IT@Intel White Paper

Intel IT
IT Best Practices
Information Security and IT Consumerization
October 2013

Android* Devices in a BYOD Environment

Intel IT found that we can add Android*-based devices to our enterprise network in a secure, timely way by adapting the same BYOD best practices that we developed for other devices.

Rob Evered
Senior Information Security Specialist, Intel IT

Steve Watson
Technical Solutions Engineer, eDiscovery, Intel IT

Paul Dockter
Privacy Engineer, Intel Security and Privacy Office

Derek Harkin
Mobility Engineer, Intel IT

Executive Overview

While the diversity of devices running the Google Android* OS can present challenges, Intel IT found that we can add them to our enterprise network in a secure, timely way. We adapted the same bring-your-own-device (BYOD) best practices developed for other devices to meet Intel's security and eDiscovery requirements and privacy policies.

There are more than 20,000 Android-based devices, encompassing over 800 combinations of Android OS versions and hardware, in Intel's BYOD program. We enable employees to work on Android devices because the OS is a powerful platform for developing innovative devices and applications. As with other BYO devices, we had to meet certain requirements:

- Support a range of Android devices while keeping enterprise data secure and meeting our eDiscovery criteria
- Develop security criteria for Android devices for use in our BYOD "trust score" algorithm
- Determine the level of enterprise network access appropriate for each Android device model
- Provide employees with options that can enhance a device's security if it does not qualify for the requested level of access
- Inform employees of how the data on their devices will be secured, who has access to it, and under what circumstances

By improving our workflow and device analysis, we have reduced the time it takes to approve a new Android device to approximately one hour. Allowing Android devices to access our enterprise network increases employees' flexibility to choose devices that fit their needs and improve their productivity. In a recent survey, BYOD program participants reported an average time savings of 57 minutes per day.[1]

We also discovered that, in general, the same best practices that we developed for eDiscovery on other devices apply to Android devices as well.

[1] 2012-2013 Intel IT Performance Report

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel IT continues to expand and strengthen our bring-your-own-device (BYOD) program offerings. As the variety of devices increases, so does our challenge to maintain security and eDiscovery while protecting employees' privacy, their data, and the enterprise. Google Android*-based devices add a level of complexity because we manage more than 20,000 devices encompassing over 800 combinations of Android OS versions and hardware.

The Android devices we manage include more variety than smartphones and tablets. Our employees have registered televisions, watches, glasses, and other Android devices in our BYOD program to access enterprise data. It is important to our culture of innovation that employees be able to use their devices of choice.

Security

There are many security complexities involved in the use of Android devices in the enterprise. For example, the same open qualities that make Android such a powerful OS for innovation and creativity also make it more vulnerable to malware.[2] Google, Android-based device manufacturers, and Intel are working to enhance Android security by adding management tools, segregating corporate and personal environments, and making the enterprise enrollment easier. Intel IT developed methods to meet our security requirements while waiting for these enhancements to come to market.

eDiscovery

In addition to achieving our security goals, we also need to make sure we can retrieve data from Android devices when legally required for eDiscovery and other requests. The numerous combinations of Android OS and hardware require us to work at the device level instead of the Android OS version level.

In certain circumstances, legal obligations may require all the data on the device to be submitted for inspection, not just data residing in the device's secure corporate-managed container. This requirement applies to BYO devices used for business purposes as well as to corporate-owned devices. We encountered many of the same inspection challenges with Android devices as we do with other devices. For example, mobile forensics application developers often do not know how to retrieve data from the device until it is in the market and they can test the new model for data retrieval. However by then employees are already potentially mixing personal and corporate data when taking pictures, texting, sending personal emails, and accessing enterprise data and applications.

Intel IT developed an approach for managing Android devices in the enterprise that incorporates our best-known methods of security and eDiscovery, while taking into consideration the employee's privacy and the ability to separate corporate information from employee-owned personal data on a particular device.

SOLUTION

Intel IT manages Android devices in the enterprise with a comprehensive security evaluation process that is applied to every personal device an employee wants to use for work purposes. Forensic evaluations on employees' devices are done only when required for an active investigation or legal matter. Respecting employee privacy is a priority across the entire lifecycle—from device onboarding and provisioning, to how data is managed and retained, including how we respond to an eDiscovery request.

[2] Juniper Networks, "Juniper Networks Finds Mobile Threats Continue Rampant Growth as Attackers Become More Entrepreneurial." http://newsroom.juniper.net/press-releases/juniper-networks-finds-mobile-threats-continue-ram-nyse-jnpr-1029552

Establishing a Trust Score

When an employee starts the process of registering a BYO device on the corporate network, our mobile device management (MDM) system determines if this particular model has already been evaluated. If so, the trust level granted to the device depends on the services the employee requests (see Figure 1). If the device model and Android OS version combination is being connected to the network for the first time, we first need to establish a "trust score" for the device.

We developed the process for establishing a trust score with the following objectives in mind:

- Intel's data must be protected to the appropriate level depending on where the user and device are located and the services being requested.[3]
- Android devices must be provided as one of many choices available to employees.
- The process must be user-friendly, productive, and easy for employees to understand.

When devices are registered on our MDM system, the device trust score is automatically calculated based on a number of device details, such as OS version, device model, and manufacturer. We also check to see whether the user has modified Android on the device (for example, by using the rooting process) and check the installed applications on the device for known malicious applications. For Android devices older than 4.2.2, we lower the trust score if developer mode (also called USB debugging) is enabled. For all devices, the trust score is based upon assessment of the device details as well as several security and eDiscovery criteria (see Table 1 for example criteria).

All devices connect to the MDM server on a scheduled basis providing information about possible security events. If the MDM detects a security issue, the trust score of the device may be downgraded.

Table 1. Sample Security and eDiscovery Criteria to Assess the Risk of a Bring-Your-Own Device

Sample Risk Categories	Sample Criteria
Intel data can be exposed if hardware is stolen	What is the device's encryption in storage quality? Does the user need to enter a password for access to the application or site? Can the device withstand a brute force attack on user authentication?
Intel infrastructure risk	Can the device store an authenticator, such as a certificate, in a secure fashion?
Legal or regulatory exposure	Can personal and company data be kept separate?
Malware or hacker targeting Intel data	Is the device's intrusion detection active?
Unauthorized use	Do we have remote delete capabilities if the device is lost?

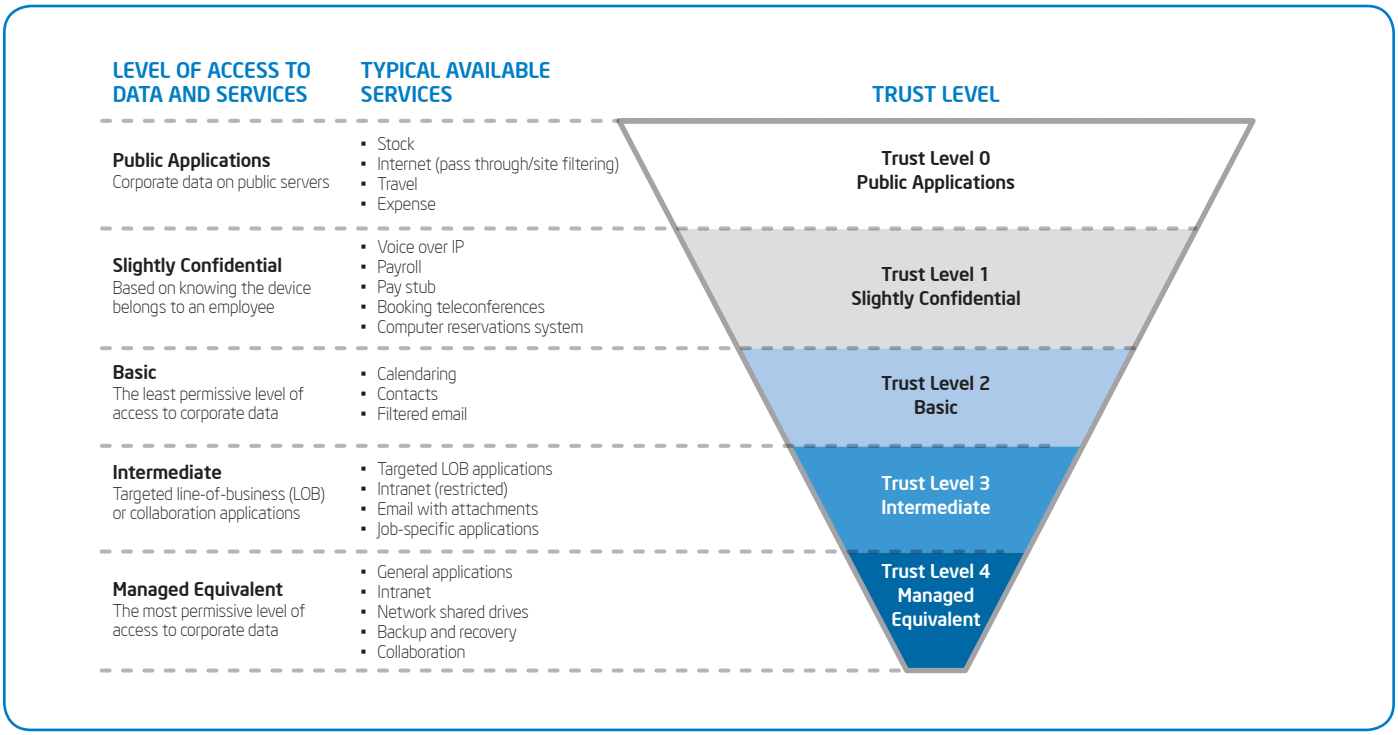

Figure 1. Like other bring-your-own devices, every Google Android*-based device that connects to the corporate network receives a trust score, which then determines the trust level and corresponding services that the employee can access.

Below are examples of how we might score the criteria in the risk category "Intel data can be exposed if hardware is stolen":

- **What is the device's encryption in storage quality?** A device with no encryption earns a score of zero. If encryption is less than 40-bit, it earns a score of one; less than 100-bit earns a score of two; and two-plus industrial strength, including secure key store, earns a score of three.
- **Does the user need to enter a password to access the application or site?** A device with a weak password policy earns a score of one. If it has a strong password policy and enables a one-time password, it earns a score of two.
- **Can the device withstand a brute force attack on user authentication?** A device that locks after a set number of attempts earns a score of one. If the device hardware can slow down a brute force attack, it earns a score of two. If 10 wrong password attempts automatically delete all the data on the device, it earns a score of three.

Today, much of the scoring is automated, especially for new device models. For these new models, we create a profile, which is accessed the next time the model is registered. This approach streamlines the assessment process.

TRUST LEVELS

After we score all the criteria—either automatically or manually—we use an algorithm to determine the "trust level" of services accessible by a certain device. We map the trust score to one of five trust levels. Each trust level provides access to certain services. The number of available services increases at higher trust levels. Figure 1 shows the five trust levels and a sample of what the user can access at each level.

AN INTERMEDIATE TRUST SCORE FOR ALL DEVICES

Our goal is to enable every device to be trustworthy enough for "intermediate" services (trust level 3), including email, calendaring, and the ability to book travel and teleconferences. We also have a goal that intermediate services deliver approximately 80 percent of the data and services that employees can access with a corporate-managed laptop or desktop. This is our best alignment of security, user experience, and access to useful data at an acceptable management cost.

To help employees meet trust level 3 access with their Android device, we employ the following steps:

- We communicate which devices have already been cleared for trust level three or higher access. Employees who use these Android devices have the benefit of the native experience without any additional security measures other than the security policies enforced by our MDM system.
- We implement security policies that enable the device features we require to achieve trust level 3. For example, password-protection is one of the minimum standards we use to minimize risk. We may need to enable the device's password-protection feature while blocking the employee's ability to turn the feature off.
- If an Android device receives a trust score that is too low for intermediate services, we can install a secure container on many user devices. This container enables Android devices that are not inherently secure enough to access services such as enterprise email. For example, the Android OS used in a television does not include the security requirements necessary for secure email access. When an employee wants to access email on an Android television, we can enable that service with a secure container.
- In situations where we are unable to deploy a secure container, we can provide view-only access to services.

ANDROID 4.0 AND HIGHER

Intel IT considers versions prior to Android 4.0 to be insecure platforms for the Intel environment. Therefore, for those earlier versions we can store data on the device using only a secure container. However, Android 4.0 and higher versions meet our key security requirements of encryption, secure credential storage, authentication, passwords, and MDM capabilities. The newest Android OS versions also meet our interface requirement, so if the employee chooses to allow us to manage the device, we can deploy applications that provide a native experience. If the user does not allow us to manage the device, we won't know its Android OS version and must default to treating that device as insecure.

Security with Android 4.0

We consider most devices running Android 4.0 or higher likely to be secure enough to access intermediate enterprise data (trust level 3) without additional software beyond basic MDM. However, managing Android devices is an ongoing process that must keep up with new patches and vulnerabilities.

As mentioned earlier, each new Android OS version is usually more secure at release than when it appears on a device because the manufacturers and service carriers adapt the OS to their devices. When patches are available for an Android OS version, it is up to the manufacturer or carrier to upgrade those patches. Some are better at staying on top of upgrades than others. We track the manufacturers and carriers that upgrade patches in compliance with our security requirements. We then notify employees when they register on the enterprise network that if their device manufacturer is known to lag on patching, some services may not be accessible. We can provide employees with resources to check on how well their devices are patched.

Intel IT considers newer Android OS versions to be robust and secure enough to enable access to all data except for data classified to the highest level.

Another major challenge with Android versions earlier than 4.2.2 is the developer mode. This mode enables developers to test new applications. However, it circumvents all encryption. But if the user has a device

Table 2. Key Security Features of Google Android* 4.0 and Higher

FEATURE	BENEFIT
Encryption	The newer Android OS versions (4.0 and higher) meet our encryption requirements including 128-bit Advanced Encryption Standard (AES) and full disk encryption (master key is also encrypted with 128-bit AES). A password is required to boot the device, and the file system is mounted on boot. After boot, a password is required to access the device.
Credential Storage	Secure credential storage requirements are met because access is now controlled through the lock screen PIN. The keychain encryption key is derived from the PIN using the PBKDF2 key-derivation function. Accessing private keys does require the employee to unlock the credential storage. With Android 4.3 this credential storage can now be in hardware.
Authentication	For authentication, Android 4.0 and higher versions include an email application that supports two-factor authentication to allow client certificate authentication for Microsoft Exchange Server* accounts. In the browser, if the server requests a certificate authentication, it uses two-factor authentication to prompt the employee for a client certificate.
Passwords	Password policies in Android 4.0 and higher meet our requirements for length, complexity, and aging.
Mobile Data Management (MDM)	Using an MDM client on Android 4.0 and higher OS versions meets most of our policy requirements, including policy enforcements, application deployment and control, debug mode detection, and making policy decisions based on rooted status.
Secure Interface	As of Android 4.2.2, the introduction of a secure developer mode (also called USB debugging) meets our minimum requirements for device interface security. A secure developer mode ensures that only computers authorized by the user can access a USB-connected Android device over the Android Debug Bridge (ADB). This addresses the potential for bypassing the password lock and encryption.

running Android 4.2.2's more secure developer mode, the risk is significantly reduced.

Any measures we take to secure an Android device, such as password protection, encryption, deploying software, or installing a secure container, are intended strictly to limit the risk to corporate information. We try not to impact the way employees interact with their own data.[3] To help clarify responsibilities, the privacy impacts are available on the registration system as well as detailed in a service agreement, which employees execute when they register the device.

Forensics Examination of Android-based Devices

Respecting employee privacy is a priority across the entire lifecycle—from device onboarding and provisioning, to how data is managed and retained, including how we respond to eDiscovery requests. To prepare for an eDiscovery request, Intel IT evaluates new Android devices using the same processes developed for other BYO devices.

Before performing any forensics examination of the device, we clarify the information requested by the legal or investigatory team. Our first choice, whenever possible, is to retrieve the information elsewhere, such as from a server, another device, or the cloud. If we need to retrieve information from a newly released device, we can run mobile forensics software on the generic Android OS. When we can't rely on the assistance of mobile forensics software, we turn to standard backup protocols that have been in existence since the early versions of Android OS. Using the native Android backup capability, we can develop scripts to target what data needs to be collected, such as application, user, and logging information, to ensure a repeatable process for data acquisition. Many mobile forensics applications are able to review these backups.[4]

As with all BYO devices, in cases where the information needed to answer an eDiscovery request may exist in text messages, photographs, videos, or elsewhere within employee-owned personal data on an Android device, we adhere to the terms and conditions set forth in the service agreement. Internal investigator protocol and guidance by the Intel legal department also govern our handling of privacy in eDiscovery cases.

Employee Communication

To help employees be as productive as possible, we communicate with them about how we manage the BYOD program and provide usage tips similar to the communications we provide for other products, such as laptops. We rely on newsletters, internal social media, and other publications to offer hints and deliver alerts on known issues.

For any potential issues, we use email or SMS alerts to inform employees with registered Android devices. We also have an easy-to-use internal web portal where we process service requests and educate managers, employees, and IT support staff about BYO devices. We train our IT service desk technicians on how to answer service agreement questions to avoid any confusion during the registration process or, if it becomes necessary, the eDiscovery process. The growing Android community within Intel has a social media blog and forums that provides mutual support. A user posting a question quickly gets feedback if others are having the same problem on the same device. Resolving issues within the social media forums reduces the number of calls to the IT service desk, helping to decrease costs.

[3] For more information on trust scores and calculation, see "Granular Trust Model Improves Enterprise Security."

[4] For more information on Intel eDiscovery, see "Successful eDiscovery in a Bring-Your-Own-Device Environment."

RESULTS

The time needed to approve a new Android device began as a fully manual process. We have automated as much of the process as possible to shorten approval time to approximately one hour. Our Android device approval process takes into consideration Intel's security, eDiscovery, and privacy requirements. This approach for managing Android devices enables us to better protect data and reduce enterprise risk. At the same time, it supports our BYOD program goals to give employees greater flexibility and choice of devices they use to perform their jobs.

The results we are seeing are reflected in our Android BYOD program. These include the following:

- With thousands of Android devices now under IT management, employees are taking full advantage of choosing their preferred device for optimal productivity.
- Low support call volume indicates that employees are becoming informed users due in part to our newsletters, email communications, and social media.
- Employees are taking the initiative to be responsible for their own devices through patch upgrades, which improves Intel's enterprise security.

Through our BYOD program we have improved the work-life balance of Intel employees. Survey data indicates a time savings of 57 minutes per day, which equals an increase in productivity of more than seven million hours over the last three years. Android users now make up about 50 percent of our BYOD environment.

CONCLUSION

We successfully implemented a process to support the use of Android OS devices in the enterprise. When a user tries to access the enterprise network, their Android device sends information to the MDM system. Through a series of automated and manual processes, we quickly determine which level of services a device can access.

Both developers and employees see tremendous benefits in the open source creativity that Android offers. The Android OS is a dynamic platform that continues to release new versions and become available on more varied devices. We plan to gather data from these new devices to further streamline the process of meeting Intel's security and eDiscovery requirements and privacy policies.

FOR MORE INFORMATION

Visit www.intel.com/IT to find white papers on related topics:

- "Granular Trust Model Improves Enterprise Security"
- "Maintaining Information Security While Allowing Personal Hand-Held Devices in the Enterprise"
- "Successful eDiscovery in a Bring-Your-Own-Device Environment"

ACRONYMS

BYOD	bring your own device
MDM	mobile device management

For more information on Intel IT best practices, visit www.intel.com/IT.