NIST SPECIAL PUBLICATION 1800-22A

Mobile Device Security:
Bring Your Own Device (BYOD)

Volume A:
Executive Summary

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

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

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

September 2023

FINAL

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

Executive Summary

Many organizations provide employees the flexibility to use their personal mobile devices to perform work-related activities. An ineffectively secured personal mobile device could expose an organization or employee to data loss or a privacy compromise. Ensuring that an organization's data is protected when it is accessed from personal devices poses unique challenges and threats.

Allowing employees to use their personal mobile devices for work-related activities is commonly known as a bring your own device (BYOD) deployment. A BYOD deployment offers a convenient way to remotely access organizational resources, while avoiding the alternative of carrying both a work phone and personal phone. This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their BYOD security and privacy needs.

CHALLENGE

BYOD devices can be used interchangeably for work and personal purposes throughout the day. While flexible and convenient, BYOD can introduce challenges to an enterprise. These challenges can include additional responsibilities and complexity for information technology (IT) departments caused by supporting many types of personal mobile devices used by the employees, enterprise security threats arising from unprotected personal devices, as well as challenges protecting the privacy of employees and their personal data stored on their mobile devices.

An ineffectively secured personal mobile device *could expose an organization or employee to data loss or a privacy compromise.*

SOLUTION

The National Cybersecurity Center of Excellence (NCCoE) collaborated with the mobile community and cybersecurity technology providers to build a simulated BYOD environment. Using commercially available products, the example solution's technologies and methodologies can enhance the security posture of the adopting organization and help protect employee privacy and organizational information assets.

This practice guide can help your organization:

- **protect data** from being accessed by unauthorized persons when a device is stolen or misplaced
- **reduce risk to employees** through enhanced privacy protections
- **improve the security of mobile devices and applications** by deploying associated technologies

- **reduce risks to organizational data** by separating personal and work-related information from each other
- **enhance visibility** into mobile device health to facilitate identification of device and data compromise, and permit efficient user notification
- **leverage industry best practices** to enhance mobile device security and privacy
- **engage stakeholders** to develop an enterprise-wide policy to inform management and employees of acceptable practices

The example solution uses technologies and security capabilities (shown below) from our project collaborators. The technologies used in the solution support security and privacy standards and guidelines including the NIST Cybersecurity Framework and NIST Privacy Framework, among others. Both iOS and Android devices are supported by this guide's example solution.

Collaborator	Security Capability or Component
IBM	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
Kryptowire (now known as Quokka)	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
Palo Alto Networks	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
Qualcomm	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
Zimperium	Mobile Threat Defense detects unwanted activity and informs the device owner and BYOD administrators to prevent or limit harm that an attacker could cause

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

This guide contains four volumes:

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

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

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-22A: Executive Summary*, to understand the impetus for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use the following:

- *NIST SP 1800-22B: Approach, Architecture, and Security Characteristics*, which describes what we built and why, the risk analysis performed, and the security/privacy control mappings.
- *NIST SP 1800-22 Supplement: Example Scenario: Putting Guidance into Practice*, which provides an example of a fictional company using this practice guide and other NIST guidance to implement a BYOD deployment with their security and privacy requirements.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-22C: How-To Guides*, which provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device. Help the NCCoE make this guide better by sharing your thoughts with us. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at mobile-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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