Strategies to Solve Challenges of BYOD in Enterprise

Samsung introduces a new comprehensive mobile security solution, Samsung KNOX

Featuring research from

Gartner

Research from Gartner

Three Crucial Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD

Shifting from an enterprise-owned mobile device fleet to having employees bringing their own devices has a major impact on the way of thinking and acting about mobile security. Organizations must consider and take action on three major impacts when taking this step.

Impacts

- The right of users to leverage capabilities of their personal devices conflicts with enterprise mobile security policies, and increases the risk of data leakage and the exploiting of vulnerabilities.
- User freedom of choice of device and the proliferation of devices with inadequate security make it difficult to properly secure certain devices, as well as keep track of vulnerabilities and updates.
- The user's ownership of device and data raises privacy concerns and stands in the way of taking corrective action for compromised devices.

Recommendations

- Secure access to enterprise resources by enforcing a mobile policy on personal devices or by separating business and personal environments, but consider user experience as a fundamental security driver when selecting a solution.
- Maintain a baseline of allowed supported devices and configurations, and define support levels using a managed-diversity matrix, but recognize that the more devices you allow, the more time you will spend securing devices and handling exceptions caused by variances in device capabilities.
- Offer the choice of enterprise-owned devices to users and job roles that have the right to – and need for – a mobile device for their work purposes, but who do not wish to have private data manipulated by the organization. Obtain explicit consent to delete data on the device in case of compromise.

Analysis

This document was revised on 3 December 2012. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

In a recent Gartner survey,[1] 70% of the organizations participating replied that they have or are planning to have "bring your own device" (BYOD) policies within the next 12 months to allow employees to use personal mobile devices to connect to enterprise applications. Thirty-three percent of all organizations in the same survey currently have BYOD policies in place for mobile devices, such as smartphones and tablets. Even though closely related, BYOD is not the same phenomenon as the consumerization of IT (see Note 1). This has significant enterprise security implications when moving from enterprise-owned devices to employee-owned ones. Policies and

FIGURE 1 Impacts and Top Recommendations for BYOD Security Hurdles

Impacts	Top Recommendations
The right of users to leverage the capabilities of their personal devices conflicts with enterprise mobile security policies and increases the risk of data leakage.	• Secure access to enterprise resources by enforcing mobile policy on personal devices or by separating business and personal environments.
User freedom of choice of device and the proliferation of devices with inadequate security make it difficult to secure certain devices.	• Maintain a baseline of allowed supported devices and configurations, and define support levels using a managed-diversity matrix.
User ownership of device and data raises privacy concerns and inhibits corrective action for compromised devices.	• Offer enterprise-owned devices to users that have the right to a mobile device but do not want private data manipulated by the organization.

Source: Gartner (November 2012)

tools initially put in place to deal with mobile devices offering consumer-grade security must be revised to deal with these devices being under the ultimate control of a private user, rather than the organization. An analysis of the impact on mobile security when shifting from an enterprise-owned-device scenario to a BYOD one is necessary to provide recommendations for maintaining security levels (see Figure 1).

Impacts and Recommendations

The right of users to leverage the capabilities of their personal devices conflicts with enterprise mobile security policies and increases the risk of data leakage and the exploiting of vulnerabilities

Outside the enterprise's premises, employees may define their own usage policy for personal devices. Users can, therefore, install apps and visit URLs of their choice, whereas enterprises can limit applications and Web access on their enterprise-owned devices. Users can also decide the level of protection for their personally owned devices. For instance, they may decide not to use any password to unlock their devices, or to use a four-digit pass code, which does not provide adequate security. (Gartner recommends alphanumeric passwords with six or more characters). When enterprise data is allowed on these devices, the risk of leakage increases for the enterprise, not just because of the rise of mobile malware (mainly for Android[2]), but also because legitimate but unsupported apps may inadvertently create security risks for the organization,[3] and, most importantly, because of device loss.[4]

Most organizations address these risks by only allowing enterprise access to BYOD users after having obtained their explicit agreement to comply with the organization's mobile device policy. This must involve a technological tool (or tools) that enforces policy. Offering access to enterprise resources such as email and documents without tools to control the usage of the device is not recommended, even if the user has explicitly accepted the policy, because compromise can inadvertently result from legitimate use – for example from unsupported apps or rogue wireless networks.

Using mobile device management (MDM) software is one way to enforce policy on mobile devices. Users should obtain access to enterprise information only after having accepted an MDM agent on their personal devices, and possibly a URL filtering tool, such as a cloud-based secure Web gateway service, to safeguard and enforce enterprise policy on Internet traffic. Enterprises should consider using application whitelisting, blacklisting and containerization, as well as setting up an enterprise app store, or app catalog, for apps that are supported. The actual link to the enterprise environment can be protected through a mobile VPN. This approach does not differ from analogous non-BYOD approaches, but does require that users accept enterprise policies and, in some cases, it does not allow full use of the capabilities of the device.

An emerging alternative solution can partition business and personal environments on the device, protecting the business side of the device with a secure container (see Note 2). This approach provides good security for the enterprise's assets, but does not always deliver native user experience (UX) – for example, for the email client, especially for iOS. It may also limit the interaction of sensitive applications (such as a calendar or contacts) with third-party applications and the possibility for users to switch between work and business tasks. BYOD users select devices because, among other factors, they find the specific device UX particularly close to their tastes. Drastic changes to the UX may lead the user to attempt to circumvent the change and restore the initial (native) UX, which presents security risks. In this context, winning approaches should try to maintain the native UX, rather than altering the user's behavior.

Recommendations:

- Secure access to enterprise resources by enforcing a mobile policy on personal devices, or by separating business and personal environments through a container strategy.
- Consider user experience as a fundamental security driver when selecting a solution.

User freedom of choice of device and the proliferation of devices with inadequate security make it difficult to properly secure certain devices, as well as keep track of vulnerabilities and updates

Allowing users, rather than the IT department, to select OSs and versions of mobile devices opens the door to devices that are inadequate from a security standpoint. An essential security baseline should require enhanced password controls, lock timeout period enforcement, lock device after password retry limit, data encryption, remote lock and/or wipe.

For instance, consider Android: There are approximately 4,000 different versions of Android devices in the market.[5] More than half of the devices currently being used do not have inherent encryption capabilities.[6] Device manufacturers can decide not to provide OS upgrades for older models; meaning that a personal Android device that does not meet the organization's security standards may stay that way permanently. Gartner recommends using Android 4.0 or higher, which significantly limits the current range of choice for devices. As another example, Windows Phone 7 does not currently support data encryption.[7]

The enterprise mobility baseline must also express minimum requirements on hardware – OS versions will not be sufficient. For example, if iOS 5 is specified as a requirement, an iPhone 3G with iOS 5.1.1 will result in compliance. However, encryption is not available in iPhone 3G. Thus, the device cannot be properly secured.

In alignment with the mobile security policy, network access control policies should be used – for example, to deny access to enterprise resources such as email and apps to devices that cannot support the security baseline. Preventive action should be taken to ban or create an alert for noncompliant devices by using tools such as MDM software.

Excessively limiting the types of allowed devices eliminates the benefits of BYOD for users. There should be no compromise of security for the sake of device variety, but where it is possible to manage and secure a new device model, it should be done. This must be a well-thought-out decision, as a stretch of support can generate significant costs or reduce flexibility in the long run. For example, a specific type of device may not have MDM APIs, but may be secured through Exchange ActiveSync (EAS). Some MDM products may support the device via a plug-in that manages the device using EAS. If this type of device is allowed, the organization will remain locked in to selecting MDM vendors that provide this plug-in in the future.

The policies that are enforced will depend on the risk appetite of the organization and the sensitivity of data allowed to reside on the device. As the former decreases, and the latter increases, the mobile policy must become increasingly strict to meet the organization's needs. On the contrary, if the organization is willing to accept a higher amount of risk than most organizations, and does not place sensitive data in mobile devices, then the policy enforcement plan may be less stringent than in other organizations with similar situations.

These principles must also be tailored to the specific organizational context, and be granular so they can address multiple categories and situations. Support for BYOD need not, and should not, be total or equal for all allowed devices. "Use Managed Diversity to Support the Growing Variety of Endpoint Devices" describes a way to differentiate levels of support depending on the device and its ownership.

Recommendations:

- Create and maintain a security baseline to identify allowed devices and configurations.
- Follow a managed-diversity matrix to define support based on device and ownership.
- Recognize that the broader the range of devices you allow, the more flexibility users will have. As a result, you will spend more time securing devices and handling exceptions caused by variances in device capabilities.

The user's ownership of device and data raises privacy concerns and stands in the way of taking corrective action for compromised devices

Most people consider data on their personal devices as their property, and would strongly object to having it manipulated by the organization without their explicit consent. When shifting from enterprise to user-owned devices, "remote wipe," which is a fundamental security feature in a mobile security policy, becomes complicated from a legal and cultural point of view. Thus, sufficient attention should be paid to this issue to avoid repercussions. In countries such as the U.S., corporate data on personal PCs and smartphones can be legally accessed. In other locations, such as Canada and Europe, regulations are particularly strict.[8] In practice, "selective wipe" is proving to be difficult in ensuring that all business data, and only business data, has been deleted from the device.

In this situation, it is recommended to liaise with the legal department to obtain advice, because there may be legal implications related to device wiping (for example, accidentally deleting personal pictures). It is good practice to obtain the user's explicit consent before manipulating the data residing on the device, in case the device is deemed compromised. Problems may arise if the user refuses a remote wipe. Time is of the essence when performing this task, and asking the user for permission after the compromise, when a remote wipe is considered necessary, will be impacted by message exchange delays that can be critical (such as when a user is out of the office). It is also not recommended that the organization send a notification that announces the wipe within a specified deadline without obtaining a receipt acknowledgment. Therefore, it is necessary to obtain permission in writing, along with the acceptance of the mobile security policy, at the time of the user's initiation to the BYOD program.

When the job role of the employee necessitates that a mobile device is required to perform job tasks, it is important to offer the option of an alternative solution to BYOD. This should be done to avoid that the employee is obliged to hand over his or her device for the organization to delete data in case of a security breach. The organization must offer the choice of an enterprise-owned device, and allow the user to freely decide whether to opt for BYOD or for the regular enterprise program.

In addition, the user should take action to safeguard information against the possibility of remote wipe by backing up his or her personal information.

Recommendations:

- Offer the choice of enterprise-owned devices to users and job roles that have the right to – and need for – a mobile device for their work purposes, but who do not wish to have private data deleted by the organization.
- Obtain the explicit, written consent of users to delete their data in case of compromises, or the loss or theft of devices.

Evidence

[1] "Survey Analysis: Tablets and Android Smartphones Enter Enterprise Mainstream"

[2] www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012

[3] www.macworld.com/article/1167113/linkedin_privacy_issues_possible_password_breach_ios_app_data_leak.html

[4] www.credant.com/news-a-events/press-releases/238-credant-survey-finds-consumers-left-thousands-of-laptops-and-smart-phones-at-airports-across-the-united-states.html

[5] http://opensignal.com/reports/fragmentation.php

[6] http://developer.android.com/about/dashboards/index.html

[7] http://social.technet.microsoft.com/wiki/contents/articles/1150.exchange-activesync-client-comparison-table.aspx

[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

Note 1

Difference Between the Consumerization of IT and Bring Your Own Device

The consumerization of IT is the specific impact that the pervasiveness of consumer-originated technologies have on enterprises. The main security hurdle brought by the consumerization of IT is the need to provide enterprise-grade security for consumer-grade devices.

BYOD can be viewed as one effect of the more general phenomenon of the consumerization of IT. In BYOD, not only are consumer-grade devices used in the workplace, they are under the ultimate control of the user – not the IT organization. The need for IT managers to manage and secure devices, while allowing users to act as owners of their devices, is the main difference between BYOD and the broader phenomenon of the consumerization of IT.

Note 2

Containerization and Dual Personas

One approach to BYOD comes under different names and technological implementations. These include partitioning, sandboxing, compartmentalization, mobile hypervisors, dual personas and containerization. The effect achieved is the differentiation of the business and personal environments on the mobile device to secure the business one. Different products provide various technical solutions that can sit on top of the existing OS, or can partition the phone into two different parts. The technical solution for Android is different than the one for iOS and is dependent on OS capabilities. Some examples of solutions include AT&T Toggle, Enterproid Divide, the Thales Group's Teopad and VMware Horizon Mobile. BlackBerry 10 offers a native dual solution that separates business and personal environments. Some MDM tools also provide containerized solutions, but the dual persona approach differs from the MDM solution in that it focuses on securing the containerized part, without using MDM APIs to manage the entire mobile device.

Source: Gartner Research, G00238350, D. Zumerle,
14 November 2012

From the Gartner Files:

Use These Comprehensive Best Practices to Manage and Secure Android in Your Enterprise

Android's increased enterprise capabilities, many versions and surge in employee uptake make it crucial to understand and control these devices. IT staff responsible for enterprise mobility should use these guidelines to decide what to support and how.

Key Challenges

- The most serious enterprise concern about Android is fragmentation, which exponentially complicates device management.
- An inadequate application curation process has led to what many enterprises consider unacceptably high incidences of malware in app stores, including Google Play.
- Some Android versions can be better secured than the Apple iOS and Windows Phone, but most enterprises lack enough understanding of the options and latest developments.

Recommendations

- Specify the allowed Android devices by brand, model, OS release or a combination thereof, and allow only Android 4.0 or greater.
- Add enterprise support for mobile platforms incrementally over cycles of at least three months, instead of in one "big bang" so that IT support has time to ramp up.
- Manage Android risks by restricting application access, deploying an anti-malware solution and using mobile device management (MDM) solutions that manage device-vendor-specific enterprise functionality.
- Carefully consider device-vendor-specific enterprise features for deeper management, containerization solutions to isolate enterprise data and network access control (NAC) solutions to implement network-level policies.

Strategic Planning Assumption

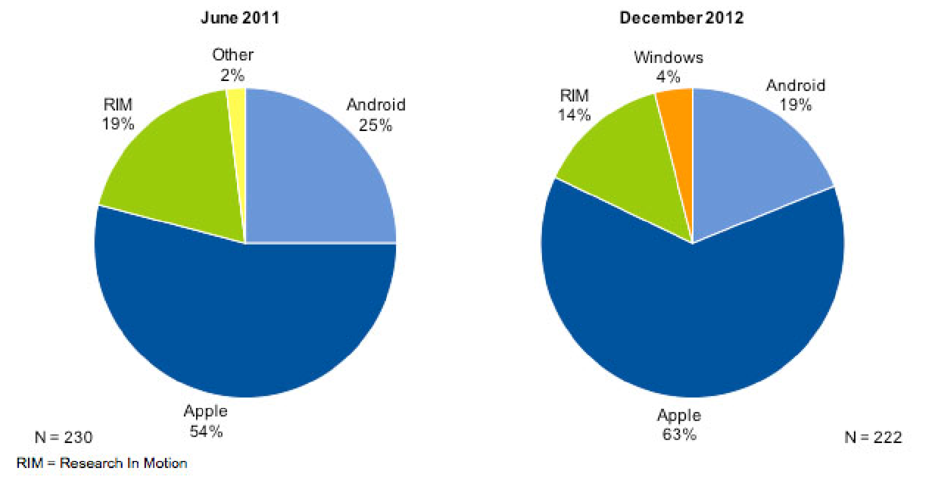
By 2016, over 40% of enterprise-supported mobile devices will be Androids.

Introduction

Android Fragmentation

Some enterprise environments now include Android devices, but each enterprise typically has only a small number of these connected to the back end, compared with BlackBerry and Apple devices, whether enterprise-owned or personally owned (see Figure 1). However, an increasing number of enterprises, notably beginning in Asia/Pacific (APAC), are starting to allow Androids relatively aggressively. Gartner expects this trend to continue globally. Meanwhile, many enterprises have consciously decided not to allow Android for several reasons.

FIGURE 1 Which Mobile Device Platform Will Be Your Primary One?



Source: Gartner (February 2013)

Two key fragmentation issues are troubling for Gartner clients:

- **Too many releases in the market**: Although Android 4.0 has been available for a year, only 39%[1] of all Android devices use this OS release. In enterprise terms, allowing any Android device is like regressing from the Windows Standard Operating Environment (SOE) concept. Security also varies; for example, early Android 2.x devices were notorious for misrepresenting themselves to the Exchange Server. Even though a user might not have employed strict enough lock settings, Android would still report a positive security status to Exchange. Another problem was the nonenforcement of device encryption. Even though these issues were fully resolved in Android 3.x and 4.x,[2] many Android devices remain at the older release versions, because the OEM didn't provide an update.

- **OEM and mobile operator variant fragmentation**: Two Android devices with the same Android release, for example, 2.3.5, usually are different. With Android, each OS release is modified by the OEM and mobile operator, because this is allowed and encouraged by Google for differentiation purposes. This moving target presented by Android is undesirable from an enterprise viewpoint; as a result, few enterprises have chosen Android as the platform for their enterprise-owned mobile devices. Similarly, few enterprises relish the idea of supporting Android and all its diversity for their bring your own device (BYOD) programs.

Android Malware

Another serious problem many enterprises have with Android is malware in the official Google Play app store. The incidents with DroidDream, from March 2011,[3] and Android.Dropdialer, from July 2012,[4] do not inspire confidence, especially when compared with how the other three mainstream mobile platforms have fared in this area. Android has many third-party app stores, some of which offer greater challenges, including a Trojan distributing a fake app store discovered in January 2013.[5]

To Google's credit, it's not that the company does no checking in this area; it has a technology called Google Bouncer that scans submitted apps for malware before the apps go live on Google Play. Instead of a simple static scan, Bouncer installs the apps and runs them to test them dynamically. Google reports that it is continually improving Bouncer to make it more effective.

Android Security

Technically, some Android versions can be better secured than the Apple iOS and Windows Phone, but this is achieved through a number of options and involves more complexity. Device-vendor-specific enterprise features are critical for filling enterprise feature gaps, but they vary across Android device vendors, and clients must take note of which devices and software versions include which enterprise features. Not all features are managed by all MDM solutions, so some may not count.

Other critical options include containerization and network-level controls via NAC. This is an emerging area for many enterprises, and Gartner advises consideration of these important technologies.

Analysis

Specify Which Android Devices Are Approved for Use

Gartner recommends that enterprises not aim to allow all types of Android devices under the auspices of BYOD. Android's fragmentation makes it incorrect to view Android as one unified platform, so Gartner encourages enterprises to create a list of approved Android devices by brand, model, OS release or some combination of these attributes. This reduces the 4,000 different Android versions to a more manageable number.

This control can be implemented by the MDM to block access to Exchange Server. When MDM is used with an NAC solution, enterprises can block access more completely at the network level. For example, rooted devices can be detected by the NAC MDM agent and blocked from all network access. Devices that have been enrolled in the company's MDM plan and include the agent can be granted full or limited access, and devices without the agent might be granted guest Internet access.

Add Enterprise Support for Mobile Platforms Incrementally

Gartner encourages enterprises to only support Android 4.0 or newer versions. There is no need to evaluate all 4,000 devices, and many enterprises have chosen to allow specific brands and models, and to leverage device-vendor-specific enterprise features, such as Samsung Approved for Enterprise (SAFE) or similar technologies from 3LM, BoxTone, HTC, Lenovo, Motorola, etc. We advise our clients to study the vendor-specific extensions, identify the required features and policies, and pair suitable devices with a suitable MDM solution.

Specifying a subset of Android releases conflicts with the intention to allow employees to use whatever personal Android devices they own, but this is the reality for a platform that has deprioritized consistency in favor of speed. To emphasize this point, consider the $50 Android devices from no-name, emerging market manufacturers that are now available and will continue to grow in volume on the consumer front. Many devices may never get a software update to fix their security vulnerabilities. Some may have completely replaced the Google registration process with a regional equivalent. The rhetorical question is, whether enterprises really want to grant enterprise access to such BYOD Androids.

Start Managing BYOD Android Access

From a practical perspective, many enterprises already allowed wholesale Android access to the Exchange Server when they configured Exchange to start accepting connections from any compatible mobile device.

Thus, removing support for Android devices will be painful, because end users find it hard to accept the rationale for why a device that was allowed to connect to Exchange yesterday can no longer do so. There is no perfect way to retract access, but a best practice is to not open the floodgates for mobile access, but to plan mobile device support carefully and to publish a proper mobile device policy before allowing Exchange Server access to the supported devices. (See the Gartner mobile policy Toolkits in the Enforce All Seven Baseline Security Policies section for comprehensive information).

For enterprises that must retract Android access, we have seen IT departments give advanced notice of when access from unsupported devices will be terminated, and/or limit Android access to just email/PIM sync.

"Use Managed Diversity to Support the Growing Variety of Endpoint Devices" formed the foundation for this research, as it explains how Gartner's enterprise architecture concept of managed diversity brings order to the chaos. Most enterprises we work with have BlackBerry and iOS in the platform tier and Android in the appliance tier, a concept outlined in the research and important for effective device management.

Gartner also will publish a Toolkit that provides more granular guidance on how to securely mobilize different applications. This will apply to all mobile platforms, including Android.

Deploy an Anti-malware Solution

Gartner encourages clients to deploy an anti-malware solution for Android, and to make the use of the solution mandatory until the malware in Android's official app stores is under control.

Anti-malware solutions are not needed for other mainstream mobile OSs. As Gartner has mentioned in our published research, the app store paradigm for other mobile OSs has dramatically changed the mobile management paradigm. Since there is no sideloading and since all apps must come from the app store, a whitelist has effectively been implemented. Anti-malware and antivirus solutions do not have the same degree of importance for mobile as for PCs, and the focus has shifted to other concerns, including data leakage protection.

The most popular solutions in this area include offerings from typical antivirus vendors, as well as solutions such as Lookout and Appthority. Consistent with our position, Lookout scans for malware on Android, but not in the Apple iOS client.

Enforce All Seven Baseline Security Policies

Gartner recommends that enterprises enforce these seven security policies as a baseline for all Android devices:

- Make sure the device has a lock code and good expiration settings.
- Ensure that the device locks when it's idle (e.g., after five minutes).
- Require a complex password, instead of a simple, four-digit PIN.
- Ensure that a remote wipe capability exists.
- Enable device encryption.
- Implement a maximum number of failed password attempts.
- Make sure rooted devices are detected and blocked.

Most enterprises take advantage of device-vendor-specific enterprise features to implement more security policies beyond this baseline.

Our research provides mobile device policy templates for enterprise-owned devices and BYOD, respectively:

- "Toolkit: BYOD Mobile Device Policy Template"
- "Toolkit: Enterprise-Owned Mobile Device Policy Template"
- "Securing BYOD With Network Access Control, a Case Study"

Carefully Consider Containerization Options

Containerization is a highly suitable and popular solution, whether for increasing overall mobile security or for managing BYOD. These solutions work by isolating enterprise information on a personal device. Containerization is available from point vendors, but most enterprises will likely use the functionality provided by their MDM.

Traditionally, enterprises that allow BYOD Androids have severely restricted application access to email, the personal information manager (PIM) and thin clients via MDM policies. With containerization, some enterprises may decide to rely solely on the container without enforcing the same MDM policies at the device level.

Consider the Android for Field Service and Asset Management, but Watch Out for the Windows Embedded 8 Handheld

A number of Gartner clients, especially in APAC, are considering the use of enterprise-owned Android tablets for specific vertical applications, such as field service management and asset management. Android tablets represent a meaningful hardware savings over the iPad, and since the device is enterprise-owned, it's possible to select a particular hardware model and remove the complexity of device diversity. Gartner clients taking this route will find a variety of valuable enterprise-class options, including ruggedized devices and enterprise support, that only certain vendors provide.

In this use case, our clients typically leverage vendor-specific management extensions, as discussed, to allow comprehensive device management and classic enterprise lockdown.

It is a critical best practice to develop a mobile device policy that includes the security policies that will be used, and identifies the MDM solutions that can manage the required vendor-specific extensions on the chosen devices.

Use the seven baseline policies we outline, along with roaming controls. In a locked-down environment, these devices could be set up with application whitelist controls to ensure that only the intended apps can be used on the device. In less locked-down environments, anti-malware and containers should still be considered.

Gartner views the Windows Embedded 8 Handheld very favorably for these vertical use cases.

Evidence

[1] Android Dashboards

[2] Android Developer and Android Ice Cream Sandwich and 4.0

[3] "Google removing virus-infected Android apps from phones, tablets"

[4] "More malware found hosted in Google's official Android market"

[5] "Android malware potentially stole up to 450,000 pieces of personal data: Symantec," "Android.Exprespam Potentially Infects Thousands of Devices" and Android.Exprespam

Source: Gartner Research, G00247839, Song Chuang, 14 February 2013

Samsung Introduces a new comprehensive mobile security solution, Samsung KNOX™

Samsung KNOX is a new Android-based solution designed from the ground up with security in mind to address the perception of the current open source Android platform. Samsung KNOX retains full compatibility with Android and the Google ecosystem while integrating fundamental security and management enhancements.

Samsung KNOX features one of the most comprehensive Mobile Device Management (MDM) capabilities available. Samsung KNOX, combined with its unique application container technology, enables enterprises to support both BYOD and Corporate-Liable models without compromising corporate security or employee privacy.

All of these advantages make Samsung KNOX the perfect choice for both regulated and general enterprise environments.

Technology Overview

This section describes the technical aspects of key features of Samsung KNOX:

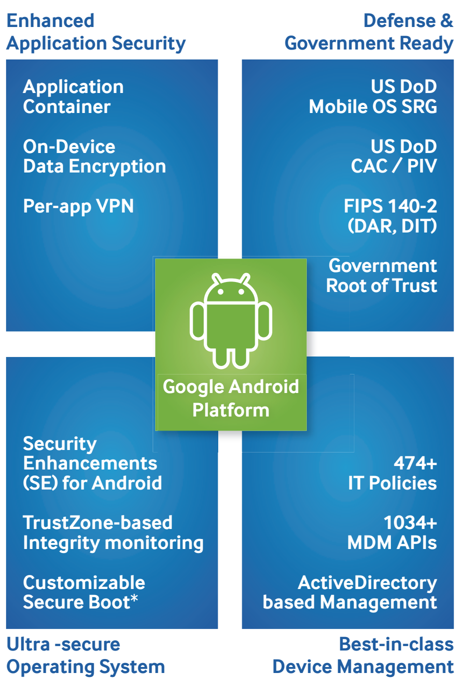
- Platform Security
    - Customizable Secure Boot
    - TrustZone-based Integrity Measurement Architecture (TIMA)
    - Security Enhancements for Android
- Application Security
    - Application Containers
    - On-device Data Encryption
    - Virtual Private Network Support
- Mobile Device Management

Platform Security

Samsung KNOX addresses security in a comprehensive, three-prong strategy:

- Customizable Secure Boot
- TrustZone-based Integrity Measurement Architecture (TIMA)
- Security Enhancements for Android

FIGURE 1 Samsung KNOX Makes Android Enterprise-Ready


Enhanced
Application Security
Application Container
On-Device Data Encryption
Per-app VPN
Defense & Government Ready
US DoD Mobile OS SRG
US DoD CAC / PIV
FIPS 140-2 (DAR, DIT)
Government Root of Trust
Google Android Platform
Security Enhancements (SE) for Android
TrustZone-based Integrity monitoring
Customizable Secure Boot*
Ultra -secure Operating System
474+ IT Policies
1034+ MDM APIs
ActiveDirectory based Management
Best-in-class Device Management

* Customizable Secure Boot availability varies depending on hardware specification.

Source: Samsung

Samsung KNOX takes full advantage of all available hardware elements to enhance this security posture.

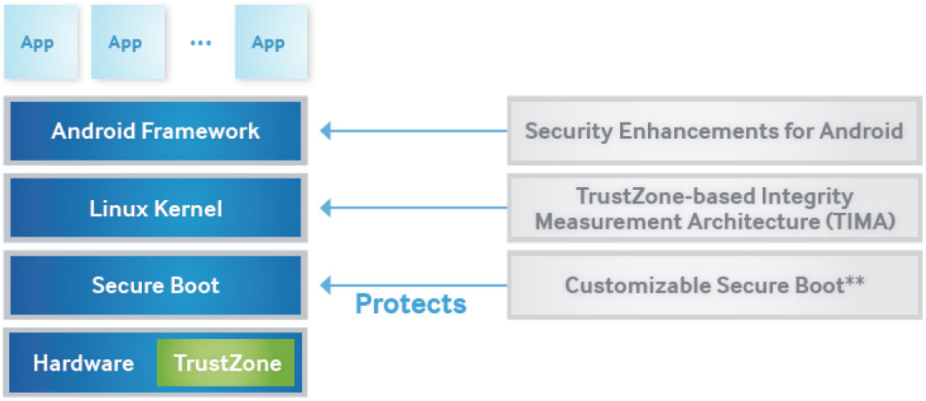
Customizable Secure Boot

Secure Boot is a procedure that prevents “unauthorized” operating systems and software from loading during the startup process. Firmware images (that is, operating systems and other system components) that are cryptographically signed by known, trusted authorities are considered as “authorized” firmware. Secure Boot is the first line of defense against malicious attacks on KNOX-based mobile devices.

Secure Boot requires the device boot loader, kernel, and system software to be cryptographically signed by a key verified by the

[1] Verification of the kernel and system image are governed by operator and market requirements.

FIGURE 2 Samsung KNOX System Security Overview


App
App
...
App
Android Framework
Linux Kernel
Secure Boot
Hardware
TrustZone
Security Enhancements for Android
TrustZone-based Integrity Measurement Architecture (TIMA)
Customizable Secure Boot**
Protects

Source: Samsung

hardware. Secure Boot uses X.509 certificates and public keys which are embedded into the boot loader of the device. A secure hash of the certificates is fused into hardware Read-Only Memory (ROM) at the time of manufacture. The Secure Boot loader will only continue if the authorized secure signed binaries are present. Next, Secure Boot verifies the cryptographic signature of the Linux kernel and system image before handing control to the OS.

The use of the industry standard X.509 certificates and keys provides a strong degree of robustness and confidence in the trusted boot scheme.

TrustZone-based Integrity Measurement Architecture

Samsung KNOX utilizes SE for Android (Security Enhancements for Android) to enforce Mandatory Access Control policies to isolate applications and data within the platform. SE for Android, however, relies on the assumption of OS kernel integrity. If the Linux kernel is compromised (by a perhaps as yet unknown future vulnerability), SE for Android security mechanisms could potentially be disabled and rendered ineffective.

Samsung's TrustZone-based Integrity Measurement Architecture (TIMA) was developed to close this vulnerability. Introduced in Samsung KNOX as a unique feature on Samsung mobile devices, TIMA uses ARM TrustZone hardware and provides continuous integrity monitoring of the Linux kernel. The ARM TrustZone hardware effectively partitions memory and CPU resources into a "secure" and "normal" world. TIMA runs in the secure-world and cannot be disabled, while the SE for Android Linux kernel runs in the "normal" world.

TIMA is used along with Customizable Secure Boot and SE for Android to form the first line of defense against malicious attacks on the kernel and core boot strap processes. When TIMA detects that the integrity of the kernel is violated, it notifies the Enterprise IT via MDM which can then take policy-driven action in response

Security Enhancements for Android

Security-Enhanced Linux (SE Linux) is a technology invented by the NSA in 2000 and has long been established as the standard for securing enterprise Linux assets. Samsung R&D teams have worked very closely with the NSA to port and integrate this technology into Android. This port of SE Linux to Android is commonly referred to as Security Enhancements for Android, or "SE for Android".

SE for Android provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. It incorporates a strong, flexible Mandatory Access Control (MAC) architecture into the major kernel subsystems and isolates applications and data into different domains.

This architecture prevents a compromise in one domain from propagating to other domains or the underlying mobile operating system (OS). This additional security, on top of Linux, reduces threats of tampering and bypassing of application security mechanisms. It also minimizes the amount of damage that can be caused by malicious or flawed applications, as applications are provided the minimum amount of permission required for their task.

SE for Android includes a set of security policy configuration files designed to meet common, generalpurpose security goals.

Out of the box, Samsung KNOX is provisioned with a set of security policy configuration files designed to strengthen the core Android platform and meet general enterprise needs. Samsung KNOX offers management APIs that allow the default SE for Android policy files to be replaced with stricter or enterprise-specific policies. These new policies can be pushed to the device.

Application Security

In addition to securing the operating system, Samsung KNOX provides solutions to address the security needs of individual applications:

- Application Containers
- On-device Data Encryption
- Virtual Private Network Support

Application Containers

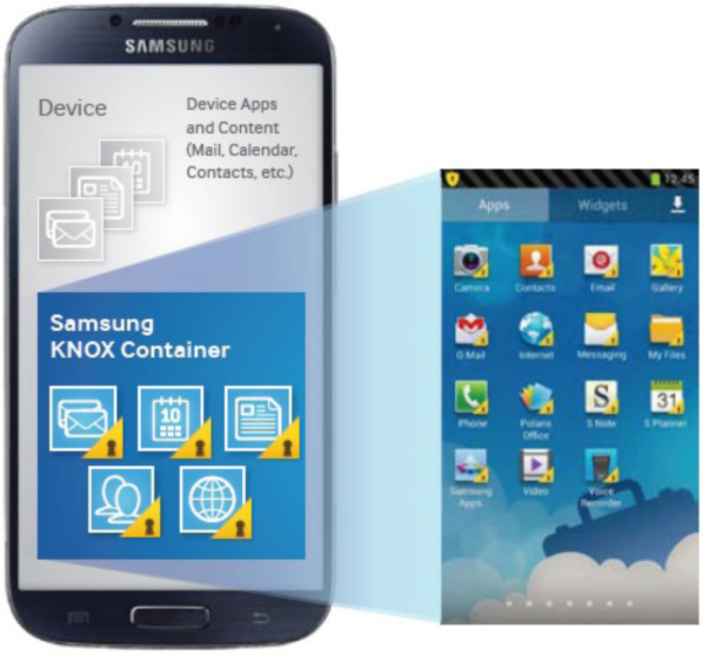
Samsung KNOX Container provides a separate Android environment within the mobile device, completed with its own home screen, launcher, applications, and widgets.

Applications and data inside the container are isolated from applications outside the container, that is, applications outside the container cannot use Android inter-process communication (IPC) or data-sharing methods with applications inside the container.

Likewise, applications inside the container generally do not have the ability to interact with applications or access data outside the container. However, some applications inside the container can be granted readonly access to data outside the container via a policy configuration.

This total isolation of applications and data within the container enables a powerful solution for the "data leakage" associated with the BYOD model. Data leakage occurs when a user sends sensitive or critical information outside of the corporate network via a personal email account, social network site, or public cloud storage system.

FIGURE 3 The Samsung KNOX Application Container



Source: Samsung

Samsung KNOX allows a "Work" container to be setup for corporate applications such as email, calendar, browser, storage clients, and so on, and the container will ensure that any data downloaded from the enterprise, such as email attachments and files, cannot be accessed by applications outside the container. All the data stored by applications inside the container are encrypted via strong encryption algorithms (AES-256). A password is required to gain access to applications inside the container.

Samsung KNOX Container is deeply integrated into the native Android platform. This deep integration allows Samsung KNOX Container to execute at the system level and leverage additional security and isolation guarantees provided by Security Enhancements for Android.

The enterprise can manage the container like any other IT asset using an MDM solution. Samsung KNOX supports many of the leading MDM solutions on the market. Container management is affected by setting policies in the same fashion as traditional MDM. Samsung KNOX Container includes a rich set of policies for authentication, data security, VPN, email, application blacklisting, whitelisting, etc.

On-Device Data Encryption

The On-device Data Encryption (ODE) feature allows users and enterprise IT administrators to encrypt data on the entire device, as well as any configured KNOX container. The ODE feature on Samsung devices uses a FIPS 140-2 certified Advanced Encryption Standard (AES) cipher algorithm with a 256-bit key (AES-256) and offers the levels of security required by government and regulated industries such as healthcare and finance. The key utilized for this encryption is developed from a user-created passphrase using well-known key-derivation algorithms such as Password-Based Key Derivation Function 2 (PBKDF2).

The encryption feature spans internal storage (system partition and internal SD card) as well as any user-installed external SD card. Hardware acceleration is employed to speed up the encryption and decryption process and minimizes the impact of the overhead on the overall user experience.

Encryption can be activated directly by the user via the "Settings" user interface, or remotely by the enterprise IT administrator as a policy setting using Exchange ActiveSync or an MDM system.

The use of NIST-compliant algorithms for ODE in Samsung KNOX devices satisfies Federal data-at-rest (DAR) requirements.

Virtual Private Network Support

Samsung KNOX offers a high level of comprehensive support for an enterprise virtual private network (VPN). This enables businesses to offer their employees an optimized, secure path to the enterprise intranet from their BYOD or corporate-issued device.

The KNOX VPN implementation offers broad support for the IPSec protocol suite:

- Internet Key Exchange (IKE and IKEv2)
- Triple DES (56/168-bit), AES (128/256-bit) encryption
- Split tunneling mode
- NSA Suite B Cryptography

The KNOX VPN is FIPS 140-2 certified enabling its use in regulated environments like government, healthcare, finance and etc.

Another distinguishing feature of the KNOX VPN feature is the ability for enterprise IT administrators to configure, provision, and manage the use of VPN on a per-application basis. This capability allows the enterprise to automatically enforce the use of VPN only on a specific set of corporate applications. This has the benefit of ensuring that enterprise data is communicated on a secure connection while keeping the user's personal data from overloading the company's Internet connection.

In addition, the per-app VPN feature allows personal-use applications to bypass the VPN and connect directly to the Internet, preserving the users privacy.

The per-app VPN capability is also available for applications within the KNOX container.

Other features of the KNOX VPN implementation include:

- Up to 5 simultaneous VPN connections
- RSA SecureID® support for Cisco VPN gateways
- Common Access Card (CAC) support for government use

FIGURE 4 KNOX MDM Policy Groups

Enterprise need	KNOX MDM Policy Groups**		
Remote Management	WiFi Bluetooth	Security Password	Email Accounts Browser
Limit Features and Functions	Kiosk Mode	Application permissions	Firewall
Secure Access to Enterprise Resources	Application	VPN	Exchange Account
Geo-fencing	Location		
Real-time Device Status and Activity	Device Inventory		
Manage Voice and Data Usage	Roaming	Phone Restrictions	APN Settings
Real-time Mobile User Support	Remote Control		
Prevent Data Leakage	Email Forwarding	Container Management	Integrity Management
Enterprise Integration	Single Sign-on	Active Directory	

** Availability of Samsung KNOX features may vary by MDM partners.

Source: Samsung

Mobile Device Management

Mobile Device Management (MDM) enables the enterprise IT department to monitor, control, and administer all deployed mobile devices across multiple mobile service providers.

Samsung KNOX builds upon Samsung's industry leading MDM capabilities by providing additional policies for security, enterprise integration, and enterprise applications such as asset tracking, remote control, and so on.

Specific MDM enhancements include:

- Policies to comply with the *US DoD Mobile OS Security Requirements Guide (MOS SRG)*
- Support for the Samsung KNOX container
- Support for management via ActiveDirectory/ Group Policy Manager
- VPN and Wi-Fi Provisioning
- Idle screen and lock screen configuration

Samsung KNOX for Government and High Security Use - Certification & Validations

FIPS 140-2 Certification

Issued by the National Institute of Standards and Technology (NIST), the Federal Information Processing Standard (FIPS) is a US security standard that helps ensure companies that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information and controlled unclassified information (CUI) can make informed purchasing decisions when choosing devices to use in their workplace.

Samsung KNOX meets the requirements for FIPS 140-2 Level 1 certification for both data-at-rest (DAR) and data-in-transit (DIT). The Samsung KNOX support for DIT covers the following:

- Web browser (HTTPS)
- Email (S/MIME)
- IPSec VPN

DISA MOS SRG Compliance

The Defense Information Systems Agency (DISA) is an agency within the US DoD that publishes Security Requirements Guides (SRGs) as processes to improve the security of DoD information systems.

In 2012, DISA published the Mobile Operating System SRG to specify the security requirements that commercially available mobile devices should meet in order to be deployed within the DoD.

Samsung KNOX complies with the June, 2012 version of the SRG specification.

Summary

Reasons cited by CIOs for the poor acceptance of Android in the enterprise stem primarily from concerns over the current state of security in the platform, as well as the lack of management policies. For example, attacks against mobile devices and especially Android devices have been increasing at an alarming rate

Furthermore, as more and more employees are bringing their own devices to work (BYOD), IT administrators are concerned about the increased risk to corporate data and network resources

With its multi-tiered security model and industry-leading device management capability, Samsung KNOX fully addresses the shortcomings of the open source Android platform for broad enterprise adoption.

- The enhanced security at the operating system level provided by Secure Boot, SEAndroid and TIMA protect against malware attacks and hacking.
- KNOX containers allow enterprises embracing the BYOD trend to create a secure zone in the employee's device for corporate applications. Access to corporate data and network resources can be restricted to applications within the container.
- The rich set of MDM policies enables IT administrators to better manage their employees' devices and offer improved support by being able to remotely configure various features including Wi-Fi, VPN and email.

Source: Samsung

Acronyms

AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CAC	U.S. Common Access Card
DAR	Data-at-Rest
DISA	U.S. Defense Information Systems Agency
DIT	Data-in-Transit
DoD	U.S. Department of Defense
FIPS	Federal Information Processing Standard
IPC	Inter Process Communication
MAC	Mandatory Access Control
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
NSA	(US) National Security Agency
ODE	On Device Encryption
PKCS	Public Key Cryptography Standards
ROM	Read-Only Memory
SBU	Sensitive But Unclassified
SE for Android	Security Enhancements for Android
SELinux	Security-enhanced Linux
SRG	Security Requirements Guide
TIMA	TrustZone-based Integrity Measurement Architecture
VPN	Virtual Private Network

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales exceeding KRW 201 trillion. To discover more, please visit www.samsung.com

For more information about Samsung KNOX, visit www.samsung.com/KNOX.

Samsung Electronics Co., Ltd.
416, Maetan 3-dong,
Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772,
Korea
www.samsung.com

Enterprise MobileSecurity is published by Samsung. Editorial content supplied by Samsung is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2013 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Samsung's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.