IBM Security
Thought Leadership White Paper

Satisfy that Android sweet tooth

Do Android's dessert-named updates improve device and data security enough to work for the enterprise?

IBM

Android is ready for the enterprise. Is your enterprise ready for Android?

Introduction

Android has long ruled the consumer market. Now, the latest security advancements from Google and device manufacturers, and support for Android by leading EMM solution providers, are expanding its presence in the enterprise. To help ensure security and compliance with industry standards and government regulations, enterprises need a way to protect and manage the wide range of available devices, versions, and idiosyncrasies of the world's most popular mobile operating system.

It's not a one-solution-fits-all situation. IT needs to examine its device and application landscape and decide what security and management capabilities are essential in a customized enterprise mobility strategy. Through platforms such as MaaS360®, which provide a flexible approach to EMM, enterprises can take advantage of native device and OS controls, data containerization, and cloud-based scalability, so that enterprises can embrace Android with confidence.

Companies are allowing employees to use their own preferred or industry-specific devices, but IT must address the very real concerns of protecting corporate data and providing standardized management.

Android almost everywhere: the fit and the fallout

With 84 percent of the worldwide mobile device market share[1], Android powers hundreds of millions of mobile devices – for work and play – in more than 190 countries around the world. It's the largest installed base of any mobile platform and continues to grow. The wide variety of Android devices available means that they are often a good fit for corporate-owned device programs. For example, many field-based employees need rugged Android devices built to stand up to dust, shock, vibration, rain, humidity, solar radiation, altitude, and temperature extremes. Others want Android devices with data capture features ideal for inventory control and warehouse operations.

This growth comes with some unintended consequences, as well as important considerations for IT. Companies are allowing employees to use their own preferred or industry-specific devices, but IT must address the very real concerns of protecting corporate data and providing standardized management.

The most popular mobile platform in the world also has a volatile security record;[2] however, Android's recent, sweetly-named versions 4.0 (Ice Cream Sandwich, Jelly Bean and KitKat), 5.0 (Lollipop) and 6.0 (Marshmallow) have helped fill the largest security cavities of the past. On the operating system side, Android 4.0 supports encryption, a new public keychain framework for authentication management, and protection from sophisticated attacks, such as memory exploits. In Android 5.0, many key security features are turned on automatically for users, including the lock screen, device encryption, and device manager (which can help to find or remotely wipe a lost device). Google has also mandated the enforcing mode for Security Enhanced Linux (SELinux), essentially limiting the privileges of applications and users to prevent security breaches on a system. To help enable BYOD for enterprise environments, a new managed provisioning process in Android 5.0 creates a protected work profile on the device. In the launcher, apps are shown with a work badge to indicate that the app and its data are administered inside of the work profile by an IT administrator.

Notifications for both the personal and work profile are visible in a unified view. The data for each profile is kept separate from each other, including when the same app is used by both profiles.

Android 5.0 also offers a guest mode for phones and tablets, which allows you to pin (or lock) apps so that a user cannot access other parts of the device. This is also an excellent way to make apps available in kiosk mode for devices on display in retail outlets.

Android for Work

It's clear that Google has been listening to the voice – and the needs – of the enterprise. As it prepares to launch Android for Work, Google brings IT the option for containerization and enterprise-ready security controls. Through a new enterprise management platform, Android for Work allows IT to:

- Separate work and personal data on Android smartphones
- Easily manage and distribute free and paid Google Play apps

Android for Work will be automatically integrated into Lollipop and available as an app for any devices running Android 4.0+.

Manufacturers: built-in security and EMM integration

Many of the top Android device manufacturers – including Samsung, HTC, LG and Amazon – have also implemented enterprise-grade protections on their latest devices. With built in features, such as SD card remote wipe and file encryption, enterprise-class WLAN security, VPN access, and the ability to support open and encrypted information simultaneously on a single device, numerous Android devices are more fit for enterprise use.

- Samsung KNOX provides a protected container where you can manage, maintain and protect enterprise intelligence.
- HTCpro-certified devices offer government grade data encryption, as well as VPN and other advanced security functions.
- Amazon Fire devices have encryption, VPN, single sign-on and certificate enrollment features.
- LG GATE-enabled mobile devices provide advanced security manageability with the support of enhanced Microsoft Exchange ActiveSync, data encryption and VPN.

These four and other Android device manufacturers have not only enabled key security features, but have also developed partnerships with industry-leading Enterprise Mobility Management (EMM) solution providers. EMM integrations and APIs allow enterprises to experience robust management and security capabilities through a single portal.

Best practices and capabilities

Given the extensive security enhancements in versions 4 and 5 of Android, IT should mandate that all devices are running Android 4.0 or later and are passcode protected. This significantly reduces the "traditional Android risks" caused by fragmentation and lack of encryption. While Android's flexibility makes the business (and users) happy with some of the best "fit for purpose" devices, it also creates exposure and requires IT to protect enterprise data and implement safeguards against rooting and mobile malware.

Risky rooting: An enterprise no-no

Users can "root" an Android device by accessing its UNIX core, which allows them to install virtually any application, including malware, and subvert application-level controls. A device that is "rooted" can expose the corporate network to the same malware that is loaded on the device and override data-loss protections.

Data loss: The business is in your pocket

Remember the good old days? It's a lot harder for workhorse desktops to expose themselves! Today, when time data moves from one device to another, it's vulnerable. Devices with removable SD cards and USB connections can easily lose data, even if the data is encrypted. Data transmitted in an unsecure Wi-Fi zone is also at risk, and corporate data loss or compromise can result in hefty fines and loss of customer trust and loyalty.

Mobile malware: dangerous whether accidental or deliberate

In its State of Mobile App Security report[3], Arxan Technologies, Inc. announced that 97 percent of the top paid Android apps and 80 percent of free popular Android apps have been hacked at some point. Because Android users can install any app from any app store (they are not limited to Google Play), there is a much higher percentage of apps that contain malware, or social engineering to connect to malware, than apps in any other mobile operating system. Arxan found "cracked" mobile apps to be widespread as even more companies move toward app-centric innovation and more employees leverage mobile technology.

Even supposedly innocuous apps on the Google Play Store can wreak havoc on your network and your brand, resulting in potential revenue loss, unauthorized access to critical data, intellectual property (IP) theft, fraud and an altered user experience. For example, if your child gets hold of your device and downloads the popular game Temple Run, its code can access your root filesystem, download cache or even the SD card you have inserted in your device. It can also record audio right through your device's microphone and track your location. With IBM® MaaS360® App Risk Management product, you can see all of these (somewhat shocking) app security details for Temple Run.

To prevent such vulnerabilities, IT needs to know what software has been installed, detect mobile malware and rooted devices, perform some level of blacklisting, and enforce compliance rules as needed.

How to approach EMM in an Android environment

Whether or not devices are corporate- or employee-owned, many IT departments are managing more than one device type, numerous apps, and likely more than one OS.

A best practice for EMM: customize to fit your precise environment and security policies.

IT should "right size" mobility management investments for different classes of users, departments, geographies, devices and applications, and apply the technology approach that best meets the needs of those use cases. For example, salespeople need to access customer contact and product data, while human resources (HR) has access to much more sensitive data, information that could be a compliance liability in the case of a breach. EMM is neither one-size-fits-all, nor egalitarian.

MaaS360 can help satisfy that Android sweet tooth

As a technology preview partner, IBM works closely with Google and manufacturers, such as Samsung, to help ensure customers get the most from their Android experience. MaaS360 directly integrates with Samsung KNOX and Android for Work. Working with MaaS360, you can have a cohesive, robust experience managing your various devices, across multiple platforms.

By working with functionality from Google, device manufacturers and MaaS360, IT has access to a wide range of mobile security options and a unified platform from which to build, manage and scale a tiered or layered security program. With MaaS360, you deploy just what you need, choosing the individual solutions that will help enable you to protect your mobile world, with the specific controls you want in your environment.

MaaS360	What you can do with it
IBM® MaaS360® Mobile Device Management The device life cycle features you need	• Control access and quarantine specific devices or Android OS versions on demand • Protect data in transit with enforced passcodes, geofencing rules and contextual management • Detect and restrict rooted devices • Remotely locate, lock and wipe lost or stolen devices
IBM® MaaS360® Mobile Application Management How to deliver the smart mobile enterprise	• Protect enterprise apps with containerization • Centrally manage mobile apps with web-based console • Blacklist, whitelist and set required apps to stop data leaks and network attacks
IBM® MaaS360® Productivity Suite World-class protection at individual levels	• Separate personal and corporate data • Set persona policies at the user level • Enable online and offline compliance checks • Wipe suite container, app containers, enterprise profiles or whole device
IBM® MaaS360® Content Suite Collaborate with control	• Centrally manage document distribution or give protected access to existing enterprise file stores, such as SharePoint, Windows File Share, IBM Connections, Box, Google Drive, CMIS sources and many others • Enable users to safely view, create, edit and save documents all in an encrypted container on Android devices • Synchronize content across device types, including iOS, Android and Windows devices
IBM® MaaS360® Gateway Suite Protect your entryway	• Provide protected mobile access to corporate data without device VPN • Mobilize SharePoint, Windows File Share and your intranet sites • Use in-app VPN tunnels to your enterprise systems

MaaS360	What you can do with it
IBM® MaaS360® Mobile Threat Management Thwart attacks before they happen	• Detect apps with malware signatures from a continually updated database • Enable a near real-time compliance rules engine to automate remediation • Discover hiders that try to mask detection of rooted devices
MasS360 App Risk Management Help eliminate risky business from your apps	• Identify hundreds of code vulnerabilities and risky app behaviors through in-depth, automated analysis • Design and test app rules before they are deployed for business units, geographies or workgroups • Enforce app security policies on users' devices and enterprise app stores

Android is officially ready for the enterprise, so contact us to find out more about how MaaS360 can get your enterprise ready for Android. Protect your corporate data while giving users seamless access to work information on their device. Take advantage of unified policies, threat management, app distribution, device management and a standard framework for a consistent experience across a wide variety of Android devices. For instant access to no cost, 30-day trial of IBM MaaS360, go to: ibm.com/maas360.

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

1 "Worldwide Smartphone Shipments Edge Past 300 Million Units in the Second Quarter; Android and iOS Devices Account for 96% of the Global Market, According to IDC", IDC Worldwide Mobile Phone Tracker, August 14, 2014 (paywall,) http://www.businesswire.com/news/home/20140814005599/en/Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 Ibid, 2014.

3 "State of Mobile App Security (Research), Apps Under Attack, Vol. 3 (previously titled: State of Security in the App Economy)", November 17, 2014, Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

Please Recycle

WGW03108-USEN-01