



QUALYS SECURITY CONFERENCE 2020

Secure your mobile devices

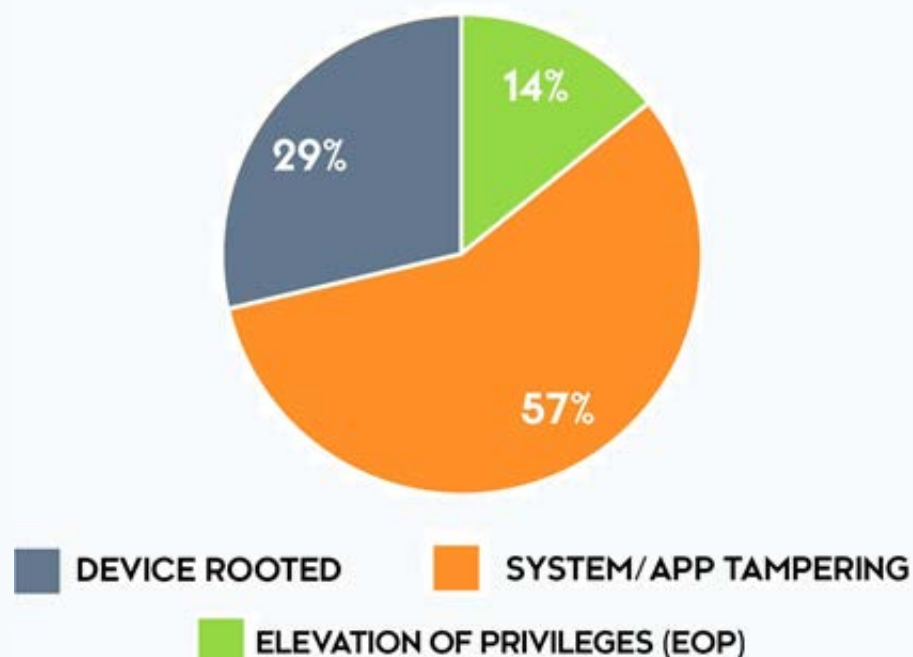
Secure Enterprise Mobility (SEM)

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.

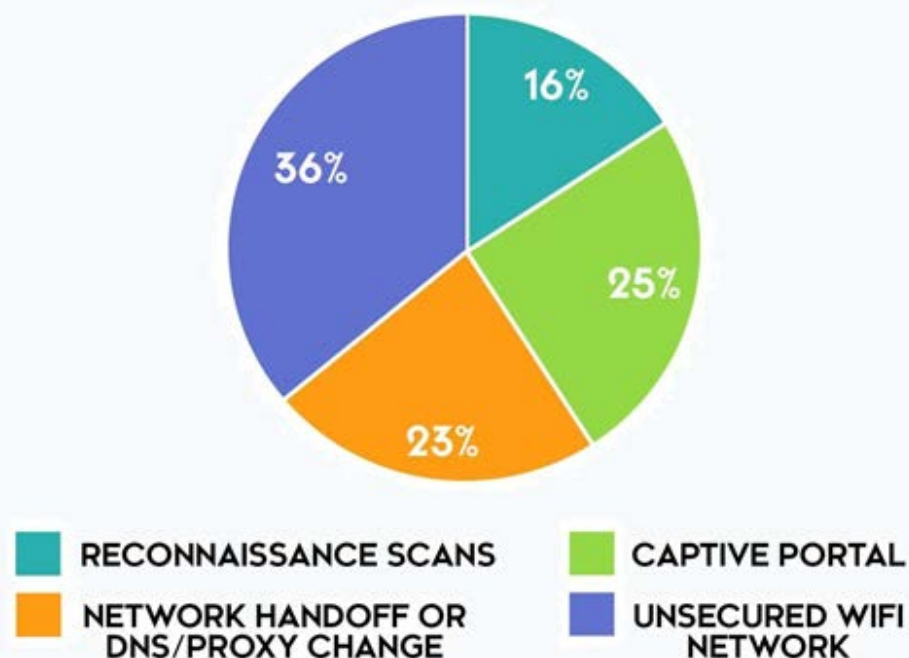
DEVICE ATTACKS (2019)



Network Threats and Attacks

Network threats were through
Unsecured or unencrypted Wi-Fi
networks **36%** , Captive portals
25%, Network handoffs **23%**

NETWORK THREATS (2019)

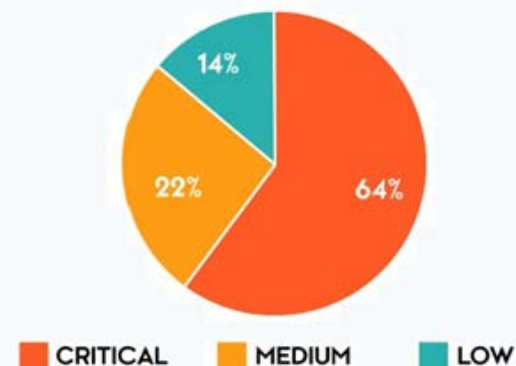


Vulnerabilities in iOS and Android OS

Mobile OS vendors created patches for **1,161** security vulnerabilities

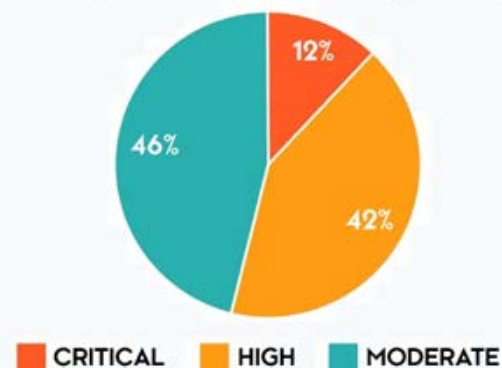
iOS: In 2019, Apple patched 306 CVEs (Common Vulnerabilities and Exposures), 64% of which were considered "critical" security threats.

iOS CVEs (2019)

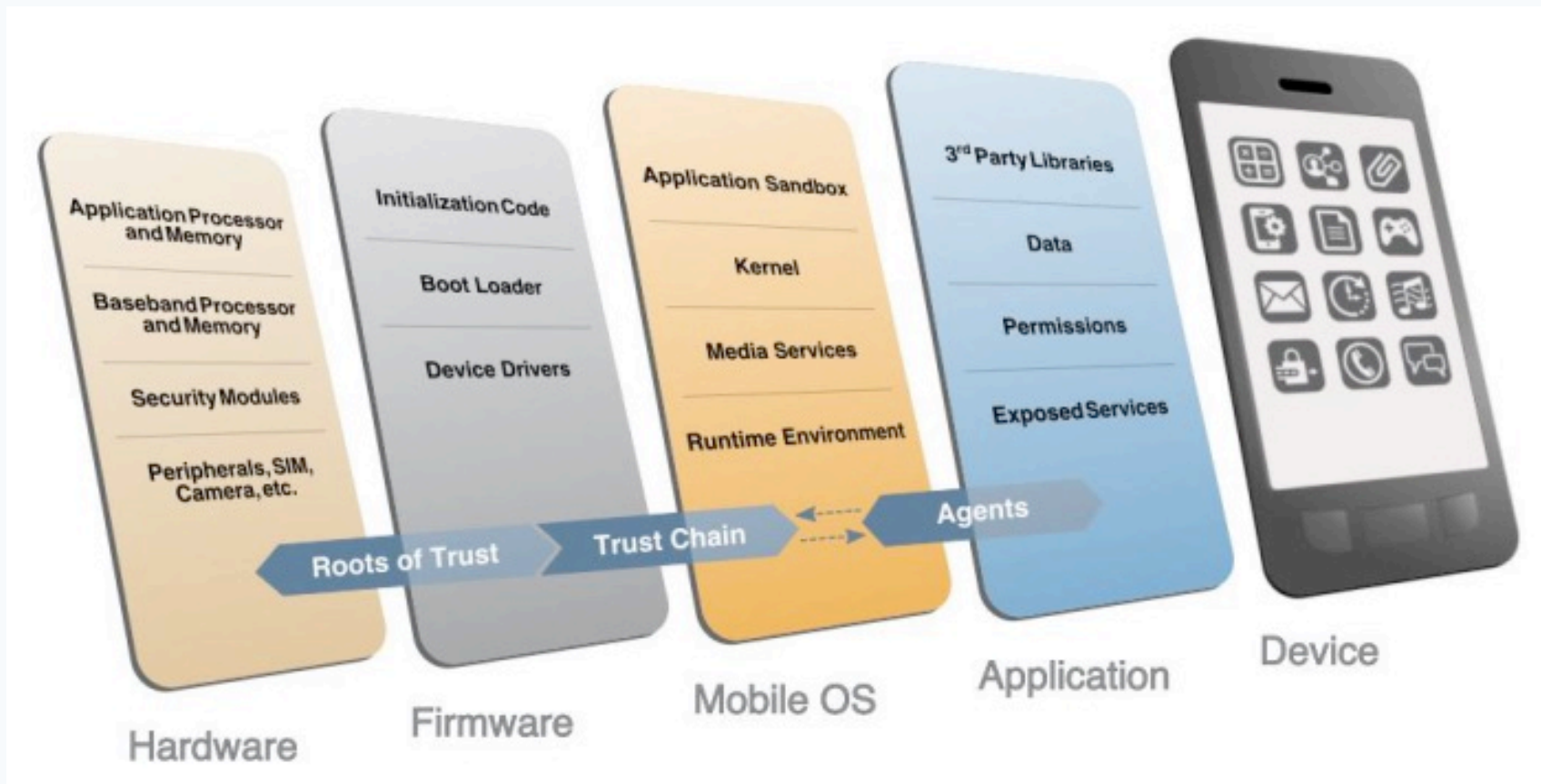


Android: In 2019, Google patched 855 CVEs, the majority of which (54%) were considered "critical" or "high" security threats.

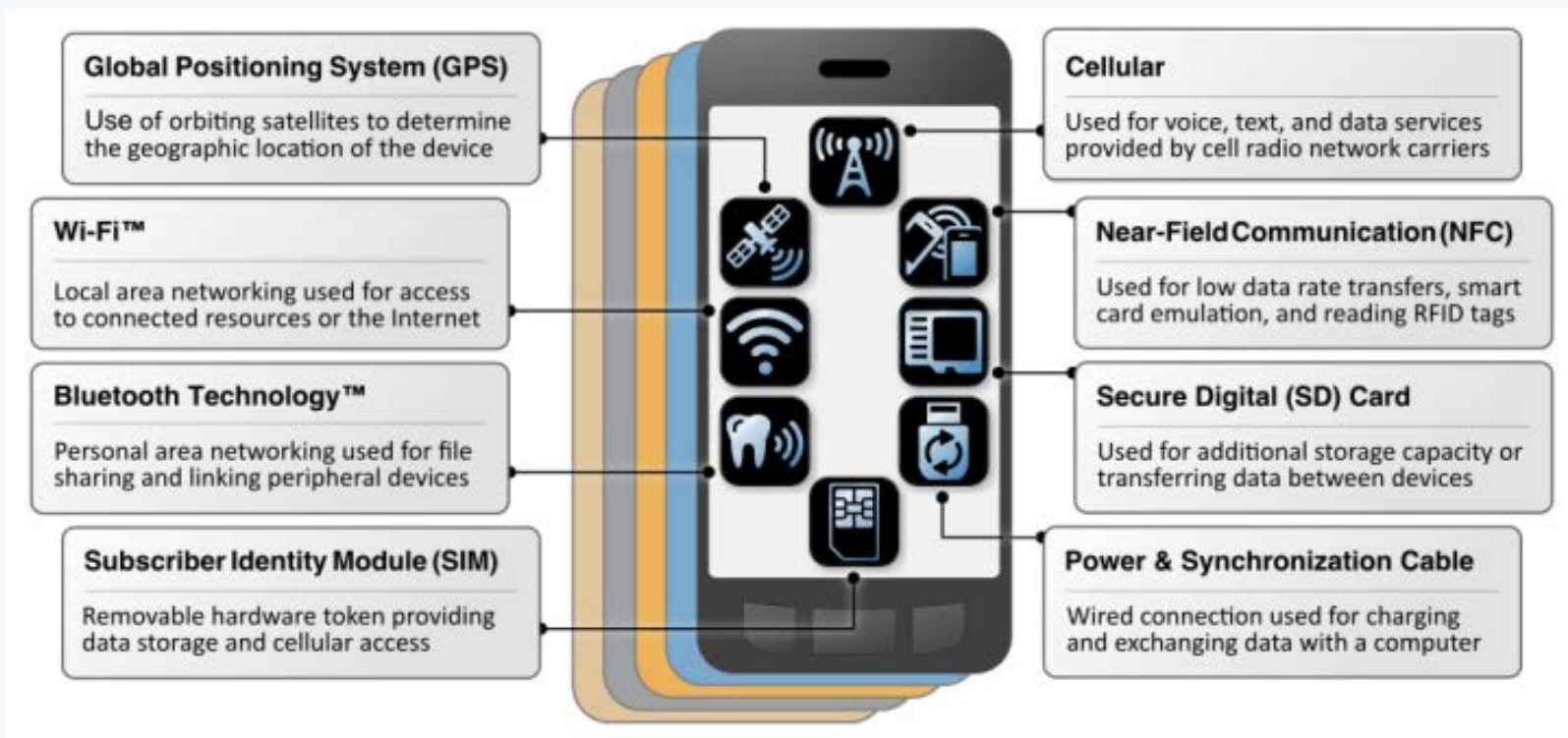
Android CVEs (2019)



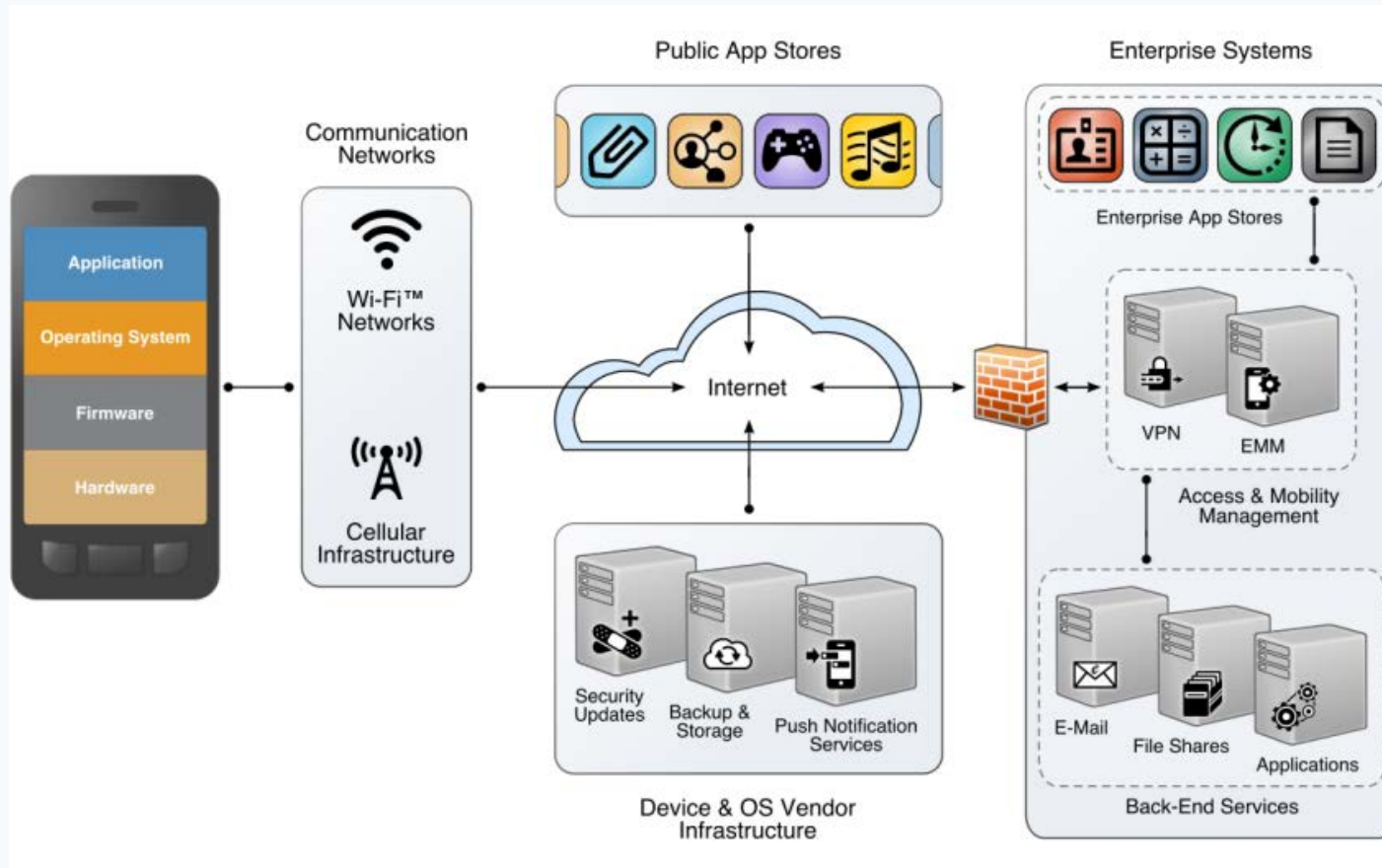
Mobile Device Technology Stack



Mobile Device Attack Surface



Mobile Ecosystem



Device Platforms

■ Android OS ^{Released}

■ Android Things

■ Android TV

■ Chrome OS

■ Wear OS



■ iOS ^{Released}

■ Mac OS

■ Apple Watch

■ Apple TV

■ Windows 10

Mobile Security Solutions

EMM/UEM

- **Lifecycle Management**
- **MDM**
- **Visibility**
- App Store
- Containerization
- Integration with Apple, Google and Microsoft eco-systems

Mobile Threat Defense

- **Device – OS versions, security update, system parameters, device configuration, firmware**
- **OS Vulnerabilities**
- Network VM
- App VM – MATD

Mobile EPP

- Anti-Virus
- Anti-Mobile Phishing
- Device Attack Protection
- Content Filtering

Mobile Policy Compliance

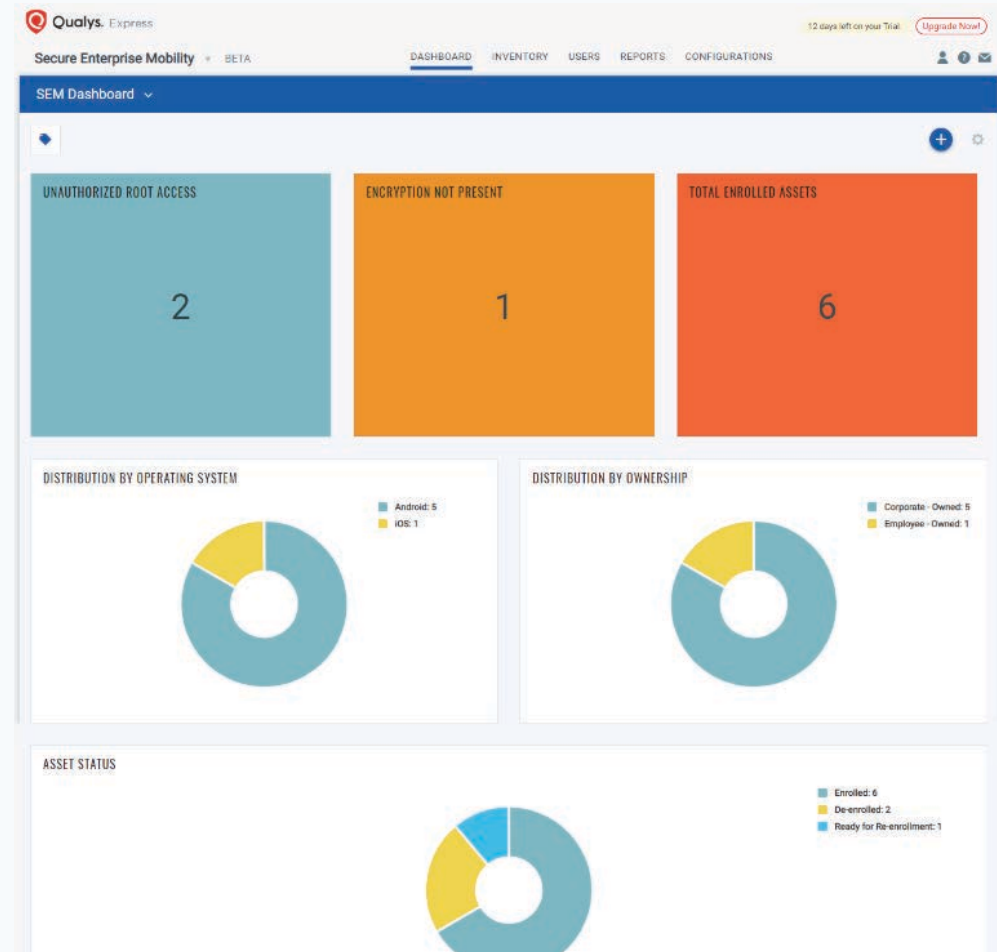
- Integration with PC module for NIST, GDPR, CIS, PCI and rest
- App Compliance
- Define Rules

Enterprise Integrations

- Mobile Identity and Access Management
- Mobile Information Protection and Control
- Mobile Gateway and Access Protection

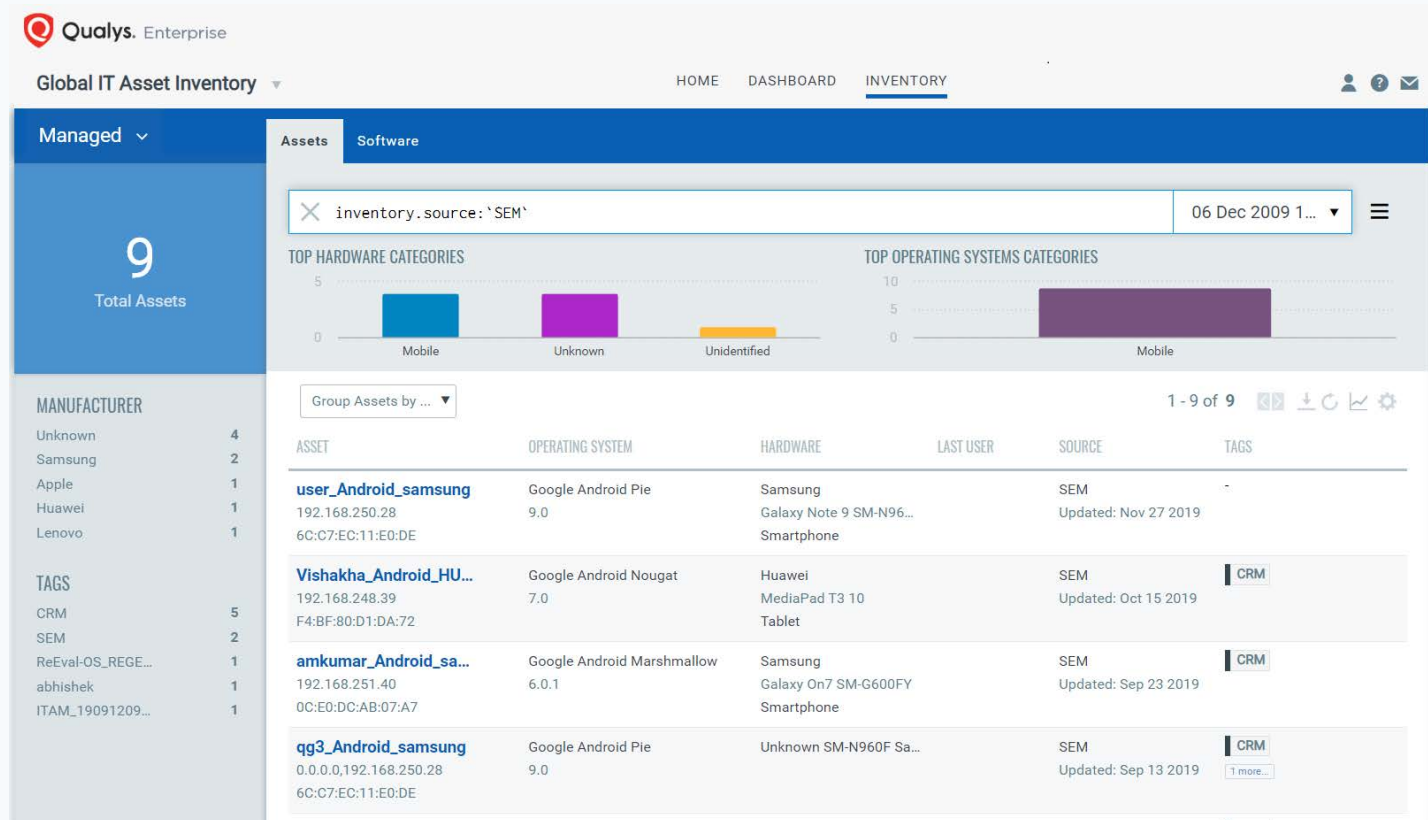
Complete Visibility

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

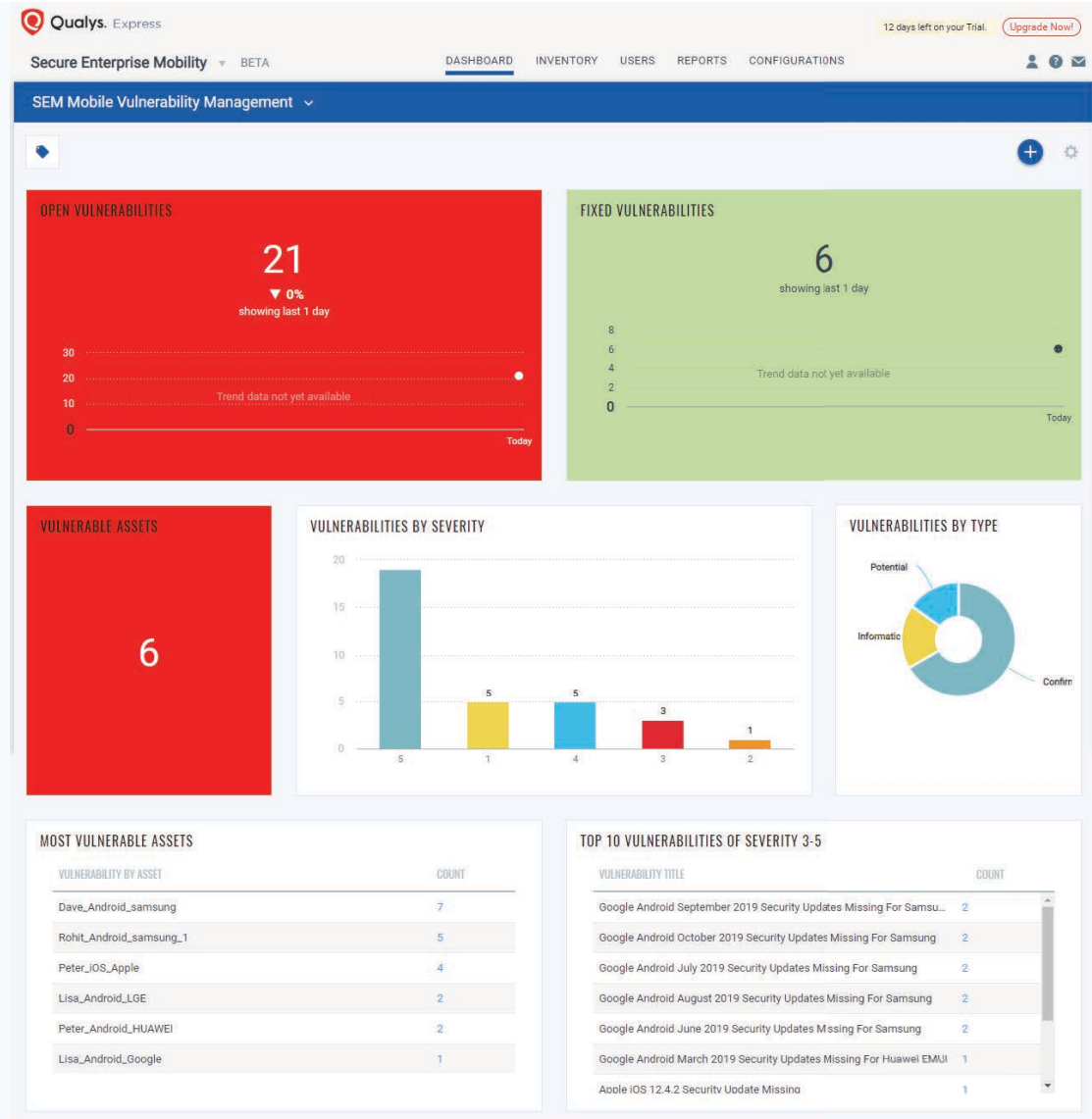


Introducing VM for Mobility (Beta)

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:	357192107030334
MAC Address:	48:9D:D1:C4:69:27
UDID:	9981B7D86481CD5BAB3CC2E663D0DA0 F4F65AD8E
Asset ID:	267219
Username:	RohitJain

Security Posture

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

Last Location

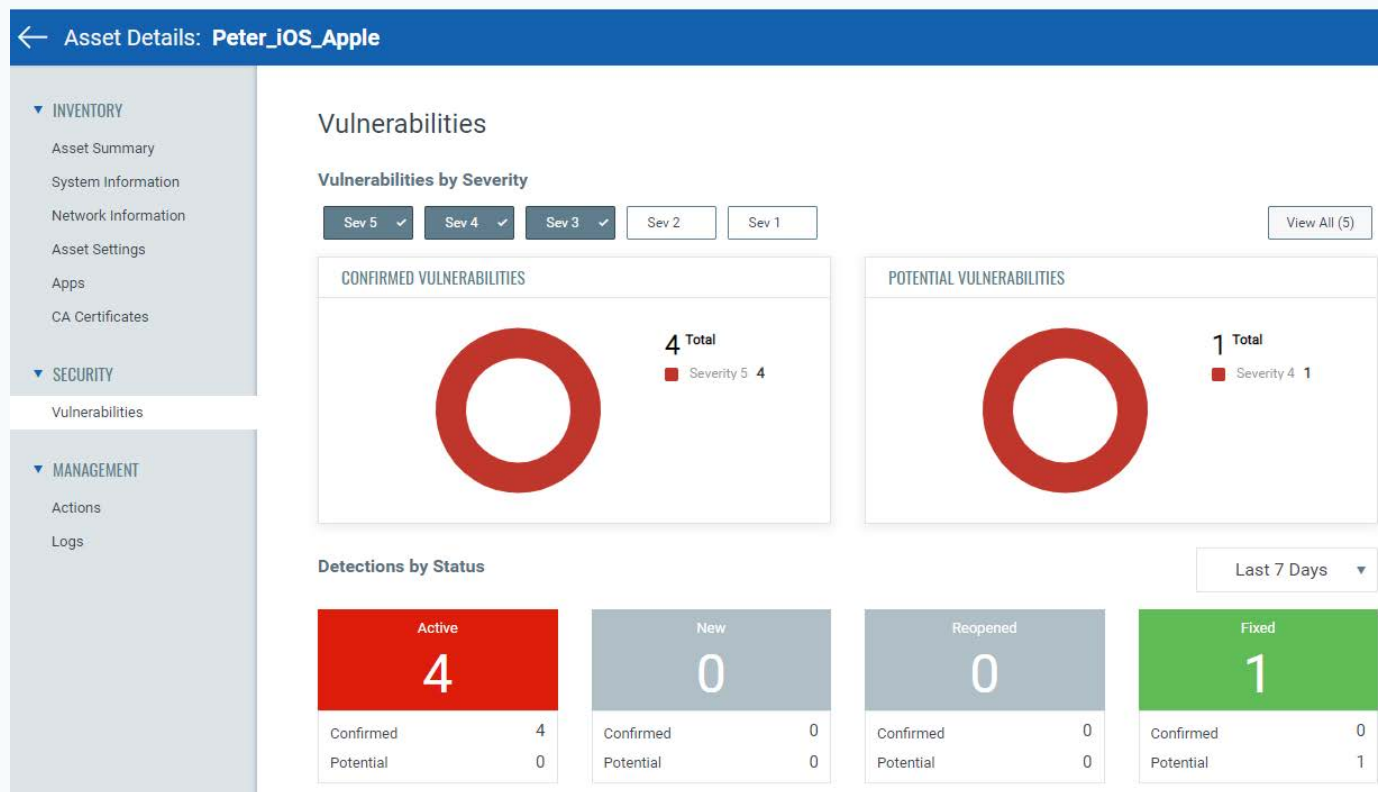


Tags

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

The screenshot displays the Qualys Express interface for managing an Android device. The left sidebar contains a navigation menu with categories: INVENTORY (Asset Summary, System Information, Network Information, Asset Settings, Apps, CA Certificates, Location), SECURITY (Vulnerabilities, Security Tokens), and MANAGEMENT (Actions, Logs). The main content area is titled 'Asset Details: Admin_Android_Samsung' and lists several actions:

- Lock Screen**: Lock the asset screen. (Lock Screen button)
- Clear Passcode**: Clear the passcode used for unlocking the asset. (Clear Passcode button)
- Send Message**: Admin can remotely send a push notification on the Android asset from the web console. (Send Message button)
- Switch to Poll Mode**: Asset will communicate to the server at the interval set for your organization under Polling Interval. Android assets, by default, are set up for Push Mode, meaning the server initiates communication with the asset. (Switch to Poll Mode button)
- Sync Data**: Sync asset data with the server. (Sync Data button)
- Find Asset**: Find geo-location of the asset as well as play ringtone on the asset. (Find Asset button)
- De-enroll Asset**: De-enroll the asset. Once an asset is de-enrolled all corporate data on the asset is deleted. (De-enroll Asset button)
- Force De-enroll Asset**: For an unreachable asset or if asset is in an unrecoverable stage, you may Force De-enroll the asset. This will mark it as 'de-enrolled'. The system will keep trying to reach the asset to complete de-enrollment. (Force De-enroll button)
- Factory Reset**: Admin can remotely perform a full wipe of the asset using this command. Wiping the asset removes all data. Prior to the wipe, BYOD asset receives a message from SEM which serves as a security precaution. For more information, refer BYOD Rules. (Factory Reset button)

Capabilities and Roadmap

Today

- Visibility
- Inventory
- Over 100 data points indexed
- Integration with GlobalAI

Q1/Q2 2020

- iOS Agent Release
- OS Vulnerabilities
- App vulnerabilities (Part 1) (Beta)

Q3/Q4 2020 and later

- 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



QUALYS SECURITY CONFERENCE 2020

Thank You

Jimmy Graham
jgraham@qualys.com