BUILDING BLOCK

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MOBILE DEVICE SECURITY: CLOUD & HYBRID BUILDS

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of mobile device security through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of NIST Special Publication 1800-4 *Mobile Device Security: Cloud & Hybrid Builds*, including background and challenge, goals, and proposed solution. The solution we propose is not meant to be authoritative; there may be other solutions in this fast-moving cybersecurity technology market. If you have feedback on the architecture or the relevance and usefulness of this practice guide, or would like to schedule a demonstration, please email mobile-nccoe@nist.gov.

CHALLENGE

If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to gain unauthorized access to that data. Even worse, a mobile device with remote access to sensitive organizational data could be leveraged by an attacker to gain access to that data, and any other data that user is allowed to access from that mobile device. The challenge lies in ensuring the confidentiality, integrity, and availability of the information that a mobile device accesses, stores, and processes. Despite the security risks posed by today's mobile devices, enterprises are under pressure to employ them for several business reasons, including anticipated cost savings and employees' need to work in remote locations.

SOLUTION

The Mobile Device Security Practice Guide demonstrates how businesses can use commercially available technologies to implement an enterprise mobility management system. The system can enable secure access to the organization's sensitive email, contacts, and calendar information from users' mobile devices. These technologies enable users to work inside and outside the corporate network with a secure mobile device while minimizing the impact on the user experience.

BENEFITS

The proposed NCCoE mobile device security solution:

- reduce risk so that employees are able to access the necessary enterprise data from nearly any location, over any network, using a wide variety of mobile devices
- enable the use of BYOD, COPE, and other mobile devices deployment models, which may provide cost savings and increased flexibility for organizations
- leverage cloud services to secure sensitive corporate data using the latest industry best practices and defense-in-depth security strategy, which may reduce infrastructure costs for organizations
- enable identity federation between an on-premise identity store and associated cloud services, which may improve user experience and enhance enterprise security
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement industry standard mobile security controls reducing long term costs and decreasing the risk of vendor lock-in

HIGH-LEVEL ARCHITECTURE

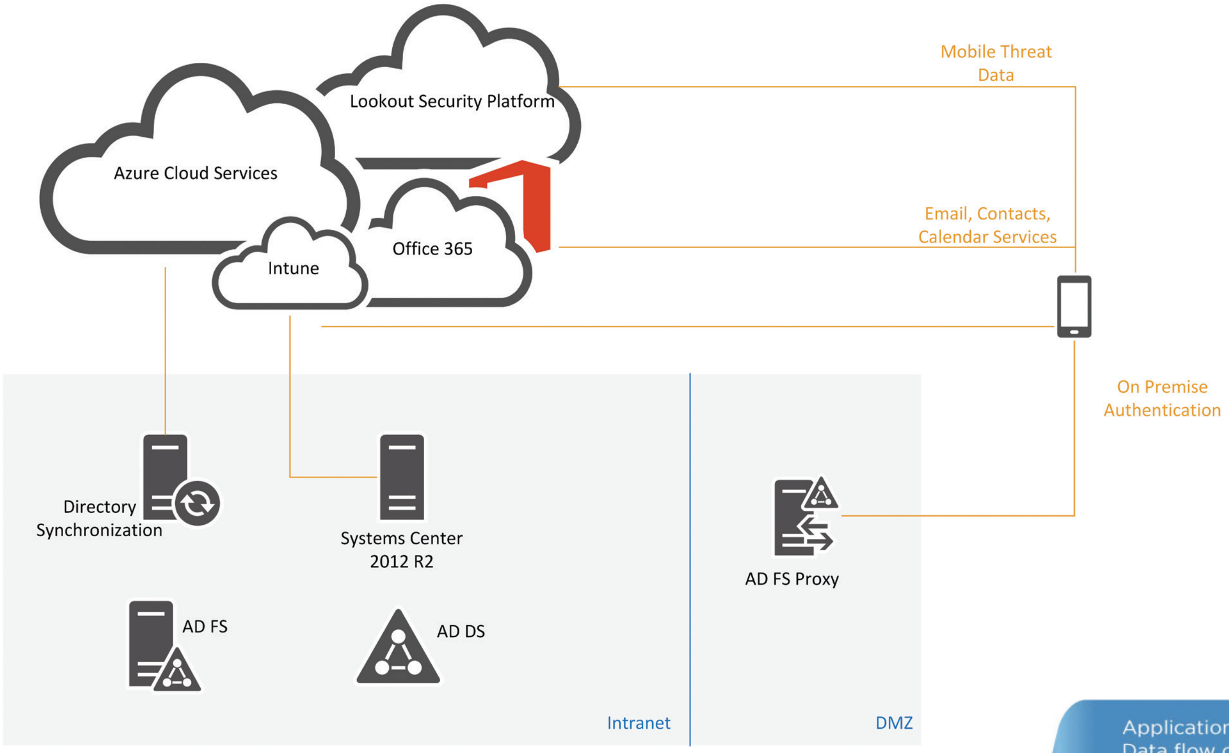
The NCCoE mobile device security solution allows employees to access enterprise resources and enterprise managers to push policies to mobile devices.

- mobile devices are enrolled in the enterprise mobility management system.
- enterprise management defines a set of policies, such as the requirement to use an 8-digit passcode.
- policies are pushed to mobile devices through email or some other communications channel.
- policies are enforced on the devices through an enforcement mechanism, such as the operating system or a mobile application

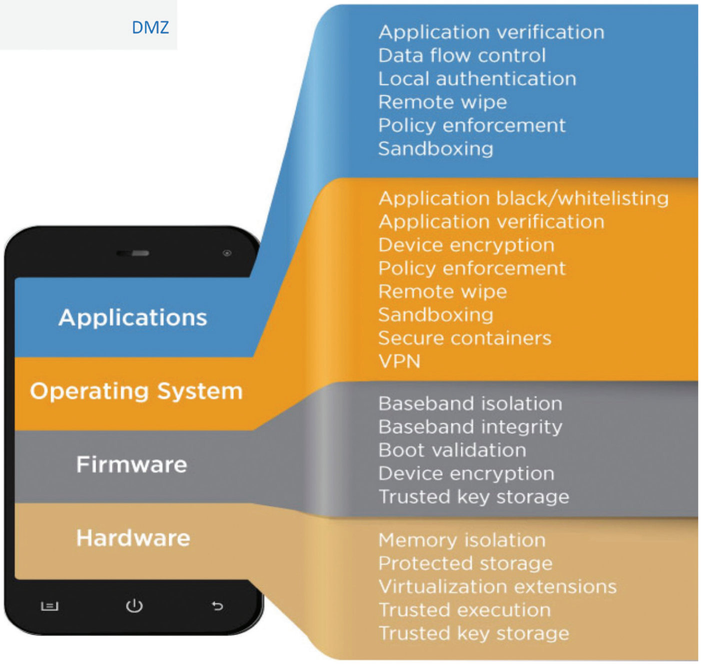
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. 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 http://nccoe.nist.gov

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


Lookout Security Platform
Azure Cloud Services
Office 365
Intune
Mobile Threat Data
Email, Contacts, Calendar Services
On Premise Authentication
Directory Synchronization
Systems Center 2012 R2
AD FS Proxy
AD FS
AD DS
Intranet
DMZ

These processes and technologies enable users to work inside and outside the corporate network using a securely configured mobile device with security capabilities such as those shown in the figure to the right.



TECHNOLOGY PARTNERS/COLLABORATORS

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:

intel Lookout Microsoft Symantec.

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 PRACTICE GUIDE

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 Practice Guide, or would like to schedule a demonstration, please email mobile-nccoe@nist.gov.

July 2017