Research

September 2016

Android in the Business Environment: Is It Safe?

A J.Gold Associates Research Report

"All mobile devices have inherent security risks associated with their use, no matter who made the device or what Operating System (OS) powers it. With the massive growth of Android in the enterprise over the past couple of years, it's time to see if there is more that can be done to make it secure. Companies can create a strategy to minimize any risk Android may pose."

Contents

Introduction

Virtually all organizations have empowered their workers to use mobile devices to get their jobs done. Indeed, the average organization may currently have more smartphones accessing corporate systems than it has traditional PCs. Many workers utilize several devices during their work lives to make sure they stay effective and efficient during their extended work days. As a result, mobile has revolutionized the workplace in bringing anytime, anywhere computing to the masses.

Most companies continue to struggle with enabling their workforce to efficiently and safely access corporate back office systems on a variety of devices and from any location. Indeed, the advent of mobile, and particularly the BYOD aspects of end user device selection, frustrated an already over burdened IT department trying to keep corporate systems secure. And while many organizations eventually discovered a way to accommodate mobile workers, it was a painful and often inefficient process.

> ***TREND**: Organizations have a compelling need to empower mobile workers, and the number of mobile devices installed continues to multiply. This provides a significant exposure for data breaches. In the next 1-2 years, we expect many companies to look at device security in a new way, especially as they move to a majority of Android powered devices being deployed. We expect devices with enhancements to the stock Android OS to dominate, both for company deployed and BYOD installations. Companies should start now to bring this needed capability on board.*
> *J.Gold Associates LLC.*

Mobile is now a mainstream technology. Yet most companies are concerned that those same devices that bring ubiquitous access may be bringing security issues that can threaten corporate data assets and create very costly data breaches. And concern about such risks is fully warranted. Mobile devices are no longer just sending a few emails. They are often full access points for corporate back end systems that run the core business processes. As a result, potentially massive data breaches are quite possible. This is especially troublesome for regulated industries and governmental agencies, where any loss of data can mean massive fines and complete loss of customer trust. But it should be a concern for any organization.

Despite the threats, there are things that businesses can do to limit their security exposure. All mobile devices have inherent security risks associated with their use, no matter who made the device or what Operating System (OS) powers it. Android has been identified in the past as having more potential risks. While this is only partially true, it is true that you can never have enough security. With the massive growth of Android in business over the past couple of years, it's time to see if there is more that can be done to make it secure. Companies can and should create a strategy to minimize any risk Android may pose.

To this end, below we look at some of the drivers of such a strategy, discuss the decision points necessary to evaluate potential capabilities, and analyze the pros and cons of enhancing Android to provide greater security.

Is Android Security a Significant Problem?

Many believe that the hype around mobile security is overblown, and that in fact smartphones are safe since we haven't seen any major public stories of security breaches. It's true that few smartphone data breaches have been publicly identified, unlike the often massive PC and server breaches that make headlines. But the notion that smartphones are not a security threat is wishful thinking. Let's take a look at some statistics.

Symantec published an Internet Security Threat Report (April 2016), in which it highlighted interesting data from its real world data collection abilities. It identified vulnerabilities of the major mobile operating systems (iOS and Android) for the past 3 years, and found:

Figure 1: Mobile Vulnerabilities by OS

	2013	2014	2015
Android	13	11	16
iOS	82	84	84

Source: Symantec Internet Security Threat Report (April 2016)

And in a similar vein, IDC reported that from 2000-2015, iOS vulnerabilities grew from a reported 27 in 2009 to 375 in 2015. Android vulnerabilities grew from 5 to 130 over the same period. These numbers are substantially higher than those cited by Symantec.

While the overall number of vulnerabilities is relatively small, they don't tell the entire story. The number of malware variants that attempted to exploit these vulnerabilities is far more numerous. The same Symantec study found that the number of malware families and variants was quite substantial.

Figure 2: Cumulative Mobile Malware for Android

	2013	2014	2015
Malware Families	231	277	295
Malware Variants	7612	9839	13783

Source: Symantec Internet Security Threat Report (April 2016)

Many of the malware variants attacked flaws in earlier versions of Android, and cease to be a threat once systems are updated to the latest version of the OS. Yet because so many users fail to update (or are unable to update) their devices, many attack vectors are still present in the installed base of devices that a company may have in service, particularly if it allows BYOD.

Indeed, according to Statista in May 2016, KitKat (version 4.4) was the most widely used version of Android at 32.5%, followed by Lollipop (version 5.1) at 19.4%, Lollipop (version 5) at 16.2% and Marshmallow (version 6) at 7.5%. Approximately 22% of the installed base was on version earlier than KitKat, which presents a major security risk.

Symantec measured a yearly adjusted rate of malware attacks against Android of approximately 181,000 in Q4 2015. Clearly, Android security is a significant problem, and especially for those companies following a BYOD strategy. Even the relatively new "Ransomware" attacks getting so much press that are attacking business PCs and servers, are now making their way to smartphones (e.g., Check Point described HummingBad as a malicious revenue-generating malware targeted at Android devices which attempts to root the device without the user being aware).

Is Apple iOS any Safer?

Many believe that the iPhone is a safe and secure smartphone. Yet the truth is more complicated. Symantec found nine iOS threat families, including the following that Symantec listed specifically:

- XcodeGhost which infected as many as 4,000 apps.
- YiSpecter bypassed the app store by using enterprise app provisioning.
- Youmi in 256 iOS apps, to display advertising, but also sends personal information.
- AirDrop wireless file transfer system could allow an attacker to install malware.

There are no 100% Security Guarantees

The truth is no OS is truly safe from malware no matter how hard the manufacturer tries to make it so. All manufacturers have had exposures. As an example, in January 2016, Samsung provided a security update to fix seven flaws specific to its very popular Galaxy devices, plus an additional six generic Android bugs. And Apple has provided multiple security updates to its devices. So no device or manufacturer should be looked at as 100% safe. The hard part is for the manufacturers to catch the flaws early and update rapidly to the user base to minimize risk.

The Need to Keep Corporate Data Safe

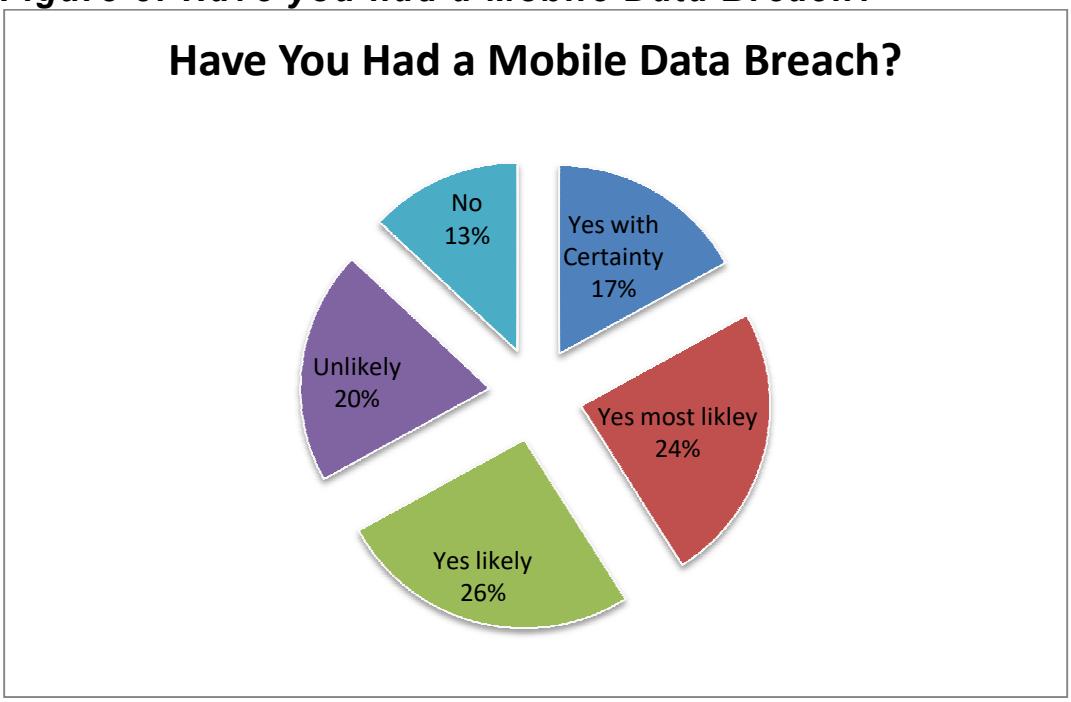
The ability to secure data and prevent corporate breaches consistently ranks among the top issues both IT and general management struggle with on a regular basis. Indeed, most surveys indicate that security is in the top 3 concerns of IT and corporate management. Regulated industry or not, the loss of such valuable assets can have a profoundly negative effect on any business. As we moved to a more mobile world over the past several years, the number of potential attack points increased dramatically, and many of them consisted of user selected and often unsecured devices as a byproduct of bring your own device (BYOD). Many companies rushed to fill this void with mobile data management (MDM) products, but this was often a stop gap measure. Much more needs to be done to protect organizations from the potential threats associated with massive mobile deployments.

How Often is Corporate Data Compromised?

We often hear about major data breaches exposing many hundreds of thousands to millions of records from high profile companies, particularly in data centers and on traditional PCs. But the number of mobile data breaches occurring in companies of all sizes is substantial, and growing. The majority are never reported or made public, but they are nevertheless real and damaging to the organizations experiencing the loss of a valuable corporate asset.

In the Ponemon Institute February 2016 study, "The Economic Risk of Confidential Data on Mobile Devices in the Workplace", which surveyed 588 IT and IT security professionals in the U.S. about whether or not they have had a mobile data breach, they found:

Figure 3: Have you had a Mobile Data Breach?



Source: Ponemon Institute "The Economic Risk of Confidential Data on Mobile Devices in the Workplace, Feb 2016

The survey results show that 67% of companies are either certain, very likely or likely to have had a security breach due to a mobile device. This is easily reinforced through responses obtained in casual conversations at most companies. Although not scientific, if asked if they have ever lost data from their personal devices through accidental exposure or other means (e.g., lost device), many users would say yes. It's clear that mobile data breaches are a significant problem affecting many organizations.

A Data Breach is Costly

Various estimates exist as to what a data breach costs a company. The Ponemon Institute 2015 Cost of Data Breach Study estimates $142 per exposed record, while the Verizon 2015 Data Breach Investigations Report loss per record estimates vary widely based on the

number of records lost and size of company, with 1K records expected to cost a company $67,000 (but could be as high as $1.5M), and a loss of 100K records expected to cost a company $475K (but could be as high as $10M).

The loss estimates vary from different sources, but even the conservative estimates are substantial. It's important to note that the cost is not only in remediation costs. For regulated industries that experience a data breach, the fines and other legal actions may increase the total cost of a data breach by many times, and may even expose officers of the organizations to prosecution. As more stringent privacy regulations become more prevalent, nearly any organization may be subject to similar fines and penalties. So the real cost of any data breach may be amplified dramatically.

Determining the Average Cost of a Data Breach

It's difficult to determine an average that can be applied to all companies, as the number and scope of data breaches may vary widely. However, it's clear that a large percentage of companies have experienced data breaches, and many more will do so in the future. And the cost of data loss is substantial, and is likely to rise as more regulations with increasing penalties are put in place.

The Verizon study estimates a company with 1K users experiencing a data breach of 100K records will cost the organization $475K (although Verizon admits that in some cases it will be many times more). That's $475 per employee. And that's for each incident. It's likely that some companies will have multiple incidents over several years.

According to the Ponemon Institute 2015 Cost of Data Breach Study, the average consolidated total cost of a data breach is $3.8 million and the average cost for each lost or stolen record containing confidential information is $154. Losing 10K records (a modest amount) will cost an organization $1.54M or $15.4M if the loss is 100K records.

Figure 4: Average per employee cost of a data breach per incident.

Cost of Data Breach	Low Estimate	High Estimate	Average Amount
Cost per user	$475	$15,400	$7,938

Figure 4 provides a cost on a per user, per incident basis for a 1000 user organization, based on a low estimate and a high estimate of data loss cost, as well as an average amount. As Figure 4 indicates, the real cost of a data breach can be quite substantial. And with so many devices being transported about by users, most of which have relatively little

inherent security but may have massive amounts of data present in their ever expanding storage capacity, it is imperative that companies focus on security as a prerequisite for deploying mobile devices.

The Growth of Android

There are a number of factors that have made Android a top choice for business users over the past couple of years, and we expect that to continue.

Why Companies are Adopting Android Despite Some Risks

There are a number of reasons why companies are moving fairly aggressively and adopting Android devices. Some are driven by an increased end user BYOD preference for some compelling Android devices that have been coming to market. Others who may purchase devices for their users are attracted to the highly competitive nature of the Android market and the fact they can select devices from a variety of vendors, often after getting a fairly aggressive competitive bidding discount. Organizations may also be influenced by the delivery channel, as many still obtain devices from carriers who have been aggressive in their promotion of Android devices. Companies are also being driven by the fact that there are an immense number of applications in the Android environment. And finally, some are doing so as a counterbalance to becoming an exclusively Apple shop.

Whatever the motivation, it's apparent that the number of Android devices being deployed in business settings is on the rise and will continue to be for the foreseeable future. And since the number of tablet devices has also been rising for business uses, the dynamic of selecting compatible devices across smartphone and tablet comes into play. It's a very complex market with many reasons for selection of Android, but the bottom line is, we expect a continued uptick in business oriented Android powered devices.

Market Traction and User Preference

We estimate that in the US, Apple has a majority of the enterprise market share for smart phones, with approximately 65% to Android's 35%. However in much of the rest of the world, these shares are reversed. And Android's share is growing rapidly, including in the US. Apple gained early market advantage especially with BYOD adherents, and it continues to be a major factor in the market. But the growing perceived quality/usability improvements of Android, and the large number of Android phone manufacturers offering compelling products, has overwhelmed the iPhone in market share. This is especially true with many BYOD users who are happy with Android features/functions. The iPhone no longer offers them the large advantage in usability it once did. Finally, we see many vendors implementing a strategy that is directly targeted at business users (e.g., BlackBerry DTEK, Samsung KNOX, Google's Android for Work). As a result, we expect the market share of iPhones to continue its decline relative to Android.

The market for mobile devices will continue to be split, and much competitive differentiation in devices will be driven by a large number of innovative products (including forcing Apple to

stay competitive). Nearly every organization supporting smartphones and tablets must have a strategy to support Android devices, despite some of the security challenges.

Are there Inherent Flaws in Android?

Many have pointed to Android over the past few years as being a relatively insecure platform that could be dangerous for business users. Android has made great strides over the past few product generations, but it still has some challenges when used in an enterprise. While it's important to note that what we discuss below is focused on Android, most other modern mobile OSes have very similar problems. Therefore, expecting to eliminate these risks by moving to another OS (e.g., iOS) may not bring the level of improvement expected.

Rooting – Although not officially endorsed by Google or most phone vendors, this is nonetheless a real security threat for organizations. There are even some vendors who explicitly support rooting. But within a security conscious business, rooting is a dangerous practice as all bets are off when it comes to securing these devices. There are many easy ways for users to root an Android device. Once done, it's impossible to look to Android and Google to provide currently verified safety, or future enhancements and security improvements, as the core OS code has been modified. Some exploits are now able to essentially root a stock Android phone and thereby bring down many of the security mechanisms Android has put in place. Rooting remains one of the single biggest threats to Android device security.

Multiple OS versions – Although Android is generally perceived as a single OS, in reality it is an open source OS that can be modified/customized by each vendor. This makes securing the OS more difficult, as some vendor modifications may add new/unique security flaws to their devices. Google is responsible for continuous security upgrades of Android and does so regularly. But vendor-specific features are at the discretion of the device manufacturer. That causes an "uneven" upgrade scenario for devices, by manufacturer, model, and even age of device. Fragmentation of OS versions within an organization can prevent a unified security model, thus requiring an approach unlike on previous devices.

Lack of rapid updating – the lack of quickly implementing updates to the latest version of the OS is often a key factor in enabling known exploits. Some manufacturers can take 60-180 days to upgrade to a new OS version after Google has made it available. And carriers add additional test time before they offer an upgrade to their subscribers, often as much as 90 days or more. Phones more than 1-2 OS generations behind may never even get an upgrade. And BYOD increases this problem as end user acquired devices are the hardest to effectively manage to assure they are up to date (in fact a substantial portion of end users never perform an upgrade of their devices). Most organizations that have a significant installed base of Android should expect to have devices in use that span 3-4 generations of the OS. We estimate less than 15% of organizations enforce a policy to mandate updates to the latest versions on mobile devices before users can access corporate systems. This is a major security issue.

User clicks – Many users download a significant number of apps from the app store. Indeed, we estimate the average user has downloaded more than 25 apps. And generally users do not read the fine print during installation, allowing downloaded apps to have access to far more device resources than they need. This over-granting of permission is very common and most users simply click and approve whatever the app requests. This could potentially be risky as Android was specifically engineered to limit app risks by requiring them to obtain permission to use specific capabilities/functions on the device. Over-granting of permission is exacerbated by the fact that users are forced to accept all permission requests at install time in order to load the app. This was changed in Marshmallow and users now have the option to deny individual permissions at runtime, but many still automatically accept all app permission requests. While apps are pre-tested in the Play Store before they are made available, it is nonetheless possible for security exploits to make their way onto the device in this fashion. This can be true of business as well as consumer apps, so extra caution is required.

Not all Android is created equal – Open source products like Android are easily modified by the phone vendor, and app developers may create a security hole by accessing a previously undetected flaw in specific implementations. Play store does check each app before it is made available to the public, but that doesn't prevent some undetected security flaws from being leveraged in an ongoing battle between Android security and malevolent actors looking to exploit anything they can find.

Not inherently able to do secure boot or OS trust model/determination – No device should be able to boot and load its OS without first determining with certainty that the OS is authentic and not somehow modified. While Android has added this capability to the latest versions of the OS, it is up to the individual device manufacturers to enable this within their own hardware designs. Not all available chips powering current devices have the ability to enable security hardware assist and thereby secure booting to verify that the OS has not been tampered with. As cost is a consideration for many low margin devices, this capability is sometimes neglected for cost reasons. Such devices should be discouraged from being selected as business devices.

Inability of Anti-Virus/Malware to protect - Antivirus doesn't work on Android like it does on Windows PCs. It can't get "under the covers" to intercept bad actors. There is no low level OS access to act as a gateway and stop actions before the OS executes them. Android uses sandboxes to isolate each app, but that allows each one to execute and potentially "break out" of the confines. No AV program can prevent execution as it has no way to enter and control the sandbox. In fact, it's just another executable like any other app. While some AV/Malware protection programs can offer a measure of monitoring and analysis of behavior, they are not able to act preemptively as we are accustomed to on the PC platform.

Is Android for Work Enough?

Google is addressing the needs of many business Android users by offering an enterprise-class upgrade to Android known as Android for Work. While it does offer a significant

enhancement to consumer-grade Android by providing segmented workspaces and profiles to keep corporate and personal apps and data separate, it does not completely solve the challenges of using Android in the workplace.

First, it still requires that companies deploy a management capability that can effectively set and enforce policies on the device, either with an MDM or EMM tool set. Next, while Android for Work compatibility may be enforced for company purchased and deployed devices, its availability for download to BYOD devices is limited and will depend on the characteristics of that specific device (e.g., OS version, manufacturer installed capabilities). Indeed, to take full advantage of all the capabilities of Android for Work, the device must be designed to be compatible. And while encryption is a key component of Android for Work, not all devices are able to take full advantage of this feature. Finally the increased cost of implementing the components within a device necessary to enable Android for Work means that only relatively higher end devices will have this capability built in.

We believe that Android for Work is a significant enhancement for use by organizations who wish to improve their security profile for mobile devices. But its lack of universal availability makes it only a partial solution. We recommend companies specify that new devices have this capability built in when upgrades are obtained to existing installations. But in general we expect it will take 2-3 years before most organizations will be in a position to fully exploit Android for Work. In the interim, companies should still create a security strategy based on obtaining enhanced capabilities as soon as is practical.

Why MDM Alone is not Enough

Mobile Device Management is an important tool to help organizations manage and secure their devices. But obtaining a standalone MDM does not insure that the devices will be secure. MDM is an over the top application that sits on top of the OS and therefore can't effectively overcome any inherent flaws within the device at the lowest levels. It is meant to manage assets, apps and policies, but can only do so if the device itself allows it and is able to take advantage of the policy setting abilities of the MDM.

To get around this limitation, many MDM suites offer a containerization approach that isolates the business side of things from the rest of the device. Indeed, containerization is an important part of securing a device, but add-on containers within MDM suites are not as effective as containerization built natively into the device itself. Add-ons may be compromised if the base level OS is compromised, so they are not as secure as one might expect (although clearly better than not having this capability at all).

Organizations should be using MDM components to manage their devices as they are a key component of securing the organization. But they should not be looked at as substitutes for obtaining the best devices that have security built in at the core levels of the device.

Where can Android Security be Enhanced?

In figure 5 we provide a comparison of some of the advantages and disadvantages of purchasing a standard Android device versus one that is designed with enhanced security features.

Figure 5: Comparison of Base Level Android vs. Enhanced Android

	Base Level Android	Enhanced Android
Boot Level Security	+	++
Resistance to Rooting	-	++
Policy Management	+	++
Malware Resistance	+	++
General Device Availability	++	-
BYOD Acceptability	++	+
Corporate Data Protection	+	++
Managing Updates to OS	+	++
App Availability	++	++

What Your Secure Android Device Needs

Companies that utilize Android devices within their corporate networks and with access to corporate applications should verify that they contain the following essential characteristics.

Latest Version of the OS – Outdated versions of the Android OS pose a significantly larger risk to business than do the latest version (currently version 6, or Marshmallow). Companies should make sure that users only employ the latest version on their device. If they are not able to do so, then access to corporate systems should be restricted to provide the maximum level of security. Protected containerized web and PIM apps or other similar methods should be required to further secure the device.

Root Detection – Some new malware has been identified as attempting to silently "root" the device without the user knowing that it has done so. This can cause the device to be completely exposed to whatever malicious software the malware chooses to infect the device with. But in most cases, devices can be protected from this by having a "root detection" capability installed on the device. This fairly common capability is unfortunately not always made available to business users and many organizations fail to deploy this functionality to their user base. This should be a key component of enhancing Android device security.

Trust zones – While root detection can be added-on to a device as a software application, it is better if it's designed-in by being built into the base level hardware of the device. Essentially this allows a way for any low level code running the device to be pre-vetted so as to determine if it is genuine. It prevents the ability to root, or to substitute a corrupted OS that

could then be used to boot the system. An unalterable part of the memory on board the processor with key signatures for comparison is an essential component of this process. This component can also be extended to other security features if the manufacturer so chooses.

Altered boot sequence detection – Not only must there be a hardware enabled system as above, but any fully protected device also requires a way to monitor and intercept any inherent "tampering" with the boot process that could be a result of a malicious attempt to modify the original, signed software. A full "identity check" of the boot process can be accomplished by having a device that adds specific monitoring capabilities beyond the typical code storage and execution mechanisms, with key stores and other enhanced code verification capabilities.

Continuous app monitoring – Monitoring of activity that is considered a security risk, based on policies that can be set, is an important component of securing any mobile device. It provides not only a check of the app, but can detect abnormal and dangerous behaviors even if an app passes app store tests, and subsequently alert security systems to take needed action. While such capability can be an add-on through an MDM/EMM suite and security software component, a more effective method is to add such capability at the base level of an enhanced OS loaded onto the device.

Secured vaulting – A key component of providing a secured workspace is first securing the data storage components on the device. Full encryption together with an ability to distinguish personal data from work related data is a critical component of enterprise-class security. And the best way to do so is to provide for a hardware-enhanced secure vaulting capability. This space can also be utilized for secured credential storage in an identity management capability if enabled by the manufacturer,

Policy enabled restrictions – based on an ability to control specific hardware functions on the device, companies can elevate the level of security by disabling features known to be used by hackers but not critical to get useful work done. This enhancement should be secured from the possibility of hackers disabling its functions. MDM/EMM suites are good at managing this capability, but only if the device enables such management.

Rapid, regular device updating – To maximally secure devices, it is important to keep them updated with the latest version of Android and all periodic incremental releases as soon as they are available. Indeed, this should be done on a regular cadence, with monthly (or more often) updates pushed to the business devices. Selecting a device vendor that provides such services can go a long way to insuring that the Android devices deployed within the organization have the latest security and manageability features so critical to thwarting exploits and limiting data breaches.

An educated user – While not a characteristic of the device itself, this is nevertheless a key component of any security strategy. Providing training to end users as to what to look out for

when their device is active, what to avoid when using the device for apps and web access, and what policies and procedures are required when obtaining access to corporate systems, can all go a long way to making the device itself and any data on the device more secure and less likely to obtain any malware or other hacks. An educated user may be one of the best lines of defense against a mobile data breach.

Recommendations

We strongly recommend that companies evaluate Android security requirements as a way to enhance user productivity, increase security and enable IT to provide improved protection against data breaches. While the number of enhanced devices available for purchase is less than for standard Android devices, the enhanced capabilities should be considered as a premium protection advantage and a good investment for business users.

We recommend organizations look at the advantages of enhanced security Android devices in the following situations:

- Any organizations dealing with a wide array of device types and/or large numbers of BYOD should consider this approach to secure and manage user access to corporate apps and systems.
- While there are relatively fewer devices available in this category, and companies may face some resistance from BYOD users who have favorite devices and/or are price conscious, enhanced devices offer a higher level of security than standard Android and should be specified for all company access.
- Device manufacturers can play a key role in making devices more secure. Organizations should acquire business devices only from manufacturers who show a commitment to rapidly detecting any flaws and then quickly providing software updates to eliminate those flaws. Some mobile device vendors have been known to delay updates for months, and this should indicate an unacceptable supplier to security conscious companies.
- Companies in regulated industries, requiring total control and management of access and particularly access to sensitive data, will find an advantage in enhanced Android as it provides a centralized policy and control mechanism that is less prone to hacking and data loss.
- Organizations should look at enhanced Android devices as a first line of defense and an enhancement to any MDM/EMM solutions already installed, offering improved security and policy management capabilities enforced at the internal device level.
- Enhanced Android devices should be preferred in any company sponsored device upgrade programs, as the modest additional acquisition costs will be far outweighed by the enhanced security provided.
- Finally, any organization wishing to stay as far ahead of the hackers and malware deliverers as possible must at a minimum deploy the most secure devices that are available. We expect that hacking of mobile devices will increase in the near term, and enhanced Android is an important step in staying ahead of the bad actors looking to compromise your organization.

Conclusions

While not a “silver bullet” to security, enhancing Android through next generation offerings provides some very attractive capabilities for many companies struggling with issues of BYOD, data security, data leak protection and policy management. As the number and severity of mobile threats continue to increase, and as Android finds increased traction in organizations large and small, implementing solutions that provide maximum security and protection from data breaches is imperative.

About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com