MOBILE DEVICE SECURITY FOR ENTERPRISES

The National Cybersecurity Center of Excellence (NCCoE) 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 for Enterprises project, including background and challenge, goals, and potential benefits. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge, please contact us at mobile-nccoe@nist.gov.

BACKGROUND

Organizations understand the value mobile devices can add to their employees' productivity by providing access to business resources at any time. Not only has this reshaped how traditional in-office tasks are accomplished, but organizations are devising entirely new ways to work. The diversity and complexity of the mobile ecosystem combined with the breadth of possibilities makes successfully deploying mobile devices a considerable challenge. Further, the rapid pace at which mobile technologies evolve requires regular reevaluation of a mobility program to ensure it's accomplishing its security, privacy, and workplace functionality.

CHALLENGE

While mobile devices can increase organizations' efficiency and effectiveness, it can also leave sensitive data vulnerable. Built-in mobile protections may not be enough to fully mitigate the security challenges associated with mobile information systems. Usability, privacy, and regulatory requirements each influence which mobile security technologies and security controls are going to be well-suited to meet the needs of an organization's mobility program.

GOALS

The Mobile Device Security for Enterprises (MDSE) project aims to help organizations across business sectors develop a series of clear and repeatable reference mobile architectures that any organization can adapt and adopt to ease design, accelerate deployment, and build in security for their mobility program from the outset.

This project will result in two Practice Guides demonstrating how different commercially available management technologies can be used to secure mobile devices:

- **Scenario 1** in which strong data confidentiality is implemented using certified and validated technologies
- **Scenario 2** in which business productivity tools are deployed to mobile users with a variety of risk profiles

BENEFITS

Potential business benefits of this explored solution include:

- provide users with protection against both malicious applications and loss of personal data when a device is stolen or misplaced
- provide mitigating mechanisms to reduce adverse effects on an organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- provide visibility for system administrators into mobile security events, quickly providing notification and identification of a compromised device
- decrease the risk of vendor lock-in using industry standards
- facilitate multiple mobile device usage scenarios such as bring your own device and corporately owned personally enabled
- increase return on investment for mobility programs by applying robust, standards-based technologies using industry best practices
- demonstrate secure mobile access to organizational resources such as email, contacts, and calendar
- illustrate the application of the NIST Risk Management Framework and the Cybersecurity Framework to mobility

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

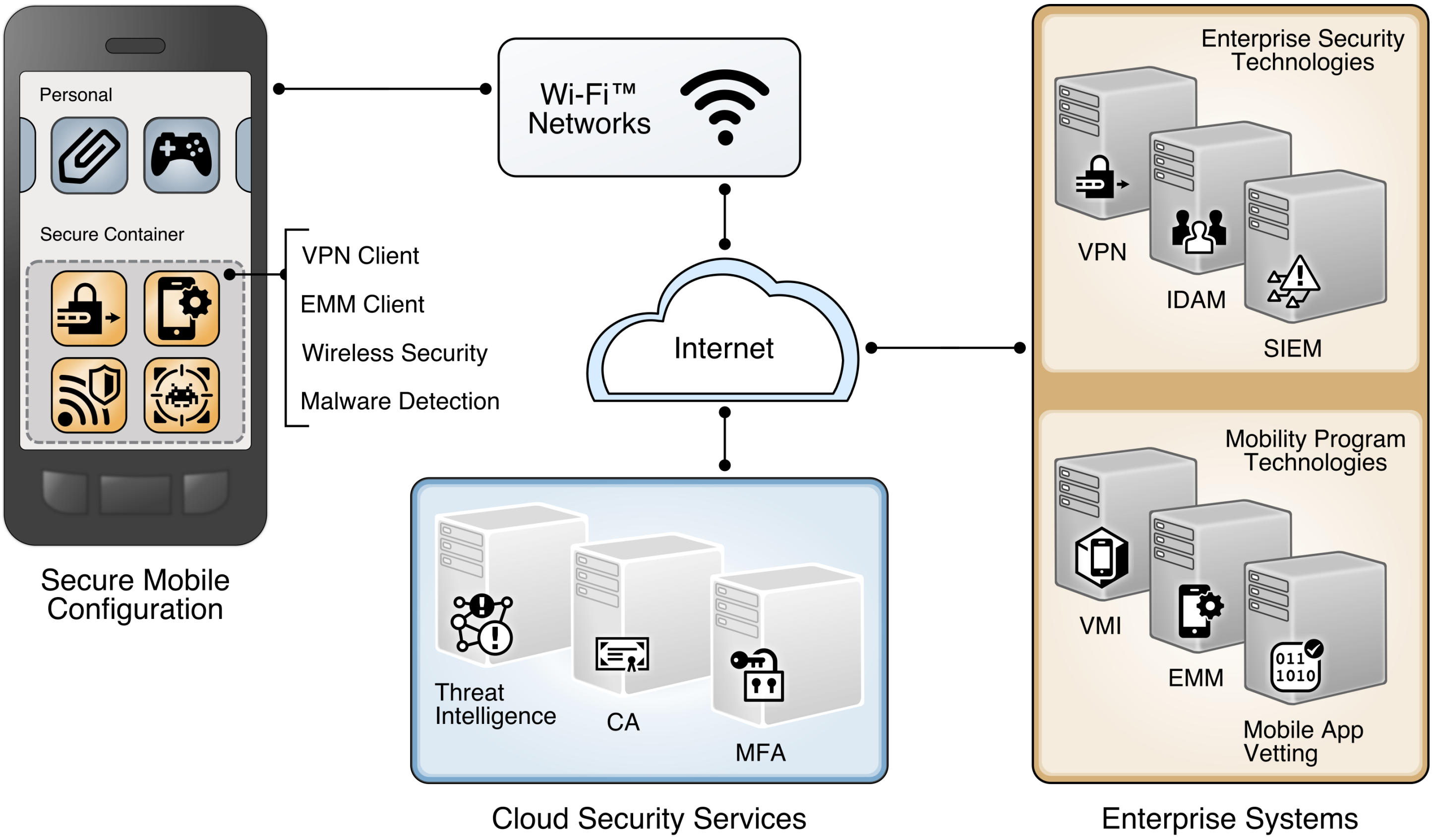
LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

The specific architecture of each build varies based on the necessary enterprise services and management technology in use. Each build will use network-based confidentiality protection mechanisms, such as a Virtual Private Network. Additionally, device-side security mechanisms will be utilized to identify known vulnerabilities and mobile malware. Enterprise Mobility Management (EMM) policy sets will be created, and then tailored to an individual user's risk profile in accordance with established best practices. Each MDSE build will include the following:

- an example risk assessment using an established methodology (e.g., NIST SP 800-32, Cybersecurity Framework)
- installation and configuration instructions for a variety of mobile security technologies, such as an enterprise mobility management system, virtual mobile infrastructure, application vetting, or mobile threat intelligence system
- aset of mobile security controls, mapped to a variety of industry and government standards (e.g., ISO, NIST, NIAP, Cloud Security Alliance)



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 are participating 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 IBM kryptowire Lookout

MobileIron paloalto NETWORKS QUALCOMM ZIMPERIUM MOBILE THREAT DEFENSE

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.

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit: https://nccoe.nist.gov/projects/building-blocks/mobile-device-security

HOW TO PARTICIPATE

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

February 2019