# MOBILE DEVICE SECURITY

CORPORATE-OWNED PERSONALLY-ENABLED

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is addressing the challenge of mobile device security for enterprises through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Mobile Device Security Corporate-Owned Personally-Enabled (COPE) project, including background, goals, and potential benefits.

## Background

Mobile technologies evolve rapidly, and mobility programs require frequent re-evaluation to ensure they are accomplishing their security, privacy, and workplace functions. Built-in mobile protections may not be enough to fully mitigate the security challenges associated with corporate-owned and personally-enabled mobile information systems. Usability, privacy, and regulatory requirements each influence which mobile security technologies and security controls will be well-suited to meet an organization's needs.

## Goals

The goal of the Mobile Device Security: Corporate-Owned Personally-Enabled project is to provide an example solution, published in a practice guide, demonstrating how organizations can use a standards-based approach and commercially available technologies to meet their security and privacy needs for using mobile devices to access enterprise resources. The example solution details tools for an enterprise mobility management (EMM) capability that is hosted on-premises, mobile threat defense (MTD), mobile threat intelligence (MTI), application vetting, secure boot/image authentication, and virtual private network (VPN) services.

## Benefits

This practice guide can help your organization:

- reduce adverse effects on the organization if a corporate-owned mobile device is compromised
- apply robust, standards-based technologies using industry best practices
- reduce capital investment by embracing modern enterprise mobility models
- decrease user privacy risks
- provide users with enhanced protection against loss of personal and business data when a device is stolen or misplaced
- deploy enterprise management technologies to improve the security of enterprise networks, devices, and applications
- reduce risk so that employees can access the necessary data from nearly any location by using a wide selection of enterprise-owned mobile devices and networks
- enhance visibility for system administrators into mobile security events, efficiently providing notification and identification of device and data compromise
- implement government standards for mobile security

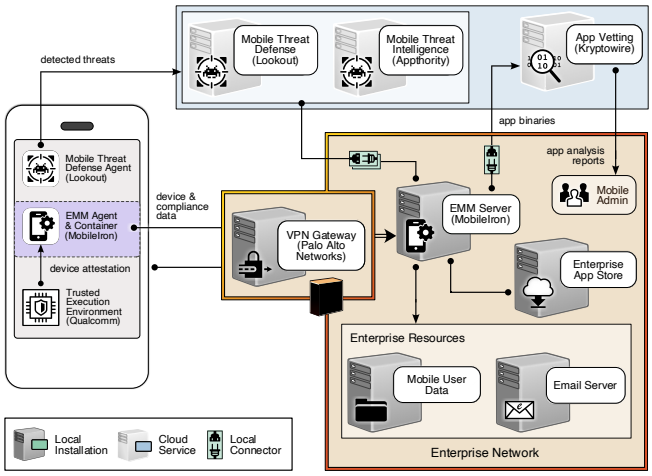
*This guide is part of a series of projects that focus on Mobile Device Security for Enterprises. For information on improving the security and privacy of Bring Your Own Device (BYOD) deployments and our other projects, please visit https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security.*

## High-Level Architecture

The NCCoE worked with industry subject matter experts to develop an open, standards-based, commercially available architecture that addresses common risks for corporate-owned personally-enabled devices. COPE architectures provide the flexibility of allowing both enterprises and employees to install applications onto organization-owned mobile devices.

This example solution consists of six mobile security technologies: trusted execution environment, enterprise mobility management, virtual private network, mobile application vetting service, mobile threat defense, and mobile threat intelligence.

These components are further integrated with broader on-premises security mechanisms and a VPN gateway. This integrated solution provides a broad range of capabilities to help securely provision and manage mobile devices; protect against and detect device compromise; and help provide authorized mobile users security-enhanced access to enterprise resources.




These processes and technologies will enable users to work inside and outside the corporate network, while mitigating threats posed from across the mobile ecosystem.

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

**Appthority** **Kryptowire** **Lookout** **MobileIron** **Palo Alto Networks** **Qualcomm**

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

### HOW TO PARTICIPATE

As a private-public partnership, we always seek insights and expertise from businesses, the public, and technology vendors. If you have feedback on this project, please email mobile-nccoe@nist.gov.

### DOWNLOAD THE PRACTICE GUIDE

For more information about this project and to download the NIST Cybersecurity Practice Guide Special Publication 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled* practice guide, visit: https://nccoe.nist.gov/projects/building-blocks/mobile-device-security/corporate-owned-personally-enabled.