IBM Security
Thought Leadership White Paper

Mobile is the new playground for thieves

How to protect against mobile malware

As mobile grows, threats grow

Introduction

Mobility is transforming enterprises at an unprecedented rate with the continued proliferation of smart devices, explosive development of mobile apps and increased access to work files. Employees are empowered by their organizations to be more productive at virtually any time and from anywhere, adopting policies for Bring Your Own Device (BYOD) and even allowing the use of personal apps for work-related activities.

However, organizations have not kept pace with this mobility explosion by deploying the enterprise-grade security needed to protect their sensitive information. Hackers and thieves are seizing on this opportunity to penetrate networks and acquire sensitive work data from mobile endpoints. IT and Security leaders need a modern and robust security solution to proactively detect, analyze and remediate these mobile threats.

An estimated 16 million mobile devices are infected by malware at any given time.

Mobile explosion in the enterprise

The numbers associated with the growth of mobility are staggering. It was predicted that in 2014 the number of cell phones (7.3 billion) will exceed the number of people on the planet (7 billion).[1]

According to Arxan Technologies, 138 billion mobile apps were downloaded in 2014 – and this number is expected to almost double to 268 billion by 2017.[2]

Consumers were the initial catalysts of this mobile movement with the adoption of smart devices and apps for personal use; however, enterprises have certainly benefited from these accelerating trends. The BYOD trend in the workplace continues to spread, helping organizations mobilize their entire workforce and save on procurement and support costs. In fact, Gartner predicts that half of employers will require BYOD by 2017.[3]

Mobile apps are creating new, efficient workflows for employees. Seamless access to work data, emails and content is growing, too, enhancing productivity gains. Organizations are beginning to think Mobile First for each of their processes, further fueling the growth of mobility in the enterprise.

When mobile apps attack

However, hackers and thieves are threatening to derail these significant gains in enterprise transformation. Infections to mobile devices continue to accelerate with an increase of 25 percent in 2014, compared with 20 percent for 2013 – an estimated 16 million mobile devices are infected by malware at any given time.[4]

> *Mobile malware is malicious software specifically built to attack mobile devices, relying on exploits of particular operating systems.*

The impact of a data breach can be very costly, where damage to a company's brand is compounded by potential financial loss. The Ponemon Institute estimated that the cost of a single breach was $3.5 million in 2014, an increase of 15 percent from a year ago.[5]

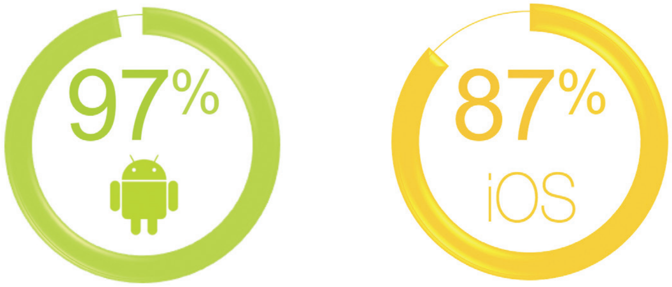


Figure 1: Top paid Android and iOS apps that have been hacked

Compromised devices due to malicious mobile apps typically are the greatest source of risk to virtually every enterprise. When users connect to unsecured networks or install risky apps from untrusted sources, mobile devices are vulnerable to malware, according to Arxan Technologies. 97 percent and 87 percent of the top paid Android and iOS apps, respectively, have been hacked and posted to third-party app stores.[6]

As uncovered in another Ponemon Institute study[7], even apps from trusted organizations and available in traditional app stores can carry enormous risks. 82 percent of respondents say mobile apps in the workplace have very significantly (50 percent) or significantly (32 percent) increased security risks. Though most employees are "heavy users of apps" (66 percent), over half (55 percent) state their organization does not have a policy which defines the acceptable use of mobile apps in the workplace.

Only 30 percent of respondents say their organization has deployed an enterprise app store, though a large majority (67 percent) of respondents admit that even if they have an app store, employees can use non-vetted mobile apps from other sources. Additionally, 55 percent of organizations say employees are permitted to download and use work apps from the enterprise app store on their personal devices.

The current state of mobile malware

What is mobile malware?

Mobile malware is malicious software specifically built to attack mobile devices, relying on exploits of particular operating systems. Three of the common types of malicious programs are:

- Spyware – device data thieves and spies that take certain kinds of data and deliver it to hackers for profit
- Trojan – malware that affect device or app functions, conduct automatic transactions, or initiate communications without the user's knowledge
- Jailbreak or root malware – gives hackers certain device administrative privileges and file access

To understand the threat and why it focuses on the mobile endpoint, let's look at the thought processes of the cybercriminals. Mobile devices are one of the easiest paths to sensitive data. While enterprise backend systems are well protected by firewalls, intrusion prevention systems and antivirus gateways, neither corporate nor personal devices typically employ the same level of protection. Personal devices (BYOD) are particularly vulnerable since they are outside of the perimeter and usually outside of an organization's control.

If hackers can attack the endpoint, they can use malware to social engineer the user, capturing personally identifiable information (PII) and credentials. They can then take over the user's account and take advantage of authenticated sessions to gather private data and conduct fraudulent transactions.

Android angst abounds

Android dominated the mobile device market with 81.2 percent market share and over one billion devices shipped in 2014, according to IDC.[8] It currently rules the consumer market, but adoption in the enterprise has been slow at best.

The fundamental design and openness of the platform and app ecosystem are why Android is one of the most vulnerable to malware infections in the mobile industry today.

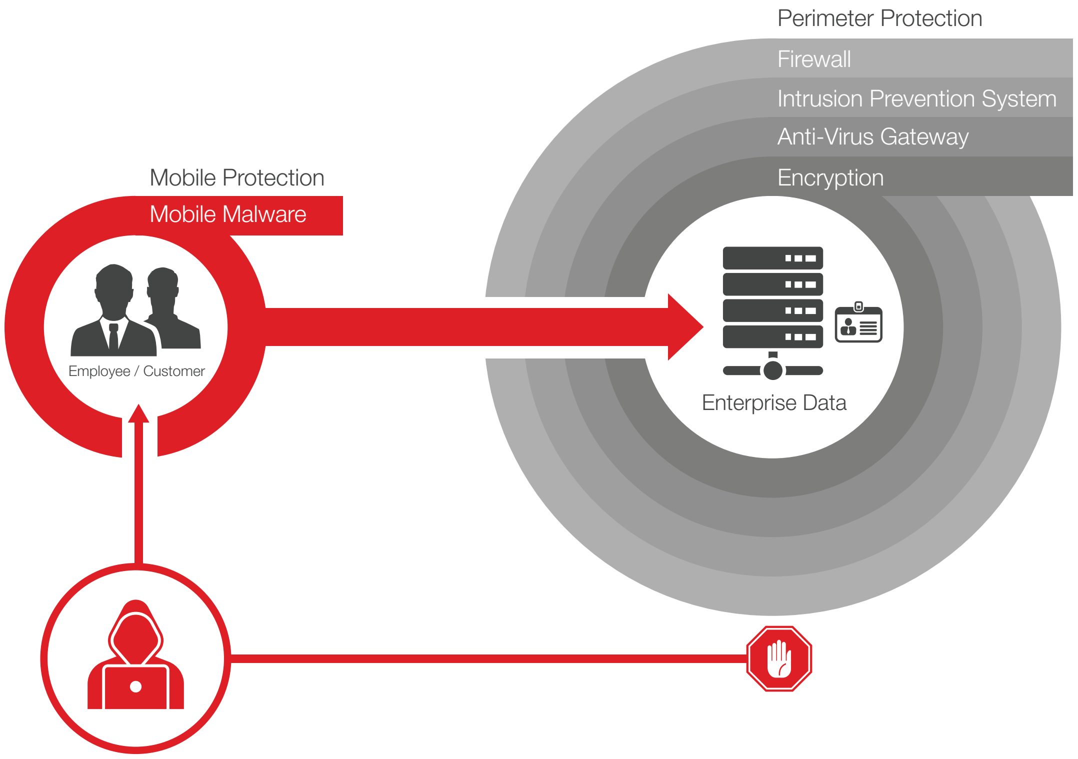


Figure 2: Criminals attack the weakest link to get access to sensitive data

The fundamental design and openness of the platform and app ecosystem are why Android is one of the most vulnerable to malware infections in the mobile industry today. The characteristics that makes Android one of the easiest target for hackers and thieves are the following:

- Android apps can be downloaded and installed from third-party app stores and websites.
- The Google Play Store does not intensively vet and approve each app, like Apple does before an iOS app is published on iTunes.
- There is no control of digital certificates to sign Android apps. These apps are typically self-signed and can't be traced to the app developer. That makes it simple to hack an Android app, inject malware and re-sign it.

Cybercriminals are continuously probing for new and creative ways to attack the vulnerabilities of mobile OS platforms that are different from those on PCs.

Google has implemented security practices to weed out malicious apps in the Google Play Store. It scans apps as they are uploaded to the store, running each app to detect and remove malware, spyware and Trojans. When Google discovers new pieces of malware, their systems are able to go back through all of Google Play and remove suspicious files from the store. Google also disables developer apps and accounts if they violate the company's terms and content policies.

However, as mentioned earlier, 97 percent of the top paid Android apps have been hacked and can be found on third-party app stores or websites. Therefore, if your employee – or her/his child – downloads and installs the latest premium game app for free on a corporate or personal Android device from one of these unofficial sources, you can expect the device will be infected with malware. Your organization can institute policies and user training to help prevent these practices, but Android devices can be vulnerable without a layer of automated protection.

An example of Android malware is a banking Trojan called SVPENG, which was discovered targeting Russian and European financial institutions. SVPENG represents a significant advancement for mobile malware. This attack directly targets mobile banking app users by tricking the victim into providing her/his credentials by using a common PC malware technique called an overlay attack.

In this attack, the malware on the infected device waits for the user to open the bank's mobile app. Once the malware identifies that a mobile banking app session is starting, it displays a screen on top of the app (hence the term "overlay") that mimics the look and feel of the bank's app, but is actually a fake page. This forces the user to unknowingly interact with the malware-generated page, thinking it is the real bank's page, and provide the banking credentials.

Similar overlay attacks could threaten sensitive corporate data. An employee could unknowingly enter their work credentials, giving thieves what they need to authenticate into enterprise systems and wreak havoc with your data.

Recently, the IBM X-Force® Application Security Research Team discovered a vulnerability in the Dropbox SDK for Android which allows attackers to connect apps on mobile devices to a Dropbox account controlled by the attacker without the victim's knowledge or authorization.[9] This vulnerability, called DroppedIn, can be exploited in two ways, using a malicious app installed on the user's device or remotely using drive-by techniques from a website.

This was a serious flaw in the authentication mechanism within the Android app using a Dropbox SDK Version 1.5.4 through 1.6.1. After the IBM Security Team disclosed the issue to Dropbox, however, it was resolved in the Dropbox SDK for Android v1.6.2 within just 4 days. An overview of the DroppedIn exploit can be found in a blog post (reference footnote 9) on SecurityIntelligence.com.

Hackers were able to use the DroppedIn exploit because of the ease of installing a malicious app on an Android device. Cybercriminals are continuously probing for new and creative ways to attack the vulnerabilities of mobile OS platforms that are different from those on PCs.

Although Android may continue to face a number of challenges in enterprise adoption, the latest security advancements from Google and device manufacturers, and support by leading Enterprise Mobility Management (EMM) solution providers, are helping to expand its presence in businesses and government agencies. When consumers, and therefore your employees, choose to use Android devices, your organization needs to enable the security and protection needed to prevent mobile malware.

iOS is not invulnerable

iOS devices have been dominant in the enterprise market for several key reasons. When the iPhone first made its debut in 2007, professionals started using their personal iPhones for work instead of their old corporate-issued smartphones. The sandboxed architecture and behavior of iOS apps have resulted in security by design in the platform, making it difficult for hackers to infect the whole device and across apps, unless users intentionally bypass their security systems.

After focusing initially on just the consumer market, Apple quickly realized the potential of the enterprise market. It began to incorporate controls to enable IT leaders to better secure and manage devices, apps and data with the help of Mobile Device Management (MDM) solution providers.

Unlike Android's open app architecture and ecosystem, Apple tends to have a much more closed device and app environment. Public iOS apps can only be downloaded and installed from the iTunes App Store, unless an iOS device has been jailbroken. Apps that are uploaded to iTunes goes through an intensive vetting process before it is officially published by Apple. In addition, digital certificates are needed to sign iOS apps, and therefore, can be traced back to the app developer.

All of these reasons have helped make iPhones and iPads popular and accepted by businesses, governments and educational institutions over the years. However, these ample security measures haven't stopped cybercriminals from attempting to hack iOS devices. In fact, there have been incidents where hackers have creatively infected iPhones and iPads, including new malware called WireLurker and Masque Attack.

WireLurker is a new class of malware that targets both Mac OS and iOS devices.[10] What is unique about WireLurker is that it can infect non-jailbroken iOS devices when they are connected to infected Mac OS devices via USB cables.

Here’s how WireLurker generally works to attack devices:

- The user downloads and installs a malware-infected OS X app on their Mac OS device, most likely from an unofficial, third-party app store.
- The user then runs the infected app and grants it root permissions, which requires knowing the admin password on the Mac OS device.
- Once running, the malware-infected OS X app downloads several iOS apps, and waits for an iOS device, which trusts the computer, to be hooked up via USB cable.
- After an iOS device is connected, which trusts the infected Mac OS device, the malware app will load the malicious iOS apps onto the iPhone or iPad.
- The iOS apps themselves are enterprise-signed apps, which means that the cybercriminals have either compromised another organization’s account or had Apple approve their own iOS apps. These apps also come with provisioning profiles, so they are trusted by iOS devices.

Once the malicious iOS apps are uploaded to the non-jailbroken iOS devices of unsuspecting users, these apps are capable of stealing information and regularly communicating with the attackers’ servers.

Perhaps even more nefarious than WireLurker is the recently discovered malware called Masque Attack,[11] which can also infect non-jailbroken iOS devices, but without needing to connect to an infected Mac OS device. With this attack, an iOS app installed with enterprise/ad-hoc provisioning could replace an approved app from the iTunes App Store, as long as both apps use the same bundle identifier.

Here’s how Masque Attack can replace users’ authentic apps and steal information:

- The user clicks on a link from any website to download and install the malicious app that is signed with an enterprise certificate and could be labeled something like “New Angry Bird”.
- The malicious app replaces a legitimate app, such as a banking or email app, that has the same bundle identifier.
- Attackers can mimic the original app’s login interface to steal the user’s credentials.
- The app can also use local data caches to emulate the replaced app’s functionality, such as recent emails for an email app.

Once the cybercriminals get a hold of login credentials and locally cached data, users’ confidential data and financial information become vulnerable to attacks and data loss.

Malware protection meets enterprise mobility management

IBM® MaaS360® Mobile Threat Management

IBM delivers a new layer of security for EMM with the integration of IBM Security Trusteer® to protect against mobile malware and compromised devices, such as jailbroken or rooted smartphones and tablets.

This distinct integration and synergy create a powerful defense against hackers and thieves that are working to acquire corporate and personal information for criminal gain.

Detect and analyze iOS and Android apps with malware signatures from a continually updated database.

Trusteer, utilized by hundreds of millions of users to protect organizations against fraud and data breaches, provides risk-awareness and security intelligence to MaaS360.

Mobile malware detection and remediation:

- Detect and analyze iOS and Android apps with malware signatures from a continually updated database
- Add app exceptions to customize acceptable app usage
- Set granular policy controls to take appropriate actions
- Use a near real-time compliance rules engine to automate remediation
- Alert user and responsible parties when malware is detected
- View compromised devices in My Alert Center and detection events in My Activity Feed dashboards
- Uninstall apps with malware automatically (for select Android devices such as Samsung SAFE)
- Block access, selectively or fully wipe devices
- Collect and view device threat attributes including:
  - Malware detected
  - Suspicious system configurations found such as an unknown SMS listener or startup package
  - Connection to an insecure Wi-Fi hot spot
  - Installation of non-market apps allowed
  - Operating system version
- Review the audit history of malware detection events

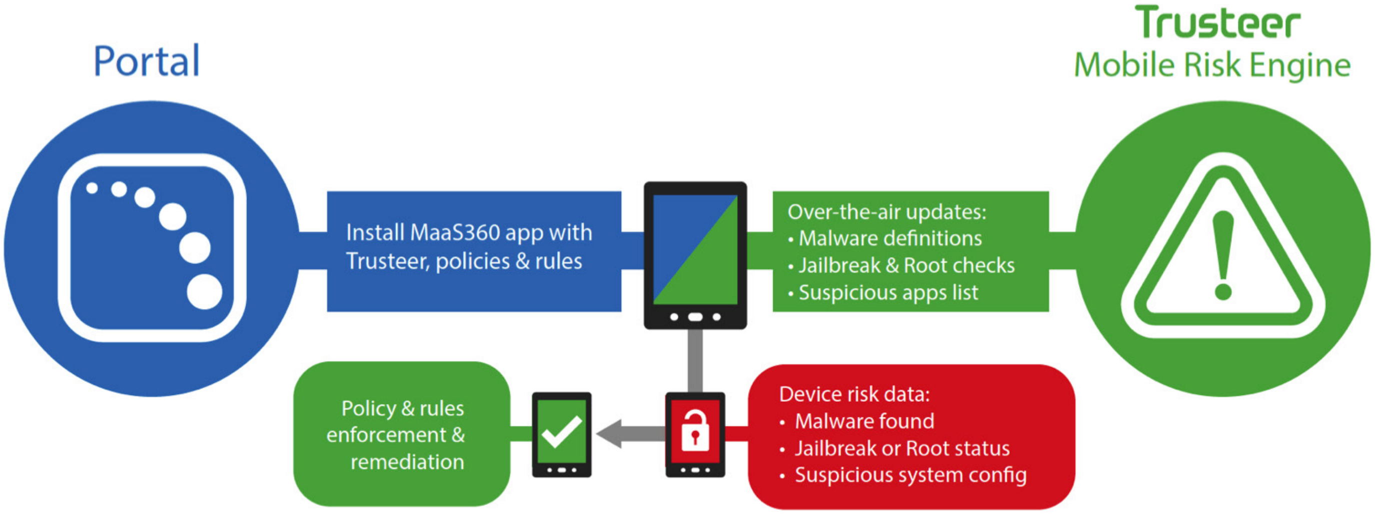
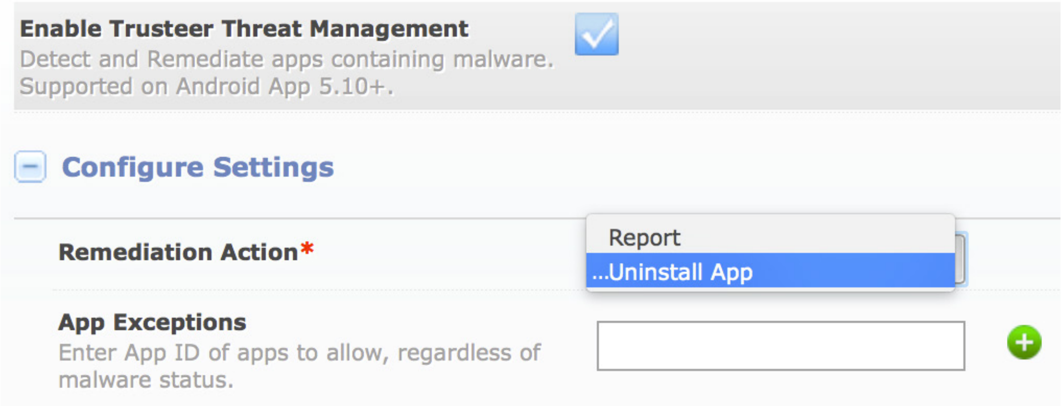

Portal
Trusteer
Mobile Risk Engine
Install MaaS360 app with Trusteer, policies & rules
Over-the-air updates:
• Malware definitions
• Jailbreak & Root checks
• Suspicious apps list
Policy & rules enforcement & remediation
Device risk data:
• Malware found
• Jailbreak or Root status
• Suspicious system config

Figure 3: MaaS360 works with Trusteer to detect, analyze and remediate mobile malware and compromised devices



Enable Trusteer Threat Management ☑

Detect and Remediate apps containing malware. Supported on Android App 5.10+.

Configure Settings

Remediation Action* Report / ...Uninstall App

App Exceptions

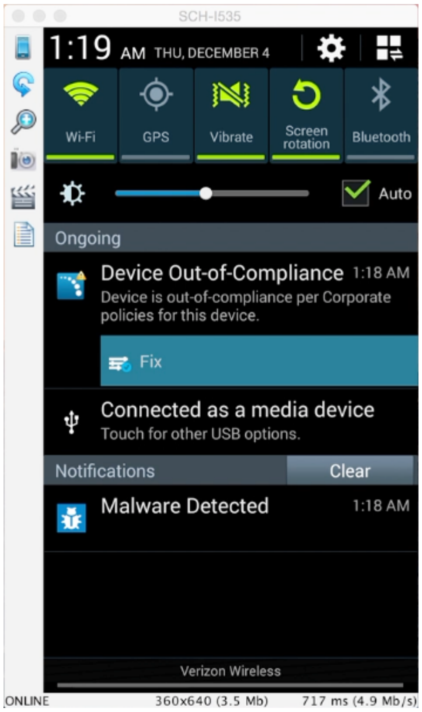
Enter App ID of apps to allow, regardless of malware status.

Figure 4: Some of MaaS360 configuration settings

Supplemental jailbreak and root detection:

- Detect compromised or vulnerable mobile devices
- Protect against jailbroken iOS and rooted Android devices that can provide attackers with additional privileges on the operating system, enabling various attack vectors
- Seek out hiders and active hiding techniques that try to mask detection of jailbroken and rooted devices
- Apply detection logic updated over-the-air without any app updates to be more responsive to fast-moving hackers
- Set security policies and compliance rules to automate remediation
- Block access, selectively or fully wipe devices or remove device control

Users' devices and information can also be protected by this layer of security, which is not readily available to consumers.



1:19 AM THU, DECEMBER 4

Ongoing

Device Out-of-Compliance 1:18 AM
Device is out-of-compliance per Corporate policies for this device.
Fix

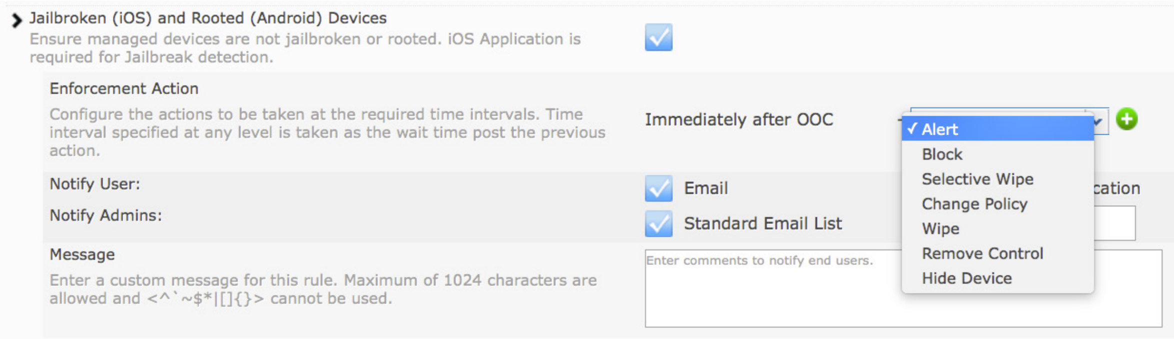
Connected as a media device
Touch for other USB options.

Notifications Clear

Malware Detected 1:18 AM

Verizon Wireless

Figure 5: Screenshot showing mobile malware detected and device out of compliance



Jailbroken (iOS) and Rooted (Android) Devices

Ensure managed devices are not jailbroken or rooted. iOS Application is required for Jailbreak detection. ☑

Enforcement Action

Configure the actions to be taken at the required time intervals. Time interval specified at any level is taken as the wait time post the previous action.

Immediately after OOC: ✓ Alert

Notify User: ☑ Email

Notify Admins: ☑ Standard Email List

Message

Enter a custom message for this rule. Maximum of 1024 characters are allowed and <^`~$*|[]{}> cannot be used.

Enter comments to notify end users.

Figure 6: Configure compliance enforcement actions for jailbroken and rooted devices

The Trusteer Mobile Risk Engine enables layers of protection and cybercrime intelligence for adaptive malware prevention to more quickly detect and adapt to the latest attack behaviors, so malware has virtually zero opportunity to commit fraud. Continually updated to provide the latest malware, jailbreak and root checks, the engine performs mobile risk assessments in near real-time based on device and app risk factors.

Key benefits

The benefits of the MaaS360 Mobile Threat Management solution go beyond just protecting corporate devices and data. Users' devices and information can also be protected by this layer of security, which is not readily available to consumers.

Organizations can to do more to help educate their users and protect their data.

Safely support both BYOD and corporate-owned devices

Protect personal data as an added employee benefit for BYOD

Proactively manage mobile threats in near real-time

Reduce risk of sensitive data leakage of corporate and personal information

Make Android adoption more palatable in the enterprise, especially with BYOD

Take automated actions to remediate mobile security risks when they occur

Educate and protect users

In addition to this MaaS360 Mobile Threat Management solution, organizations can do more to help educate their users and protect their data.

Organizations should consider the following mobile security activities:

- Educate employees about application security: Educate employees about the dangers of downloading third-party applications and the potential dangers that can result from weak device permissioning.
- Protect BYOD devices: Apply enterprise mobility management capabilities to enable employees to use their own devices while maintaining organizational security.
- Permit employees to download from authorized app stores only: Allow employees to download applications solely from authorized application stores, such as Google Play, the Apple App Store and your organization's app store, if applicable.
- Act quickly when a device is compromised: Set automated policies on smartphones and tablets that take automatic action if a device is found compromised or malicious apps are discovered. This approach protects your organization's data while the issue is remediated.

Why MaaS360?

With MaaS360, IBM integrated advanced malware protection with industry-leading enterprise mobility management and security. It is fast and simple to set up and use to safeguard sensitive data on both corporate and personal mobile devices.

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, MaaS360® Secure Mobile Mail, MaaS360® Mobile Document Sync, MaaS360® Mobile Document Editor, and MaaS360® Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch, and iOS are registered trademarks or trademarks of Apple Inc., in the United States and other countries.

Trusteer Apex™, Trusteer Management Application™, Trusteer Pinpoint™, Trusteer Pinpoint Account Takeover (ATO) Detection™, Trusteer Pinpoint Malware Detection™, Trusteer Rapport Payment Card Protection Add-On™, and Trusteer Rapport Torpedo Add-On™ are trademarks or registered trademarks of Trusteer, an IBM Company.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

[1] World to have more cell phone accounts than people by 2014, January 2013 International Telecommunications Union, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

[2] State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

[3] Bring Your Own Device: The Facts and the Future, May 2013, Gartner, http://www.gartner.com/newsroom/id/2466615

[4] Motive Security Labs Malware Report, H2 2014, Motive Security Labs, http://www.gartner.com/newsroom/id/2466615

[5] 2014 Cost of Data Breach Study: Global Analysis, May 2014, Ponemon Institute, http://www-03.ibm.com/security/data-breach/

[6] State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

[7] The State of Mobile Application Insecurity, February 2015, Ponemon Institute, https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

[8] IDC Worldwide Quarterly Mobile Phone Tracker, February 2015, IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25450615

[9] DroppedIn: Remotely Exploitable Vulnerability in the Dropbox SDK for Android, March 2015, IBM Security, http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

[10] Wirelurker: A new Era in OS X and iOS Malware; Blog, PaloAlto Networks, 11/5/14; http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

[11] Xue, H., Wie, T., Yulong, Z.; Masque: All Your iOS Apps Belong to Us; Fire Eye; 11/10/14; https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html