Lookout for Healthcare

Healthcare organizations must comply with HIPAA and other privacy regulations. Lookout delivers security to prevent leakage of patient data.

Industry-Wide Security Challenges

In a post-perimeter world where healthcare professionals rely on mobile devices and apps to access patient medical records, regulations such as HIPAA pose a challenge. Security teams must adapt their vision and strategy to include security tools that protect mobile apps and sensitive data. Man-in-the-middle attacks, application sideloading, and phishing attacks are becoming more prevalent, and it's necessary to protect against those threats while simultaneously strengthening the organization's compliance posture.

Industry Challenges

1. Significant adoption of mobile
2. Stringent privacy regulations
3. Wide range of device ownership models

Real World Use Case for Healthcare Providers

HIPAA requires organizations to protect patient data accessed by mobile devices and applications, and as more healthcare organizations build out a mobile-heavy infrastructure, there must be assurance that those devices and applications are monitored and protected. More specifically, HIPAA calls for protection against malicious software and procedures for guarding against, detecting, and reporting malicious software. Furthermore, the organization must be able to identify and respond to security incidents and mitigate the incident to the organization's best capabilities[1]. Malicious pieces of software can try to access patient data on devices used by healthcare professionals. A Top 5 healthcare system in the U.S. ensured that no other unauthorized apps had access to the address book containing patient information on corporate-owned iPads.

Lookout Critical Capability

Lookout Mobile Endpoint Security allows admins to create over 55 types of custom app security policies, so this organization was easily able to create a security policy to block the use of apps that requested access to the address book on corporate-issued iPads. Lookout provides security capabilities lacking in MDM that provide unmatched visibility and control to ensure compliance with key regulations like HIPAA.

Why Lookout?

Lookout Mobile Endpoint Security ensures continuous security and compliance on every device, leveraging a large data set fed by over 170 million devices, and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts on malicious apps, network connections, and system anomalies at the OS level in real time; accompanied by simple on-device remediation capabilities. For Healthcare organizations, Lookout simultaneously delivers the security and visibility necessary to ensure compliance and gain visibility into every aspect of the mobile risk landscape. Learn how a Top 5 healthcare system in the U.S. is protecting patient data on iPads.

[1] "45 CFR § 164.308 - Administrative Safeguards." 45 CFR § 164.308 - Administrative Safeguards., Cornell Law School Legal Information Institute, 25 Jan. 2013, www.law.cornell.edu/cfr/text/45/164.308.