QUALYS SECURITY CONFERENCE 2020

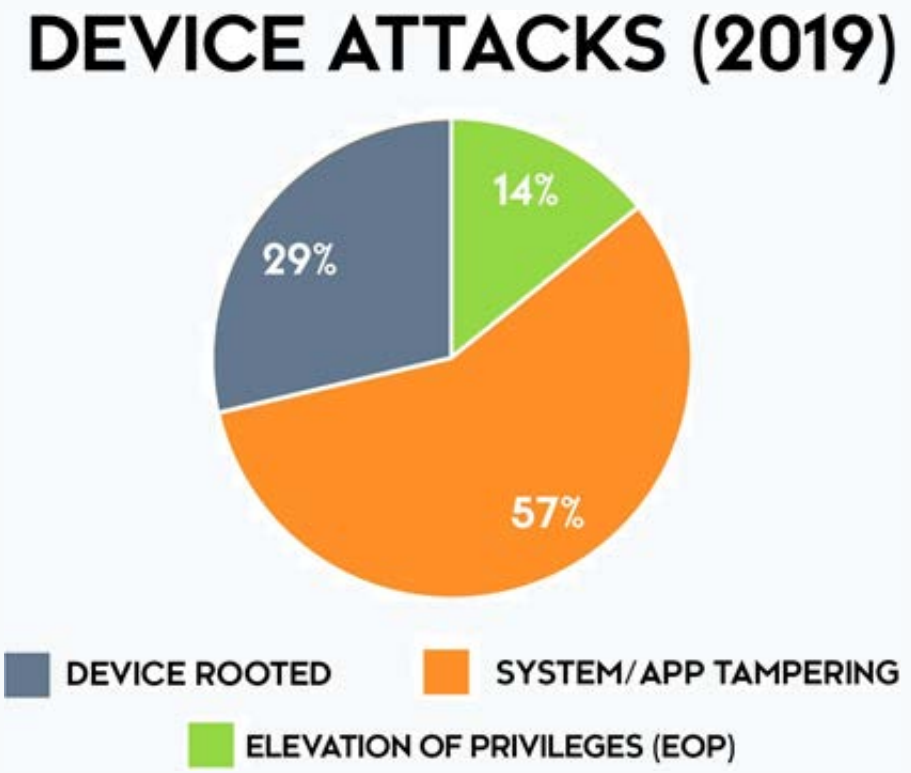
# Secure your mobile devices

Secure Enterprise Mobility (SEM)

Jimmy Graham
Senior Director, Product Management
Qualys, Inc.

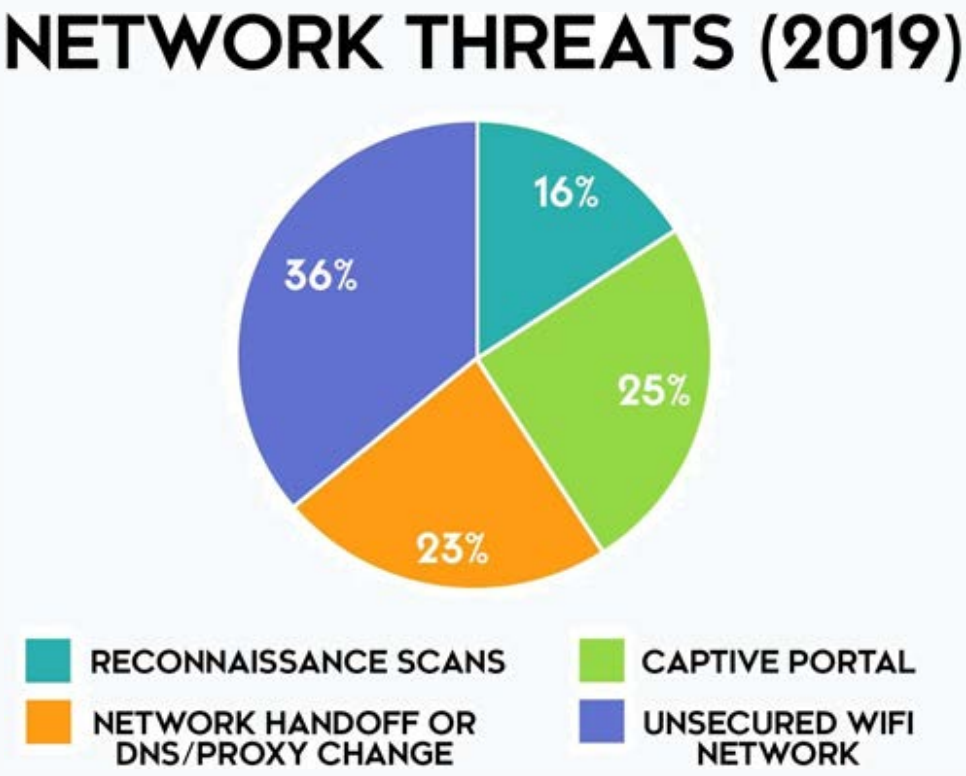
# Device and System Attack

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%

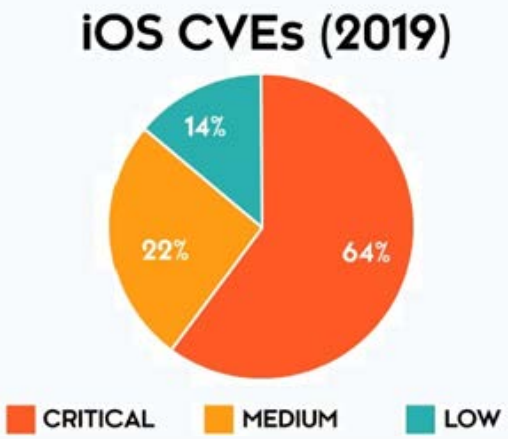


# Vulnerabilities in iOS and Android OS

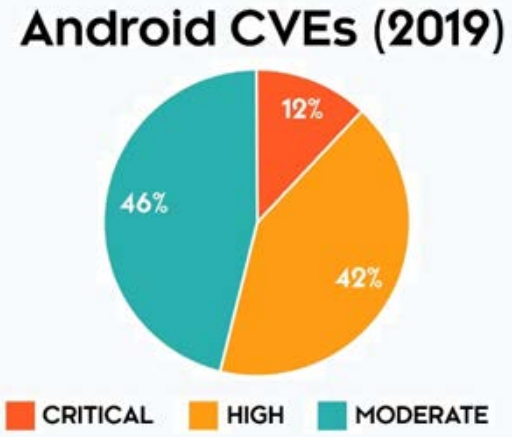
Mobile OS vendors created patches for

1,161 security vulnerabilities

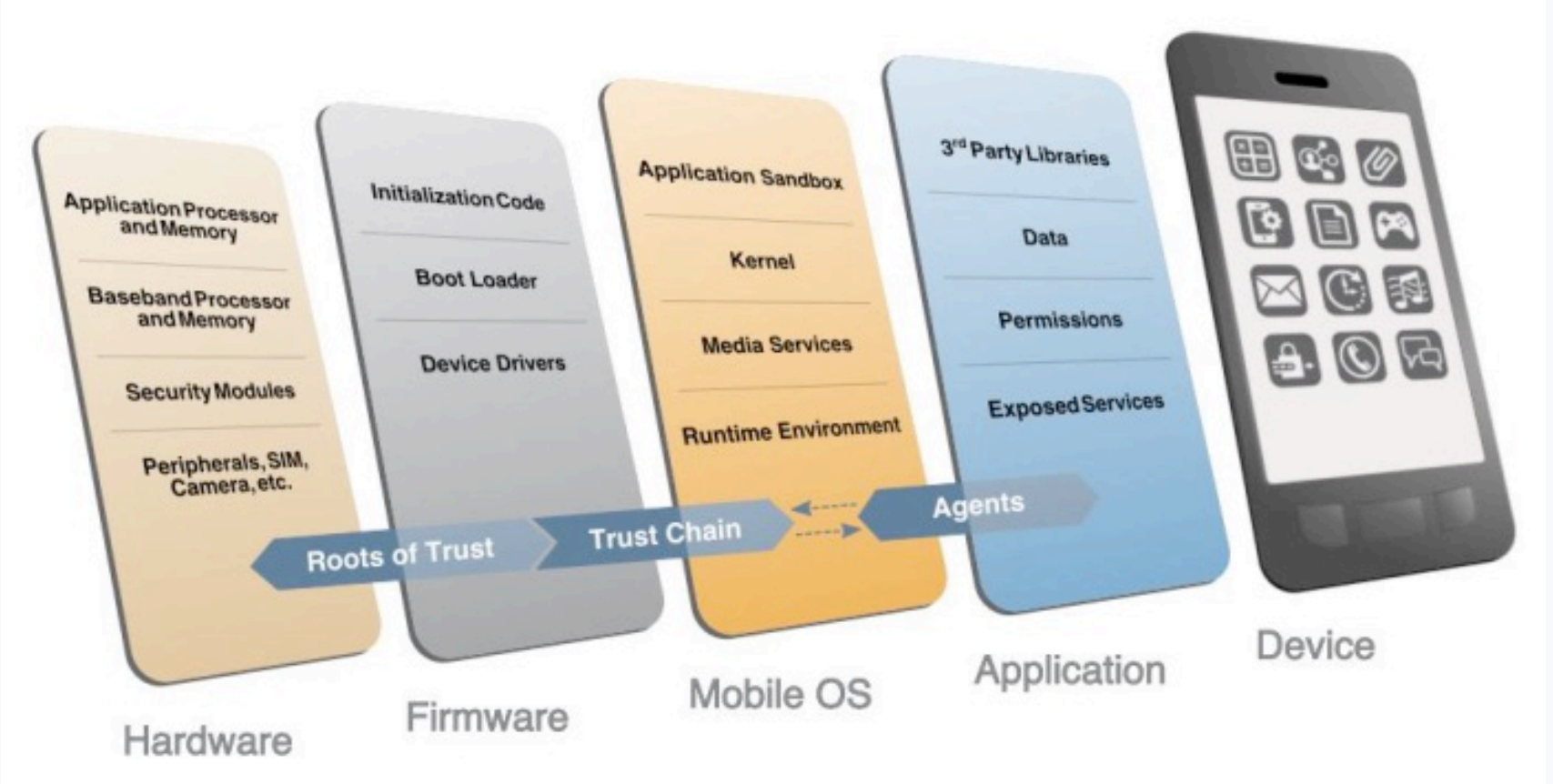
iOS: In 2019, Apple patched 306 CVEs (Common Vulnerabilities and Exposures), 64% of which were considered "critical" security threats.



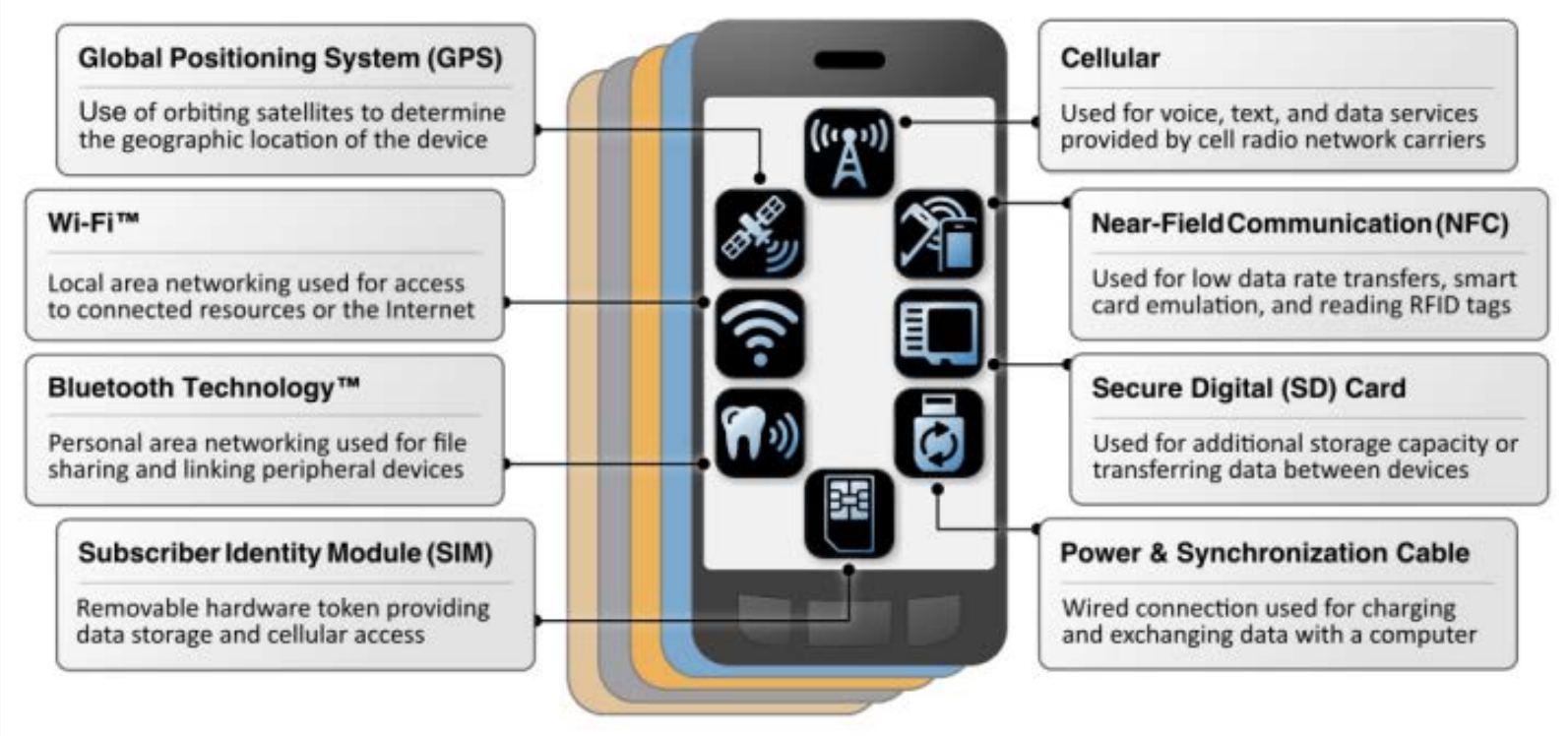

Android: In 2019, Google patched 855 CVEs, the majority of which (54%) were considered "critical" or "high" security threats.



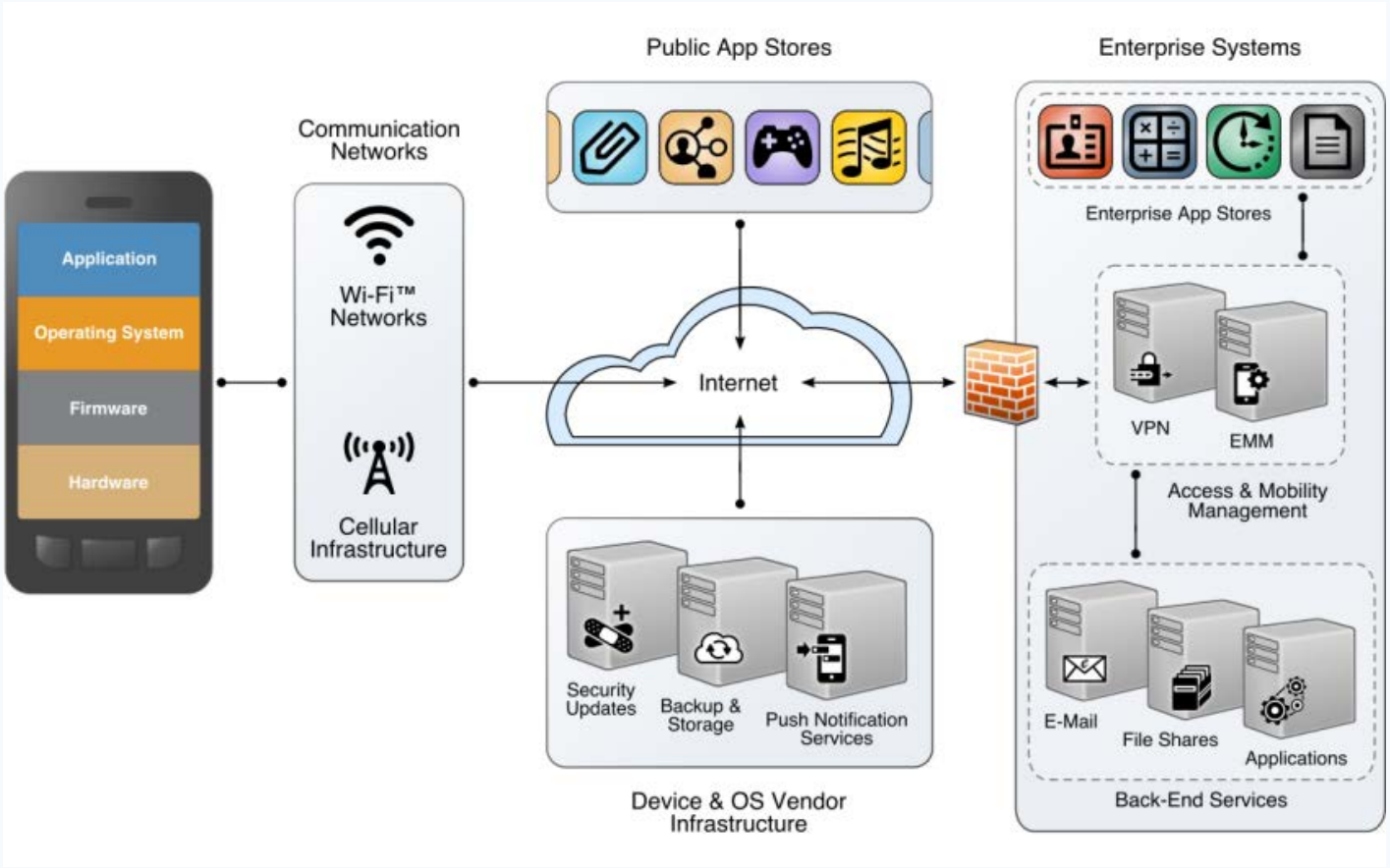
# Mobile Device Technology Stack



# Mobile Device Attack Surface



# Mobile Ecosystem






Qualys.

# Device Platforms

- Android OS Released
- Android Things
- Android TV
- Chrome OS
- Wear OS

- iOS Released
- Mac OS
- Apple Watch
- Apple TV
- Windows 10

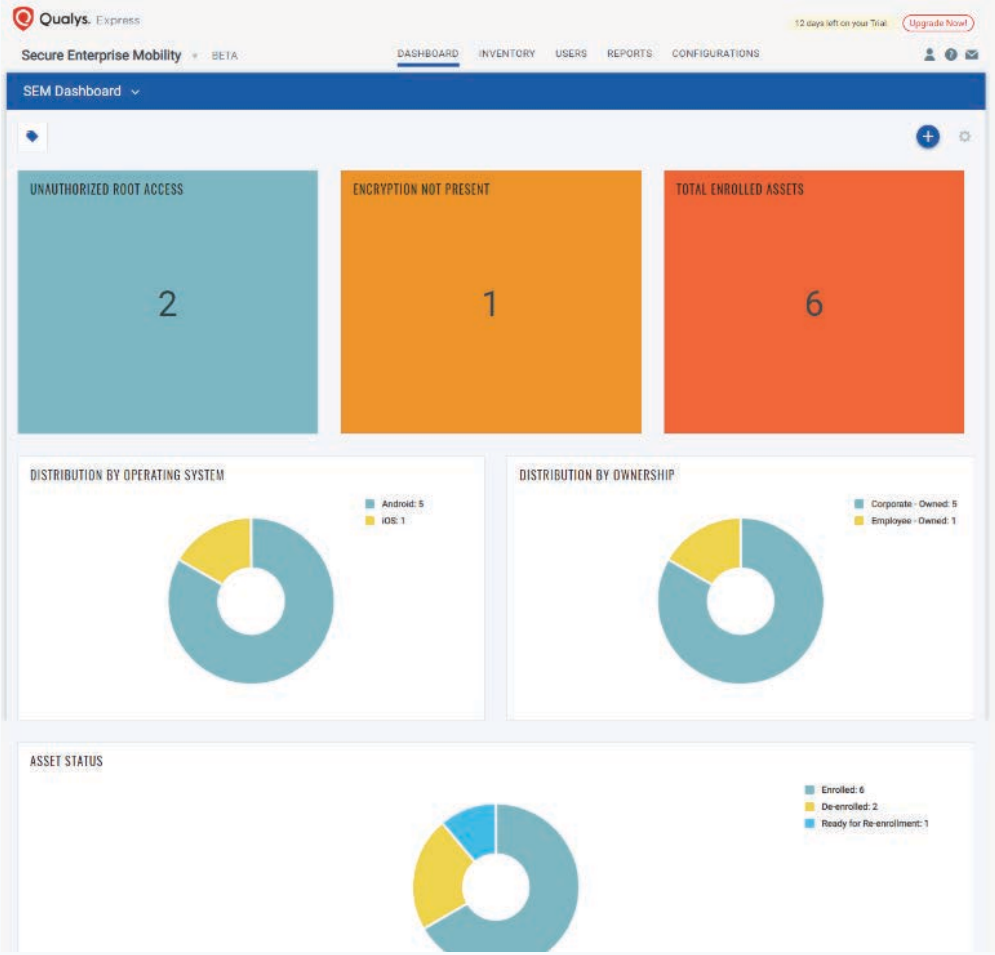
Qualys.

# Mobile Security Solutions

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

# Complete Visibility

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

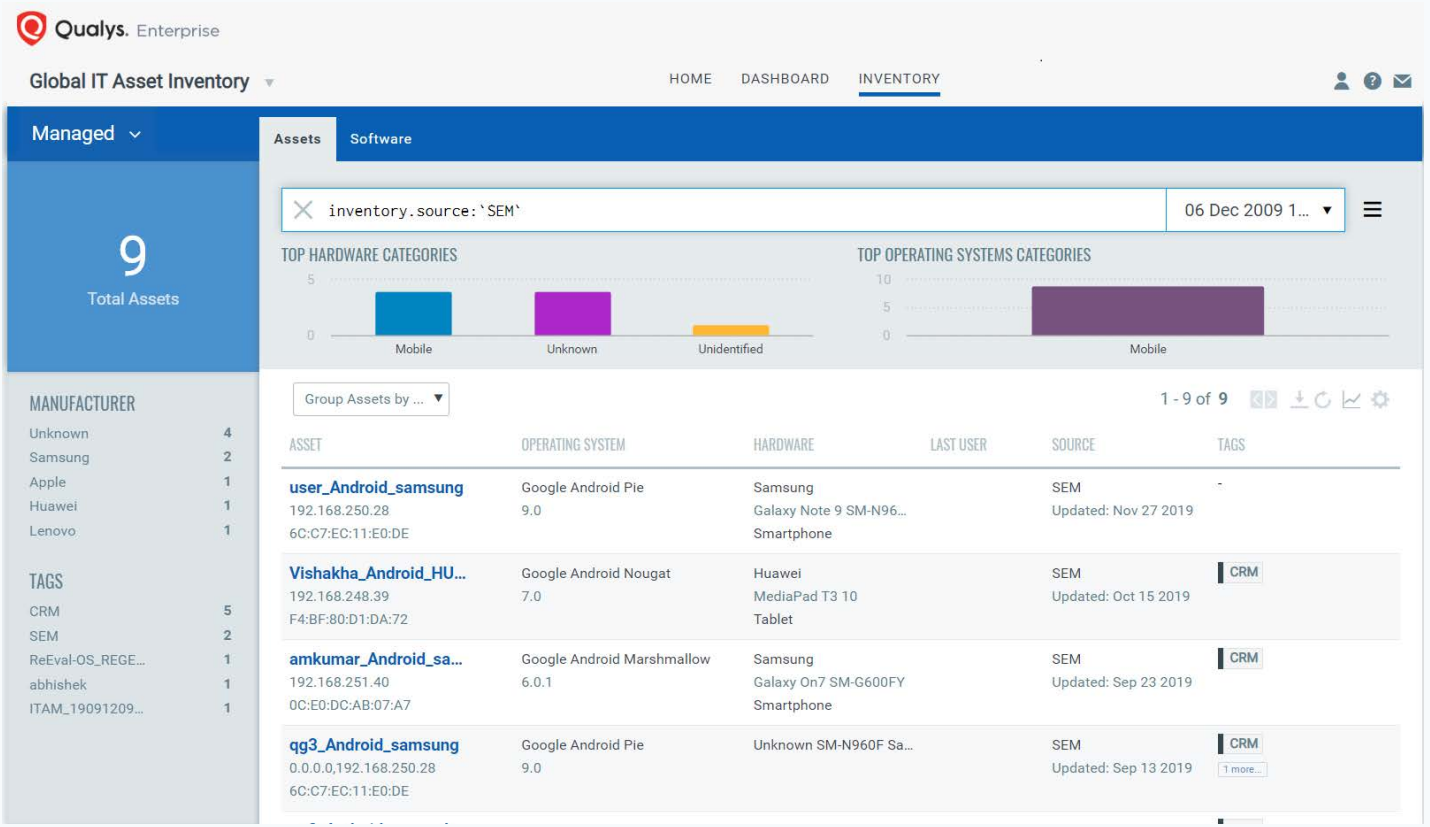





Qualys.

# Integration with Global Asset Inventory

Devices enrolled in SEM will get listed in Global Asset Inventory





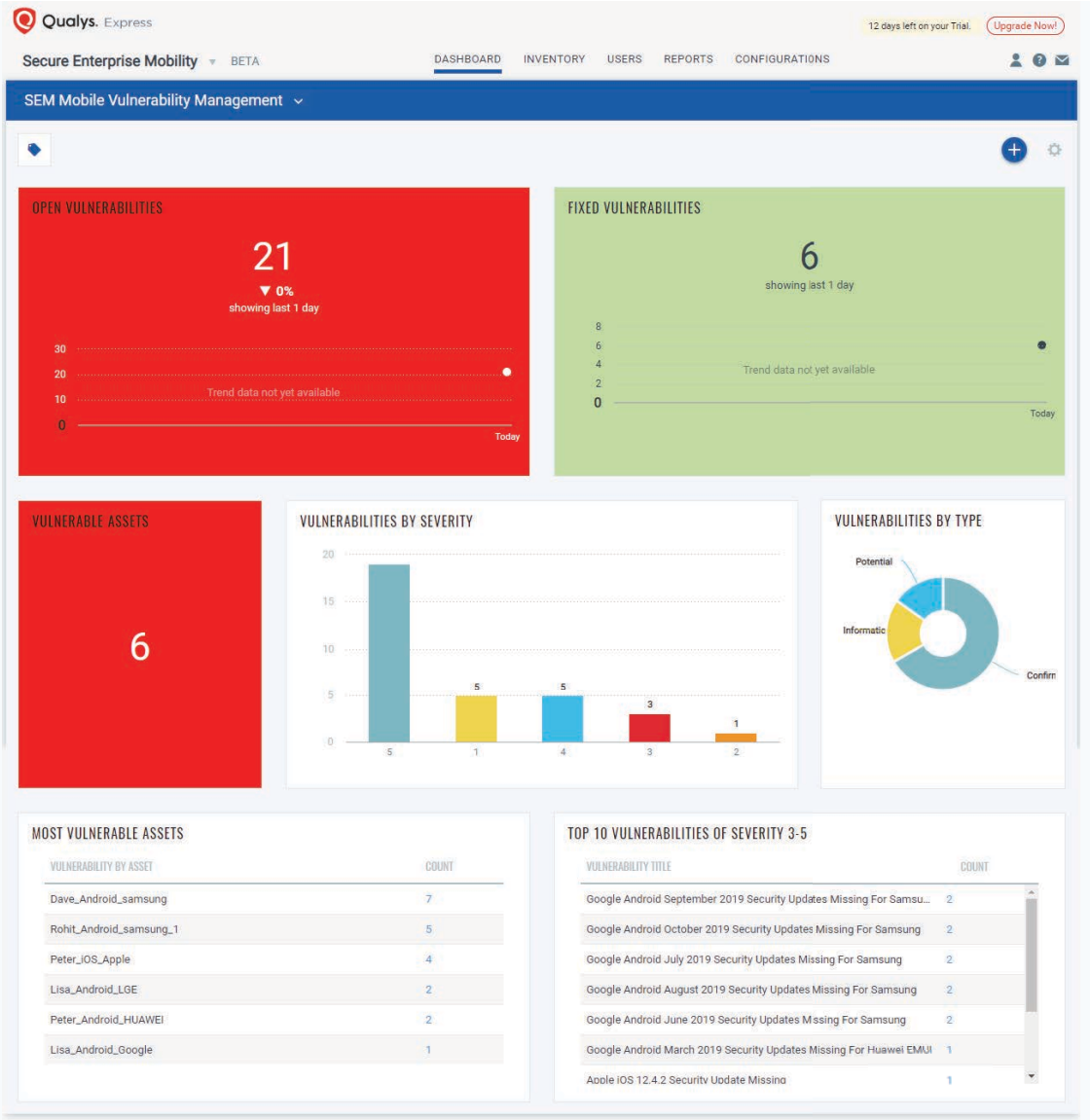

Qualys.

# 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: | 357192107030334 |
| MAC Address: | 48:9D:D1:C4:69:27 |
| UDID: | 9981B7D86481CD5BAB3CC2E663D0DA0F4F65AD8E |
| Asset ID: | 267219 |
| Username: | RohitJain |

### Security Posture

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

### Last Location


### Tags

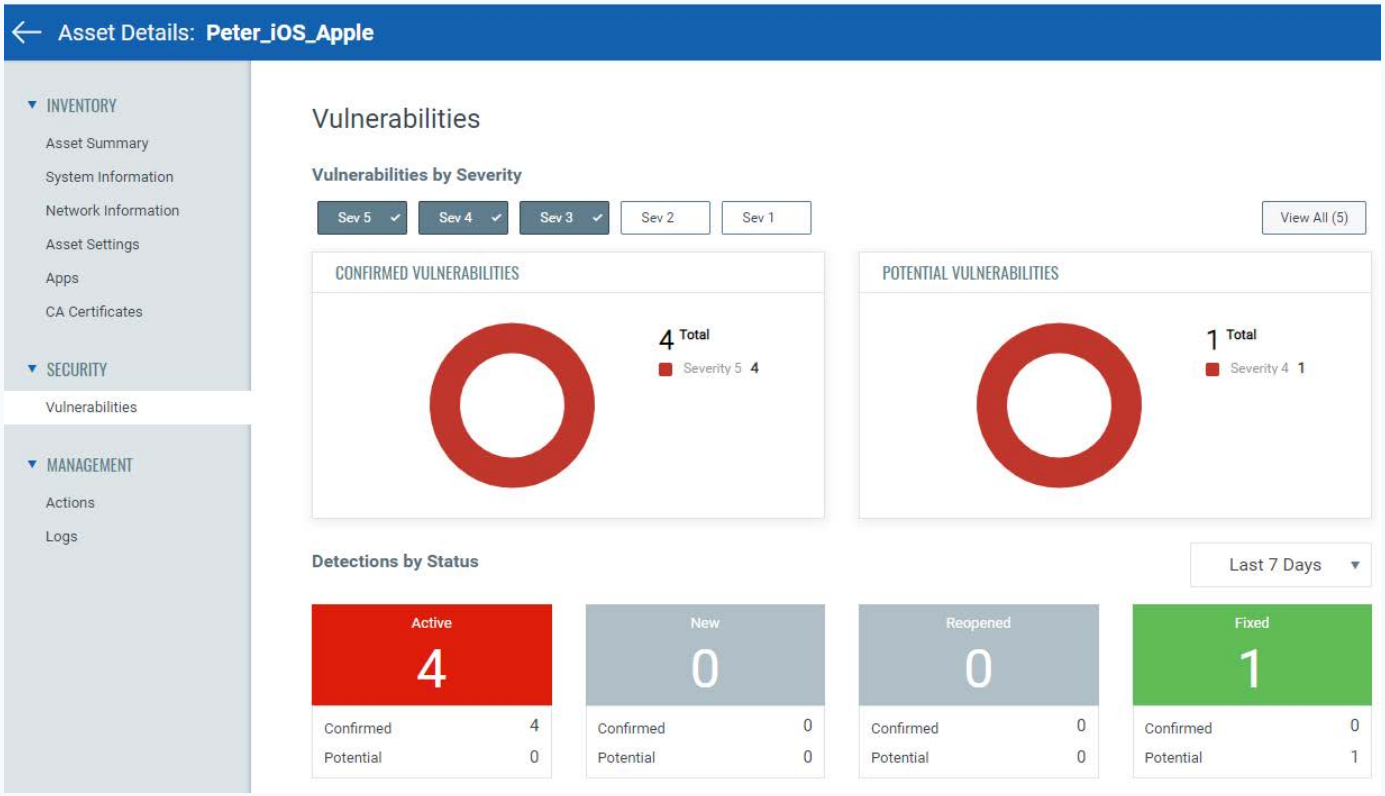
SEM



Qualys.

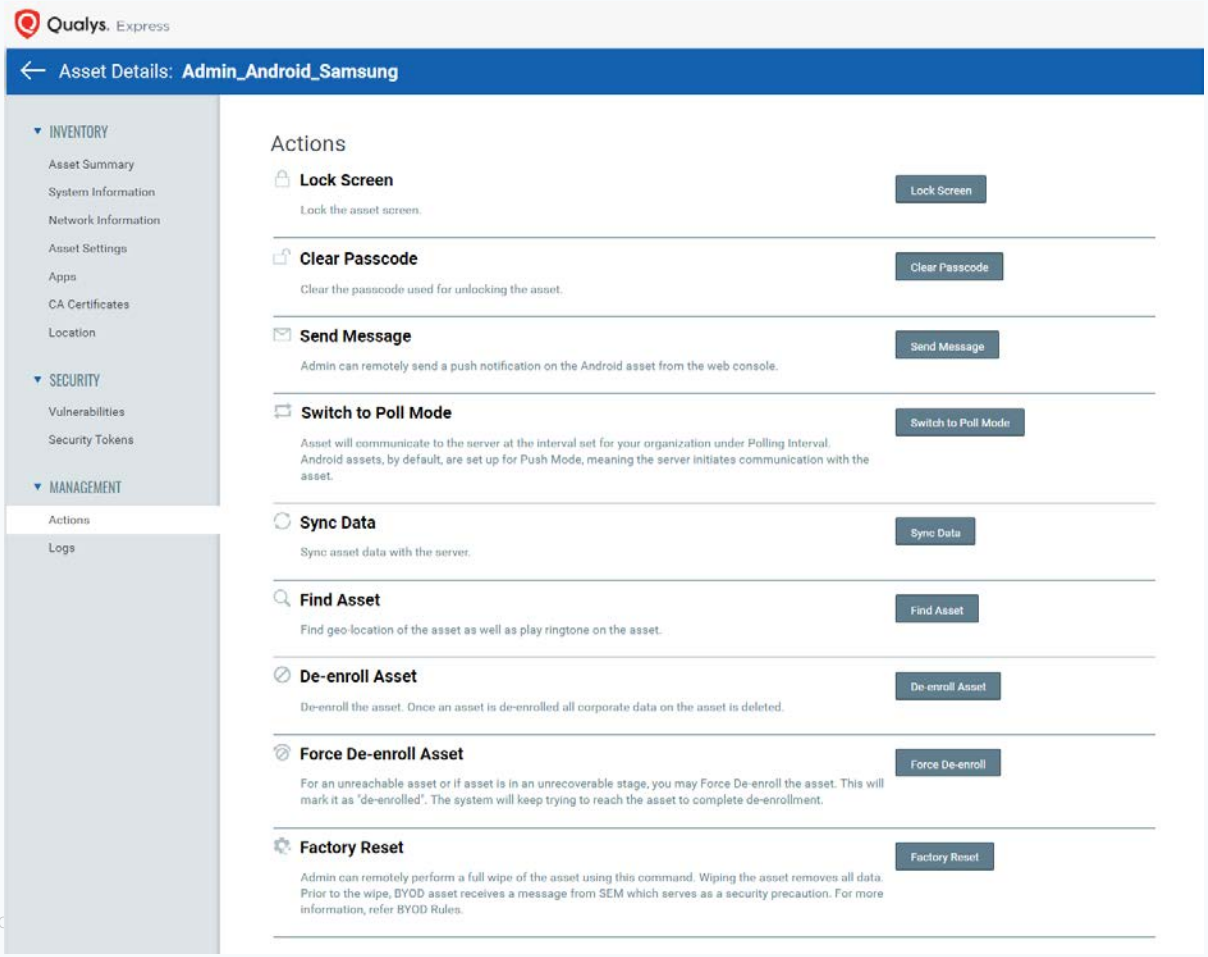
# Vulnerabilities

Same user experience as any other asset in Qualys



# Active Device Operations

These actions helps you to manage and prevent the data loss present on the mobile device



# Capabilities and Roadmap

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

# Thank You

Jimmy Graham
jgraham@qualys.com