Android for Work:
Top 8 Security Considerations Every CISO Should Know

v 1.0

MKT-8000

MobileIron

Table of Contents

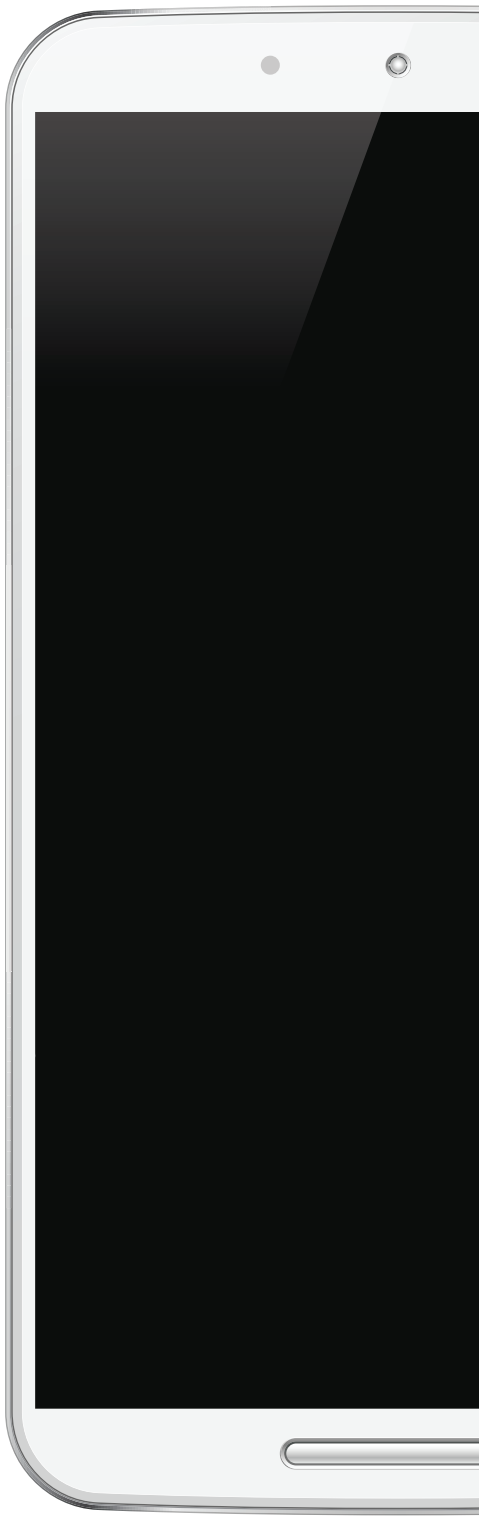
Executive Summary

Enterprises around the world have been searching for a way to securely enable Android™ devices for work, but have shied away from the platform due to ongoing security and fragmentation concerns. Delayed or non-existent Android security patches, malicious app store activity, and other security gaps have led organizations to distrust the platform, particularly those in industries with tight security and compliance requirements.

In recent months, Google has made great strides toward improving Android security with the release of Lollipop, which includes new security features such as default encryption, increased protection against brute-force attacks, secure device-sharing features, and SELinux enforcing mode.[1] In addition, Google has introduced Android for Work, a Google program that enables secure, containerized app deployment to a range of Android devices through an ecosystem of enterprise mobility management (EMM) providers.

In addition to providing a way to securely deploy enterprise apps to Android devices, Lollipop and Android for Work help simplify many key compliance processes with features such as key binding, SELinux sandbox reinforcement, Smart Lock, restricted profiles for multiple users, automated OS updates, and more. These security enhancements help put IT organizations that much closer to enabling Android devices as part of a bring-your-own-device (BYOD) program.

This white paper is intended to help CISOs understand how Lollipop and Android for Work can meet critical security and compliance requirements, even in high-security organizations. It also provides recommendations for implementing Lollipop and Android for Work as part of a BYOD program.



1 "Security Enhancements in Android 5.0" https://source.android.com/devices/tech/security/enhancements/enhancements50.html

Glossary

Android for Work Profile (or Work Profile):
This version of Android for Work can be enabled on devices running Lollipop. The Android for Work Profile offers the most comprehensive set of management options for mixed-use scenarios, including BYOD, choose-your-own-device (CYOD), and more.

Android for Work app:
This is a downloadable app needed to run Android for Work on devices running 4.0 through 4.4. It provides key management options on these pre-Lollipop devices that don't have the Work Profile. (Note: This paper will primarily focus on the Work Profile, but may include some references to the app version of Android for Work as well.)

Work managed device:
This is ideal for corporate-liable deployments, and will be available on all Lollipop devices going forward.

Device policy client (DPC):
The DPC is an EMM app for devices running Android 5.0 with managed profile capabilities. The DPC is normally the MDM agent app, but it could be a separate, special app registered with Google Play and authorized to invoke Android for Work management features on behalf of the EMM's enterprise customers who have registered their domains with Google.

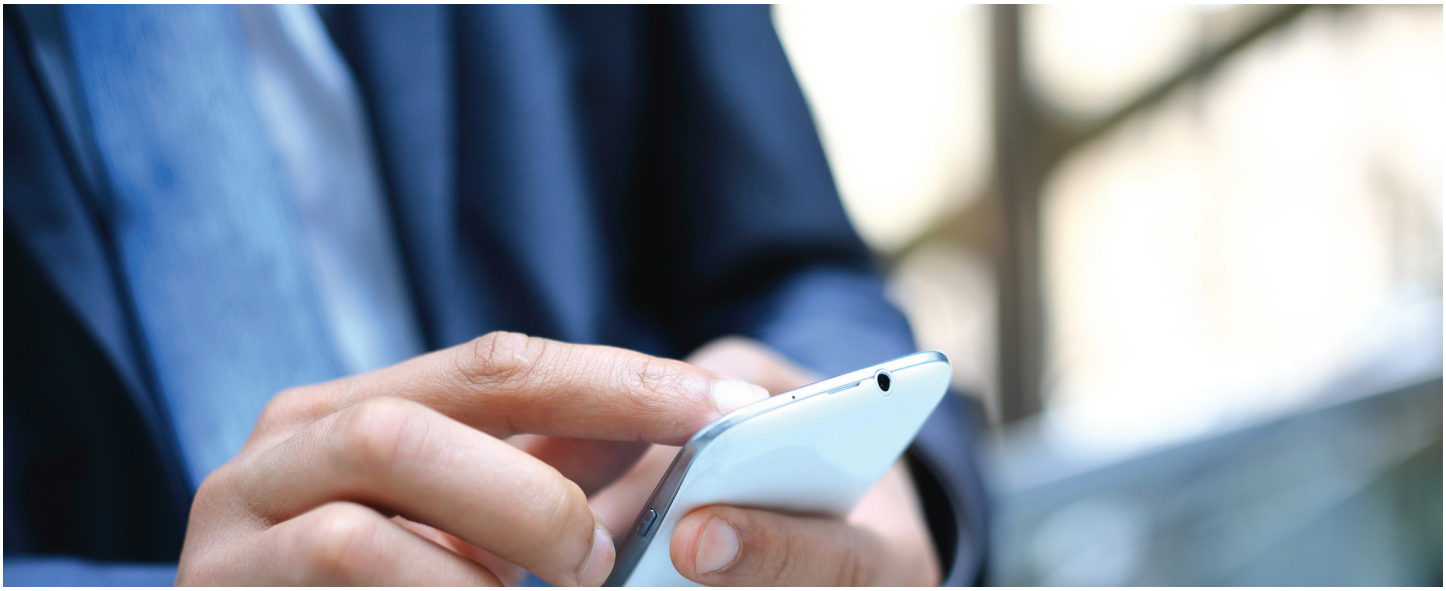
Managed profile:
In a BYOD scenario on Lollipop, the device contains both an Android for Work Profile and a personal profile. The Work Profile is managed by IT, which can wipe the profile while leaving the user's personal apps and data intact on the device. The profile owner is the DPC client on the device that creates and manages the Work Profile.

The Top 8 Android for Work Takeaways

With Lollipop and Android for Work, enterprise IT organizations can:

1. Use Google Play Services to reduce Android fragmentation and security vulnerabilities by delivering critical over-the-air (OTA) security updates to BYOD and corporate-owned devices.
2. Install all apps through Google Play, which prevents users from side-loading apps into the Android for Work Profile from unauthorized sources such as USB storage or file-sharing sites.
3. Silently install business apps and policy configurations on the device, which simplifies IT management and ensures users can't circumvent controls or access configuration information such as license keys or server addresses.
4. Wipe work apps and data from the Android for Work Profile if a personal device falls out of compliance.
5. Simplify the distribution of secure PIM and productivity apps through an EMM provider.
6. Use Google Identity and Google Play Store integration to quickly and easily authorize or revoke access to Android for Work-protected data through the EMM provider.
7. Enable default full disk encryption with Lollipop.
8. Support a range of Android devices running 4.0-5.0, but CISOs will need to research these options in detail to ensure the capabilities address their unique security and compliance requirements.

MobileIron



Introduction

Android has become the dominant mobile platform for consumers around the world. It's no surprise that these mobile users want to access their devices for work as well, and are putting tremendous pressure on IT to support Android. Enterprises with complex security and compliance requirements have been slow to support these user demands. In particular, many organizations in highly regulated industries such as healthcare, retail, public sector, and financial services have concluded that Android is too risky to deploy. Issues such as Android fragmentation and a fear of malicious apps in the Google Play Store have led many companies to put their Android deployments on hold. Given the rapid growth of Android adoption and pressure from end users, however, they can't afford to exclude the platform much longer.

The good news is, Google's introduction of Lollipop and Android for Work will greatly simplify and accelerate Android adoption in the enterprise. To help CISOs understand how Lollipop and Android for Work enhancements will impact their organizations, this white paper includes an overview of security compliance regulations such as HIPAA, HITECH, HIT, NIST SP 800-163, and PCI for mobile transactions. It will also discuss the SANS 20 Critical Security Controls (CSC) and explain how Lollipop and Android for Work can help IT organizations meet some of these recommendations.

Note that Android for Work has two versions: an Android for Work Profile on Lollipop devices and an Android for Work app for devices running 4.x. This paper will primarily focus on the Lollipop Work Profile, with references to the Android for Work app noted where applicable. To learn more about the different versions of Android for Work and how they are deployed, please refer to the MobileIron white paper, "What Android for Work Means for the Enterprise." Organizations should thoroughly research these options to determine how Android for Work can meet their unique security and compliance requirements.

Activating Android for Work

To understand how the security and management features of Android for Work are enabled, it's important to know how IT admins activate Android for Work and add users.

First, the IT admin sets up or "claims" a managed Google domain. The IT admin must go through this one-time web registration process with Google to claim a domain. Once the domain admin account is created and verified, the admin will receive a token to bind to the company's EMM provider. **An EMM provider must be selected before proceeding.** This will enable IT admins to interact with Android for Work primarily through their EMM provider console.

After the IT admin creates the Google domain, the next step is to add and activate users. Note that all users must have a personal and corporate Google account to use Android for Work. In a BYOD case, the user will most likely have a personal Google account already, which will be used to download the device policy client (DPC) from the Google Play Store to the device. (The DPC is an EMM app for devices running Android 5.0.) The DPC is normally the MDM agent app, but it could be a separate, special app registered with Google Play and authorized to invoke Android for Work management features on behalf of the EMM's enterprise customers who have registered their domains with Google.

The IT admin will then create corporate Google accounts for all Android for Work users and add them to the Google directory. Once this setup process is complete, the admin can configure the Android for Work profile.

This new deployment process is a much-needed security improvement because users must first be enabled by the IT admin, and then they can only choose from secure apps that IT has configured for them. Users cannot download unapproved third-party apps to the Android for Work Profile. The new process also prevents users from side-loading apps from USB storage, the Android Debug Bridge, or unauthorized file-sharing sites into the Work Profile (although apps can still be side-loaded into the personal profile on BYOD devices). And, if an app from the Google Play Store is determined to be a threat, the IT admin can quickly unauthorize the app and execute a silent uninstall.

Now that we've provided a quick overview of Lollipop and Android for Work, let's look at how they can help CISOs ensure BYOD and corporate-owned devices comply with security regulations and guidelines.

Security Regulations

Although IT organizations must comply with various regulations all over the world, this white paper will primarily focus on U.S. regulations such as HIPAA, HITECH, and HIT along with a recent NIST Special Publication 800-163 regarding mobile app security vetting. We will examine how these regulations and guidelines can be supported by some of the improved security capabilities in Lollipop and Android for Work.

HIPAA, HITECH, and HIT

When it comes to adopting new technology, the healthcare industry runs the gamut from early adopters to latecomers. All of these organizations, however, are subject to complex regulations and the challenges of protecting data at rest, in use, and while in motion.

To help U.S.-based healthcare companies meet compliance requirements, HealthIT.gov provides recommendations for protecting and securing mobile devices. Below is a summary of the recommendations and how Lollipop and Android for Work can support them:

Recommendation #1:
Install and enable security software

With Android for Work, Google addresses the problem of Android-targeted malware by requiring IT to set up a managed Google domain in the Google Identity service. This process enables IT to approve and enable apps through the Google Play Store. It also enhances security by blocking employees from installing apps through their personal Google account, because only IT-approved apps are allowed in the Android for Work Profile. The Google Identity service also enables enterprise binding, which allows an IT admin to verify the ownership of a Google domain using one of three options:

- Add a meta tag
- Add a TXT or CNAME record to your DNS records
- Add an HTML file to your website root

By requiring an EMM provider to deploy and manage Android for Work, Google has taken a major step toward building a trust model between the user and the organization.

By requiring an EMM provider to deploy and manage Android for Work, Google has taken a major step toward building a trust model between the user and the organization. Although users may still inadvertently download malware to the device, it will only infect the device owner's personal profile. Data and apps inside the Android for Work Profile remain completely separate and protected.

Recommendation #2:

Delete all stored health information before discarding or reusing the mobile device.

Android for Work enables the EMM to easily retire lost or stolen devices and remotely wipe all work data while leaving personal content intact on the device.

Device retirement or unprovisioning is a general IT responsibility, but organizations need the ability to retire devices while leaving personal apps and data untouched. Through the DPC, Android for Work enables the EMM to easily retire lost or stolen devices and remotely wipe all work data while leaving personal content intact on the device. With corporate-owned devices, IT has total device-wide controls, which include a full device wipe if necessary.

Recommendation #3:

Research mobile apps before downloading.

Android for Work requires IT admins to approve app permissions as part of the app authorization process. As part of this process they should double-check to be sure those permissions make sense based on the app's functionality, as well as how those permissions might impact data contained on the device or within other apps.

Recommendation #4:

Keep your security software up to date.

Lollipop provides several new capabilities to help reduce hardware fragmentation among carriers and OEMs. Google Play Services enables OTA updates to devices to help ensure OS upgrades and security patches are delivered more consistently. With Lollipop, organizations can also secure data at rest with out-of-the-box, block-level encryption.

In addition, data moving between authorized apps within the Android for Work Profile remains encrypted during use. For example, a slide can be copied from Google Slides and pasted into the badged, Android for Work email app. Because Android for Work apps are inherently protected by the container and consistently updated by IT, overall device security is increased.

NIST -> FISMA

Although this paper won't be able to discuss all active Federal Information Security Management Act (FISMA) regulations, we will cover one of the most relevant to Android for Work. In January 2015, The National Institute of Standards and Technology (NIST) released Special Publication 800-163, "Vetting the Security of Mobile Applications."[2] This document addresses the need for mobile app security within organizations that either develop their own in-house apps or purchase apps from a third party.

The new app deployment process in Android for Work supports the mobile app security guidelines outlined in this document. To start, Google has introduced a whole new set of Google Play APIs for EMM providers to enable app management and distribution. EMM providers are the only mechanism for app deployment in Android for Work. This means apps cannot be side-loaded into the native client, which adds greater protection from malicious apps. For IT organizations, this enables three key benefits:

1. **New secure installation process**
   By allowing apps to be distributed exclusively through EMM providers using the Google Play Store APIs, Android for Work introduces a new installation process that prevents apps from being installed from unknown sources outside the container, such as Dropbox and other file-sharing sites.
2. **Separation of personal and business content on the device**
   The Android for Work Profile protects business apps and data from the user's personal activity outside the Work Profile, such as side-loading web apps, ordering from unknown websites, and other potentially insecure activity.
3. **Exceptions for self-hosted apps**
   Organizations concerned about security for their private, in-house apps can choose to self-host these apps either internally or through their EMM provider. Either way, self-hosted apps can be excluded from public search results in the Google Play Store.

Android for Work introduces a new installation process that prevents apps from being installed from unknown sources outside the Work Profile, such as Dropbox and other file-sharing sites.

This new process, combined with the Android for Work Profile, enables IT managers to deploy any Play app in the Google Play Store to a secure Android container without any additional wrapping. This offers tremendous advantages to both IT and end users. IT can ensure apps and data can be safely enabled in a secure, separate container on the device, and users have the flexibility to choose from a pool of secure apps that IT has pre-selected.

2 S. Quirolgico, J. Voas, T. Karygiannis, C. Michael, and K. Scarfone, "Vetting the Security of Mobile Applications." National Institute of Standards and Technology, January, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf

PCI Mobile Payment Acceptance Security Guidelines 1.1

The PCI Security Standards Council (PCI SSC) published recommendations for mobile devices titled, "PCI Mobile Payment Acceptance Security Guidelines for Developers."[3] This document is intended for organizations that use smartphones and other mobile devices to process payment transactions. It specifically addresses security requirements for these payments when plaintext data may also be stored locally on the device. The guidelines also address security requirements for the cardholder data environment (CDE) on mobile devices.

In the section below, we will map Section 4, "Guidelines for the Risk and Controls in the Supporting Environment" of the PCI SSC publication to new features in Lollipop and Android for Work. Section 4 of the document applies specifically to platform integrity and the application environment.

Subsection 4.1 requires device access and USB debugging controls, and full disk encryption.

Lollipop and Android for Work support these recommendations by requiring the device to be encrypted before a managed profile can be enabled on the device. The Android for Work client app running on pre-Lollipop operating systems will encrypt the protected data within a database. If devices upgrading to Lollipop do not have storage encryption enabled, the device will remain in plaintext post-upgrade.

Device access controls are typically supported by most EMMs, but Lollipop has introduced an additional feature called Smart Lock. Smart Lock is ideal for users who don't want to type in a passcode several times a day. It allows a phone or tablet to be unlocked by pairing it with a trusted Android Wear device, Android Auto, or other Bluetooth and NFC devices. When the phone or tablet is close enough to the paired device, users can unlock the smartphone, similar to unlocking a car with keyless entry. Smart Lock also offers a facial unlock capability, which was originally introduced in Android 4.0.

It's important to note that Smart Lock integrates with technologies known to have security weaknesses, so organizations will need to determine if this capability is appropriate for their security and compliance environment.

Subsection 4.6 requires the use of hardened systems.

SELinux has been the underlying operating system for Android since version 4.3. Starting with Lollipop, SELinux uses scrypt to protect against brute-force attacks and, if available, binds the key to the hardware keystore. SELinux on Android is in enforcing mode for all domains. The Android sandbox also uses a mandatory access control (MAC) system to enhance the discretionary access control (DAC) security model

3 Emerging Technologies, PCI Mobile Payment Acceptance Security Guidelines for Developers, PCI Security Standards Council, July 2014. https://www.pcisecuritystandards.org/documents/Mobile%20Payment%20Acceptance%20Security%20Guidelines%20for%20Developers%20v1%201%20.pdf

already available in SELinux. Although these are not all the factors required to fully harden a system, they provide improved protection.

Subsection 4.9 requires the protection from properly disclosed vulnerabilities.

Lollipop supports this requirement by providing automated, critical OS updates over the air. With Lollipop, Google has unbundled, or separated, many core components from the OS and moved them into the Google Play Store and Google Play Services. With this upgrade, Google can now ensure that important OS changes are distributed consistently as OTA updates instead of relying on the carriers and OEMs to deliver them.

> *OTA updates in Lollipop, which are designed to increase OS consistency across more devices, have been described as Google's "best weapon in the war on fragmentation."*

For example, Lollipop unbundled WebView so it can be upgraded separately from the OS. This will help Google ensure users receive important security updates as well as make new features and APIs available to developers of applications that rely on WebView. This move, which is designed to increase OS consistency across more end-user devices, has been described as Google's "best weapon in the war on fragmentation."[4] Overall, this will help ensure OS consistency across Android devices and eliminate patching fragmentation due to OEM and carrier delays.

Subsection 4.10 requires secure distribution of installed apps to come from a trusted source.

In Android for Work, all apps deployed to the Work Profile must come from an EMM provider that has integrated with Google Identity services. Also, Android for Work includes a `setApplicationRestrictions` API that allows the IT admin to configure the settings for a particular application. When Android for Work is configured, the app settings are pushed to the device. App wrapping is no longer required, except in the Android for Work app on pre-Lollipop devices. A single binary is used for both personal and business apps, but their data is kept completely separate at the profile level.

Subsection 4.11 requires anti-malware protection on the mobile device.

Insecure activity outside the Work Profile, such as side-loading apps, is a common end-user mistake that can result in device infection. Android for Work helps block malicious downloads by preventing users from installing apps from untrusted sources into the Work Profile. Instead, users can install apps that have been pre-selected by IT in the Google Play Store, which puts the responsibility for app security on IT admins.

4 Amadeo, Ron. "Unwrapping Lollipop: Ars talks to Android execs about the upcoming OS." Oct. 27, 2014. http://arstechnica.com/gadgets/2014/10/unwrapping-lollipop-ars-talks-to-android-execs-about-the-upcoming-os/

SANS 20 Critical Security Controls (CSC) for Effective Cyber Defense

20 Critical Security Controls for Effective Cyber Defense

1	Inventory or Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware & Software on Laptops, Workstations and Servers
4	Continuous Vulnerability Assesment and Remediation
5	Malware Defenses
6	Application Software Security
7	Wireless Device Control
8	Data Recovery Capability
9	Security Skills Assesment and Appropriate Traning to Fill Gaps
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11	Limitation and Control of Network Ports, Protocols, and Services
12	Controlled Administrative Privileges
13	Boundary Defense
14	Maintenance, Monitoring, and Analysis of Security Audit Logs
15	Controlled Access Based on the Need to Know
16	Account Monitoring and Control
17	Data Loss Prevention
18	Incident Response Management
19	Secure Network Engineering
20	Penetration Tests and Red Team Excercises

The SANS Institute, which develops, maintains, and distributes the largest collection of research documents about various aspects of information security, also publishes The SANS 20 Critical Security Controls (CSC) for Effective Cyber Defense. This publication offers guidelines that address practical IT and IS processes and procedures to help organizations establish and test a strong enterprise security posture.[5] In this section, we'll map Android for Work security capabilities to the SANS Top 20 CSC to see how they compare.

5 Critical Security Controls for Effective Cyber Defense - Version 5. SANS https://www.sans.org/critical-security-controls/

Mapping SANS 20 CSC to Android for Work on Lollipop

Inventory of Authorized and Unauthorized Devices

CSC 1-3 recommends ensuring that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
New APIs introduced with Lollipop and Android for Work can help organizations maintain better device tracking, which is a common problem when provisioning devices for BYOD programs.

Lollipop addresses this CSC recommendation by including APIs for managed provisioning. This allows the device to have only one owner — the user or the company — and the user is not allowed to change device ownership. During the managed provisioning process, the intent known as `ACTION_PROVISION_MANAGED_PROFILE` is called. If the user has a preexisting personal account, the managed profile is separate, but copresent. Upon successful provisioning, the EMM calls `setProfileEnabled()` to activate the managed profile. All apps associated with the managed profile appear alongside the non-managed app in the Launcher, Recents screen, and notifications, but are separate.

In a BYOD scenario, the device contains both an Android for Work managed profile and a personal profile. IT only manages the Android for Work Profile, and can wipe it if necessary. All the user's personal apps and data remain intact. If the provisioning fails because device-level encryption hasn't been activated, for example, the managed profile is removed and the device returns to the original state controlled by the user. A possible reason for encryption failing would be an older version of Android upgraded to Lollipop where the device storage was in plaintext. For unencrypted Lollipop devices, the user will be prompted to encrypt the device when the system is rebooted. For pre-Lollipop operating systems using the Android for Work app, the protected data will be stored in an encrypted database.

Inventory of Authorized and Unauthorized Software

- **CSC 2-1 recommends that enterprises deploy application whitelisting technology that allows systems to run software only if it is included in the whitelist and prevents execution of all other software on the system.**
  Android for Work requires apps to be provisioned through the Google Play Store and administered through the EMM provider, which automatically provides application whitelisting because only apps approved by IT can be downloaded to the Android for Work Profile.

- **CSC 2-2 requires a list of authorized apps for Android devices.**
  The apps are expected to be monitored for file integrity checks to ensure there has been no tampering. Although the Google Play Store has validation checks to detect malicious apps, these checks cannot fully guarantee against malware. To provide an added control measure, the authorized apps in the Android for Work Profile are centrally controlled via EMM integration. This enables the IT admin to quickly revoke user access to risky apps along with the associated data. Integration with third-party services and automated compliance actions can further enhance protection.

Android for Work requires apps to be provisioned through the Google Play Store and administered through the EMM provider, which automatically provides application whitelisting because only apps approved by IT can be downloaded to the Android for Work Profile.

- **CSC 2-4 requires the utilization of deployment software tools that track the operating system version, installed software including version number, and patch level.**
  Patch levels are irrelevant to Android apps because, generally speaking, patched apps receive a new version number. Together the EMM API enhancements and Google Play Store meet this requirement.

Secure Configurations for Hardware and Software on Android Devices

Although this security control is intended for laptops, workstations, and servers, this white paper will only refer to Android devices.

- **CSC 3-2 requires the implementation of patching tools for both applications and operating systems.**
  This control is satisfied through OTA updates to devices through Google Play Services.

- **CSC 3-3 requires the limitation of the administrative privileges and restricting other administrative abuses.**
  When Android for Work is installed, a new user is created in SELinux specifically for Android for Work data access.

Continuous Vulnerability Assessment and Remediation

- **CSC 4-5 requires the deployment of automated patch management tools for the operating system and software.**
  Lollipop enables critical OS-level patching with OTA updates through Google Play Services. This is a great advantage for developers who have been juggling multiple versions of their apps on end-user devices. Automatic updates through Google Play Services should help greatly reduce or even eliminate OEM and carrier fragmentation and simplify regulatory compliance efforts.

Malware Defenses

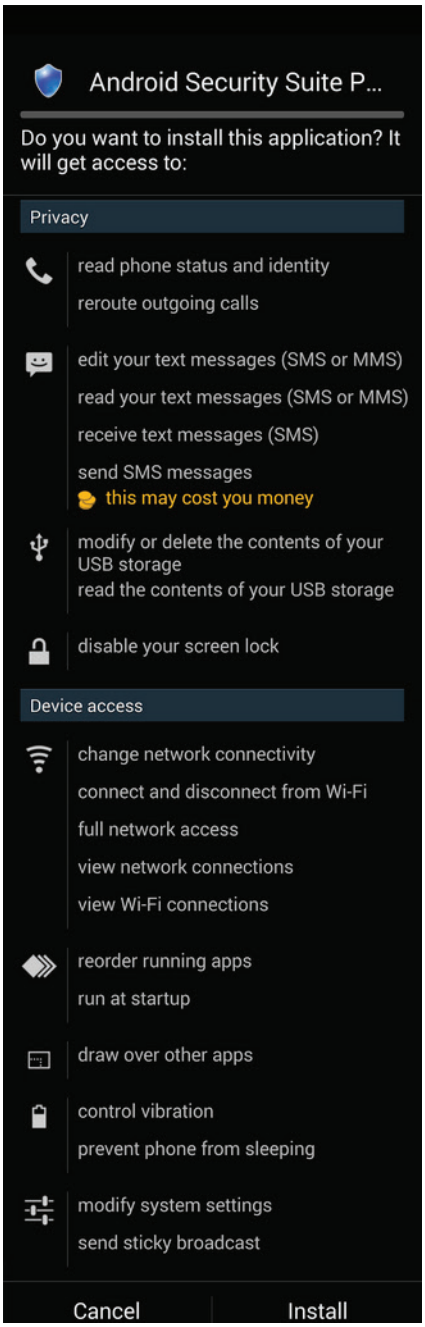
- **CSC 5-7 recommends that organizations limit the use of external devices to those that have a business need.**
  On Android, there isn't a feature that directly supports this recommendation, but it does restrict mobile app side-loading. For example, users frequently install applications on Android using an SD card or the app of a cloud storage provider. Android for Work prevents this type of insecure activity by restricting app installation from untrusted sources.

  An additional step in the authorization of a new app is for the IT admin to view the `<uses-permission>` element found in the AndroidManifest.xml file. Permissions can be defined by other applications or be a system permission such as "`android.permission.INTERNET`" or "`android.permission.ACCESS_NETWORK_STATE.`" This is important because the decision to accept element requests are presented to the IT admin and not the end user. Malware installed from side-loading is a common mistake end users make because they don't understand all of the permission requests. By putting more security controls in the hands of IT, Lollipop and Android for Work make it easier to protect corporate data and apps and achieve compliance.

Boundary Defense

The line between business and work use on mobile devices is increasingly blurry, which is why security boundaries must be well defined but invisible to the end user. Although SANS doesn't have a current CSC for boundary defenses on mobile platforms, Android for Work does allow business and personal data and apps to be separated at the OS level. IT can also selectively wipe business data if the device falls out of compliance.

Authorized business apps that interact with containerized data can only be provisioned by the EMM.



Android malware use-permission requests

This is an example of Android mobile malware requesting permissions during installation. This type of attack usually requests access to a long list features such as the ability to receive, read, edit, and send SMS or MMS transmissions. Android for Work on Lollipop reduces the risk of this type of attack because apps can only be deployed to the Work Profile after the IT admin verifies the permission request on behalf of the users through the EMM console.

Controlled Access Based on Need to Know

Controlling access to data on mainframes, servers, NAS, cloud storage, etc. has traditionally been managed using Access Control Lists (ACLs). When data lands on the mobile device, the ACLs are abandoned and can result in unintentional data leakage. This critical security control requires the use of processes and tools to minimize the risks.

- **CSC 15-5 recommends using on-device data loss prevention (DLP) to emulate remote storage access permissions.**
  Android for Work helps prevent intentional or accidental data loss because the ability for the user to share into and outside of the Android for Work Profile is managed by EMM governance policies. This includes the ability to block copy/paste or block screen capture for apps inside the managed profile. (Note that copy/paste can be disallowed from the managed profile to the personal profile, but not vice versa.)

Account Monitoring and Control

The inability to control network access for former employees, contractors, attackers, and other unauthorized users is a common problem for many enterprises. This challenge has been addressed with the use of directory services to control OS-level account access and disablement for PCs, Macs, and Linux systems. By requiring integration with an EMM provider, Android for Work helps minimize the challenges of controlling access to mobile devices.

- **CSC 16-12 requires centralized authentication.**
  Android for Work requires organizations to use Google Identity for EMM integration. The current LDAP or Active Directory accounts can be mapped to Google Identity accounts after the Google domain has been created and verified and the generated token is bound to the EMM provider. If token verification is successful then the enterprise is ready to implement Android for Work.

- **CSC 16-15 mandates authenticated web services access via an encrypted channel.**
  Android Lollipop uses HTTPS for transport layer security (TLS) to Google Identity services. For additional details about the TLS versions used for HTTPS on Lollipop, please refer to CSC 17-7.

Data Protection

SANS defines data protection as "the processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information." In this section we'll cover how Lollipop and Android for Work support those controls.

Examples of Data Exfiltration Egress

- Malware using email
- Malware using FTP drop sites
- Malware using SMS and MMS
- USB to a rooted Android that's unencrypted
- USB to Android Debug Bridge enabled
- NFC
- Bluetooth
- WiFi Man-in-the-Middle (MitM) attacks
- WiFi Direct
- Android IMSI Catcher
- Infrared

- **CSC 17-1 recommends that organizations deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.**
  Lollipop supports this recommendation because its underlying operating system, SELinux, provides its own storage-level encryption. This means that the core operating system, account database, apps, and data are always safe from data-at-rest attacks.

> *The Android for Work app provides its own encryption layer independent of SELinux.*

- **CSC 17-2 requires the use of cryptography to use publicly vetted algorithms.**
  Lollipop's underlying operating system, SELinux, is protected at the storage block-level. It uses `dm-crypt` for default encryption with a key generated from the AES 128-bit with Cipher Block Chaining (CBC) and ESSIV:SHA256 algorithms. For more details about how the master key is created and stored, please refer to the Android encryption documentation.

- **CSC 17-7 requires any data in motion to be encrypted and authenticated.**
  HTTPS socket connections from Android Lollipop now utilize SSL/TLS 1.2 and TLS 1.1 with AES-GCM enabled, with Forward Secrecy preferred and disabled weak ciphers such as MD5, 3DES, and export cipher suites. For additional details on how Lollipop has implemented HTTPS, please refer to the SSLSocket documentation.

- **CSC 17-11 requires an annual review of algorithms and key lengths in use for protection of sensitive data.**
  This security control can easily be achieved with an annual review of the Lollipop update documentation to the algorithms and key lengths used for encryption and key storage, if applicable.

- **CSC 17-13 is aimed at stopping exfiltration by blocking known file drop and email sites.**
  By default, corporate-owned devices using Android for Work will only permit authorized apps to be installed in the sandbox. Side-loading of apps that may exfiltrate data through drop sites are blocked. Apps within the Android for Work Profile are able to share data with each other because they will be pre-approved by the IT admin. From a mobility standpoint, it's difficult to fully comply with CSC 17-13 without the use of additional third-party tools. This is important to keep in mind for enterprises seeking absolute compliance versus best-effort compliance.

- **CSC 17-15 suggests the encryption implementation use a Hardware Security Module (HSM) or Key Encryption Keys (KEK) to protect the private keys.**
  For details about how the master key KEK is generated and layered with additional ciphers, please refer to the Android encryption documentation.

Recommendations

Achieving compliance is challenging enough without the adding the security complexity of a BYOD program. Organizations can address both of these challenges by considering the following recommendations for implementing Lollipop and Android for Work:

1. **Create an Android for Work pilot program for business unit leaders.**
   A pilot program that includes executives and other "power users" can help you determine if the Android for Work experience is as smooth as the native experience. By gathering critical feedback from a small but dedicated user group, you can refine your deployment to ensure a seamless user experience across the larger enterprise. Ultimately, the success of your program depends on delivering a native-like device experience that supports compliance without forcing users to jump through security hoops.
2. **Mobile device management alone does not provide complete control.**
   Although device management is a key component of an overall mobile security strategy, you will also need to include application and content management as part of a holistic mobile management approach.
3. **Map compliance objectives to user requests.**
   Find out which devices your employees use the most, and which business processes they want enabled for mobile. Then determine how your EMM platform, together with the capabilities of Lollipop and Android for Work, can securely enable them while meeting compliance goals.

Conclusion

Companies in high-security industries face the complex challenge of supporting a broad range of Android devices without compromising security or compliance efforts. With Lollipop and Android for Work, Google has introduced a set of capabilities that can help organizations achieve these objectives much more quickly and easily:

Lollipop tackles the issue of Android security and fragmentation head-on. It includes key security upgrades such as default encryption, increased protection against brute-force attacks, secure device-sharing features, and SELinux enforcing mode. Google is also taking more control over updates to the Android OS. Instead of relying on OEMs and carriers to issue OS updates, Google will distribute critical updates directly to users through the Google Play Store and Google Play Services. By automatically delivering critical security patches and OS updates, Google not only ensures users get the latest updates faster, it increases Android security and reduces fragmentation by enabling OS consistency across more devices.

Android for Work is a major effort to deliver a deeper and more consistent security model to enterprise customers. Android for Work is not just a product, it's a complete Google program that enables secure, containerized app deployment to a range of Android devices through an ecosystem of EMM providers. With this new offering, IT gains a more consistent and unified way to securely manage enterprise apps as well as the ability to separate work and personal data on every managed device.

The new security enhancements in Lollipop, combined with secure app distribution and IT management capabilities in Android for Work, should help position Android as a strong mobile platform for the enterprise.

For More Information

Learn more about Lollipop and Android for Work by visiting http://www.mobileiron.com/android.

For questions regarding your Android implementation, please contact us at globalsales@mobileiron.com.