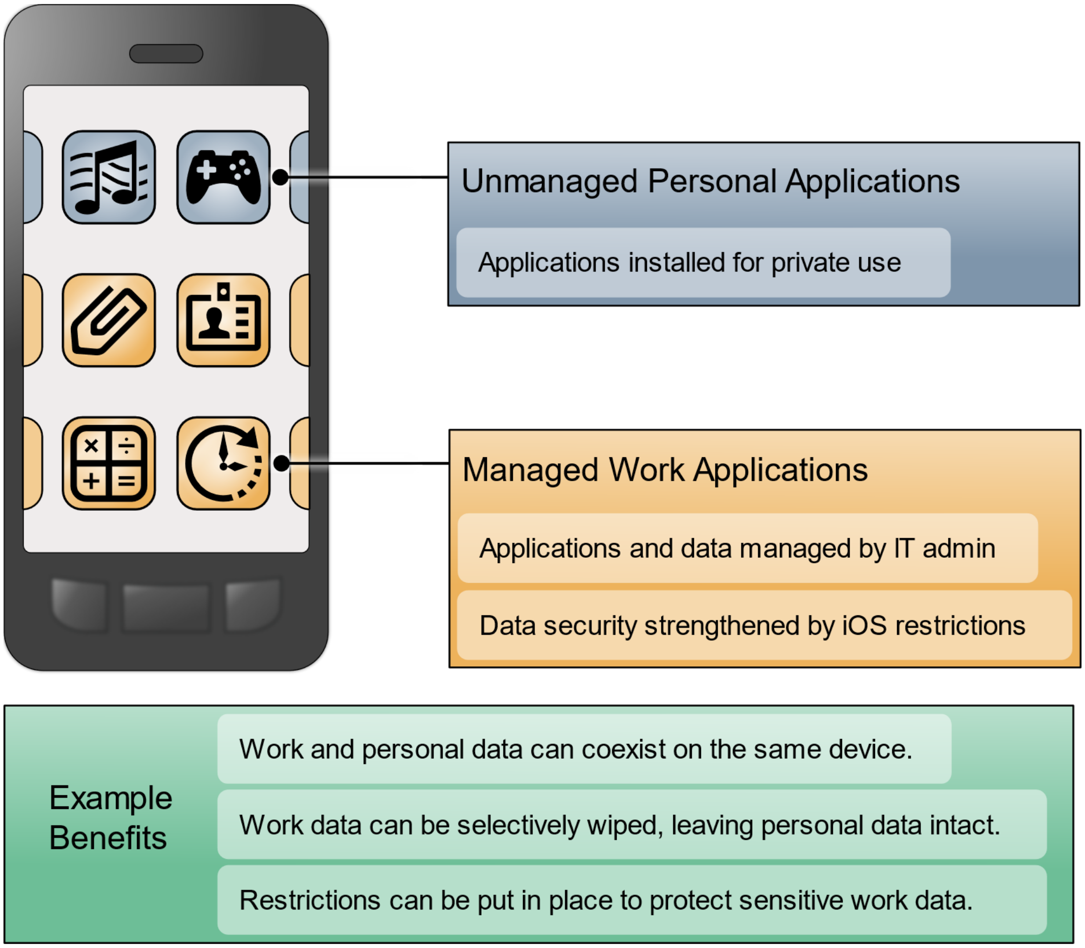
## 4.5 Enterprise Integration of the Employees’ Personally Owned Mobile Devices

One key benefit of BYOD solutions for employees is the ability to access both work and personal data on the same device. While the technical approaches differ between iOS and Android devices, both operating systems offer the following types of features for managing the coexistence of work and personal data on devices [22], [23]:

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

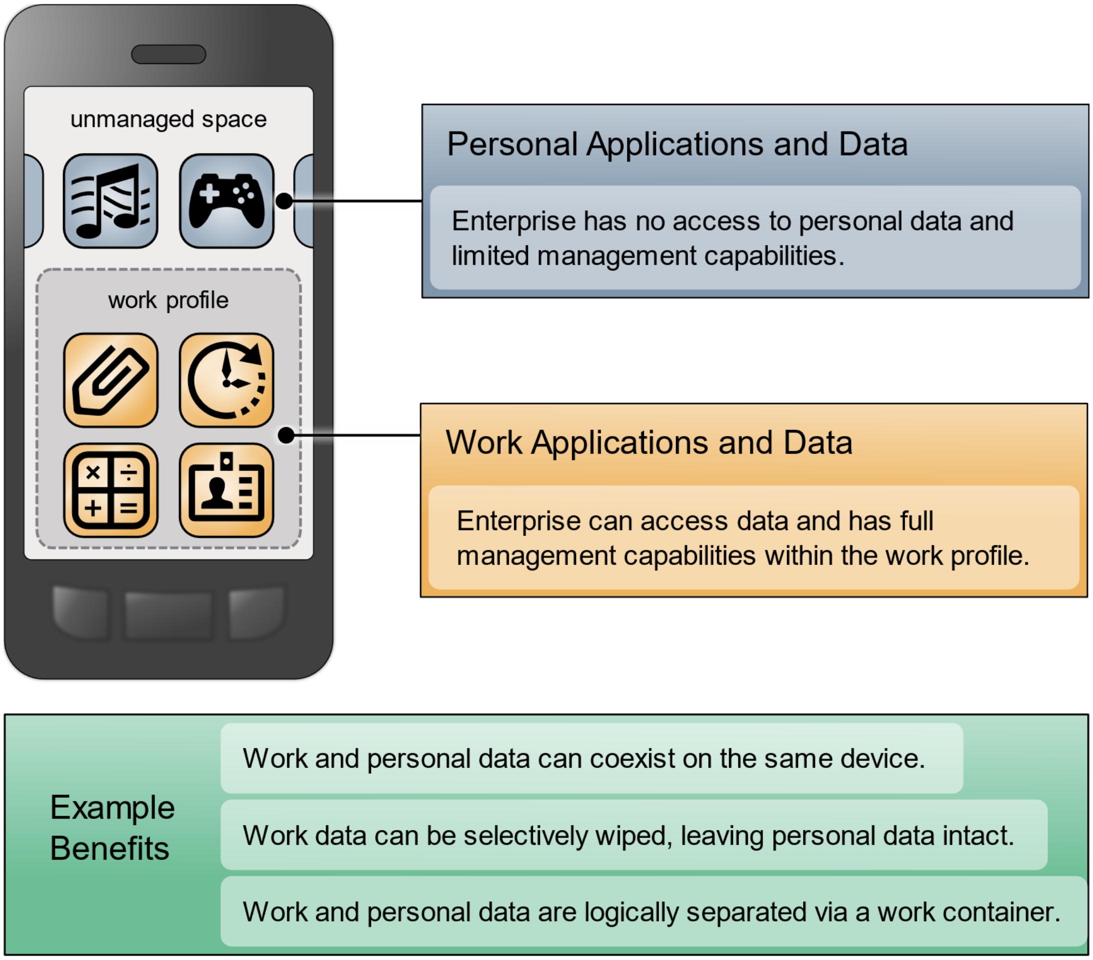
868 Illustrating this concept, Figure 4-4 iOS Application Management and Benefits, shows enterprise integration for managed and unmanaged applications on iOS devices. To protect sensitive work data, application restrictions, such as preventing the ability to copy data between work and personal application, are applied.

872 **Figure 4-4 iOS Application Management and Benefits**


Unmanaged Personal Applications
Applications installed for private use
Managed Work Applications
Applications and data managed by IT admin
Data security strengthened by iOS restrictions
Example Benefits
Work and personal data can coexist on the same device.
Work data can be selectively wiped, leaving personal data intact.
Restrictions can be put in place to protect sensitive work data.

As illustrated in Figure 4-5, for Android devices, work applications can be separated into a container, with data access restricted between the personal and work container applications.

**Figure 4-5 Android Application Management and Benefits**



Enterprise has no access to personal data and limited management capabilities.

Enterprise can access data and has full management capabilities within the work profile.

Work and personal data can coexist on the same device.

Work data can be selectively wiped, leaving personal data intact.

Work and personal data are logically separated via a work container.

## 4.5.1 Microsoft Active Directory Integration

The example solution is integrated with Microsoft Active Directory (AD), which provides both enterprise identity management and certificate enrollment services via public key infrastructure. International Business Machines (IBM) MaaS360 connects directly to the domain controller and the Network Device Enrollment Service (NDES) servers via an IBM Cloud Extender installed on the local intranet, while GlobalProtect connects to the domain controller via the Palo Alto Networks firewall’s Lightweight Directory Access Protocol service route.

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

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

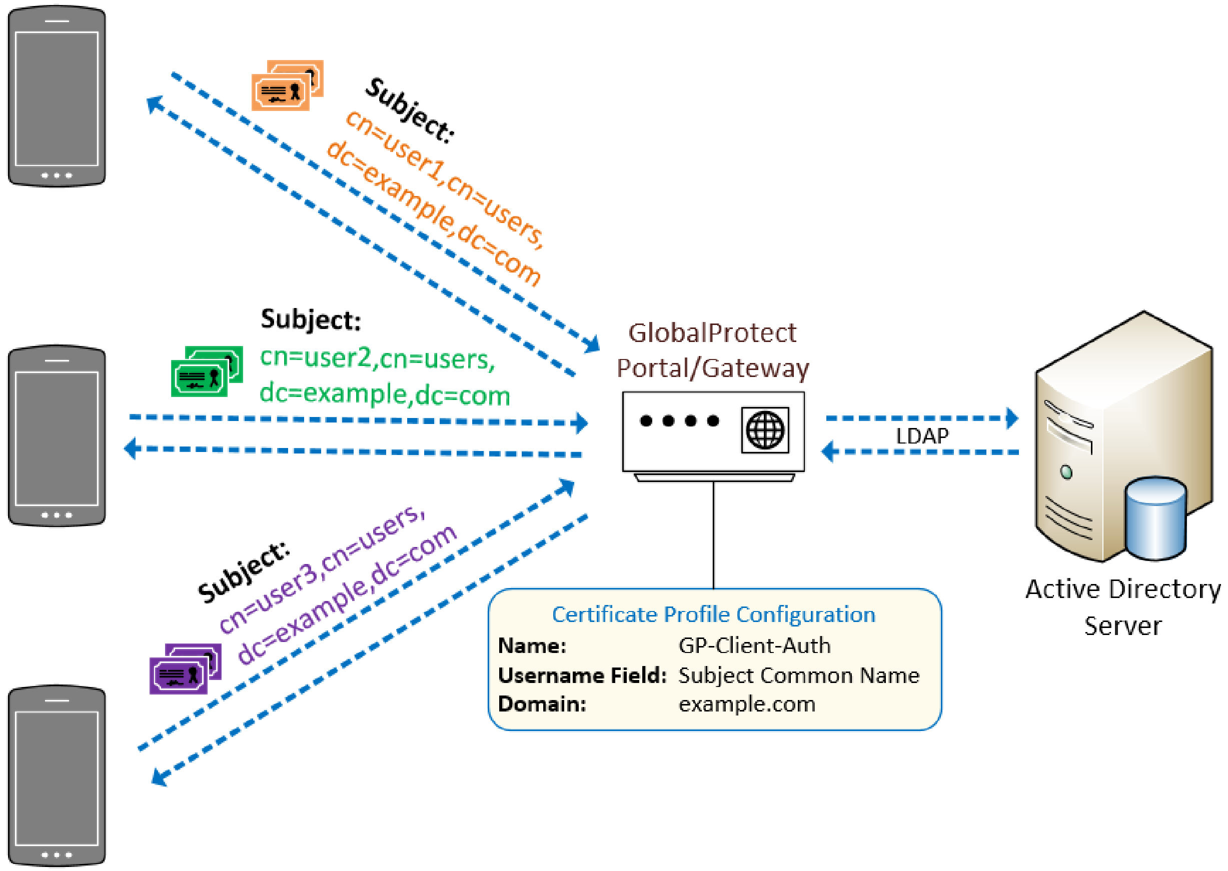
### 4.5.2 Mobile Device Enrollment

The example solution shown in Figure 4-6 mitigates the potential for SCEP to be remotely exploited by restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network. The uniform resource locator (URL) of the NDES server is resolvable only on this managed Wi-Fi network.

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

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

**Figure 4-6 Example Solution VPN Authentication Architecture**



## 4.6 Mobile Components Integration

IBM MaaS360 supports integration of third-party applications and cloud services via a representational state transfer (REST) API [24]. External services are authenticated via access tokens, obtained through MaaS360 support. Zimperium and Kryptowire used the REST API [25].

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

Table 4-3 Commercially Available Products Used

| Commercially Available Product | Mobile Security Technology |
|---|---|
| IBM MaaS360 Mobile Device Management (SaaS) Version 10.73<br>IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)<br>IBM MaaS360 Cloud Extender<br>Cloud Extender Modules:<br>Certificate Integration Module Version 2.96.000<br>Cloud Extender Base Module Version 2.96.000<br>Cloud Extender Basic Module Device Version 2.96.000<br>MaaS360 Configuration Utility Module Version 2.96.200<br>Mobile Device Management Module Version 2.31.020<br>User Authentication Module Version 2.96.200 | mobile device management |
| Kryptowire Cloud Service | application vetting |
| Palo Alto Networks PA-VM-100 Version 9.0.1<br>Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android) | firewall<br>virtual private network |
| Qualcomm (Version is mobile device dependent) | trusted execution environment |
| Zimperium Defense Suite<br>Zimperium Console Version vGA-4.23.1<br>Zimperium zIPS Agent Version 4.9.2 (Android and iOS) | mobile threat defense |

### 4.6.1 Zimperium–MaaS360

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

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

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

- low
- normal
- elevated
- critical

### 4.6.2 Kryptowire–MaaS360

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

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

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

- low
- medium
- high
- critical

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

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

### 4.6.3 Palo Alto Networks–MaaS360

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

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

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

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

### 4.6.4 iOS and Android MDM Integration

Both iOS and Android integrate directly with MaaS360. Configuration profiles manage iOS devices. Configuration profiles can force security policies such as VPN usage, ActiveSync support, access to cloud services, application compliance, passcode policy, device restrictions, and Wi-Fi settings.

Android devices are managed by Android Enterprise, which provides controls for both the device itself and the work container. The work container is a special folder on the phone that stores all the enterprise applications and data, ensuring separation from personal applications and data. This is implemented as a profile owner solution, as opposed to Corporate-Owned Personally-Enabled (COPE), which is implemented as a device owner solution.

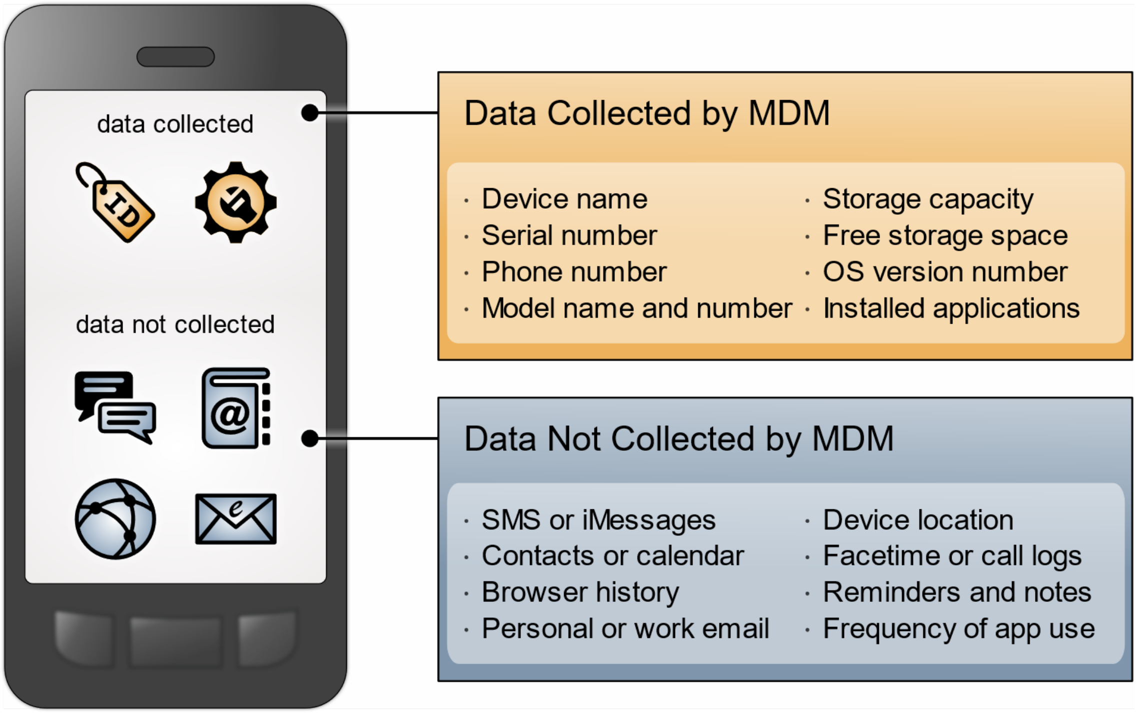
## 4.7 Privacy Settings: Mobile Device Data Processing

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

### 4.7.1 EMM: MaaS360

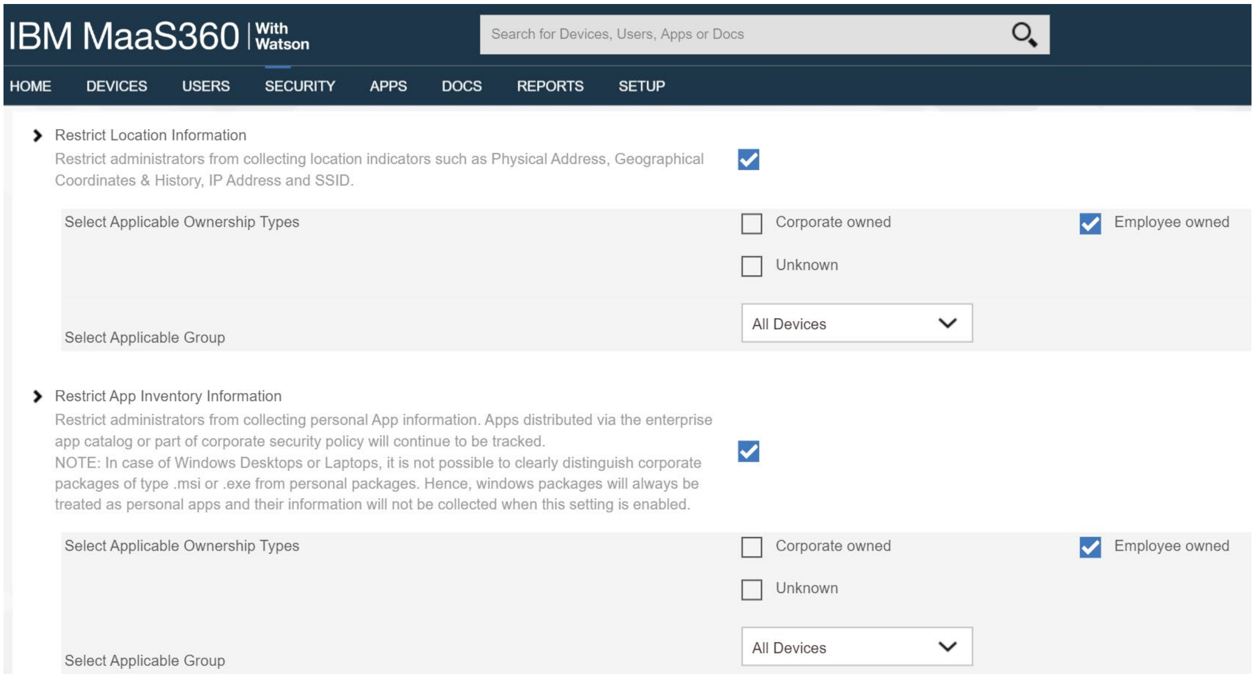
When a personal mobile phone is connected to an EMM system, some data is collected and visible to the enterprise. While additional data can be collected, our example solution collects only the data shown in Figure 4-7 to help protect employee privacy. This information is provided by MaaS360 to Kryptowire’s application vetting capability. Kryptowire then uses the MaaS360 supplied information to determine application security characteristics. IBM provides documentation with more details on the information that MaaS360 collects and processes [26].

989 **Figure 4-7 Data Collected by Example Solution Mobile Device Management**



As shown in Figure 4-8, administrators can restrict collection of location and/or application inventory information. When an administrator restricts location collection, the administrator cannot see any location information about devices. Similarly, when an administrator restricts application inventory information, MaaS360 will not collect applications that are not distributed through the enterprise and therefore, will not transmit them to third-party application-vetting services. Both privacy controls can be applied to specific device groups—for example, COPE devices could have their location information collected—but location collection can be disabled for personal devices.

**Figure 4-8 Example Solution Mobile Device Management Privacy Settings**


IBM MaaS360 | With Watson
Search for Devices, Users, Apps or Docs
HOME
DEVICES
USERS
SECURITY
APPS
DOCS
REPORTS
SETUP

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

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

Select Applicable Group: All Devices

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

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

Select Applicable Group: All Devices

## 4.7.2 MTD: Zimperium

Zimperium provides configurable settings for both what data is collected, as well as when it is collected. Data is collected:

- at login when the user launches the zIPS application
- when a threat is reported
- periodically, when the zIPS application checks in to the zConsole

Table 4-4 shows the data that is collected during each of the three scenarios above. Additional information regarding data item contents follows the table.

Note: Administrators who are managing Zimperium cannot disable the collection of the bolded data items (Network, Device, and Carrier Information) shown in Table 4-4 Data Collected by Zimperium.

**Table 4-4 Data Collected by Zimperium**

| Time | Data Item |
|---|---|
| At login | ▪ Location (Street, City, or Country)<br>▪ Application Binaries (Android)<br>▪ **Network**<br>▪ **Device**<br>▪ Application Forensics<br>▪ **Carrier Information**<br>▪ User Details |
| Threat | ▪ Location (Street, City, or Country)<br>▪ Network<br>▪ Application Forensics<br>▪ Running Processes (Android)<br>▪ Site Insight Risky URLs<br>▪ Attacker's Network |
| Periodically | ▪ Location (Street, City, or Country)<br>▪ Network<br>▪ Application Binaries (Android)<br>▪ Application Forensics |

The Device data item contains the following information:

- root/jailbreak status
- OS version
- OS known vulnerabilities
- developer mode enabled
- process list
- file system changes

- device international mobile equipment identity (IMEI)
- device IP
- device media access control (MAC) address
- location

The Network data item contains the following information:

- address resolution tables
- routing tables
- nearby networks
- network SSID
- external IP
- gateway MAC

The Application data item contains the following information:

- application ID
- application version
- hash
- malware detection (yes or no with type of malware)
- libraries used
- permissions
- privacy risk
- security risk
- location in device file system
- network connections

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

- user credentials (email address, Zimperium-specific password)
- device hash (MD5 of IMEI or serial number as an identifier)
- device operating system
- device push token
- hash of local z9 database
- time and name of threat detection when a threat occurs

### 4.7.3 VPN: Palo Alto Networks

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

- device name
- logon domain
- operating system
- app version
- mobile device network information to which the device is connected
- in addition, GlobalProtect collects whether the device is rooted or jailbroken

# 5 Security and Privacy Analysis

This section familiarizes the reader with:

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

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

## 5.1 Analysis Assumptions and Limitations

The security and privacy characteristics analysis has the following limitations:

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

## 5.2 Build Testing

Test activities are provided to show how the example architecture addresses each threat event and problematic data action. The NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into*

*Practice*, provides insights into how an organization may determine its susceptibility to the threat before implementing the architecture detailed in this practice guide. The test activities contained in Appendix E, Build Testing Details, demonstrate to the reader how Great Seneca validated their desired outcomes for the identified threat events and problematic data actions. Appendix F, Threat Event Test Information, shows examples of test results for this build.

## 5.3 Scenarios and Findings

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

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

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

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

### 5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings

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

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

The products, frameworks, security controls, and workforce mappings are in Appendix G.

### 5.3.2 Threat Events and Findings

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

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

Table 5-1 Threat Events and Findings Summary

| Threat Event | How the Example Solution Architecture Helped Mitigate the Threat Event | The Technology Function that Helps Mitigate the Threat Event |
|---|---|---|
| **Threat Event 1:** unauthorized access to sensitive information via a malicious or privacy-intrusive application | Provides administrators with insight into what corporate data that applications can access. | MTD<br>EMM |
| **Threat Event 2:** theft of credentials through a short message service (SMS) or email phishing campaign | Utilized PAN-DB and URL filtering to block known malicious websites. | Firewall |
| **Threat Event 3:** unauthorized applications installed via URLs in SMS or email messages | Alerted the user and administrators to the presence of a sideloaded application. | EMM<br>MTD |
| **Threat Event 4:** confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware | Alerted the user that their OS is noncompliant. | EMM<br>MTD |
| **Threat Event 5:** violation of privacy via misuse of device sensors | Application vetting reports indicated the sensors to which an application requested access. | Application vetting |
| **Threat Event 6:** loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications | Application vetting reports indicated if an application sent data without proper encryption. | Application vetting |
| **Threat Event 7:** compromise of device integrity via observed, inferred, or brute-forced device unlock code | Enforced mandatory device wipe capabilities after ten failed unlock attempts. | EMM<br>MTD |
| **Threat Event 8:** unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications | Application vetting reports indicated if an application used credentials improperly. | Application vetting |

| Threat Event | How the Example Solution Architecture Helped Mitigate the Threat Event | The Technology Function that Helps Mitigate the Threat Event |
|---|---|---|
| **Threat Event 9:** unauthorized access of enterprise resources from an unmanaged and potentially compromised device | Devices that were not enrolled in the EMM system were not able to connect to the corporate VPN. | VPN |
| **Threat Event 10:** loss of organizational data due to a lost or stolen device | Enforced passcode policies and device-wipe capabilities protected enterprise data. | EMM |
| **Threat Event 11:** loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services | Policies that enforce data loss prevention were pushed to devices. | EMM |
| **Threat Event 12:** unauthorized access to work applications via bypassed lock screen | The VPN requires the user to reenter their password after a predefined amount of time. | VPN |

### 5.3.3 Privacy Problematic Data Actions and Findings

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

Table 5-2 Summary of Privacy Problematic Data Actions and Findings

| Problematic Data Actions (for Employees) | How the Example Solution Architecture Helps Mitigate the Problematic Data Action | The Technology Function that Helps Mitigate the Problematic Data Action |
|---|---|---|
| **PDA-1:** unwarranted restriction | Blocks staff access to enterprise resources by removing the device from MDM control instead of wiping the device. | EMM |

| Problematic Data Actions (for Employees) | How the Example Solution Architecture Helps Mitigate the Problematic Data Action | The Technology Function that Helps Mitigate the Problematic Data Action |
|---|---|---|
| | Enables only selectively wiping corporate resources on the device.<br>Restricts staff access to system capabilities that permit removing device access or performing wipes. | |
| **PDA-2:** surveillance | Restricts staff access to system capabilities that permit reviewing data about employees and their devices.<br>Limits or disables collection of specific data elements (e.g., location data). | EMM |
| **PDA-3:** unanticipated revelation | De-identifies personal and device data when not necessary to meet processing objectives.<br>Encrypts data transmitted between parties.<br>Limits or disables access to data.<br>Limits or disables the collection of specific data elements. | EMM |

## 5.4 Security and Privacy Control Mappings

The security and privacy capabilities of the example solution were identified, and example security and privacy control maps were developed to show these in a standardized methodology.

The control maps show the security and privacy characteristics for the products used in the example solution.

The security control map can be found in Appendix G. The privacy control map is in Appendix H.

# 6 Example Scenario: Putting Guidance into Practice

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

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

In the narrative example, Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30 [27] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [8] to perform a privacy risk assessment. Appendix F and Appendix G of the Supplement describe these risk assessments in more detail. These risk assessments produce two significant conclusions:

1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the controls discussed in the example solution are relevant to their environment.
2. The organization determines that it has a high-impact system, based on the impact guidance in NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* [28], and needs to implement more controls beyond those identified in NIST SP 1800-22 to support the additional system components in its own solution (e.g., underlying OS, the data center where the equipment will reside).

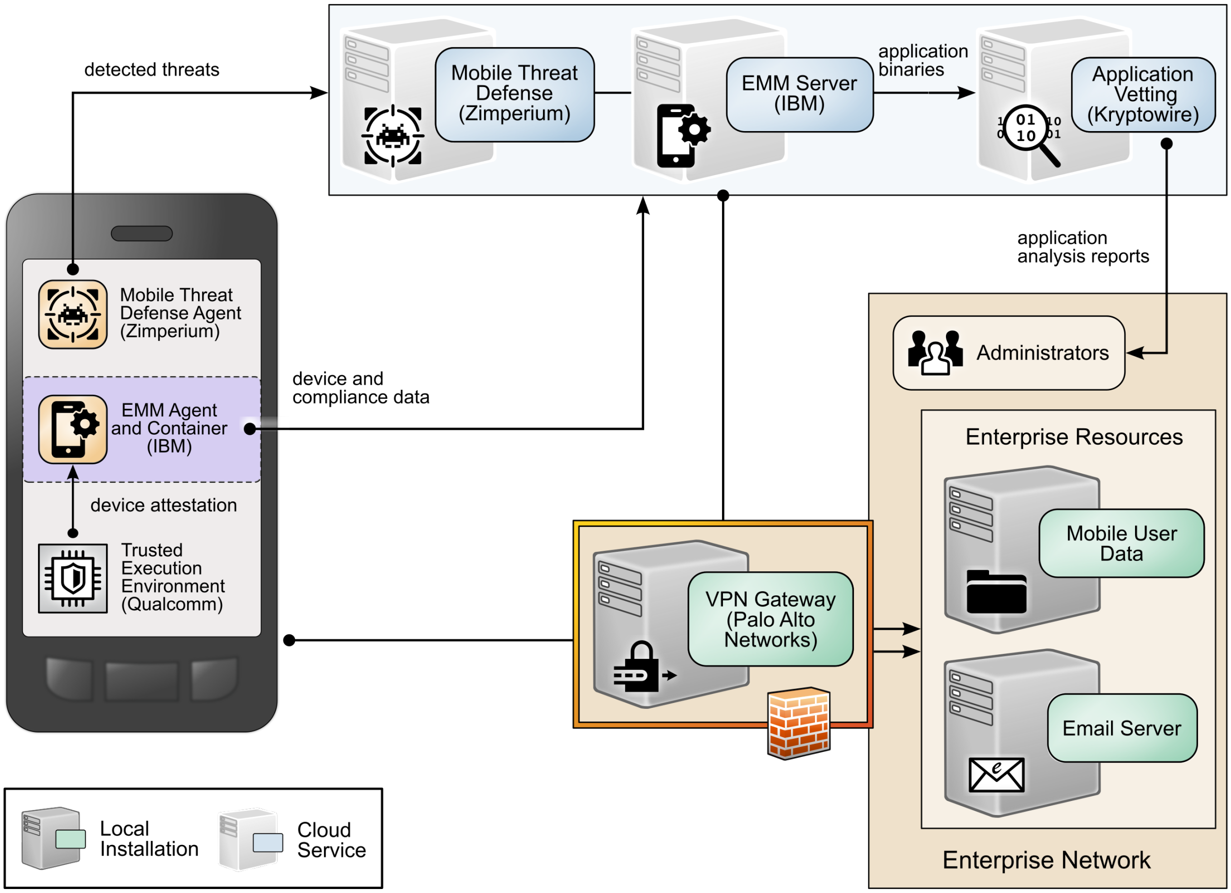
As part of their review of NIST FIPS 200, Great Seneca Accounting selects security and privacy controls from NIST SP 800-53 [29] for their BYOD architecture implementation. They then tailor the control baselines based on the needs identified through the priority Subcategories in its cybersecurity and privacy Target Profiles.

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

# 7 Conclusion

This practice guide provides an explanation of mobile device security and privacy concepts and an example solution for organizations implementing a BYOD deployment. As shown in Figure 7-1, this example solution applied multiple mobile device security technologies. These included a cloud-based EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities that support the example solution.

**Figure 7-1 Example Solution Architecture**


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

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

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

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

# 8 Future Build Considerations

For a future build, the team is considering a virtual mobile infrastructure (VMI) or unified endpoint management (UEM) solution.

The VMI deployment could include installing an application on a device at enrollment time, which would grant access to a virtual phone contained within the corporate infrastructure. The virtual phone would then contain the corporate-supplied applications that an employee would require for performing standard mobile work tasks. The thin client deployment limits the storage of organizational data on the device and helps ensure that access to the organization's data uses security-enhancing capabilities.

UEM would entail managing a user's mobile device ecosystem, potentially including laptops, mobile phones, and IoT devices (e.g., smart watches and Bluetooth headsets).

# Appendix A List of Acronyms

| | |
|---|---|
| **AD** | Active Directory |
| **API** | Application Programming Interface |
| **ATS** | App Transport Security |
| **BYOD** | Bring Your Own Device |
| **CIS** | Center for Internet Security |
| **COPE** | Corporate-Owned Personally-Enabled |
| **EMM** | Enterprise Mobility Management |
| **FIPS** | Federal Information Processing Standards |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **IEC** | International Electrotechnical Commission |
| **IMEI** | International Mobile Equipment Identity |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **MDM** | Mobile Device Management |
| **MTD** | Mobile Threat Defense |
| **NCCoE** | National Cybersecurity Center of Excellence |
| **NIAP** | National Information Assurance Partnership |
| **NIST** | National Institute of Standards and Technology |
| **OS** | Operating System |
| **PII** | Personally Identifiable Information |
| **PIN** | Personal Identification Number |
| **REST** | Representational State Transfer |
| **RMF** | Risk Management Framework |
| **SCEP** | Simple Certificate Enrollment Protocol |
| **SMS** | Short Message Service |
| **SP** | Special Publication |
| **SSL** | Secure Sockets Layer |
| **TE** | Threat Event |

| | |
|---|---|
| **TEE** | Trusted Execution Environment |
| **TLS** | Transport Layer Security |
| **UEM** | Unified Endpoint Management |
| **URL** | Uniform Resource Locator |
| **VPN** | Virtual Private Network |

# Appendix B Glossary

**Access Management** Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [30].

**Availability** Ensure that users can access resources through remote access whenever needed [31].

**Bring Your Own Device (BYOD)** A non-organization-controlled telework client device [31].

**Confidentiality** Ensure that remote access communications and stored user data cannot be read by unauthorized parties [31].

**Data Actions** System operations that process PII [32].

**Disassociability** Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [32].

**Eavesdropping** An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [33] (definition located under eavesdropping attack).

**Firewall** Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [34].

**Integrity** Detect any intentional or unintentional changes to remote access communications that occur in transit [31].

**Manageability** Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [32].

**Mobile Device** A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [29].

**Personally Identifiable Information (PII)** Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [35] (adapted from Government Accountability Office Report 08-536).

**Predictability** Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system [32].

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

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

**Threat** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [27].

**Vulnerability** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [27].

# Appendix C References

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

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

[3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST Special Publication (SP) 800-181 (2017 version), NIST, Gaithersburg, Md., Aug. 2017. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final.

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

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

[6] J. Franklin et al., *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST SP 800-124 Revision 2 (Draft), NIST, Gaithersburg, Md., Mar. 2020. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.

[7] J. Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds,* NIST SP 1800-4, NIST, Gaithersburg, Md., Feb. 21, 2019. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid.

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

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

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

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

[12] M. Sabt, “Trusted Execution Environment: What It is, and What It is Not.” 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland, Aug. 2015. Available: https://hal.archives-ouvertes.fr/hal-01246364/file/trustcom_2015_tee_what_it_is_what_it_is_not.pdf.

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

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

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

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

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

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

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

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

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

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

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

[24] International Business Machines (IBM). “Web Services Integration Details.” [Online]. Available: https://developer.ibm.com/security/maas360/maas360-getting-started/maas360-web-services-integration-details/.

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

[26] IBM. “IBM MaaS360 GDPR Data Map (Persona Data Attributes).” [Online]. Available: http://public.dhe.ibm.com/software/security/products/maas360/GDPR/Personal_Data_in_IBM_MaaS360.pdf.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Appendix D Standards and Guidance

- National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) Version 1.1 [1]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2]
- NIST Mobile Threat Catalogue [5]
- NIST Risk Management Framework [4]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [7]
- NIST SP 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* [36]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [27]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [9]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [31]
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [37]
- NIST SP 800-53 Revision 4 (Final)*, Security and Privacy Controls for Information Systems and Organizations* [29]
- NIST SP 800-53 Revision 5 (Final), *Security and Privacy Controls for Information Systems and Organizations* [38]
- NIST SP 800-63-3, *Digital Identity Guidelines* [33]
- NIST SP 800-113, *Guide to SSL VPNs* [39]
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [40]
- NIST SP 800-124 Revision 2 (Draft)*, Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [41]
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [42]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017)* [3]
- NIST Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* [28]

- NIST Privacy Risk Assessment Methodology [8]
- Center for Internet Security [43]
- Executive Office of the President, Bring Your Own Device toolkit [44]
- Federal Chief Information Officers Council and Department of Homeland Security *Mobile Security Reference Architecture*, Version 1.0 [45]
- Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis* [46]
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, "Information technology – Security techniques – Information security management systems – Requirements" [47]
- Mobile Computing Decision example case study [48]
- Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobility Strategy Development Guidelines Working Group Document" [49]
- MSCT ATARC, "Mobile Threat Protection App Vetting and App Security," Working Group Document [50]
- MSCT, "Device Procurement and Management Guidance" [51]
- MSCT, "Mobile Device Management (MDM)," MDM Working Group Document [52]
- MSCT, "Mobile Services Roadmap, MSCT Strategic Approach" [53]
- National Information Assurance Partnership (NIAP), U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0 [54]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1 [55]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0 [56]
- NIAP, Product Compliant List [57]
- Office of Management and Budget, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* [58]
- United States Government Configuration Baseline [59]
- Department of Homeland Security (DHS), "DHS S&T Study on Mobile Device Security" [60]
- NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework* [61]

# Appendix E Example Solution Lab Build Testing Details

This section shows the test activities performed to demonstrate how this practice guide's example solution that was built in the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) lab addresses the threat events and problematic data actions defined from the risk assessment.

## E.1 Threat Event 1

**Summary:** Unauthorized access to sensitive information via a malicious or privacy-intrusive application is tested.

**Test Activity:** Place mock sensitive enterprise contact list and calendar entries on devices, then attempt to install and use applications that access and back up those entries.

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

Alternatively, built-in device mechanisms such as Apple's managed applications functionality and Google's Android enterprise work profile functionality could be used to separate the contact and calendar entries associated with enterprise email accounts so that they can only be accessed by enterprise applications (applications that the enterprise mobility management (EMM) authorizes and manages), not by applications manually installed by the user. The user should not be able to manually provision their enterprise email account. Only the EMM should be able to provision the account, enabling enterprise controls on the enterprise contact list and calendar data.

**Observed Outcome:** Once MaaS360 was aware that an application had access to sensitive data (e.g., calendar entries, contacts), it applied a policy to the device and took appropriate actions automatically. MaaS360 sent an alert to the mobile device about an application compliance policy violation and requested that the user remove the application(s) within an administrator-set time frame. In our test, the simulated user account did not remove the restricted applications within the predefined time frame, and MaaS360 removed mobile device management (MDM) control from the mobile device.

## E.2 Threat Event 2

**Summary:** A fictional phishing event was created to test protection against the theft of credentials through a short message service (SMS) or email phishing campaign.

**Test Activity:**

- This threat event can be tested by establishing a web page with a form that impersonates an enterprise login prompt.
- Then send the web page’s uniform resource locator (URL) via SMS or email and attempt to collect and use enterprise login credentials.

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

**Observed Outcome:** The example solution used Palo Alto Networks’ next-generation firewall. The firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The URL filtering database is updated regularly to help protect users from malicious URLs. The next-generation firewall blocked the attempt to visit the phishing site. However, if the malicious URL were not present in PAN-DB, the user would be allowed to access the website.

## E.3 Threat Event 3

**Summary:** Testing to discover for unauthorized applications that are not present on the official Apple App Store or Google Play Store, that can be installed via URL links in SMS, email messages, or third-party websites.

**Test Activity (Android):**

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

**Test Activity (iOS):**

- Send an email to the user with a message urging the user to click the link to install the application.
- On the device, read the received email, click the link, and attempt to install the application.

**Desired Outcome:** Zimperium should alert both the administrators and user of the presence of a side-loaded application.

**Observed Outcome:** Zimperium alerted both the user and MaaS360 about the presence of a side-loaded application. MaaS360 sent an email notification to the user and administrator about the presence of side-loaded applications and required actions.

## E.4 Threat Event 4

**Summary:** Confidentiality and integrity loss due to exploitation of known vulnerability in the operating system or firmware.

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

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

**Observed Outcome:** Zimperium was able to identify devices that were running an outdated version of iOS or Android, and it informed MaaS360 when a device was out of compliance.

## E.5 Threat Event 5

**Summary:** This threat event test shows collection of location, camera, or microphone data by an application that has no need to access this data.

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

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

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

**Observed Outcome:** The Kryptowire report identified the usage of privacy-intrusive permissions when not required.

## E.6 Threat Event 6

**Summary:** Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications.

**Test Activity:** Test if applications will attempt to establish a hypertext transfer protocol or unencrypted connection.

**Desired Outcome:**

- Android: Because all work applications are inside a work container, a container-wide virtual private network (VPN) policy can be applied to mitigate this threat event; all communications, both encrypted and unencrypted, will be sent through the VPN tunnel. This will prevent eavesdropping on any communication originating from a work application.
- iOS: Apply a per-application VPN policy that will send all data transmitted by managed applications through the VPN tunnel. This will prevent eavesdropping on any unencrypted communication originating from work applications.
- Kryptowire can identify if an application attempts to establish an unencrypted connection.

**Observed Outcome:** The Kryptowire report indicated that the application did not use in-transit data encryption.

## E.7 Threat Event 7

**Summary:** Compromise of device integrity via observed, inferred, or brute-forced device unlock code.

**Test Activity:**

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

**Desired Outcome:** Policies set on the device by the EMM (MaaS360) should require a device unlock code to be set, prevent the device unlock code from being removed, require a minimum complexity for the device unlock code, and factory resetting the device after 10 failed unlock attempts.

Additionally, Zimperium can identify and report devices with a disabled lock screen.

**Observed Outcome:** MaaS360 applies a policy to the devices to enforce a mandatory PIN and device-wide capability. Zimperium reports devices with a disabled lock screen.

## E.8 Threat Event 8

**Summary:** Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications.

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

**Desired Outcome:** Discover and report credential weaknesses.

**Observed Outcome:** Kryptowire recognized within an application that the application uses hardcoded credentials. The application's use of hardcoded credentials could introduce vulnerabilities if unauthorized entities used the hardcoded credentials to access enterprise resources.

## E.9 Threat Event 9

**Summary:** Unauthorized access of enterprise resources from an unmanaged and potentially compromised device.

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

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

**Observed Outcome:** Devices that were not enrolled in MaaS360 were unable to access enterprise resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper client certificates—obtainable only through enrolling in the EMM.

## E.10 Threat Event 10

**Summary:** Loss of organizational data due to a lost or stolen device.

**Test Activity:** Attempt to download enterprise data onto a mobile device that is not enrolled in the EMM system (may be performed in conjunction with TE-9). Attempt to remove (in conjunction with TE-7) the screen lock passcode or demonstrate that the device does not have a screen lock passcode in place. Attempt to locate and selectively wipe the device through the EMM console (will fail if the device is not enrolled in the EMM).

**Desired Outcome:** It should be possible to locate or wipe EMM enrolled devices in response to a report that they have been lost or stolen. As demonstrated by TE-9, only EMM enrolled devices should be able to access enterprise resources. As demonstrated by TE-7, EMM enrolled devices can be forced to have a screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of organizational data) if the device has been lost or stolen.

**Observed Outcome (Enrolled Devices):** Enrolled devices are protected. They have an enterprise policy requiring a PIN/lock screen, and therefore, the enterprise data on the device could not be accessed. After 10 attempts to access the device, the device was selectively wiped, removing all enterprise data. Additionally, the device could be remotely wiped after it was reported as lost to enterprise mobile device service management, ensuring no corporate data is left in the hands of attackers.

**Observed Outcome (Unenrolled Devices):** As shown in Threat Event 9, only enrolled devices could access enterprise services. When the device attempted to access enterprise data, no connection to the enterprise services was available. Because the device cannot access the enterprise, the device would not contain enterprise information.

In both outcomes, both enrolled and unenrolled, it would be at the user's discretion if they wanted to wipe all personal data as well. Because this is a Bring Your Own Device (BYOD) scenario, only corporate data (managed applications on iOS, and the work container on Android) would be deleted from a device if the device were lost or stolen.

## E.11 Threat Event 11

**Summary:** Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services.

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

**Desired Outcome:** The EMM will prohibit screenshots and other data-sharing actions while using managed applications.

**Observed Outcome:** Through MaaS360 device policies, an administrator could prevent the following actions on BYODs:

**Android**

- clipboard sharing
- screen capture
- share list
- backup to Google
- Secure Digital card write
- Universal Serial Bus storage
- video recording
- Bluetooth
- background data sync
- Android Beam
- Sbeam

**iOS**

- opening, writing, and saving from managed to unmanaged applications
- AirDrop for managed applications
- screen capture
- AirPlay
- iCloud backup
- document, photo stream, and application sync
- print
- importing files

## E.12 Threat Event 12

**Summary:** Unauthorized access to work applications via bypassed lock screen (e.g., sharing the device's PIN with family members).

**Test Activity:** Assume the user is an unauthorized person attempting to access enterprise resources. Unlock the device and attempt to open a work application.

**Desired Outcome:** The user will be prompted to log in to the VPN using their corporate username and password. Because the user does not know this password, they are unable to log in and access corporate resources. However, if the user attempts to access a work application within the idle log-out time, they will be granted access because no password will be requested.

**Observed Outcome:** GlobalProtect prompted the unauthorized user for a password. Not knowing the password, the unauthorized user was unable to access corporate resources.

## E.13 Problematic Data Action 1

**Summary:** The user retains personal data and applications while access to corporate applications and data is removed.

**Test Activity:** Selectively wipe a device using MaaS360.

**Desired Outcome:** The user will no longer be able to access work applications and data on the device and retains all access to their personal applications and data.

**Observed Outcome:** Corporate data and applications are removed while personal data is untouched.

## E.14 Problematic Data Action 2

**Summary:** Collection of application and location data is restricted.

**Test Activity:** Disable location and application inventory collection in MaaS360.

**Desired Outcome:** The MDM does not collect an inventory of applications on the device and does not collect location information, including physical address, geographic coordinates and history, internet protocol (IP) address, and secure set identifier (SSID).

**Observed Outcome:** When inspecting a device, location and application inventory information are not shown to the user, and application inventory information is not transmitted to Kryptowire.

## E.15 Problematic Data Action 3

**Summary:** Access to monitoring data from the device is restricted to administrators. Application and location data are not shared with third parties that support monitoring, data analytics, and other functions for operating the BYOD solution.

**Test Activity:** Attempt to log in to the MaaS360 admin portal without domain administrator permissions.

**Desired Outcome:** System provides access controls to monitoring functions and logs. Data flow between the organization and third parties does not contain location information, including physical address, geographic coordinates and history, IP address, and SSID.

**Observed Outcome:** Domain administrators were allowed to log in, but non-administrator users were not.

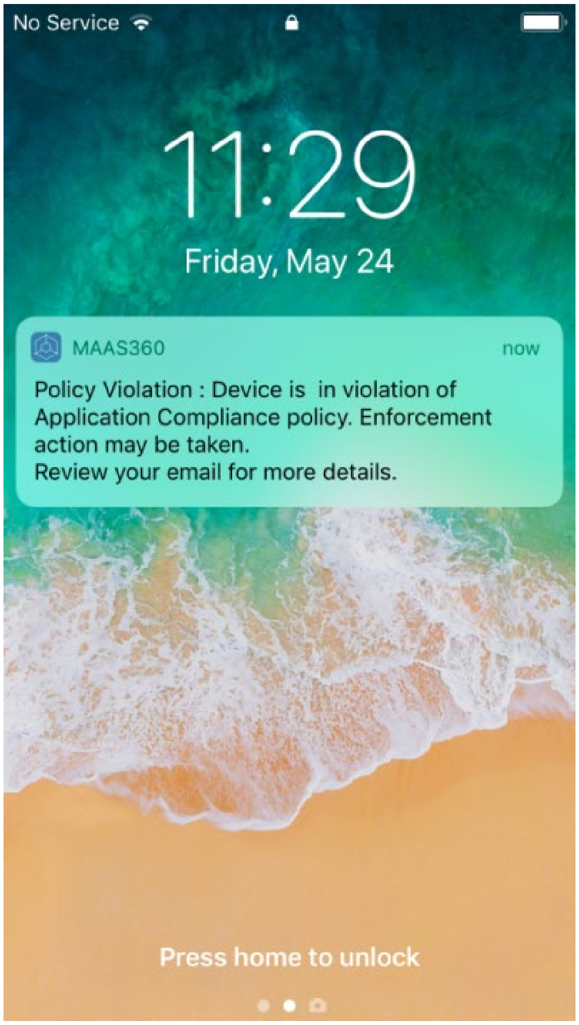
# Appendix F Threat Event Test Information

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

## F.1 Threat Event 1

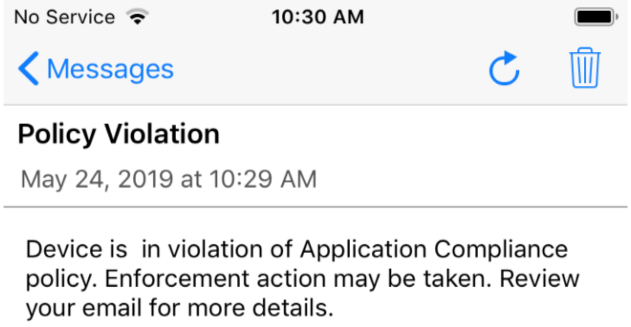
Threat Event 1 demonstrates unauthorized access attempts to sensitive information via a malicious or privacy-intrusive application. The following figures show the alerts that the device user received regarding the policy violations and their remediation actions.

**Figure F-1 Policy Violation Notification**



Policy Violation : Device is  in violation of Application Compliance policy. Enforcement action may be taken.
Review your email for more details.

1673 **Figure F-2 Policy Violation Email**

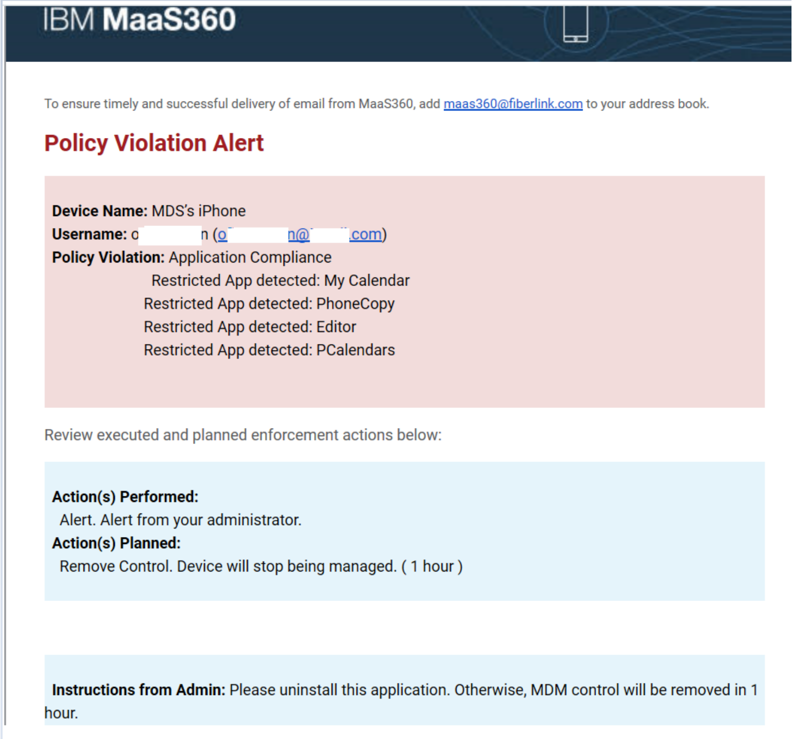


**Policy Violation**

May 24, 2019 at 10:29 AM

Device is  in violation of Application Compliance policy. Enforcement action may be taken. Review your email for more details.

1674 **Figure F-3 Policy Violation Alert Details Email**



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

**Policy Violation Alert**

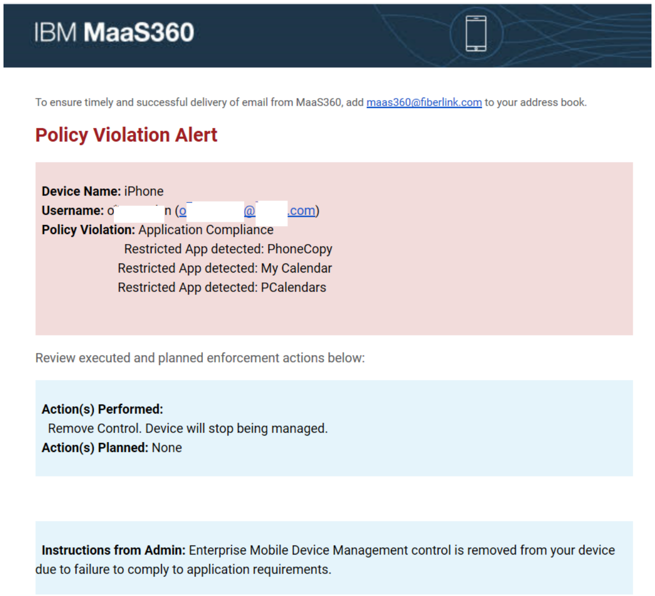
**Device Name:** MDS's iPhone
**Username:** o[redacted]n (o[redacted]n@[redacted].com)
**Policy Violation:** Application Compliance
Restricted App detected: My Calendar
Restricted App detected: PhoneCopy
Restricted App detected: Editor
Restricted App detected: PCalendars

Review executed and planned enforcement actions below:

**Action(s) Performed:**
Alert. Alert from your administrator.
**Action(s) Planned:**
Remove Control. Device will stop being managed. ( 1 hour )

**Instructions from Admin:** Please uninstall this application. Otherwise, MDM control will be removed in 1 hour.

1675 **Figure F-4 Enterprise Mobility Management Removal Alert**



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

**Policy Violation Alert**

**Device Name:** iPhone
**Username:** o[redacted]n (o[redacted]@[redacted].com)
**Policy Violation:** Application Compliance
Restricted App detected: PhoneCopy
Restricted App detected: My Calendar
Restricted App detected: PCalendars

Review executed and planned enforcement actions below:

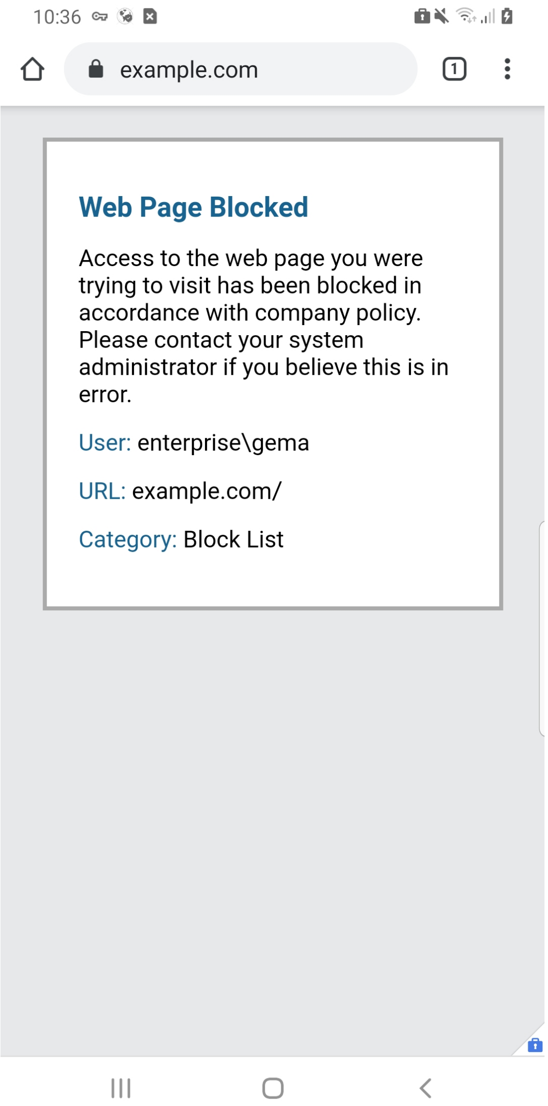
**Action(s) Performed:**
Remove Control. Device will stop being managed.
**Action(s) Planned:** None

**Instructions from Admin:** Enterprise Mobile Device Management control is removed from your device due to failure to comply to application requirements.

## 1676 F.2 Threat Event 2

1677 The following screen capture shows Threat Event 2's testing outcome, where Palo Alto Networks' PAN-
1678 DB is blocking a website manually added to the malicious uniform resource locator (URL) database.

1679 **Figure F-5 PAN-DB Blocked Website**



### Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: enterprise\gema

URL: example.com/

Category: Block List

1680 ## F.3 Threat Event 3

1681 Threat Event 3 shows applications that are not present on the official Apple App Store or Google Play
1682 Store being installed via unauthorized means (sideloading).

**Figure F-6 Zimperium Threat Detected**

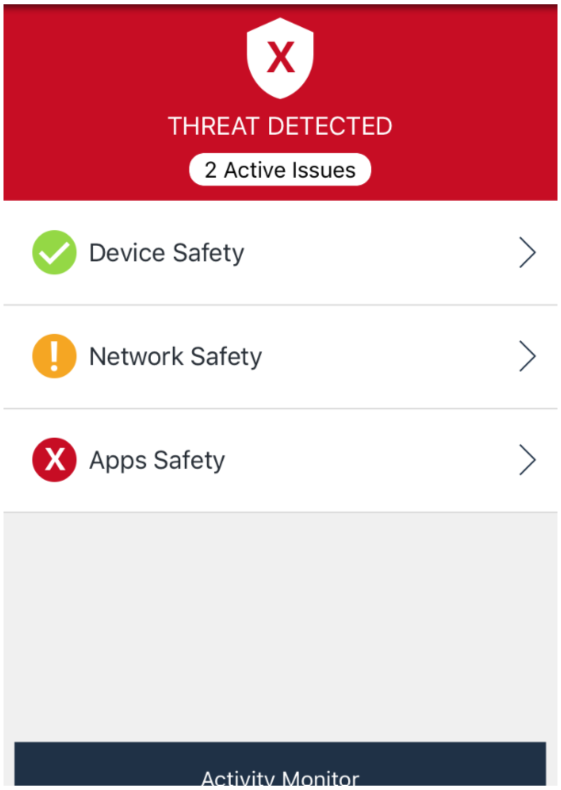
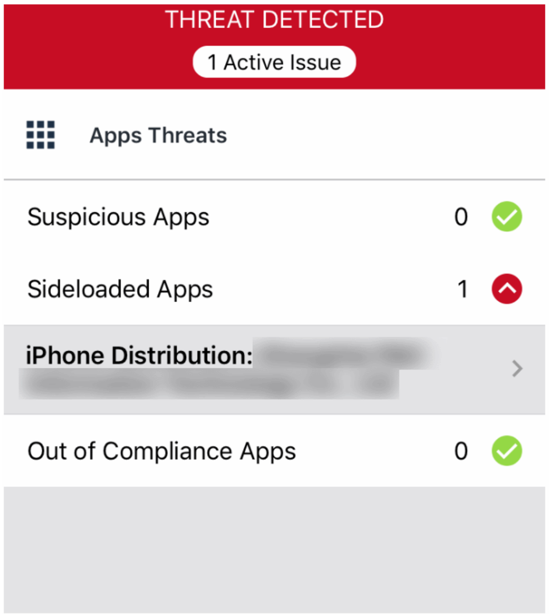


**Figure F-7 Zimperium Sideloaded Application Alert**



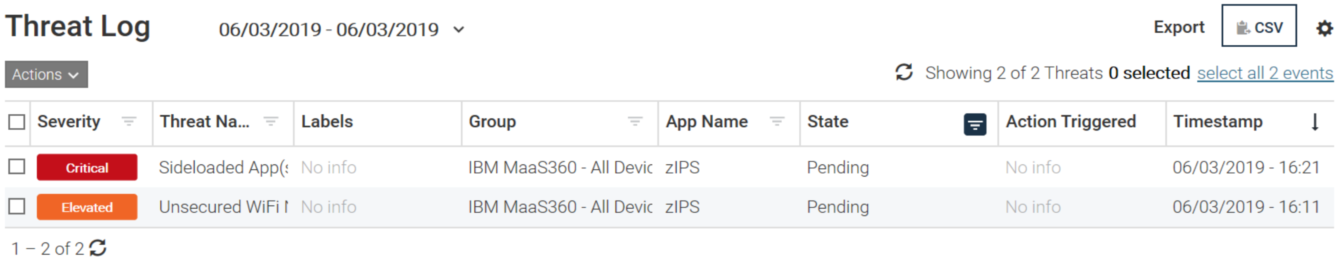
THREAT DETECTED

1 Active Issue

Apps Threats

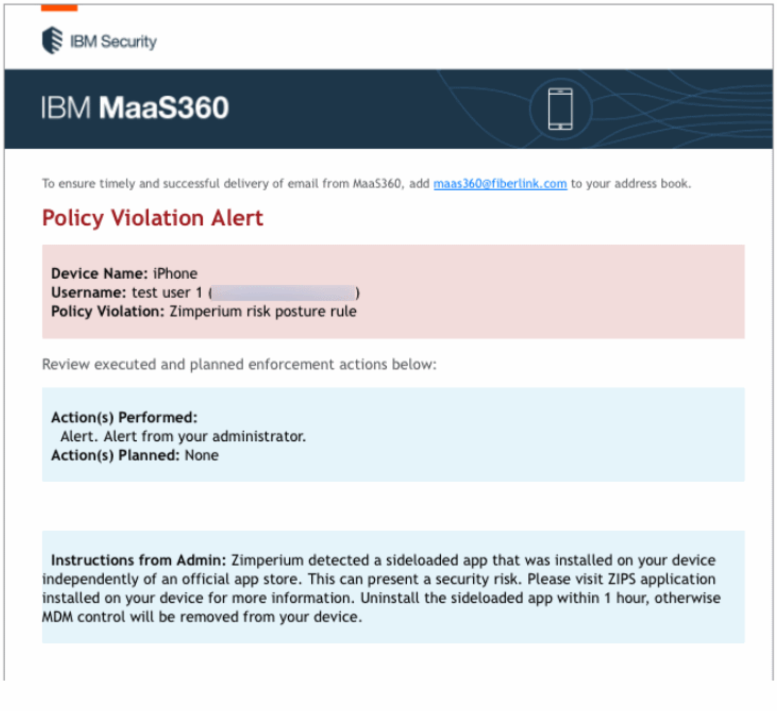
| | |
|---|---|
| Suspicious Apps | 0 ✓ |
| Sideloaded Apps | 1 |
| **iPhone Distribution:** [redacted] | |
| Out of Compliance Apps | 0 ✓ |

**Figure F-8 Zimperium Threat Log with Sideloaded Application Alert**



| □ | Severity | Threat Na... | Labels | Group | App Name | State | Action Triggered | Timestamp |
|---|---|---|---|---|---|---|---|---|
| □ | Critical | Sideloaded App(s | No info | IBM MaaS360 - All Devic | zIPS | Pending | No info | 06/03/2019 - 16:21 |
| □ | Elevated | Unsecured WiFi I | No info | IBM MaaS360 - All Devic | zIPS | Pending | No info | 06/03/2019 - 16:11 |

**Figure F-9 Email Regarding MaaS360 Policy Violation Alert**



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

**Device Name:** iPhone
**Username:** test user 1 ([redacted])
**Policy Violation:** Zimperium risk posture rule

Review executed and planned enforcement actions below:

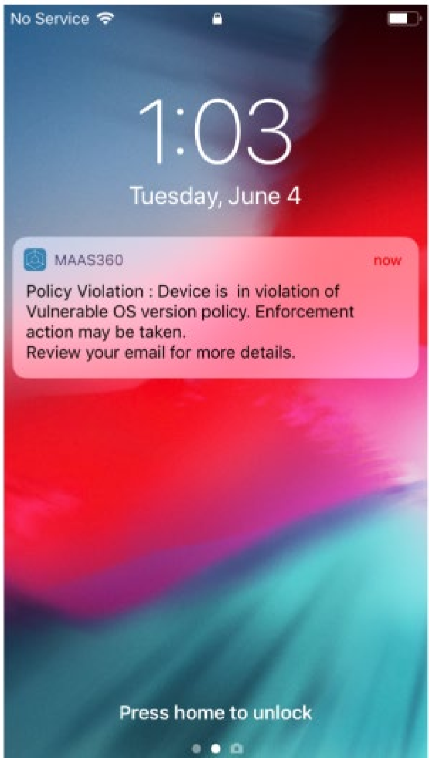
**Action(s) Performed:**
Alert. Alert from your administrator.
**Action(s) Planned:** None

**Instructions from Admin:** Zimperium detected a sideloaded app that was installed on your device independently of an official app store. This can present a security risk. Please visit ZIPS application installed on your device for more information. Uninstall the sideloaded app within 1 hour, otherwise MDM control will be removed from your device.

## F.4 Threat Event 4

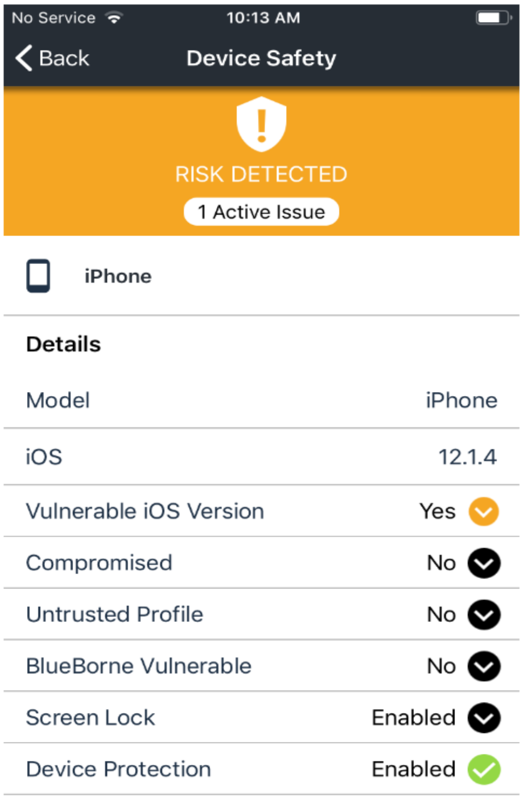
Threat Event 4 shows a risk detection during an operating system rules compliance status check.

1689 **Figure F-10 MaaS360 Policy Violation Alert**



Policy Violation : Device is  in violation of Vulnerable OS version policy. Enforcement action may be taken.
Review your email for more details.

1690 **Figure F-11 Zimperium Risk Detected**



No Service 10:13 AM

Back Device Safety

RISK DETECTED

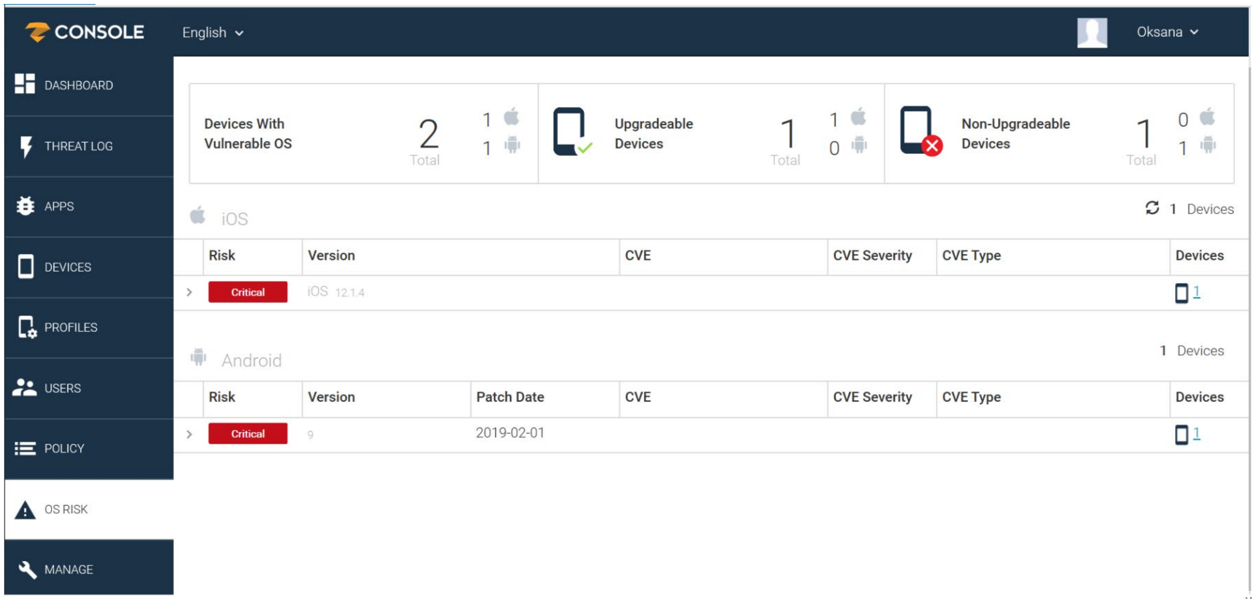
1 Active Issue

iPhone

**Details**

| | |
|---|---|
| Model | iPhone |
| iOS | 12.1.4 |
| Vulnerable iOS Version | Yes |
| Compromised | No |
| Untrusted Profile | No |
| BlueBorne Vulnerable | No |
| Screen Lock | Enabled |
| Device Protection | Enabled ✓ |

1691 **Figure F-12 Zimperium OS Risk**



Devices With Vulnerable OS 2 Total 1 1

Upgradeable Devices 1 Total 1 0

Non-Upgradeable Devices 1 Total 0 1

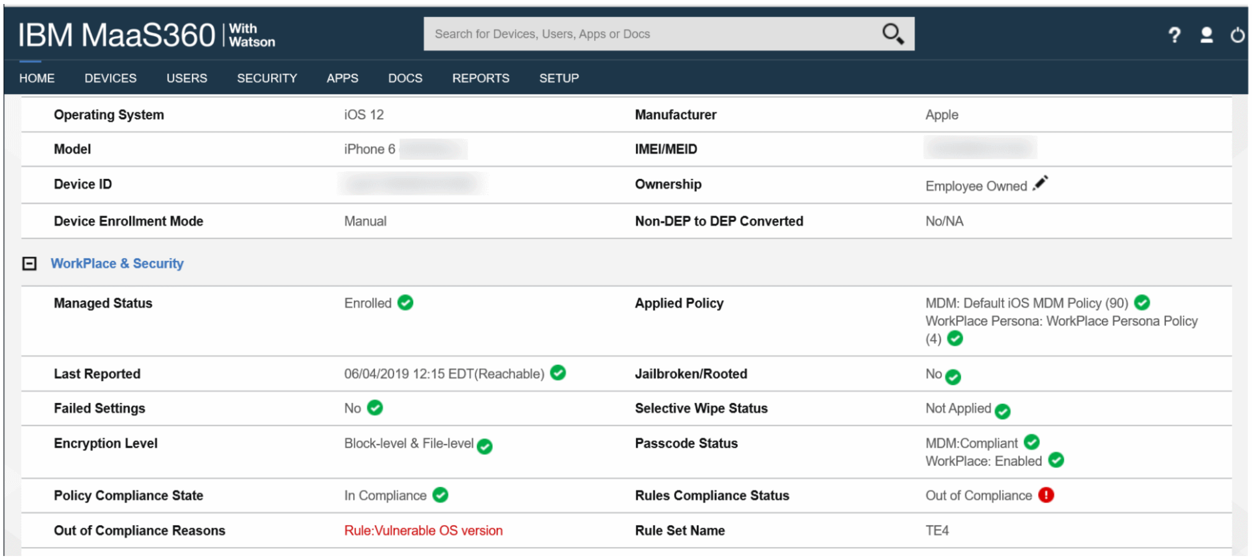
iOS 1 Devices

| Risk | Version | CVE | CVE Severity | CVE Type | Devices |
|---|---|---|---|---|---|
| Critical | iOS 12.1.4 | | | | 1 |

Android 1 Devices

| Risk | Version | Patch Date | CVE | CVE Severity | CVE Type | Devices |
|---|---|---|---|---|---|---|
| Critical | 9 | 2019-02-01 | | | | 1 |

1692 **Figure F-13 MaaS360 Compliance Rule Violation**

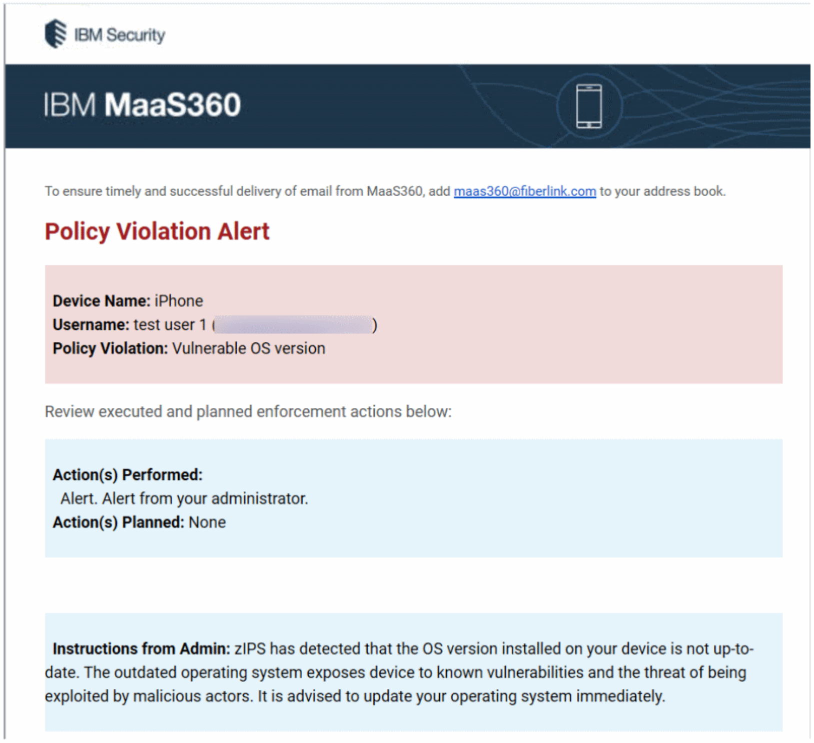


| | | | |
|---|---|---|---|
| Operating System | iOS 12 | Manufacturer | Apple |
| Model | iPhone 6 [redacted] | IMEI/MEID | [redacted] |
| Device ID | [redacted] | Ownership | Employee Owned |
| Device Enrollment Mode | Manual | Non-DEP to DEP Converted | No/NA |

⊟ WorkPlace & Security

| | | | |
|---|---|---|---|
| Managed Status | Enrolled ✓ | Applied Policy | MDM: Default iOS MDM Policy (90) ✓<br>WorkPlace Persona: WorkPlace Persona Policy (4) ✓ |
| Last Reported | 06/04/2019 12:15 EDT(Reachable) ✓ | Jailbroken/Rooted | No ✓ |
| Failed Settings | No ✓ | Selective Wipe Status | Not Applied ✓ |
| Encryption Level | Block-level & File-level ✓ | Passcode Status | MDM:Compliant ✓<br>WorkPlace: Enabled ✓ |
| Policy Compliance State | In Compliance ✓ | Rules Compliance Status | Out of Compliance ! |
| Out of Compliance Reasons | Rule:Vulnerable OS version | Rule Set Name | TE4 |

**Figure F-14 MaaS360 Policy Violation Email**



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

**Policy Violation Alert**

**Device Name:** iPhone
**Username:** test user 1 ([redacted])
**Policy Violation:** Vulnerable OS version

Review executed and planned enforcement actions below:

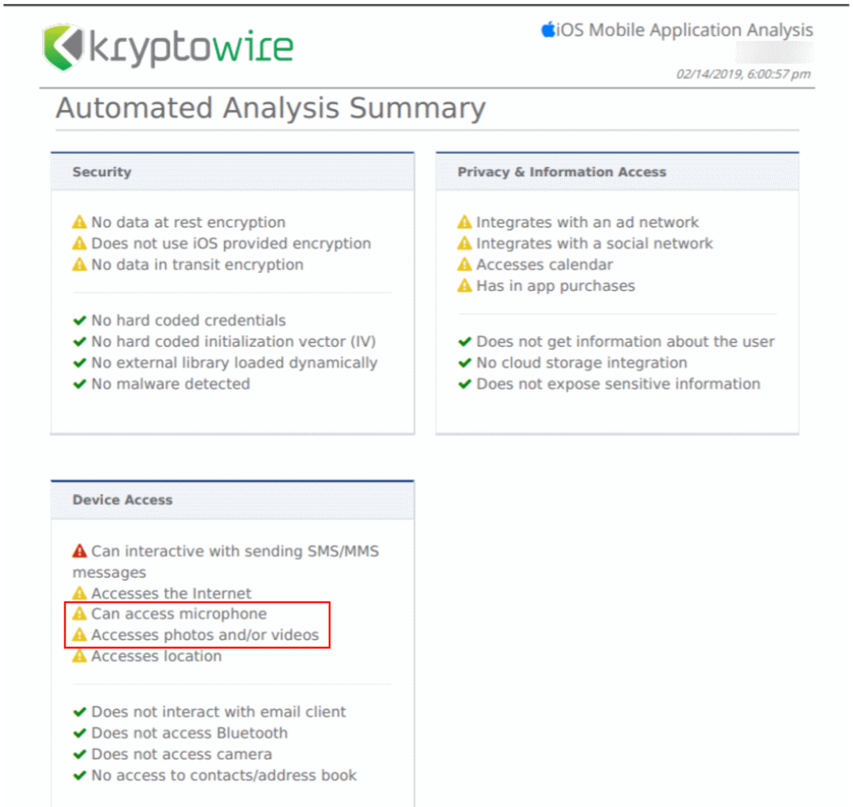
**Action(s) Performed:**
Alert. Alert from your administrator.
**Action(s) Planned:** None

**Instructions from Admin:** zIPS has detected that the OS version installed on your device is not up-to-date. The outdated operating system exposes device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update your operating system immediately.

## F.5 Threat Event 5

Threat Event 5 demonstrates a report detailing **c**ollection of information such as location, camera, or microphone data by an application.

**Figure F-15 Kryptowire iOS Application Report**



kryptowire

iOS Mobile Application Analysis

[redacted]

02/14/2019, 6:00:57 pm

Automated Analysis Summary

**Security**

⚠ No data at rest encryption
⚠ Does not use iOS provided encryption
⚠ No data in transit encryption

✓ No hard coded credentials
✓ No hard coded initialization vector (IV)
✓ No external library loaded dynamically
✓ No malware detected

**Privacy & Information Access**

⚠ Integrates with an ad network
⚠ Integrates with a social network
⚠ Accesses calendar
⚠ Has in app purchases

✓ Does not get information about the user
✓ No cloud storage integration
✓ Does not expose sensitive information

**Device Access**

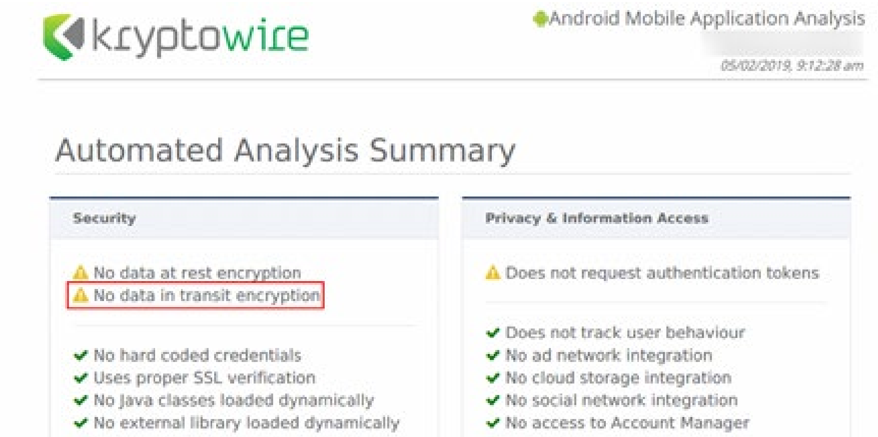
⚠ Can interactive with sending SMS/MMS messages
⚠ Accesses the Internet
⚠ Can access microphone
⚠ Accesses photos and/or videos
⚠ Accesses location

✓ Does not interact with email client
✓ Does not access Bluetooth
✓ Does not access camera
✓ No access to contacts/address book

## F.6 Threat Event 6

Threat Event 6 demonstrates a report of an application that can lose confidentiality of sensitive information via eavesdropping on unencrypted device communications.

**Figure F-16 Kryptowire Android Application Report**



kryptowire

Android Mobile Application Analysis

[redacted]

05/02/2019, 9:12:28 am

Automated Analysis Summary

**Security**

⚠ No data at rest encryption
⚠ No data in transit encryption

✓ No hard coded credentials
✓ Uses proper SSL verification
✓ No Java classes loaded dynamically
✓ No external library loaded dynamically

**Privacy & Information Access**

⚠ Does not request authentication tokens

✓ Does not track user behaviour
✓ No ad network integration
✓ No cloud storage integration
✓ No social network integration
✓ No access to Account Manager

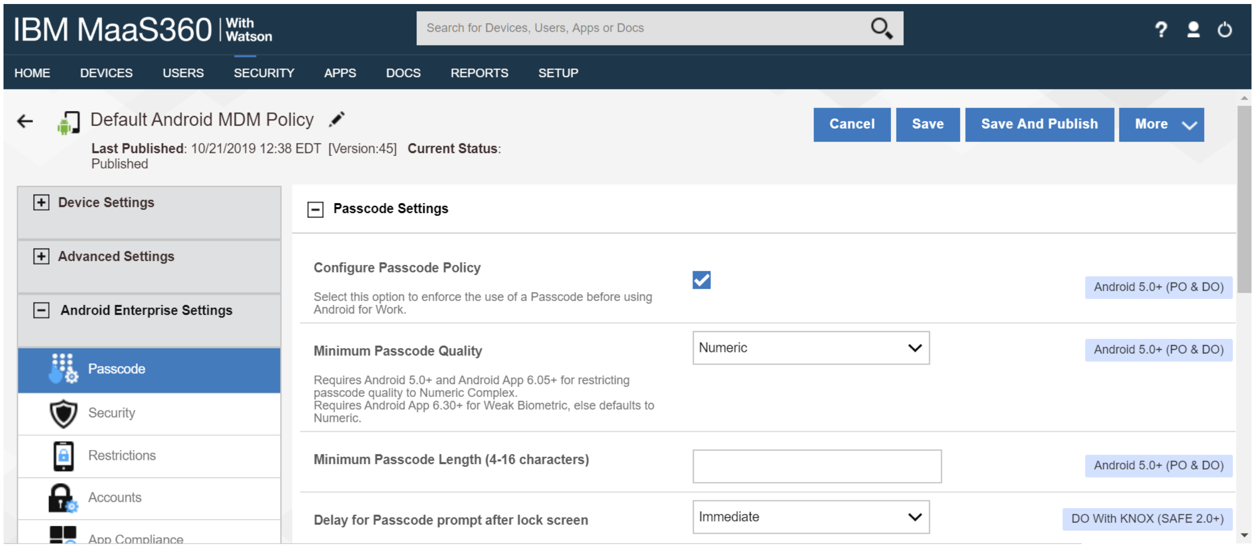
## F.7 Threat Event 7

Two scenarios are shown for Threat Event 7:

- The first scenario shows MaaS360 applying a policy to the devices to enforce a mandatory PIN and device-wipe capability.
- The second scenario shows Zimperium reporting a disabled lock screen.

1707 The diagram shows the MaaS360 configuration requirements for Passcode Settings for its managed
1708 devices, including a mandatory PIN configuration.

1709 **Figure F-17 MaaS360 Applying Mandatory PIN Policy**



Default Android MDM Policy

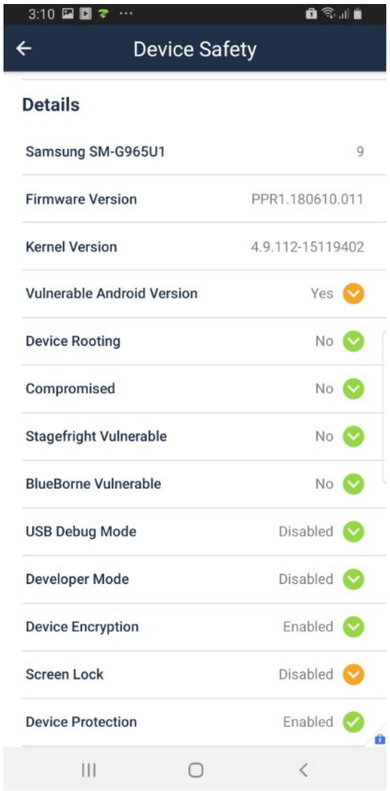
**Last Published**: 10/21/2019 12:38 EDT [Version:45] **Current Status**: Published

**Passcode Settings**

| | | |
|---|---|---|
| **Configure Passcode Policy**<br>Select this option to enforce the use of a Passcode before using Android for Work. | ☑ | Android 5.0+ (PO & DO) |
| **Minimum Passcode Quality**<br>Requires Android 5.0+ and Android App 6.05+ for restricting passcode quality to Numeric Complex.<br>Requires Android App 6.30+ for Weak Biometric, else defaults to Numeric. | Numeric | Android 5.0+ (PO & DO) |
| **Minimum Passcode Length (4-16 characters)** | | Android 5.0+ (PO & DO) |
| **Delay for Passcode prompt after lock screen** | Immediate | DO With KNOX (SAFE 2.0+) |

The figure shows Zimperium reporting discovery of a disabled lock screen.

Figure F-18 Zimperium Reporting Devices with a Disabled Lock Screen



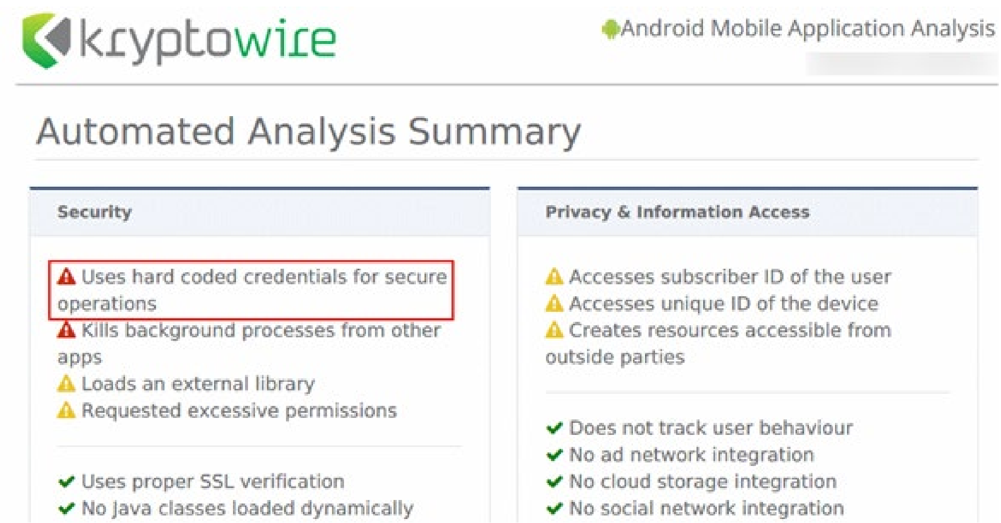
**Details**

| | |
|---|---|
| Samsung SM-G965U1 | 9 |
| Firmware Version | PPR1.180610.011 |
| Kernel Version | 4.9.112-15119402 |
| Vulnerable Android Version | Yes ✓ |
| Device Rooting | No ✓ |
| Compromised | No ✓ |
| Stagefright Vulnerable | No ✓ |
| BlueBorne Vulnerable | No ✓ |
| USB Debug Mode | Disabled ✓ |
| Developer Mode | Disabled ✓ |
| Device Encryption | Enabled ✓ |
| Screen Lock | Disabled ✓ |
| Device Protection | Enabled ✓ |

## F.8 Threat Event 8

Threat Event 8 testing images show a report that detected unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications.

**Figure F-19 Application Report with Hardcoded Credentials**



Android Mobile Application Analysis

Automated Analysis Summary

**Security**

- ⚠ Uses hard coded credentials for secure operations
- ⚠ Kills background processes from other apps
- ⚠ Loads an external library
- ⚠ Requested excessive permissions

- ✓ Uses proper SSL verification
- ✓ No Java classes loaded dynamically

**Privacy & Information Access**

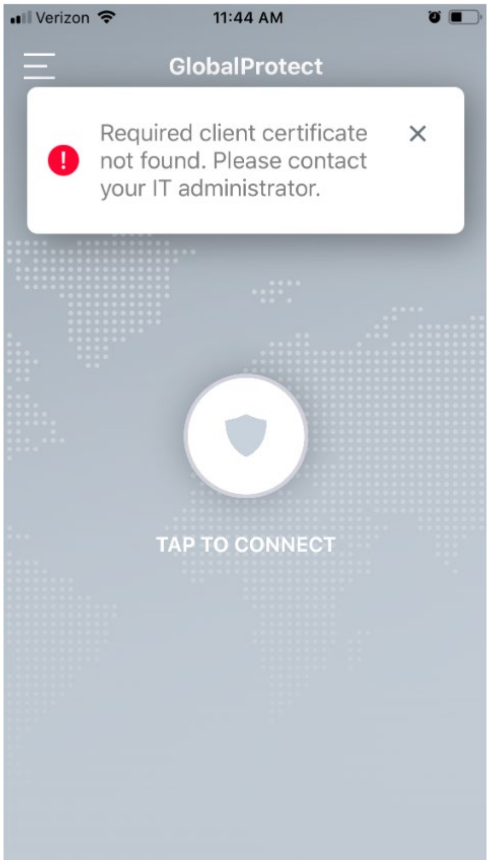
- ⚠ Accesses subscriber ID of the user
- ⚠ Accesses unique ID of the device
- ⚠ Creates resources accessible from outside parties

- ✓ Does not track user behaviour
- ✓ No ad network integration
- ✓ No cloud storage integration
- ✓ No social network integration

## F.9 Threat Event 9

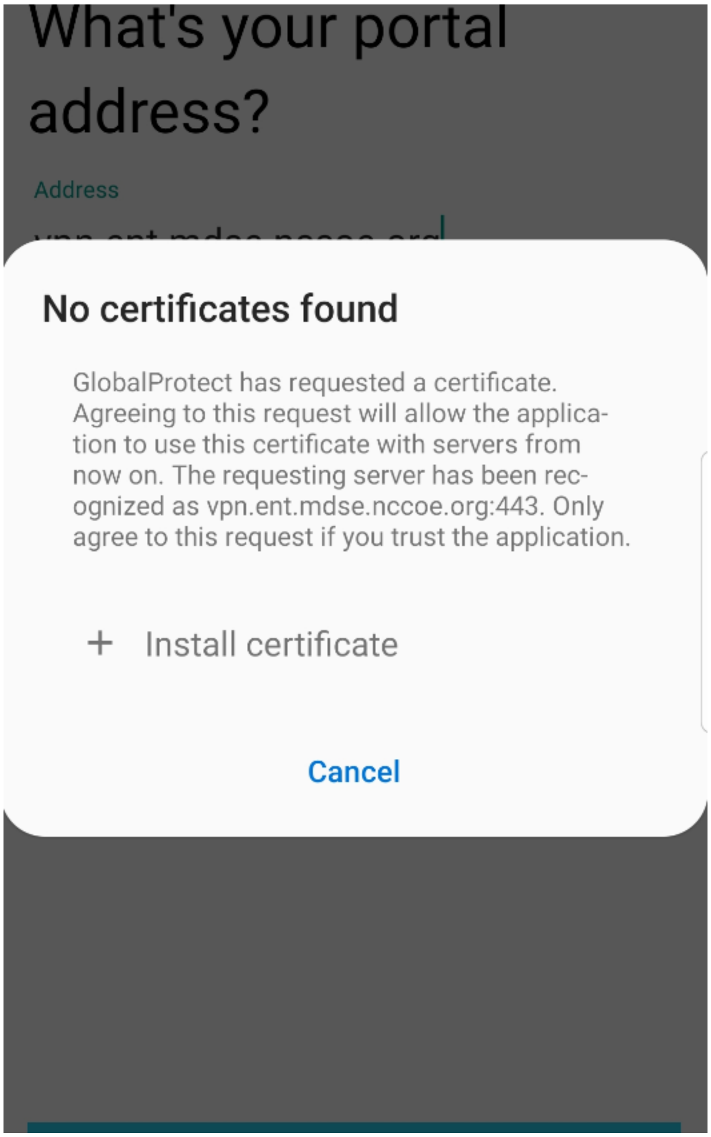
Threat Event 9 shows an unsuccessful attempt to access enterprise resources from an unmanaged and potentially compromised device.

1719 **Figure F-20 Attempting to Access the Virtual Private Network (VPN) on an Unmanaged Device**



Required client certificate not found. Please contact your IT administrator.

1720 **Figure F-21 Android: Attempting to Access the VPN on an Unmanaged Device**



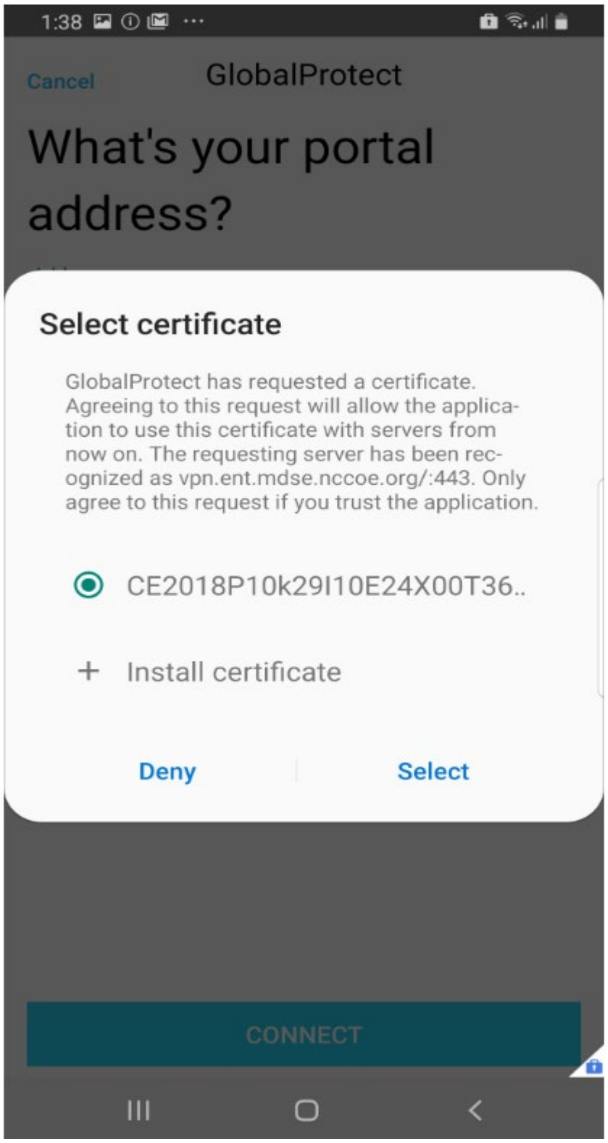
What's your portal address?

Address

No certificates found

GlobalProtect has requested a certificate. Agreeing to this request will allow the application to use this certificate with servers from now on. The requesting server has been recognized as vpn.ent.mdse.nccoe.org:443. Only agree to this request if you trust the application.

**Figure F-22 Android: Attempting to Access the VPN on a Managed Device**



What's your portal address?

Select certificate

GlobalProtect has requested a certificate. Agreeing to this request will allow the application to use this certificate with servers from now on. The requesting server has been recognized as vpn.ent.mdse.nccoe.org/:443. Only agree to this request if you trust the application.

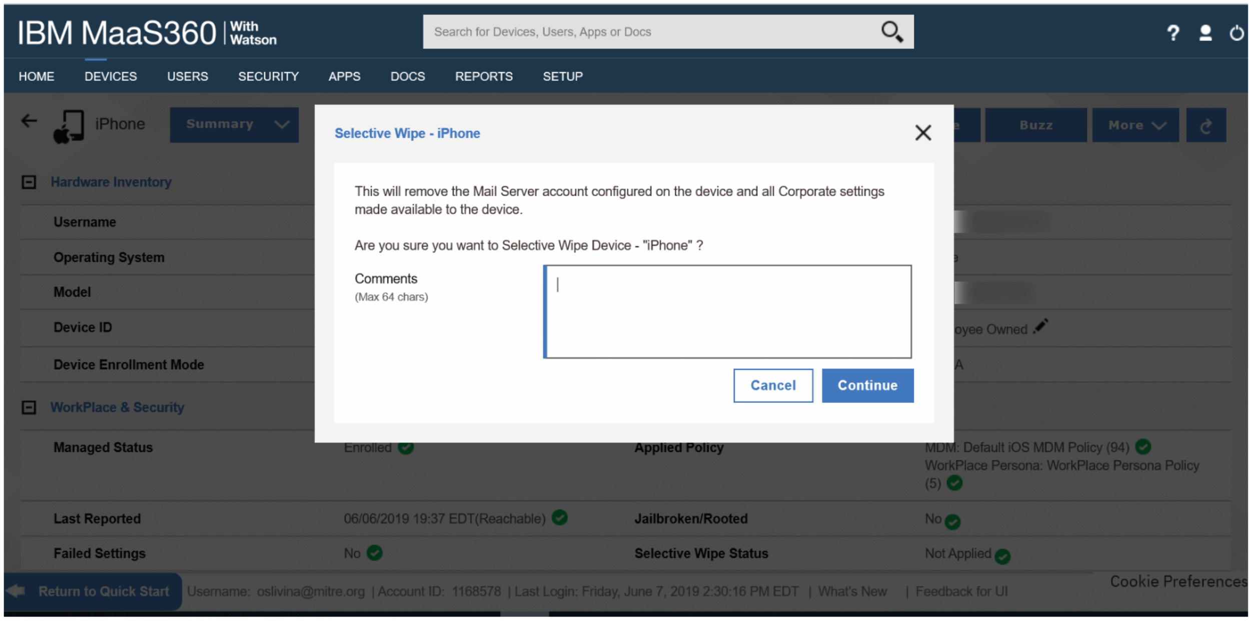
◉ CE2018P10k29I10E24X00T36..

+ Install certificate

## F.10 Threat Event 10

These screen captures show selectively wiping the device to remove organizational data. This prevents the loss of organizational data due to a lost or stolen device.

1725 **Figure F-23 Selectively Wiping an iOS Device**



**Selective Wipe - iPhone**

This will remove the Mail Server account configured on the device and all Corporate settings made available to the device.

Are you sure you want to Selective Wipe Device - "iPhone" ?

Comments
(Max 64 chars)

Cancel | Continue

Hardware Inventory

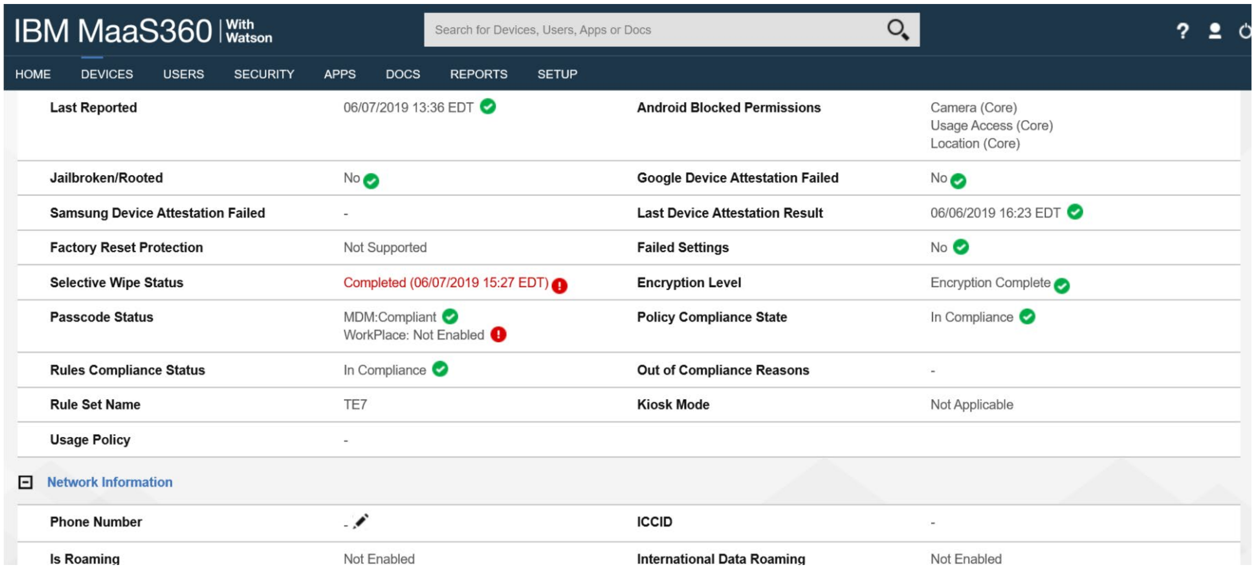
| | | | |
|---|---|---|---|
| Username | | | |
| Operating System | | | |
| Model | | | |
| Device ID | | | oyee Owned |
| Device Enrollment Mode | | | A |

WorkPlace & Security

| | | | |
|---|---|---|---|
| Managed Status | Enrolled ✓ | Applied Policy | MDM: Default iOS MDM Policy (94) ✓<br>WorkPlace Persona: WorkPlace Persona Policy (5) ✓ |
| Last Reported | 06/06/2019 19:37 EDT(Reachable) ✓ | Jailbroken/Rooted | No ✓ |
| Failed Settings | No ✓ | Selective Wipe Status | Not Applied ✓ |

Username: oslivina@mitre.org | Account ID: 1168578 | Last Login: Friday, June 7, 2019 2:30:16 PM EDT | What's New | Feedback for UI

1726 **Figure F-24 Selective-Wipe Completed**

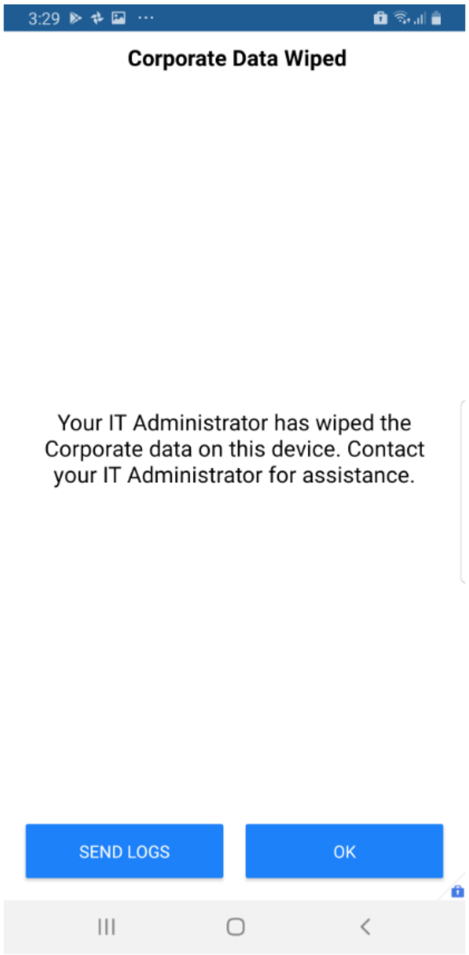


| | | | |
|---|---|---|---|
| Last Reported | 06/07/2019 13:36 EDT ✓ | Android Blocked Permissions | Camera (Core)<br>Usage Access (Core)<br>Location (Core) |
| Jailbroken/Rooted | No ✓ | Google Device Attestation Failed | No ✓ |
| Samsung Device Attestation Failed | - | Last Device Attestation Result | 06/06/2019 16:23 EDT ✓ |
| Factory Reset Protection | Not Supported | Failed Settings | No ✓ |
| Selective Wipe Status | Completed (06/07/2019 15:27 EDT) ! | Encryption Level | Encryption Complete ✓ |
| Passcode Status | MDM:Compliant ✓<br>WorkPlace: Not Enabled ! | Policy Compliance State | In Compliance ✓ |
| Rules Compliance Status | In Compliance ✓ | Out of Compliance Reasons | - |
| Rule Set Name | TE7 | Kiosk Mode | Not Applicable |
| Usage Policy | - | | |

Network Information

| | | | |
|---|---|---|---|
| Phone Number | - | ICCID | - |
| Is Roaming | Not Enabled | International Data Roaming | Not Enabled |

**Figure F-25 No Corporate Data Left on Device**



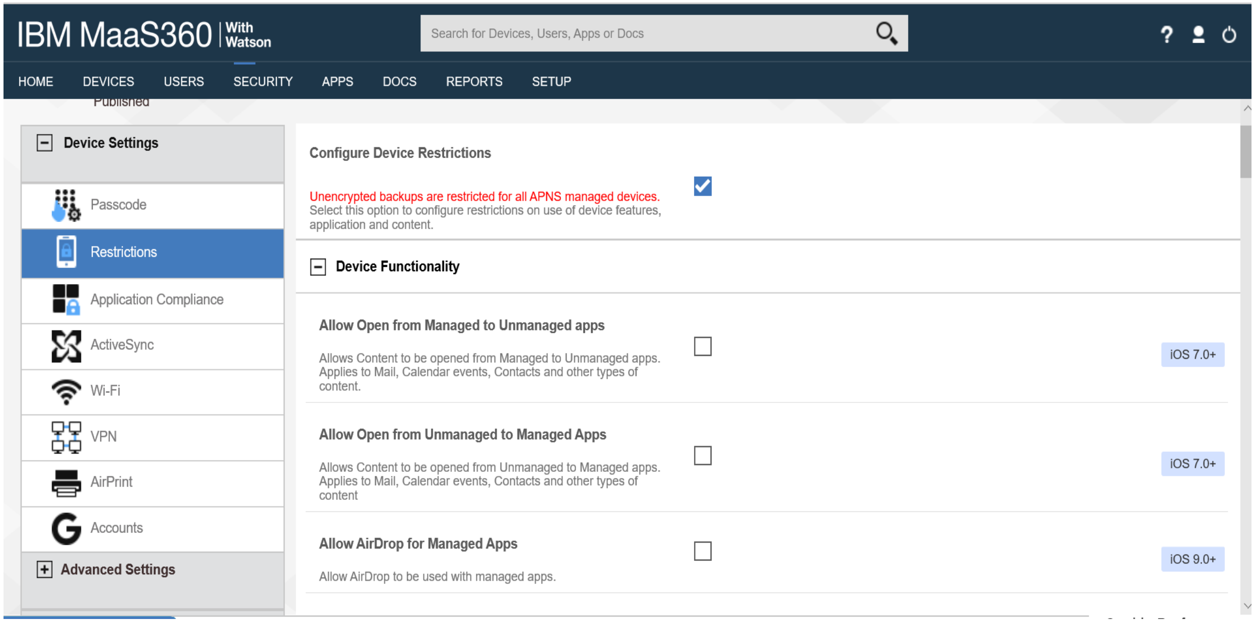
Corporate Data Wiped

Your IT Administrator has wiped the Corporate data on this device. Contact your IT Administrator for assistance.

## F.11 Threat Event 11

These images show an example configuration and outcome to prevent data from being pasted from one application to another application.

1731 **Figure F-26 MaaS360 DLP Configuration**



Configure Device Restrictions ☑

Unencrypted backups are restricted for all APNS managed devices.
Select this option to configure restrictions on use of device features, application and content.

Device Functionality

Allow Open from Managed to Unmanaged apps ☐ iOS 7.0+

Allows Content to be opened from Managed to Unmanaged apps. Applies to Mail, Calendar events, Contacts and other types of content.

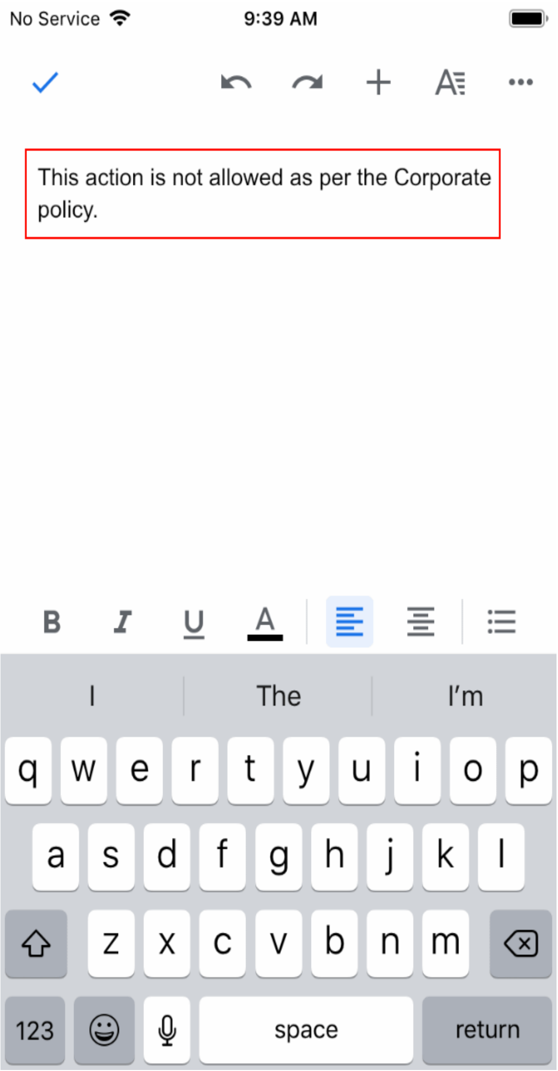
Allow Open from Unmanaged to Managed Apps ☐ iOS 7.0+

Allows Content to be opened from Unmanaged to Managed apps. Applies to Mail, Calendar events, Contacts and other types of content

Allow AirDrop for Managed Apps ☐ iOS 9.0+

Allow AirDrop to be used with managed apps.

**Figure F-27 Attempting to Paste Text on iOS**

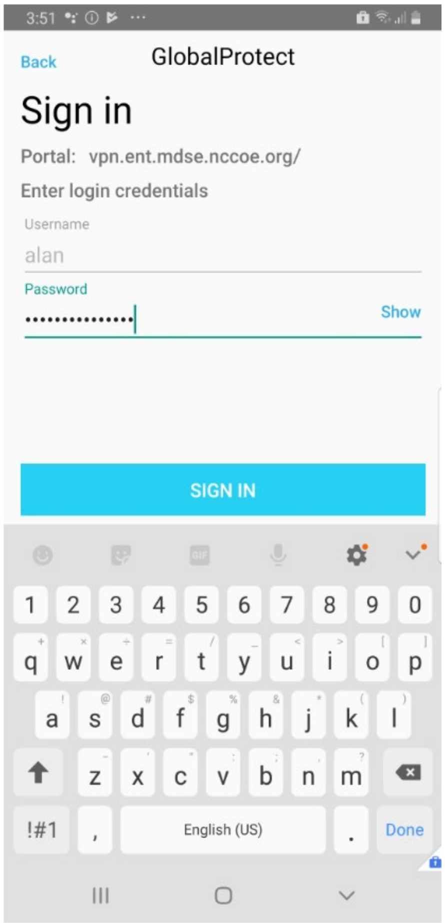


This action is not allowed as per the Corporate policy.

## F.12 Threat Event 12

This image shows a required password to prevent unauthorized access to work applications via a bypassed lock screen. If the lock screen is bypassed, individuals would not be able to connect to the VPN without knowing the user's domain password.

**Figure F-28 GlobalProtect Requires the User's Password**



GlobalProtect

Sign in

Portal: vpn.ent.mdse.nccoe.org/

Enter login credentials

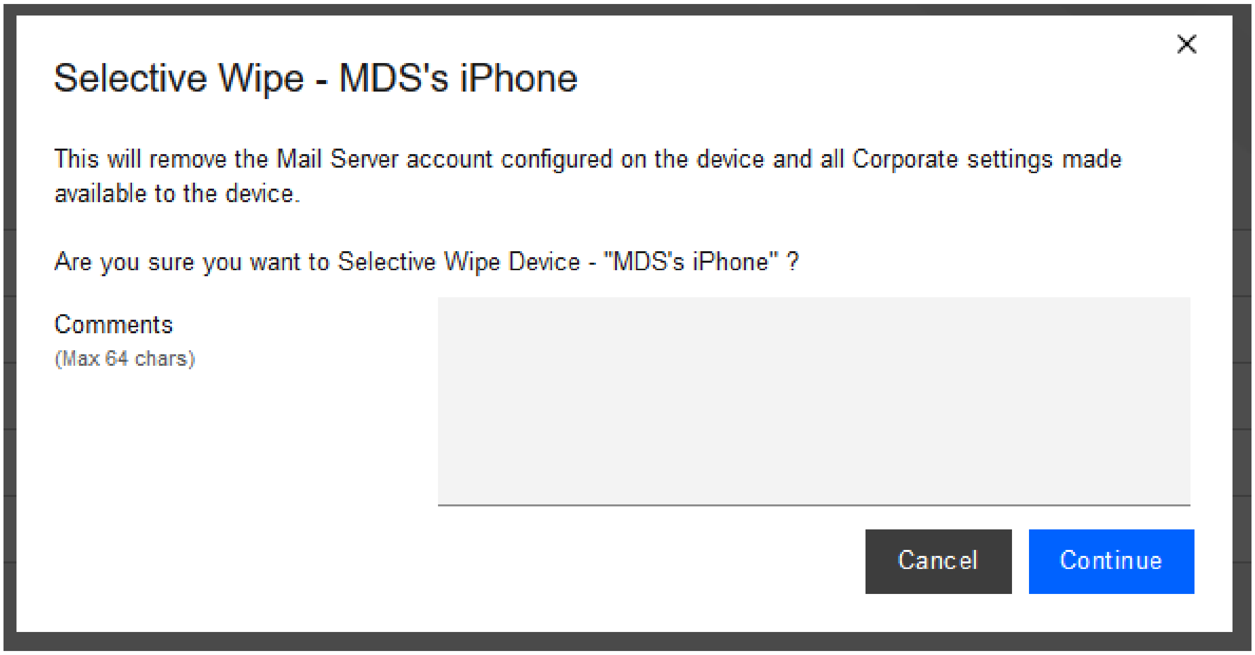
Username: alan

Password: •••••••••••••••

## F.13 Problematic Data Action 1

This image shows initiation of a selective wipe. The selective wipe will remove the Mail Server account and all corporate settings available to the device.

Figure F-29 Initiating a Selective Wipe



Selective Wipe - MDS's iPhone

This will remove the Mail Server account configured on the device and all Corporate settings made available to the device.

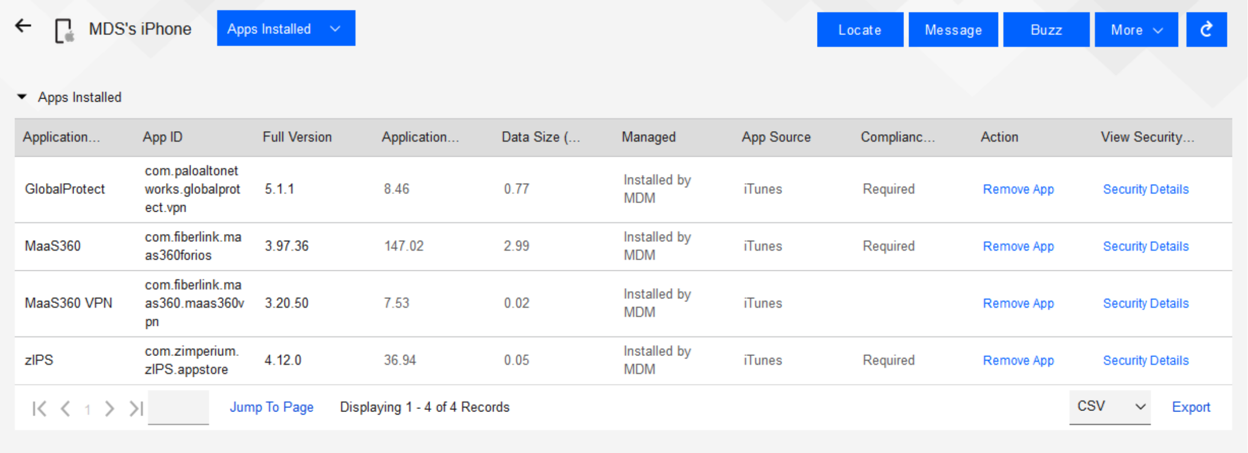
Are you sure you want to Selective Wipe Device - "MDS's iPhone" ?

Comments
(Max 64 chars)

## F.14 Problematic Data Action 2

This shows inventory information for applications and the location information restriction.

Figure F-30 Application Inventory Information



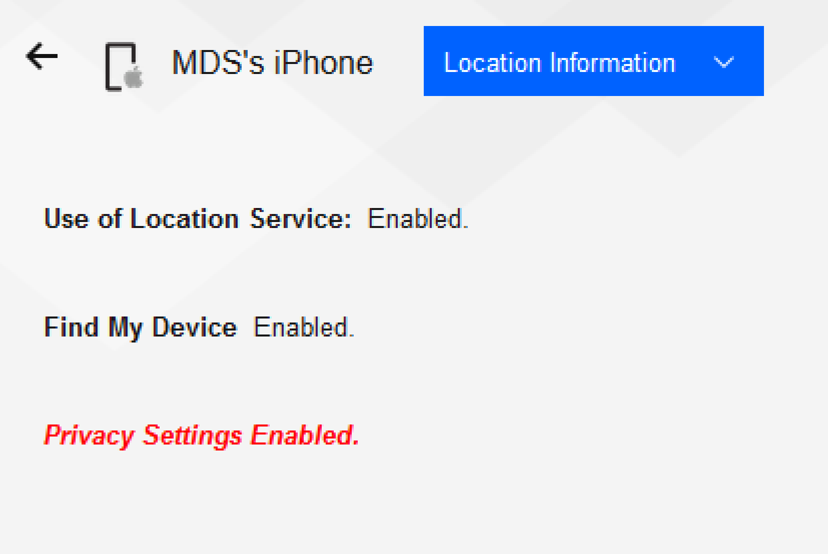
Apps Installed

| Application... | App ID | Full Version | Application... | Data Size (... | Managed | App Source | Complianc... | Action | View Security... |
|---|---|---|---|---|---|---|---|---|---|
| GlobalProtect | com.paloaltonetworks.globalprotect.vpn | 5.1.1 | 8.46 | 0.77 | Installed by MDM | iTunes | Required | Remove App | Security Details |
| MaaS360 | com.fiberlink.maas360forios | 3.97.36 | 147.02 | 2.99 | Installed by MDM | iTunes | Required | Remove App | Security Details |
| MaaS360 VPN | com.fiberlink.maas360.maas360vpn | 3.20.50 | 7.53 | 0.02 | Installed by MDM | iTunes |  | Remove App | Security Details |
| zIPS | com.zimperium.zIPS.appstore | 4.12.0 | 36.94 | 0.05 | Installed by MDM | iTunes | Required | Remove App | Security Details |

Displaying 1 - 4 of 4 Records

When privacy restrictions are configured, only corporate application inventory information is collected.

1746 **Figure F-31 Location Information Restricted**



Use of Location Service: Enabled.

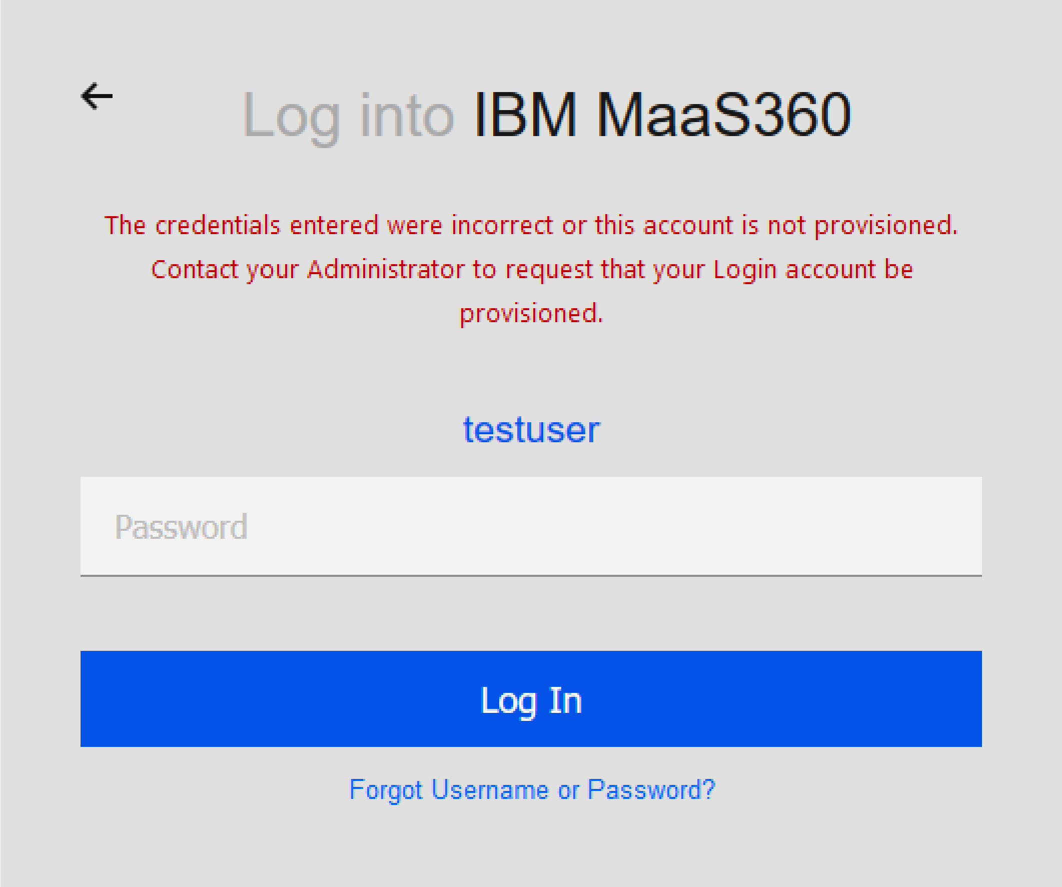
Find My Device Enabled.

*Privacy Settings Enabled.*

## 1747 F.15 Problematic Data Action 3

1748 This demonstrates how a non-administrator account will be prevented from logging in to the MaaS360
1749 portal.

1750 **Figure F-32 Non-Administrator Failed Portal Login**



The credentials entered were incorrect or this account is not provisioned. Contact your Administrator to request that your Login account be provisioned.

testuser

Password

# Appendix G Example Security Subcategory and Control Map

Using the developed risk information as input, the security characteristics of the example solution were identified. A security control map was developed documenting the example solution's capabilities with applicable Subcategories from the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1]; NIST Special Publication (SP) 800-53 Revision 5*, Security and Privacy Controls for Information Systems and Organizations* [38]; International Organization for Standardization (ISO); International Electrotechnical Commission (IEC) 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* [47]; the Center for Internet Security's (CIS) control set Version 6 [43]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

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

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

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

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

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

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | Information Integrity | **A.12.6.2:** Restrictions on Software Installation | **CSC 8:** Malware Defenses | **SP-DEV-002:** Secure Software Assessor |
| **Zimperium Console version vGA-4.23.1** | Cloud service that complements the zIPS Agent | **ID.AM-1:** Physical devices and systems within the organization are inventoried. | **CM-8:** Information System Component Inventory<br>**PM-5:** Information System Inventory | **A.8.1.1:** Inventory of Assets<br>**A.8.1.2:** Ownership of Assets | **CSC 1:** Inventory of Authorized and Unauthorized Devices | **OM-STS-001:** Technical Support Specialist<br>**OM-NET-001:** Network Operations Specialist<br>**OM-ADM-001:** System Administrator |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| **zIPS agent Version 4.9.2 (iOS), 4.9.2 (Android)** | Endpoint security for mobile device threats | **ID.AM-2:** Software platforms and applications within the organization are inventoried. | **CM-8:** Information System Component Inventory<br>**PM-5:** Information System Inventory | **A.8.1.1:** Inventory of Assets<br>**A.8.1.2:** Ownership of Assets<br>**A.12.5.1:** Installation of Software on Operational Systems | **CSC 2:** Inventory of Authorized and Unauthorized Software | **SP-DEV-002:** Secure Software Assessor<br>**SP-DEV-001:** Software Developer<br>**SP-TRD-001:** Research and Development Specialist |
| | | **DE.CM-8:** Vulnerability scans are performed. | **RA-5:** Vulnerability Monitoring and Scanning | **A.12.6.1:** Management of technical vulnerabilities | **CSC 4:** Continuous Vulnerability Assessment and Remediation<br>**CSC 20:** Penetration Tests and Red Team Exercises | **PR-VAM-001:** Vulnerability Assessment Analyst<br>**PR-INF-001:** Cyber Defense Infrastructure Support Specialist<br>**PR-CDA-001:** Cyber Defense Analyst |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | **DE.AE-5:** Incident alert thresholds are established. | **IR-4:** Incident Handling<br>**IR-5:** Incident Monitoring<br>**IR-8:** Incident Response Plan | **A.16.1.4:** Assessment of and decision on information security events | **CSC 6:** Maintenance, Monitoring, and Analysis of Audit Logs<br>**CSC 19:** Incident Response and Management | **PR-CIR-001:** Cyber Defense Incident Responder<br>**AN-TWA-001:** Threat/Warning Analyst |
| | | **DE.CM-5:** Unauthorized mobile code is detected. | **SC-18:** Mobile Code<br>**SI-7:** Software, Firmware, and Information Integrity | **A.12.5.1:** Installation of Software on Operational Systems<br>**A.12.6.2:** Restrictions on Software Installation | **CSC 7:** Email and Web Browser Protections<br>**CSC 8:** Malware Defenses | **PR-CDA-001:** Cyber Defense Analyst<br>**SP-DEV-002:** Secure Software Assessor |
| **Enterprise Mobility Management** | | | | | | |
| **IBM MaaS360 Mobile Device Management (SaaS)** | Enforces organizational mobile endpoint security policy | **ID.AM-1:** Physical devices and systems within the organization are inventoried. | **CM-8:** System Component Inventory<br>**PM-5:** System Inventory | **A.8.1.1:** Inventory of Assets<br>**A.8.1.2:** Ownership of Assets | **CSC 1:** Inventory of Authorized and Unauthorized Devices | **OM-STS-001:** Technical Support Specialist<br>**OM-NET-001:** Network Operations Specialist |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| **Version 10.73** | | | | | | **OM-ADM-001:** System Administrator |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried. | **CM-8:** System Component Inventory<br>**PM-5:** System Inventory | **A.8.1.1:** Inventory of Assets<br>**A.8.1.2:** Ownership of Assets<br>**A.12.5.1:** Installation of Software on Operational Systems | **CSC 2:** Inventory of Authorized and Unauthorized Software | **SP-DEV-002:** Secure Software Assessor<br>**SP-DEV-001:** Software Developer<br>**SP-TRD-001:** Research and Development Specialist |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. | **AC-3:** Access Enforcement<br>**IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11:** Identification and Authentication Family | **A.9.2.1:** User Registration and De-Registration<br>**A.9.2.2:** User Access Provisioning<br>**A.9.2.3:** Management of Privileged Access Rights<br>**A.9.2.4:** Management of Secret Authentication Information of Users<br>**A.9.2.6:** Removal or Adjustment of Access Rights<br>**A.9.3.1:** Use of Secret Authentication Information | **CSC 1:** Inventory of Authorized and Unauthorized Devices<br>**CSC 5:** Controlled Use of Administrative Privileges<br>**CSC 15:** Wireless Access Control<br>**CSC 16:** Account Monitoring and Control | **OV-SPP-002:** Cyber Policy and Strategy Planner<br>**OM-ADM-001:** System Administrator<br>**OV-MGT-002:** Communications Security (COMSEC) Manager |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | | **A.9.4.2:** Secure logon Procedures<br>**A.9.4.3:** Password Management System | | |

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

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | and Authentication<br>**PE-2:** Physical Access Authorizations | | | (COMSEC) Manager |
| | | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality). | **CM-8:** System Component Inventory<br>**SA-10:** Developer Configuration Management | **A.12.1.2:** Change Management<br>**A.12.5.1:** Installation of Software on Operational Systems<br>**A.12.6.2:** Restrictions on Software Installation<br>**A.14.2.2:** System Change Control Procedures<br>**A.14.2.3:** Technical Review of Applications After Operating Platform Changes | **CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers<br>**CSC 9:** Limitation and Control of Network Ports, Protocols, and Services<br>**CSC 11:** Secure Configurations for Network Devices such as | **SP-ARC-002:** Security Architect<br>**OV-SPP-002:** Cyber Policy and Strategy Planner<br>**SP-SYS-001:** Information Systems Security Developer<br>**OM-ADM-001:** System Administrator<br>**PR-VAM-001:** Vulnerability Assessment Analyst |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | | **A.14.2.4:** Restrictions on Changes to Software Packages | Firewalls, Routers, and Switches | |

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

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

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity. | **SA-10(1):** Developer Configuration Management<br>**SI-7:** Software, Firmware, and Information Integrity | **A.12.2.1:** Controls Against Malware<br>**A.12.5.1:** Installation of Software on Operational Systems<br>**A.14.1.2:** Securing Application Services on Public Networks<br>**A.14.1.3:** Protecting Application Services Transactions<br>**A.14.2.4:** Restrictions on Changes to Software Packages | **CSC 2:** Inventory of Authorized and Unauthorized Software<br>**CSC 3:** Secure Configurations for Hardware and Software on Mobile | **OV-SPP-002:** Cyber Policy and Strategy Planner<br>**PR-CDA-001:** Cyber Defense Analyst<br>**SP-ARC-001:** Enterprise Architect |
| | | **PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity. | **SA-10:** Developer Configuration Management | **A.11.2.4:** Equipment maintenance | Not applicable | **OM-ADM-001:** System Administrator |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | **SI-7:** Software, Firmware, and Information Integrity | | | **SP-ARC-001:** Enterprise Architect |
| | | **DE.CM-4:** Malicious code is detected. | **SC-35:** External Malicious Code Identification<br>**SI-7:** Software, Firmware, and Information Integrity | **A.12.2.1:** Controls Against Malware | **CSC 4:** Continuous Vulnerability Assessment and Remediation<br>**CSC 7:** Email and Web Browser Protections<br>**CSC 8:** Malware Defenses<br>**CSC 12:** Boundary Defense | **PR-CDA-001:** Cyber Defense Analyst<br>**PR-INF-001:** Cyber Defense Infrastructure Support Specialist |
| **Virtual Private Network** | | | | | | |
| **Palo Alto Networks PA-220** | Enforces network security policy for remote devices | **PR.AC-3:** Remote access is managed. | **AC-1, AC-3:** Access Control Policy and Procedures | **A.6.2.1:** Mobile Device Policy<br>**A.6.2.2:** Teleworking | **CSC 12:** Boundary Defense | **OV-SPP-002:** Cyber Policy and Strategy Planner<br>**OV-MGT-002:** |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | **AC-19:** Access Control for Mobile Devices | **A.11.2.6:** Security of equipment and assets off-premises<br>**A.13.1.1:** Network Controls<br>**A.13.2.1:** Information Transfer Policies and Procedures | | Communications Security (COMSEC) Manager |
| | | **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation). | **AC-3:** Access Enforcement<br>**SC-7:** Boundary Protection | **A.13.1.1:** Network Controls<br>**A.13.1.3:** Segregation in Networks<br>**A.13.2.1:** Information Transfer Policies and Procedures<br>**A.14.1.2:** Securing Application | **CSC 9:** Limitation and Control of Network Ports, Protocols, and Services<br>**CSC 14:** Controlled Access Based on the Need to Know<br>**CSC 15:** Wireless Access Control | **PR-CDA-001:** Cyber Defense Analyst<br>**OM-ADM-001:** System Administrator |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | | | Services on Public Networks<br>**A.14.1.3:** Protecting Application Services Transactions | **CSC 18:** Application Software Security | |
| | | **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions. | **AC-3:** Access Enforcement<br>**IA-2, IA-4, IA-5, IA-8:** Identification and Authentication (Organizational Users)<br>**PE-2:** Physical Access Authorizations<br>**PS-3:** Personnel Screening | **A.7.1.1:** Screening<br>**A.9.2.1:** User Registration and De-Registration | **CSC 16:** Account Monitoring and Control | **OV-SPP-002:** Cyber Policy and Strategy Planner<br>**OV-MGT-002:** Communications Security (COMSEC) Manager |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
| | | **PR.DS-2:** Data-in-transit is protected. | **AC-17(2):** Protection of Confidentiality and Integrity Using Encryption<br>**SC-8:** Transmission Confidentiality and Integrity | **A.8.2.3:** Handling of Assets<br>**A.13.1.1:** Network Controls<br>**A.13.2.1:** Information Transfer Policies and Procedures<br>**A.13.2.3:** Electronic Messaging<br>**A.14.1.2:** Securing Application Services on Public Networks<br>**A.14.1.3:** Protecting Application Services Transactions | **CSC 13:** Data Protection<br>**CSC 14:** Controlled Access Based on the Need to Know | **OV-SPP-002:** Cyber Policy and Strategy Planner<br>**OV-MGT-002:** Communications Security (COMSEC) Manager<br>**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager |
| | | **PR.PT-4:** Communications and control networks are protected. | **AC-3, AC-4, AC-17, AC-18:** Access Control Family | **A.13.1.1:** Network Controls | **CSC 8:** Malware Defenses | **PR-INF-001:** Cyber Defense Infrastructure |

| Specific product used | How the component functions in the example solution | Applicable NIST Cybersecurity Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Controls | ISO/IEC 27001:2013 | CIS 6 | Applicable NIST SP 800-181 NICE Framework Work Roles (2017) |
|---|---|---|---|---|---|---|
|  |  |  | **CP-2:** Contingency Plan<br>**SC-7, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-38, SC-39, SC-40, SC-41, SC-43:** System and Communications Protection Family | **A.13.2.1:** Information Transfer Policies and Procedures<br>**A.14.1.3:** Protecting Application Services Transactions | **CSC 12:** Boundary Defense<br>**CSC 15:** Wireless Access Control | Support Specialist<br>**OV-SPP-002:** Cyber Policy and Strategy Planner<br>**PR-CDA-001:** Cyber Defense Analyst |

# Appendix H Example Privacy Subcategory and Control Map

Using the developed privacy information as input, we identified the privacy characteristics of the example solution. We developed a privacy control map documenting the example solution's capabilities with applicable Functions, Categories, and Subcategories from the National Institute of Standards and Technology *(NIST) Privacy Framework* [2]; and NIST SP 800-53 Revision 5 [38]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

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

Table H-1's example privacy control map identifies the privacy characteristic mapping for the products as they were used in the example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the mapping not be used as a reference for all of the privacy capabilities these products may be able to address. The comprehensive mapping of the NIST Privacy Framework to NIST SP 800-53, Revision 5 controls can be found on the NIST Privacy Framework Resource Repository website, in the event an organization's mobile device security solution is different to determine other controls that are appropriate for their environment [62].

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

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| **IBM MaaS360** | MaaS360 can be used to capture an inventory of the types and number of devices deployed and shows the administra- | **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). | **CM-12:** Information Location<br>**CM-13:** Data Action Mapping | **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager<br>**OV-TEA-001:** Cyber Instructional Curriculum Developer |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | tors what data is collected from each enrolled device. | | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**PT-3:** Personally Identifiable Information Processing Purposes<br>**RA-3:** Risk Assessment<br>**RA-8:** Privacy Impact Assessment | |
| | Administrators can view data elements in the administration portal. Users can see collected data within the MaaS360 application on their device. Data can be edited and deleted from within the administration console. | **CT.DM-P1:** Data elements can be accessed for review. | **AC-2:** Account Management<br>**AC-3:** Access Enforcement<br>**AC-3(14):** Access Enforcement \| Individual Access<br>**PM-21:** Accounting of Disclosures | **OM-DTA-002:** Data Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | **CT.DM-P3:** Data elements can be accessed for alteration. | **AC-2:** Account Management<br>**AC-3:** Access Enforcement<br>**AC-3(14):** Access Enforcement \| Individual Access<br>**PM-21:** Accounting of Disclosures<br>**SI-18:** Personally Identifiable Information Quality Operations | **OM-DTA-002:** Data Analyst |
| | | **CT.DM-P4:** Data elements can be accessed for deletion. | **AC-2:** Account Management<br>**AC-3:** Access Enforcement<br>**SI-18:** Personally Identifiable Information Quality Operations | **OM-DTA-002:** Data Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | **CT.DM-P5:** Data are destroyed according to policy. | **MP-6:** Media Sanitization<br>**SA-8(33):** Security and Privacy Engineering Principles \| Minimization<br>**SI-18:** Personally Identifiable Information Quality Operations<br>**SR-12**: Component Disposal | **OM-DTA-002:** Data Analyst |
| | | **CT.DP-P4:** System or device configurations permit selective collection or disclosure of data elements. | **CM-6:** Configuration Settings<br>**SA-8(33):** Minimization<br>**SC-42(5):** Collection Minimization<br>**SI-12(1):** Information Management and Retention \| Limit Personally Identifiable Information Elements | **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | Devices may be backed up to the cloud. | **PR.PO-P3:** Backups of information are conducted, maintained, and tested. | **CP-4:** Contingency Plan Testing<br>**CP-6:** Alternate Storage Site<br>**CP-9:** System Backup | **OM-ADM-001:** System Administrator |
| | Devices are issued identity certificates via on-premises certificate infrastructure. | **PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | **IA-2:** Identification and Authentication (Organizational Users)<br>**IA-3:** Device Identification and Authentication<br>**IA-4:** Identifier Management<br>**IA-4(4):** Identifier Management \| Identifier User Status | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | MaaS360 enforces a device personal identification number (PIN) for access. | **PR.AC-P2:** Physical access to data and devices is managed. | **PE-2:** Physical Access Authorizations<br>**PE-3:** Physical Access Control<br>**PE-3(1):** System Access | **OM-DTA-001:** Database Administrator<br>**OM-DTA-002:** Data Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | | **PE-4:** Access Control for Transmission<br>**PE-5:** Access Control for Output Devices<br>**PE-6:** Monitoring Physical Access<br>**PE-18:** Location of System Components<br>**PE-20:** Asset Monitoring and Tracking | |
| | | **PR.DS-P1:** Data-at-rest are protected. | **MP-2:** Media Access<br>**MP-4:** Media Storage<br>**PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**SC-28:** Protection of Information at Rest | **OM-DTA-001:** Database Administrator<br>**OM-DTA-002:** Data Analyst |

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

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| **Zimperium** | Zimperium checks the device for unauthorized modifications. | **PR.DS-P1:** Data-at-rest are protected. | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**SC-28:** Protection of Information at Rest | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | | **PR.DS-P2:** Data-in-transit are protected. | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**SC-8:** Transmission Confidentiality and Integrity<br>**SC-11:** Trusted Path | **OM-DTA-002:** Data Analyst<br>**OM-ANA-001:** Systems Security Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | **PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity. | **PM-22:** Personally Identifiable Information Quality Management<br>**SC-16:** Transmission of Security Attributes<br>**SI-7:** Boundary Protection<br>**SI-10:** Network Disconnect<br>**SI-18:** Personally Identifiable Information Quality Operations | **OM-DTA-002:** Data Analyst<br>**OM-ANA-001:** Systems Security Analyst |
| **Kryptowire** | Kryptowire can identify applications that do not use best practices, such as lack of encryption or hardcoded credentials. | **CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests | **AC-8:** System Use Notification | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | are established and in place. | | |
| | | **CM.AW-P3:** System/ product/ service design enables data processing visibility. | **PL-8:** Security and Privacy Architecture<br>**PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | | **CM.AW-P6:** Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure. | **AC-16:** Security and Privacy Attributes<br>**SC-16:** Transmission of Security Attributes | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | | **PR.DS-P1:** Data-at-rest are protected. | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**SC-28:** Protection of Information at Rest | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | | **PR.DS-P2:** Data-in-transit are protected. | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | | **SC-8:** Transmission Confidentiality and Integrity<br>**SC-11:** Trusted Path | |
| **Palo Alto Networks PA-220** | Provides firewall and virtual private network capabilities. | **PR.DS-P2:** Data-in-transit are protected. | **PM-5(1):** System Inventory \| Inventory of Personally Identifiable Information<br>**SC-8:** Transmission Confidentiality and Integrity<br>**SC-11:** Trusted Path | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |
| | | **PR.AC-P4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | **AC-2:** Account Management<br>**AC-3:** Access Enforcement<br>**AC-5:** Separation of Duties<br>**AC-6:** Least Privilege<br>**AC-24:** Access Control Decisions | **SP-ARC-002:** Security Architect<br>**PR-CDA-001:** Cyber Defense Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | **PR.AC-P5:** Network integrity is protected (e.g., network segregation, network segmentation). | **AC-4:** Information Flow Enforcement<br>**AC-10:** Access Control<br>**SC-7:** Boundary Protection<br>**SC-10:** Network Disconnect | **OM-DTA-002:** Data Analyst<br>**OM-ANA-001:** Systems Security Analyst |
| | | **PR.PT-P3:** Communications and control networks are protected. | **AC-12:** Session Termination<br>**AC-17:** Remote Access<br>**AC-18:** Wireless Access<br>**SC-5:** Denial of Service Protection<br>**SC-7:** Boundary Protection<br>**SC-10:** Network Disconnect<br>**SC-11:** Trusted Path | **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager<br>**PR-CDA-001:** Cyber Defense Analyst |

| Product | How the component functions in the build | Applicable Privacy Framework Subcategories | Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls | Applicable NIST SP 800-181, NICE Framework Work Roles (2017) |
|---|---|---|---|---|
| | | | **SC-21:** Secure Name/Address Resolution Service (Recursive or Caching Resolver)<br>**SC-23:** Session Authenticity | |
| **Qualcomm** | The trusted execution environment provides data confidentiality and integrity. | **PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity. | **PM-22:** Personally Identifiable Information Quality Management<br>**SC-16:** Transmission of Security and Privacy Attributes<br>**SI-7:** Software, Firmware, and Information Integrity<br>**SI-10:** Information Input Validation<br>**SI-18:** Personally Identifiable Information Quality Operations | **PR-INF-001:** Cyber Defense Infrastructure Support Specialist<br>**OM-ANA-001:** Systems Security Analyst |