How Lookout SSE Technologies Helps a Leading Hospital System Modernize Its DLP Capabilities and Ensure HIPAA Compliance

Digital transformation has forever changed the way healthcare organizations deliver care. By pivoting to cloud based platforms, health systems can liberate data from silos and connect it in ways that enable them to gain insights, take action and collaborate across a patient's care journey.

While an increasing number of healthcare CIOs are considering the software-as-a-service (SaaS) model for their IT solutions, financial pressures compel them to find effective solutions that maximize existing resources and minimize costs. Unless you've come into a huge reserve of capital, starting over is simply not realistic. Instead of a complete outright replacement of existing technology, hybrid models that bridge the gap between legacy systems and new cloud-based solutions are the preferred approach.

One such "old" technology is the large embedded base of Data Loss Prevention (DLP) appliances and associated processes used to ensure that sensitive data is not lost, misused or accessed by unauthorized users. The use of DLP tools in healthcare is typically driven by the Health Insurance Portability and Accountability Act (HIPAA) regulation mandates. HIPAA rules provide guidance for the proper use and disclosure of protected health information (PHI), including how to secure PHI and what to do if there is a PHI breach. DLP is used to both identify violations and enforce remediation with alerts, encryption and other protective actions to prevent accidental or malicious sharing of data that could put the hospital at risk.

The Customer

A leading U.S.-based university hospital system

Industry: Healthcare

The Solution

Lookout Secure Service Edge (SSE) technologies including Lookout Cloud Access Security Broker (CASB) with native Data Loss Prevention (DLP) and Lookout Enterprise Digital Rights Management (EDRM).

The Results

- Lookout SSE with native DLP and EDRM functionality allows users to collaborate and share data across both internal and external (e.g. researchers and caregivers) boundaries while protecting it from unauthorized access, use and distribution.
- A strong HIPAA-compliant implementation that incorporates encryption.
- Lookout helped the customer bridge the gap between the legacy systems and new cloud based solutions.

Challenges

A leading hospital system was faced with this hybrid integration problem when they moved terabytes of PHI from on-premises to its Box cloud storage. They had invested significant time and effort in a legacy DLP hardware solution from Forcepoint that resided inside the network perimeter. This included customizing and configuring DLP rules and policies, testing for accuracy and effectiveness, and further refining to eliminate noise and false positives. With years of validation, the customer was confident in its ability to keep sensitive data safe.

Unfortunately, when data was moved to the cloud, this legacy DLP hardware could no longer access it. It became clear to the IT and security teams that they needed to modernize their DLP capabilities in a way that wouldn't throw away the years of work they had put into their existing appliance.

Solution

The customer needed a solution that could integrate with its existing Forcepoint DLP engine and use the proven controls as actionable signals to mitigate data loss incidents in the cloud. That's when the Lookout Cloud Access Service Broker (CASB) solution with native DLP was introduced.

According to the hospital's IT Security Manager, "Integration with our on-premises DLP environment and its support applications was a big factor in our decision to move forward with Lookout."

Lookout DLP integrates directly with Box cloud storage through APIs, enabling it to scan and classify cloud data during creation, upload and collaboration. When the cloud DLP detector discovers a policy violation, the data in question is transferred from the cloud to their on-premises DLP solution where further policy checks can be applied and remedial action taken.

> "We needed something to take charge of our cloud storage platform that provided visibility into what data users were accessing, how they accessed it and with whom they shared it."
>
> IT security manager of a major university hospital system

Customer Quote

> "Integration with our on-premises DLP environment and its support applications was a big factor in our decision to move forward with Lookout."
>
> **The hospital's IT Security Manager**

Results

Encryption: The First Step to Ensure HIPAA Compliance

In a world of electronic data transfers and mobile devices, there are dozens of ways that security can break down and lead to HIPAA non-compliance. All of these ways point back to the need for a strong HIPAA-compliant implementation that incorporates encryption. In fact, HIPAA requires encryption of PHI when the data is at rest, meaning the data is stored on, for example, a local disk or USB drive.

To accommodate this requirement, the hospital is planning to implement Lookout native Enterprise Digital Rights Management (EDRM) which can automatically provide file encryption and access policy enforcement. When DLP identifies sensitive data being deliberately moved from inside the hospital to outside of its perimeter (i.e. data exfiltration), Lookout takes action by encrypting the file to ensure data remains protected and HIPAA compliance is maintained.

EDRM enables users to collaborate and share data across both internal and external (e.g. researchers and caregivers) boundaries while protecting it from unauthorized access, use and distribution.

Bridging the Gap with Lookout SSE

The conventional data center continues to evolve as new cloud services are introduced alongside legacy technologies to meet today's business demands. While some IT managers might be inclined to tear it all down and build anew, that is generally not a practical option. Instead, modernizing a data center involves creating a hybrid environment where the old and new each play a role in delivering modern services.

The Lookout SSE Platform with native DLP plays an important role in extending the life of legacy DLP solutions by extending their reach into the cloud. As organizations undergo cloud transformation, Lookout bridges the gap between these legacy systems and new cloud based solutions.

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, VMware, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.