Fortune 500 Financial Services Firm Closes its Mobile Security Gap with Lookout

The Challenge

A global financial services firm, having successfully managed employee mobile devices with an EMM solution, recognized that they still lacked critical security visibility and risk management on these endpoints. In an initiative led by their VP of Mobile Engineering, they sought a complementary mobile security solution to address the following challenges:

Security Challenges

- Gain visibility into app- and device-based security threats such as sideloaded apps on iOS and rooted devices on Android
- Satisfy an internally mandated compliance goal to protect data on mobile endpoints
- Reduce data leakage risks to customer information since mobile devices have become a primary endpoint for accessing this type of information

In speaking with numerous Fortune 500 security architects and mobility managers across a range of industries, Lookout sees many companies experiencing these same challenges when faced with the reality that smartphones and tablets have become a primary computing device for employees.

Customer Profile	
Size	Fortune 500
Industry	Financial Services
iOS devices	> 10,000
Android devices	> 2,500
Mobility policy	COPE & BYOD
EMM solution	MobileIron
Mobile security solution	Lookout

The Criteria

This financial services firm needed a mobile security solution that met the following criteria.

Solution Criteria

- Robust, cross-platform security protection for both iOS and Android devices from app- and device-based threats
- Integration with MobileIron's app provisioning and device remediation capabilities to leverage their existing investment in EMM

With thousands of iOS and Android devices spanning a global workforce and a BYOD-friendly mobility policy, the customer also needed a security vendor who could offer worldwide support and deliver an endpoint solution that would be welcomed on personally owned employee devices.

The Lookout Choice

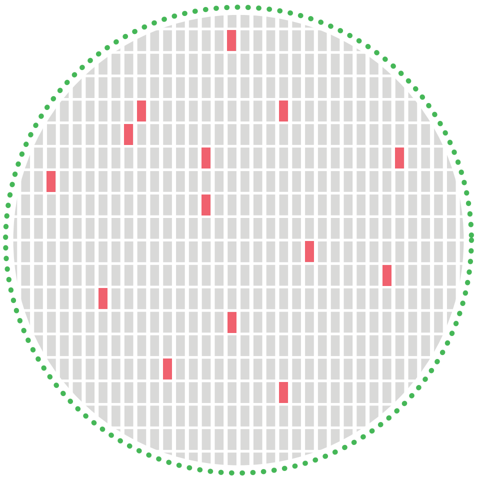
After conducting due diligence on a number of mobile security solutions, this financial services firm chose Lookout Mobile Threat Protection for its superior defense capabilities afforded by the security intelligence Lookout gathers from its mobile sensor network of over 100 million devices worldwide.

As an official Threat Protection Partner of MobileIron, Lookout also integrated with the firm's current EMM provider and allowed the firm to automatically provision Lookout's endpoint application across their mobile workforce and to develop custom device remediation policies based on security intelligence and threat detections transmitted from Lookout's endpoint client.

Success Through Measurable Risk Reduction

Within weeks of Lookout deployment to thousands of devices, the customer saw measurable risk reduction via mobile security incidents that Lookout detected and successfully resolved, largely through employee self-remediation.

Customer Business Objectives	Outcomes Achieved with Lookout
Gain security visibility into mobile app and device threats	Lookout's console provides admins with real-time visibility into app- and device-based threats in the mobile fleet
Satisfy internal endpoint-compliance mandate	Lookout Mobile Threat Protection serves as a technical control to protect mobile end-points
Reduce customer data leakage risks	Lookout detects and successfully remediates mobile threats such as XcodeGhost that could cause customer data leakage



Detections over 30 days of deployment (7,700 devices)

iOS	Sideloaded applications:	110 sideloaded app detections
	Sideloaded apps are not reviewed by Apple and can run on non-jailbroken iOS devices because they use enterprise provisioning certificates. Thus, they present a potential security risk and can also be a vector for malware that steals enterprise data if attackers compromise or otherwise fraudulently obtain an enterprise provisioning certificate.	
	Trojans	1 detection (XcodeGhost) | 1 detection (YiSpecter)
	XcodeGhost, a trojan that steals data from affected devices, was inserted into a number of iOS apps in the App Store via a compromised version of Apple's development tool, Xcode. This threat can be used to phish end-user credentials by prompting them to visit fraudulent webpages. YiSpecter is a trojan that can install and execute arbitrary iOS apps and steal data from affected devices.	

Android	Compromised devices	1 rooted device detection
	Rooting a device gives potential attackers access to escalated administrative privileges and can compromise native Android security features such as app sandboxing, or potentially compromise OS-dependent security features like app containers.	
	App-based threats	102 riskware detections | 2 chargeware detections | 7 adware detections
	Riskware apps include code, libraries, or network services that pose a risk to devices due to known vulnerabilities or the low reputation of service providers used by the apps. Chargeware misleadingly charges the victim's wireless bill. Adware serves intrusive ads or sends excessive personal data like IMEI to ad networks, exceeding standard advertising practices.	

After implementing Lookout Mobile Threat Protection, this financial services firm closed a critical gap in their mobile data protection strategy and successfully met their core business objectives.

Moreover, within weeks of Lookout deployment to thousands of devices, the VP of Mobile Engineering could demonstrate measurable risk reduction to internal stakeholders via a report of the security incidents Lookout had detected and resolved. In summary, Lookout Mobile Threat Protection enabled this Fortune 500 firm to achieve secure mobility across their global workforce.

To obtain a free mobile risk assessment and better understand
your organization's risk profile, please reach out to sales@lookout.