Preventing Data Exfiltration and **Automating PCI Audit Readiness**: California Bank replaces legacy tech with LightBeam's AI-Driven Data Classification

COMPANY	**INDUSTRY**
California Bank	Banking

Overview

As cyber threats and data breaches become more common and sophisticated, a California bank faced the challenge of protecting sensitive financial and customer information from these growing risks. Serving retail and commercial clients across the western United States, the bank has always prided itself on delivering personalized service while maintaining a strong commitment to regulatory compliance.

To further bolster its data security, the bank sought to enhance its defenses against potential data breaches, prevent unauthorized sharing of sensitive information, and optimize its data management processes as part of a large-scale migration to the cloud. Key goals included **improving data security**, **ensuring compliance with regulations such as PCI and CCPA**, and **reducing cloud storage costs** by eliminating outdated or unnecessary files. To achieve these objectives, the bank turned to LightBeam's AI-driven data classification platform.

Customer Story Summary

CHALLENGES

- Prevent employees from sharing sensitive data with unauthorized locations

- Cutting storage costs by eliminating outdated files during cloud migration

APPROACH

- Sensitive data detection

- Data exfiltration detection

- Pilot program for document labeling in SharePoint

RESULTS

- LightBeam helped the bank prevent the exposure of sensitive customer/ company info

- Identified redundant and outdated files & replacing legacy tech, hence, enabling the bank to reduce cloud storage costs

Challenge

A primary concern was preventing data exfiltration, particularly the risk of employees sharing sensitive company data with personal email accounts or other unauthorized locations.

The bank has been using a legacy data discovery platform. They had also implemented Microsoft Purview for data classification but it found the tool lacking in accuracy and reliant on a "best-effort" approach. Additionally, the bank had ProofPoint as a data loss prevention (DLP) solution, but it wasn't offering comprehensive coverage across all platforms and applications.

With an ongoing migration to the cloud, the bank also needed to ensure that sensitive data remained secure and compliant throughout the transition. One of the main challenges was reducing the cost of cloud storage by identifying and removing outdated or unnecessary files.
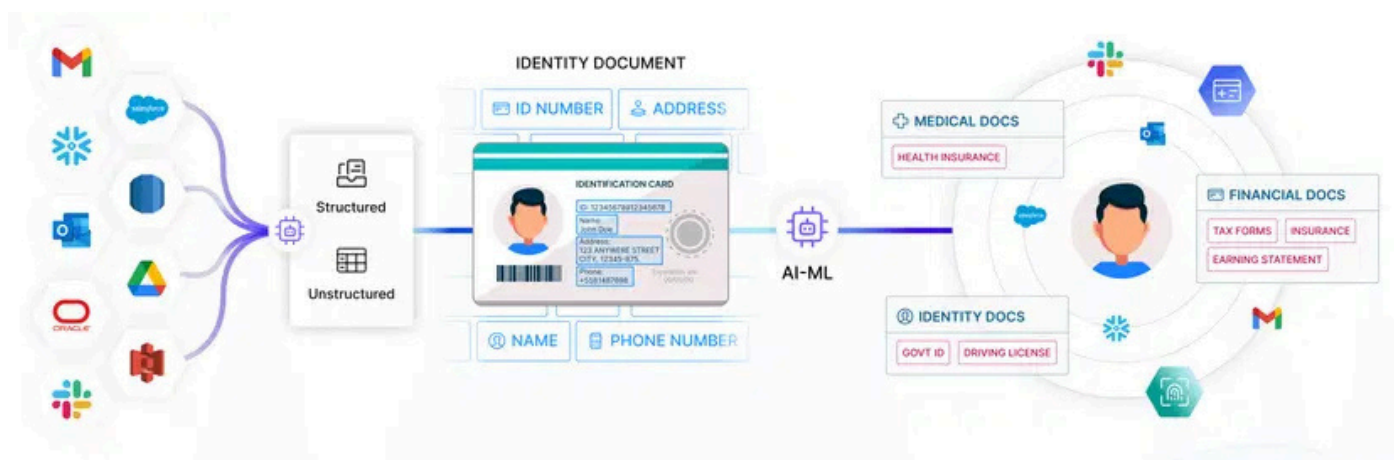
Solution

To address these challenges, LightBeam worked closely with the bank's data governance officer and Chief Information Security Officer (CISO) to deploy a comprehensive solution tailored to the bank's specific needs. The solution included:

Sensitive data detection

LightBeam's platform scanned over 20 data sources — including O365, SharePoint, OneDrive, Teams, Salesforce, and SMB file shares — to detect and mitigate data security threats.

For example, the bank had been receiving customer data through Salesforce but lacked visibility into its origin. LightBeam cross-referenced the data across various applications and identified the complete flow of sensitive customer data, mapping it back to multiple data sources.

The solution discovered a total of 189 million sensitive data instances across these platforms, providing the bank with detailed insights into where its data was coming from and how it was being used.

Data exfiltration detection

LightBeam's solution enabled the bank to detect suspicious activities related to employee data exfiltration. In one instance, LightBeam flagged an employee who was sending mortgage statements and other sensitive company data to their personal email. The platform analyzed the email and attachment activity, hardening controls against unauthorized sharing of personally identifiable information (PII) and payment card industry (PCI) data. This enabled the bank to take immediate action, including further investigation and policy updates to minimize the risk of any breaches.

Pilot program for document labeling in SharePoint

LightBeam also implemented a pilot project to apply data labels to documents in SharePoint, enhancing Microsoft Purview's DLP functionality. The pilot resulted in improved classification accuracy, which bolstered the bank's data loss prevention efforts and strengthened its compliance and governance measures.

Enhanced security

By identifying and addressing potential data exposures in real-time, LightBeam helped the bank prevent the exposure of sensitive customer and company information, safeguarding both privacy and trust.

Operational efficiency

The deployment of LightBeam's solution significantly strengthened the bank's DLP capabilities, streamlined compliance efforts, and reduced the time spent managing sensitive data. This was especially valuable during the ongoing cloud migration, allowing the bank to prioritize secure data transfer and minimize operational disruption.

Cost savings

Through data minimization and cleanup, LightBeam identified redundant and outdated files, enabling the bank to reduce cloud storage costs. In fact, the bank removed one security and governance tool from its portfolio, optimizing its overall technology stack. The solution also helped the bank prioritize which data needed to be moved from on-premises SMB file shares to SharePoint, ensuring only necessary files were migrated — avoiding network strain and unnecessary storage expenses.

Get a free security assessment today!

Improved data governance and compliance

With LightBeam's help, the bank was able to better manage sensitive data and ensure strict compliance with the California Consumer Privacy Act (CCPA).

With LightBeam's AI-driven data classification solution, the bank was equipped to safeguard its sensitive data, support its cloud migration, and streamline data management practices. This sets a strong foundation for future growth and security.

Conclusion

The partnership with LightBeam enabled the bank to implement scalable, cost-effective solutions for data security and optimization. By improving data classification, enhancing DLP performance, and ensuring compliance, the bank was able to achieve both short-term goals — such as strengthened security and cost savings — and long-term objectives related to regulatory compliance and operational efficiency.

About LightBeam

PROTECT YOUR SENSITIVE DATA

Simplify your data security posture with LightBeam. Our unified platform converges security, privacy, and governance into a seamless stack. By integrating AI-powered identity mapping and context-based insights, we eliminate silos and provide end-to-end protection across SaaS, cloud, and on-premises environments.

For any questions or suggestions, please contact us at: sales@lightbeam.ai