Investment bank Greenhill & Co secures BYOD by protecting highly sensitive client data accessed by employee devices across the globe

The Challenge

Greenhill & Co's Senior IT Manager Dan Dougherty was an early adopter of mobile security when he led the pilot deployment of a less-mature Mobile Threat Defense product in the first half of 2016. However, a full deployment was never completed due to high numbers of false positive detections for network-based attacks and that product's approach of "blackholing" all traffic from the end-users' device to the vendor's servers, which was a problem for both end-user privacy and highly sensitive client data.

Dan and his global team knew they had to find a new solution to address Greenhill's challenges of securing company and client data accessed by employees on their BYO devices, gaining visibility into data leaking malware such as keyloggers, and complying with Sarbanes–Oxley regulations for safeguarding sensitive data.

Greenhill

Customer Profile

Greenhill is an independent, New York based investment bank considered one of the most elite and prestigious firms on Wall Street. The firm has 14 offices globally and provides advice on mergers, acquisitions, restructurings, financings, and capital raisings to leading corporations, partnerships, institutions, and governments.

Industry: Finance

Mobility Policy: BYOD

EMM Solution: Citrix XenMobile

Security Challenges

- Protecting client financial data including material information in high profile mergers & acquisitions
- Gaining detailed visibility into network attacks and data leaking malware such as keyloggers
- Complying with Sarbanes–Oxley regulations for safeguarding sensitive data

The Solution

Greenhill selected Lookout Mobile Endpoint Security in early 2017 to replace their pilot and secure mobile devices in their BYOD program after seeing how the Lookout admin console provides actionable alerts when mobile risks are detected and helps prioritize which events admins should focus on.

The Greenhill team is fully aware that mobile malware is becoming more prevalent and sophisticated, and they are particularly concerned with keyloggers due to the amount of client information exchanged via email that is often accessed from the personally owned mobile devices of the firm's 82 managing directors. Dan's perspective is that, "Without Lookout, we'd never know if malware or a data leaking app got on an employee's device. For example, a keylogger could steal information from notes or contacts that sync to phone."

> "As a global organization that advises multi-billion dollar mergers and acquisitions, we know we're being targeted and the consequences of data becoming compromised would be significant. That's why we trust Lookout to secure the sensitive data being accessed by our employees' mobile devices while providing actionable alerts for our admins."
>
> **Dan Dougherty,** Senior IT Manager, Greenhill & Co.

Additionally, Dan viewed the Lookout approach to network threat remediation as superior since Lookout detects network threats immediately upon connection and alerts end-users so they won't transmit sensitive data.

The Greenhill team is now looking into the ways they can leverage the exclusive deep integration between Lookout and Microsoft Enterprise Mobility + Security to enable conditional access policies through Microsoft Intune and Office 365, by restricting access to corporate data until Lookout verifies no mobile threats are present on a device.

The Results

Greenhill has completed deployment of the Lookout app to employee mobile devices via their Citrix XenMobile MDM. Since Greenhill employees have completed cybersecurity awareness training they are more security-conscious, and so the Greenhill team expects to deal with fewer user-initiated risks like sideloaded apps or jailbroken devices, and more targeted threats like malware.

While having security-conscious end-users is an advantage, Dan doesn't consider it a cure-all since Greenhill employees regularly travel on business to high risk countries where the risks may be more prevalent and sophisticated. He takes a pragmatic approach to these potential threats, "As a global organization that advises multi-billion dollar mergers and acquisitions, we know we're being targeted and the consequences of data becoming compromised would be significant. That's why we trust Lookout to secure the sensitive data being accessed by our employees' mobile devices while providing actionable alerts for our admins."