How a Major Hospital Chain Secured Sensitive Data with Lookout

The Challenge: Enable Access to Sensitive Data While Remaining Compliant

- As one of the world's largest private operators of healthcare facilities, this major hospital chain possesses terabytes of sensitive compliance-related data.
- The team needed a way to develop a portal for connecting its hospitals to service providers without violating HIPAA, HITECH and GDPR compliance standards for its patient records. To achieve this, they not only needed a way to encrypt sensitive data but also ensure that only authorized users at these providers could access this data.
- After having built out solutions in-house for years that quickly became obsolete, the hospital needed to move to a cloud-centric strategy to remove the cost of constantly updating and rebuilding its on-premises, home-built systems.
- Encrypting sensitive healthcare data was of key importance – especially as they leveraged cloud-based email and Salesforce where they couldn't risk having unencrypted data stored. This was difficult as data constantly moved between users, devices and locations.

Customer Overview

One of the world's largest private operators of healthcare facilities with over 200,000 employees across 162 hospitals and 113 surgery centers in the United States and England.

Industry: Healthcare

Solution: Lookout Cloud Access Security Broker (CASB)

Results

- Secure access and encryption policies for HIPAA, HITRUST, and GDPR-related data.
- Broader migration to the cloud and implementation of cloud services, which reduced maintenance and security costs.
- Secure collaboration with external parties without the fear of compliance-related data being leaked or lost.
- Unified platform approach to securing all cloud and SaaS apps.

The Solution: Lookout Cloud Access Security Broker (CASB)

- This major hospital chain realized that they needed a CASB solution that could grow with them as they moved more resources into the cloud. They started by implementing dynamic data access and encryption policies for all patient data stored in Salesforce and have since been able to extend those same policies and more to other cloud apps and services.
- Over the course of implementation, Lookout enabled them to create a secure email integration via Easylink that enabled employees and third parties to collaborate over sensitive data without putting the hospital at risk of violating compliance.
- Thanks to the automated data classification and encryption capabilities of Lookout CASB, all its sensitive data was automatically protected via AES 256 encryption across its highly available and load-balanced architecture.
- By leveraging Lookout CASB for all its data protection needs, this hospital chain was able to reduce the costs of security and infrastructure maintenance while continuously implementing more cloud-based architecture.
- Lookout helped this hospital chain reduce its reliance on on-premises infrastructure and securely leverage the cloud, which in turn reduced costs of maintaining and securing internal infrastructure.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more about Lookout CASB, visit lookout.com.