MaaS360® by IBM

IBM MaaS360® Mobile Threat Management

Stop mobile malware on iOS and Android devices

Mobile Malware is 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.
- Damage to a company's brand is compounded by financial loss, with the cost of a single breach estimated at more than **$11 million.**[3]

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

Stop Mobile Threats in Your Enterprise

IBM MaaS360 Mobile Threat Management 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.

Through integration with IBM Trusteer®, leveraged by hundreds of millions of end users to protect organizations against fraud and data breaches, IBM MaaS360 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 IBM MaaS360.

[1] Arxan Technologies "State of Mobile App Security" report – November 2014.
[2] Kindsight Security Labs Malware Report – Q4 2013.
[3] 2013 Cost of Cyber Crime Study, Ponemon Institute.

Mobile Malware Prevention

IBM MaaS360 Mobile 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.

Key Benefits

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

Malware Detection & Remediation

- Detect apps with malware signatures 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 & responsible parties when malware is detected
- Uninstall apps with malware automatically (for select Android devices such as Samsung SAFE)

Supplemental Jailbreak & Root Detection

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

IBM MaaS360® Mobile Threat Management

Mobile Malware Detection & Remediation

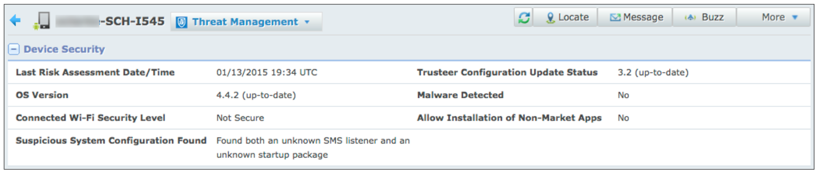
- Detect & analyze iOS & Android apps with malware signatures from a continually updated database
- Add app exceptions to customize acceptable app usage
- Set granular policy controls to take appropriate actions
- Use a near real-time compliance rules engine to automate remediation
- Alert user & responsible parties when malware is detected
- View compromised devices in My Alert Center & 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 MaaS360 container solutions
- Collect & 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 & Root Detection

- Detect compromised or vulnerable mobile devices
- Protect against jailbroken iOS & rooted Android devices that can provide attackers with additional privileges on the operating systems
- Discover hiders & active hiding techniques that try to mask detection of jailbroken & rooted devices
- Leverage detection logic updated over-the-air without any app updates to be more responsive to fast moving hackers
- Set security policies & compliance rules to automate remediation
- Block access, selectively or fully wipe devices

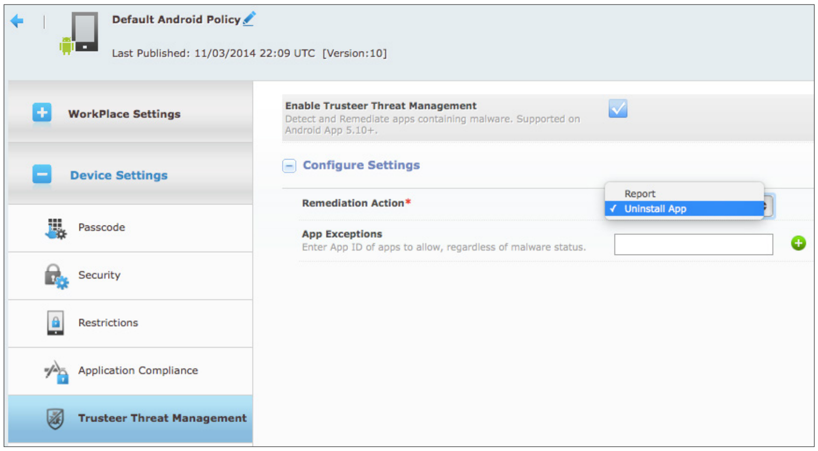
IBM Security Trusteer Mobile Risk Engine

- Provides layers of protection & cybercrime intelligence for adaptive malware prevention
- Quickly detects & 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 & app risk factors
- Continually updates to provide the latest malware, jailbreak & root checks



Device Security

Last Risk Assessment Date/Time	01/13/2015 19:34 UTC	Trusteer Configuration Update Status	3.2 (up-to-date)
OS Version	4.4.2 (up-to-date)	Malware Detected	No
Connected Wi-Fi Security Level	Not Secure	Allow Installation of Non-Market Apps	No
Suspicious System Configuration Found	Found both an unknown SMS listener and an unknown startup package		



Default Android Policy

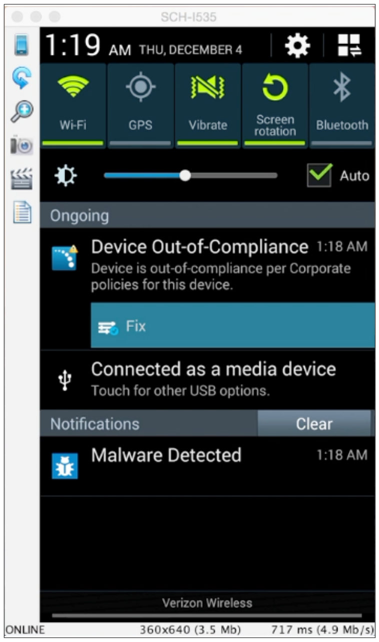
Last Published: 11/03/2014 22:09 UTC [Version:10]

Enable Trusteer Threat Management ☑
Detect and Remediate apps containing malware. Supported on Android App 5.10+.

Configure Settings

Remediation Action*: Uninstall App

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



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

Connected as a media device
Touch for other USB options.

Malware Detected 1:18 AM

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.

For More Information

To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | **Fax** 215.664.1601 | sales@fiberlink.com