# Global 2000 bank secures 9,000 Android smartphones to fulfill internal compliance requirements

## The Challenge

To enable their Corporate Owned, Personally Enabled (COPE) mobility policy, this leading bank needed a mobile security solution that would comply with their internal policy for data protection, integrate with VMware AirWatch, and provide visibility into mobile threats encountered by their international workforce.

The IT team decided to implement a COPE mobility policy in order to reduce support time by having a limited number of device models and Android versions to maintain. In addition, the bank has developed their own enterprise application that enables their employees to deliver banking services to customers via mobile devices. With no visibility into threats or data leakage on mobile devices, the IT mobility team knew that their unprotected mobile endpoints were an attack surface that presented a major security risk.

### Customer Profile

This financial services firm is based in the middle east, has an international network of 1400 branches globally, and is a member of the Forbes Global 2000 list.

**Industry:** Financial services

**Mobility Policy:** COPE

**EMM Solution:** VMware AirWatch

### The Solution

- Lookout Mobile Endpoint Security

### The Results

- Achieved compliance with internal policies for endpoint protection
- Gained visibility into high-risk threats
- Improved employee productivity with no increase in support tickets

> "Lookout delivers a solution that collects threat data from around the world, and gives us visibility into all the risks to our mobile data."

Manager, IT Infrastructure Division

As a financial services firm, this bank is part of a regulated industry, but national compliance and privacy rules for mobile devices are still new and not well defined in its home country. However, the IT mobility team views mobile devices as no different from laptops, and simply another endpoint to access corporate resources. So, in order to comply with their internal policies to secure all endpoints this bank needed a mobile security solution that would complement AirWatch, the bank's own encryption policies, and employee security awareness education.

## The Solution

The IT team evaluated a number of solutions to solve their mobile security challenges. They found that legacy endpoint security vendors either didn't offer Android support, or approached mobile security by relying on signature-based threat detection that can't keep up with rapidly evolving threats on mobile platforms.

The IT team selected Lookout due to its unique mobile threat intelligence which collects data from around the world. The team concluded that Lookout Mobile Endpoint Security was the right solution to enable their mobile workforce to access productivity apps freely, eliminating the need to manually maintain app "blacklists" and "whitelists." The team then worked with Lookout to deploy and activate Lookout Mobile Endpoint Security on approximately 9,000 Samsung Galaxy smartphones. They easily deployed the Lookout For Work app via AirWatch to employees by pushing the app to the devices without the need for employee action.

## The Results

The bank is very happy with how quickly they were able to deploy Lookout, including pushing the Lookout For Work app out to 2,000 devices a day towards the end of the process.

As the deployment progressed, Lookout Mobile Endpoint Security detected a significant number of high-risk apps, auto-rooting malware, and man-in-the-middle attacks in the bank's mobile fleet. The detection of these significant threats validates the bank's decision to prioritize compliance with their internal policies for endpoint protection.

## The Conclusion

Since deployment, the bank is very pleased to note no increase in new support tickets, since employees are self-remediating mobile threats, after getting alerted by the Lookout For Work app on their device.

Now that the bank's IT team has achieved their goals of meeting compliance objectives and getting visibility into mobile threats and risky apps in their mobile fleet, they're focused on next steps, which include using the Lookout and AirWatch integration to activate automated remediation policies in AirWatch for threats detected by Lookout to further reduce remediation time.

| By the numbers: threats detected | |
|---|---|
| **Trojans** | |
| 16 trojan detections<br>5 detections (Shedun) | Shedun is a family of Android malware first discovered by Lookout in 2015. It pretends to be a legitimate application, but is malicious and will attempt to root the device and allow a third party to install additional apps. This can cause the installation of additional malware. |
| **Compromised Devices** | |
| 37 root enablers detected | Rooting a device gives potential attackers access to escalated administrative privileges and can compromise native Android security features such as app sandboxing. |
| **Network-based Attacks** | |
| 91 Man-in-the-Middle attacks | Attackers can use a number of techniques to intercept network traffic to and from a mobile device. If physically nearby a target device, an attacker can use a malicious Wi-Fi or cellular network to gain access to network traffic. If not nearby, attackers can use malware or socially engineer users to configure a device to route all network traffic through malicious proxy or VPN connection. |
| **App-based threats** | |
| 172 riskware detections<br>61 adware detections<br>3 chargeware 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 device, and adware serves intrusive ads or sends excessive personal data to ad networks that exceeds standard advertising practices. |