Secure your mobile devices

Secure Enterprise Mobility (SEM)

Jimmy Graham
Senior Director, Product Management
Qualys, Inc.
Device and System Attack

Attempts to tamper with the system or apps which requires having compromised the device, accounted for 57% of detected device attacks in 2019.
Network Threats and Attacks

Network threats were through Unsecured or unencrypted Wi-Fi networks 36%, Captive portals 25%, Network handoffs 23%
Vulnerabilities in iOS and Android OS

Mobile OS vendors created patches for 1,161 security vulnerabilities
Mobile Device Technology Stack
Mobile Device Attack Surface

- **Global Positioning System (GPS)**
  - Use of orbiting satellites to determine the geographic location of the device

- **Wi-Fi™**
  - Local area networking used for access to connected resources or the Internet

- **Bluetooth Technology™**
  - Personal area networking used for file sharing and linking peripheral devices

- **Subscriber Identity Module (SIM)**
  - Removable hardware token providing data storage and cellular access

- **Cellular**
  - Used for voice, text, and data services provided by cell radio network carriers

- **Near-Field Communication (NFC)**
  - Used for low data rate transfers, smart card emulation, and reading RFID tags

- **Secure Digital (SD) Card**
  - Used for additional storage capacity or transferring data between devices

- **Power & Synchronization Cable**
  - Wired connection used for charging and exchanging data with a computer
Mobile Ecosystem
Device Platforms

- Android OS
- Android Things
- Android TV
- Chrome OS
- Wear OS
- iOS
- Mac OS
- Apple Watch
- Apple TV
- Windows 10
# Mobile Security Solutions

<table>
<thead>
<tr>
<th>EMM/UEM</th>
<th>Mobile Threat Defense</th>
<th>Mobile EPP</th>
<th>Mobile Policy Compliance</th>
<th>Enterprise Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle Management</td>
<td>Device – OS versions, security update, system parameters, device configuration, firmware</td>
<td>Anti-Virus</td>
<td>Integration with PC module for NIST, GDPR, CIS, PCI and rest</td>
<td>Mobile Identity and Access Management</td>
</tr>
<tr>
<td>MDM</td>
<td>OS Vulnerabilities</td>
<td>Anti-Mobile Phishing</td>
<td>App Compliance</td>
<td>Mobile Information Protection and Control</td>
</tr>
<tr>
<td>Visibility</td>
<td>Network VM</td>
<td>Device Attack Protection</td>
<td>Define Rules</td>
<td>Mobile Gateway and Access Protection</td>
</tr>
<tr>
<td>App Store</td>
<td>App VM – MATD</td>
<td>Content Filtering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Containerization</td>
<td>Integration with Apple, Google and Microsoft eco-systems</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Complete Visibility

In a single pane of glass, gain the visibility of all mobile devices.
Integration with Global Asset Inventory

Devices enrolled in SEM will get listed in Global Asset Inventory
Introducing VM for Mobility (Beta)

In a single pane of glass, gain the visibility of all vulnerable mobile devices

Initial release include device-based threats
- Android and iOS OS vulnerabilities
- Detection of rooted/Jailbroken devices
- Encryption status
Visibility into Security Posture

Asset Summary

**Rohit_Android_samsung_1**

Last Seen: Nov 21, 2019 10:42:02 PM IST (12 days ago)

Status: Enrolled

**Identification**

- **Mode:** Active
- **Ownership:** Corporate - Owned
- **IMEI:** 35719210703334
- **MAC Address:** 48:9D:11:C4:69:27
- **UDID:** 9981B7D86481CD5B8AB3CC2E663D0DA0, F4F65AD8E
- **Asset ID:** 267219
- **Username:** Rohit.Jain

**Security Posture**

- **Vulnerable:** Yes
- **Encryption:** Encryption Complete
- **Unauthorized Root Access:** No
- **Passcode Present:** No

**Last Location**

[Map showing last location in the United States]

**Tags**

- SEM
Vulnerabilities

Same user experience as any other asset in Qualys
Active Device Operations

These actions help you to manage and prevent the data loss present on the mobile device.
# Capabilities and Roadmap

<table>
<thead>
<tr>
<th>Today</th>
<th>Q1/Q2 2020</th>
<th>Q3/Q4 2020 and later</th>
<th>...</th>
</tr>
</thead>
</table>
| • Visibility  
• Inventory  
• Over 100 data points indexed  
• Integration with GlobalAI | • iOS Agent Release  
• OS Vulnerabilities  
• App vulnerabilities (Part 1) (Beta) | • Policy Compliance  
• CIS, NIST, NIAP, OWASP Top 10  
• App vulnerabilities (Part 2) (Beta)  
• Application Management Phase 1 (Beta)  
• AFW (Beta)  
• DEP (Beta) | • Integration with other EMM  
• Zero Trust  
• Enterprise Connectors  
• Agentless |
Thank You

Jimmy Graham
jgraham@qualys.com