Leading healthcare provider deploys Lookout to protect against data compromise on mobile

The Challenge

When this healthcare provider's IT Manager and Security Architect reviewed the results of a recent compliance audit, they found recommendations to add technical safeguards to mobile devices in order to protect Personal Health Information (PHI) and Electronic Health Records (EHR). As technology and security leaders of a healthcare organization, they were concerned about HIPAA protected patient data being accessed on mobile devices. Specifically, they wanted to address the risk of data being compromised by app-based threats like malware and leakage from non-compliant apps.

Even though they had already been using the blacklist feature of their MobileIron EMM to restrict employees from using certain apps on their corporate owned iOS devices, the team recognized the need to improve on the manual process of vetting apps, and the limits of blacklisting apps one at a time. Blacklisting, and its opposite whitelisting where specific apps are approved for use, isn't effective or sustainable for all apps due to the volume of new apps and app updates, which can occur up to 26 times a year, with a major app like Facebook updating approximately every two weeks. Relying on manual app reviews and a hand-curated lists hurts employee productivity and limits employees from using the most helpful apps available.

Customer Profile

Industry: Healthcare

Size: Top 5 healthcare system in the U.S.

Mobility Policy: COPE

EMM Solution: MobileIron

Security Challenges

- Fulfilling recommendations from regulatory compliance audit
- Finding a more cost effective solution than manually blacklisting apps
- Gaining detailed visibility into malware on mobile endpoints

The Solution

This healthcare organization chose Lookout Mobile Endpoint Security because of its superior malware detection, detailed visibility into app behaviors, and end user experience. The first phase of implementation included working with their IT services provider to deploy Lookout on 5,000 managed iOS devices used by visiting nurses and home health care workers.

> "As a healthcare organization, our priority is protecting patient data. But with the sheer volume of mobile apps available, it was a challenge to know what data was being accessed and how. We selected Lookout because it provides us with the visibility we need into app behaviors, eliminating the time-consuming process of blacklisting each individual app."
>
> **IT Site Manager**

To mitigate the risk of data leakage from non-malicious apps, the team wanted the ability to quickly blacklist any set of apps exhibiting behaviors that violate compliance policies, including the ability to set custom policies for which apps employees are approved to use based on how those apps handle and send sensitive data.

With Lookout, the team is now able to set custom policies that prevent potential leakage of patient data. For example, to prevent HIPAA protected patient contact records from being leaked, admins can set a policy to prevent home care nurses from using any app that accesses contact records on their corporate owned iPads.

Next Steps

The next two phases of their mobile security initiative include working with Lookout to review the security of legacy healthcare applications as they're ported to iOS, and rolling out Mobile Endpoint Security to additional mobile devices.

As a leading healthcare organization, both the IT and Security teams understand that comprehensive mobile security is a critical part of maintaining compliance and protecting against data compromise.