IBM MobileFirst Protect Threat Management

Stop mobile malware on iOS and Android devices

Key benefits

- Safely support both BYOD and corporate-owned devices
- Proactively manage mobile threats in near real-time
- Reduce risk of sensitive data leakage of corporate and personal information
- Take automated actions to remediate mobile security risks

Mobile malware – the next big security threat

Organizations are being transformed at an unprecedented pace with mobility. The Bring Your Own Device (BYOD) trend continues to spread in the enterprise. Mobile apps are creating new and efficient workflows for employees. Seamless access to work data, emails and content is growing in parallel, enhancing the productivity gains from these trends.

As a result of the popularity and speed at which mobile devices have become a mainstay of the enterprise, hackers and thieves are targeting mobile devices with malware, creating the next big security threat. Corporate data is especially vulnerable to rogue apps and malicious websites.

- 138 billion apps were downloaded in 2014.[1]
- Mobile malware is growing. Malicious code is infecting more than 11.6 million mobile devices at any given time.[2]
- Recent WireLurker and Masque attacks threaten iOS devices.[3,4]
- Damage to a company's brand is compounded by financial loss, with the cost of a single breach estimated at more than $11 million.[5]

IT and Security leaders need a modern and robust security solution to proactively detect, analyze and remediate mobile malware.

Stop mobile threats in your enterprise

IBM® MobileFirst® Protect Threat Management (formerly MaaS360®) delivers a state-of-the-art system to protect against malware on iOS and Android devices. You can detect risks and manage threats before they compromise your enterprise data.

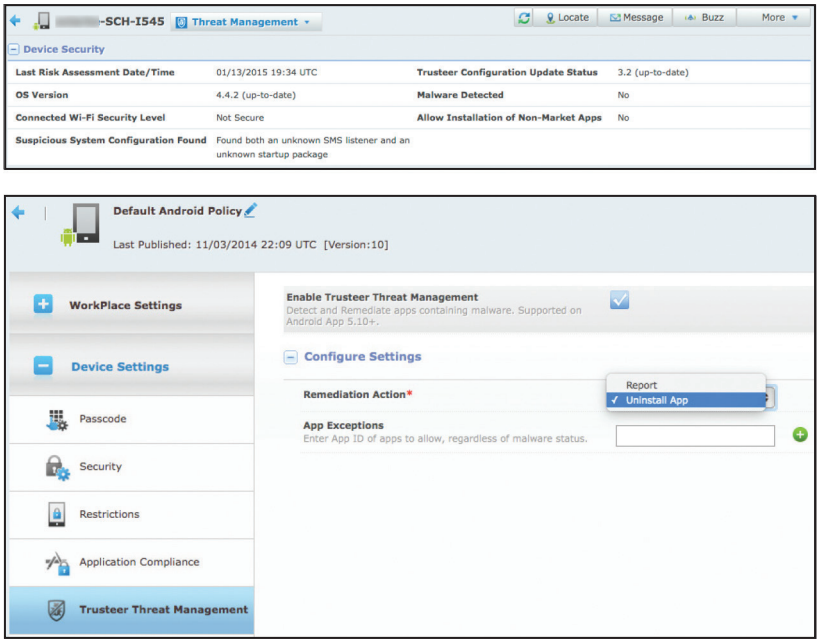

Figure 1: Examples of reported data about a protected device and policy settings in MobileFirst Protect Threat Management

Through integration with IBM Trusteer®, used by hundreds of millions of users to protect organizations against fraud and data breaches, IBM MobileFirst Protect provides a new layer of security to Enterprise Mobility Management (EMM).

Don't let malware derail your organization's mobile transformation. Balance your enterprise productivity initiatives with security delivered by MobileFirst Protect.

Mobile malware detection and remediation

- Detect and analyze iOS and Android apps with malware signatures and malicious behavior 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
- Restrict use of MobileFirst Protect container solutions
- 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 audit history of malware detection events

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 systems
- Discover hiders and active hiding techniques that try to mask detection of jailbroken and rooted devices
- Use detection logic updated over-the-air without 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

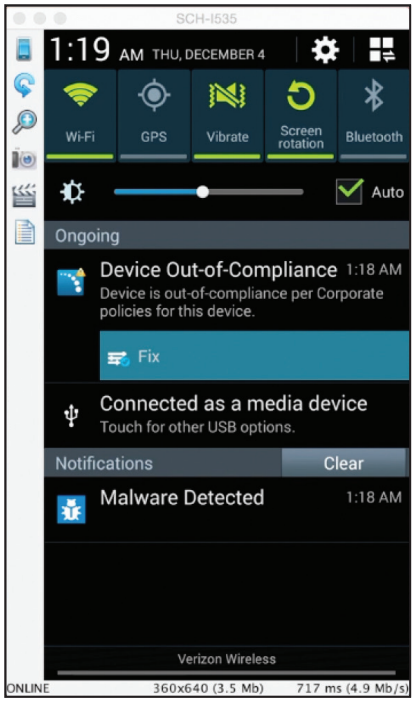

Figure 2: Example of a malware notification on a device

IBM Security Trusteer Mobile Risk Engine

- Provides layers of protection and cybercrime intelligence for adaptive malware prevention
- Quickly detects and adapts to the latest attack behaviors so malware has virtually zero opportunity to commit fraud
- Performs a mobile risk assessment in near real-time based on device and app risk factors
- Continually updates to provide the latest malware, jailbreak and root checks

Mobile malware prevention

MobileFirst Protect Threat Management detects, analyzes and remediates mobile risks, including malware, suspicious system configurations and compromised devices, delivering a new layer of security for Enterprise Mobility Management.

Malware detection and remediation

- Detect apps with malware signatures and malicious behavior from a continually updated database
- Set granular policy controls to take appropriate actions
- Enable a near real-time compliance rules engine to automate remediation
- Alert users and responsible parties when malware is detected
- Uninstall apps with malware automatically (for select Android devices such as Samsung SAFE)

Supplemental jailbreak and root detection

- Detect compromised or vulnerable mobile devices
- Discover hiders that try to mask detection of jailbroken and rooted devices
- Use detection logic updated over-the-air
- Set security policies and compliance rules to automate remediation
- Block access, selectively or fully wipe devices or remove device control

About IBM MobileFirst

IBM's 6,000 mobile experts have been at the forefront of mobile enterprise innovation. IBM has secured more than 4,300 patents in mobile, social and security, which have been incorporated into IBM MobileFirst solutions that enable enterprise clients to radically streamline and accelerate mobile adoption, help organizations engage more people and capture new markets. Through IBM's partnership with Apple, the two organizations are transforming enterprise mobility with a new class of industry specific business apps. For more information on IBM MobileFirst, visit www.ibm.com/mobilefirst. To learn more about IBM MobileFirst Protect and start a no cost 30-day trial, visit ibm.biz/mobilefirst-protect.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees, and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.To learn more about IBM Security fraud-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM® X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

Please Recycle

1 Arxan's Annual Report: "*State of Mobile App Security Reveals an Increase in App Hacks for Top 100 Mobile Apps*", November 2014, Arxan Technologies, Inc., https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

2 Kindsight Security Labs Malware Report – Q4 2013, Alcatel-Lucent, http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf

3 Xiao, Claud, WireLurker: A New Era in OS X and iOS Malware, Blog post on Palo Alto Networks; November 5, 2014, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

4 Zue, Hui, Wei, Tao and Zhang, Yulong; Masque Attack: All Your iOS Apps Belong to Us, November 10, 2014, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

5 2013 Cost of Cyber Crime Study: United States, Sponsored by HP Enterprise Security, Ponemon Institute, October 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

WGD03057-USEN-00