MOBILE DEVICE SECURITY

BRING YOUR OWN DEVICE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is addressing the challenge of improving mobile device security for enterprises through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions.

Background

Many organizations now authorize employees to use their personal mobile devices to perform work-related activities. This increasingly common practice known as Bring Your Own Device (BYOD) provides employees with increased flexibility to access organizational information resources. Ensuring that an organization's data is protected when it is accessed from personal devices poses unique challenges.

Goals

To help address the security and privacy challenges of a BYOD deployment, NIST built an example solution in a lab environment at the NCCoE. 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.

Benefits

Organizations can use this practice guide to help:

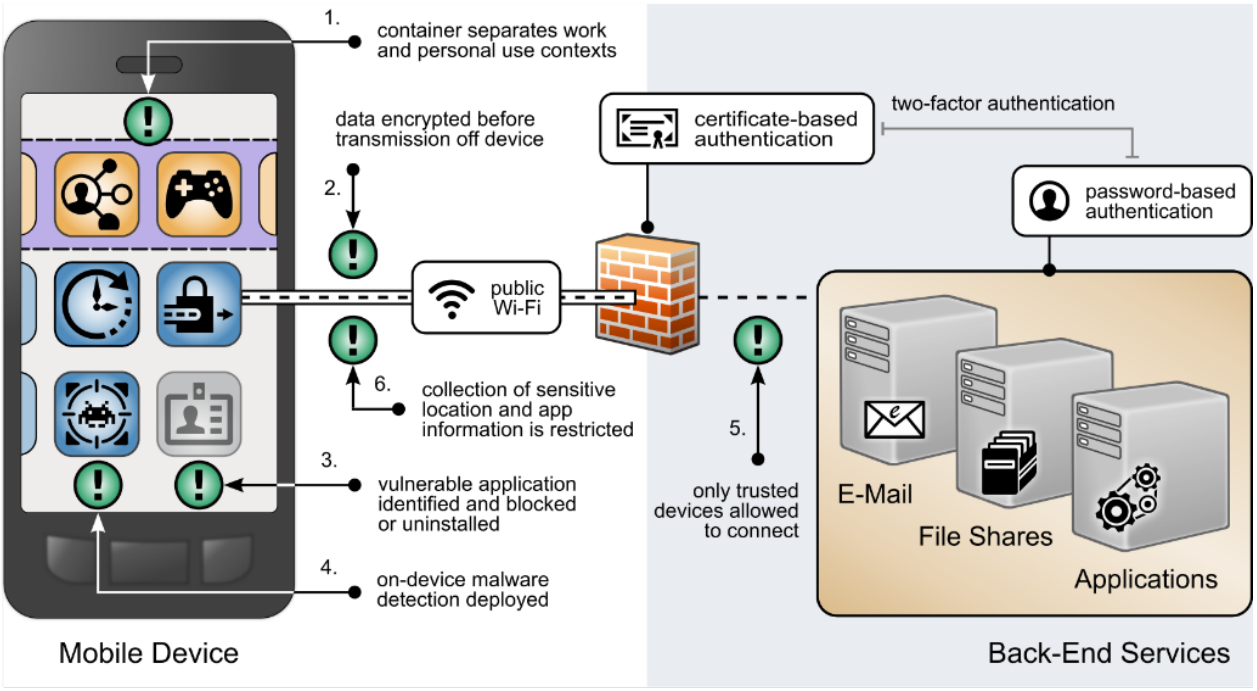
- improve the security and privacy of mobile devices and their applications
- implement mobile device security and privacy best practices and standards
- lower the risks associated with remotely accessing organizational data
- apply robust, standards-based technologies by using industry best practices
- protect data from unauthorized access if a device is stolen or misplaced
- protect information when using a selection of communication networks and personally owned mobile devices
- enhance visibility into the health and compliance of mobile devices
- facilitate identification of device and data compromise, and permit efficient user notification
- improve privacy protections for employees' personal mobile devices

This guide is part of a series of projects that focus on Mobile Device Security for Enterprises. Information on our other projects can be found at 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 helps address the risks for BYOD deployments identified during a risk assessment.

This example solution helps address the six security and privacy goals illustrated below with green exclamation marks. Organizations can leverage these goals to help improve the security and privacy of BYOD deployments.



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:

IBM **Kryptowire** **Palo Alto Networks** **Qualcomm** **Zimperium**

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 DRAFT PRACTICE GUIDE

For more information about this project and to download the NIST Cybersecurity Practice Guide Special Publication 1800-22, *Mobile Device Security: Bring Your Own Device* practice guide, visit: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device.