INFOLOCK

CASE STUDY:

INFOLOCK IMPROVES DATA PROTECTION, REDUCES DLP COSTS FOR LEADING U.S. HEALTH INSURER

CUSTOMER PROFILE

LOCATION
United States of America

INDUSTRY
Healthcare Services

ORGANIZATIONAL SIZE
2,000+ Employees

ORGANIZATIONAL FOOTPRINT

Revenue
700+ billion in annual revenue

110+ Million
More than 110+ million individuals insured

With a footprint in more than 170 countries around the world, the organization generates and stores a large volume of Personal Identifiable Information (PII), Protected Health Information (PHI) that is subject to HIPAA privacy laws, and sensitive legal information such as contract data.

PROJECT BACKGROUND

The organization employs a 10-person information security (InfoSec) team responsible for DLP, which consists of a Director of GRC, three managers, and six administrators, engineers, and analysts. The Director reports to the client's Chief Information Security Officer (CISO).

The client historically ran an on-prem IT environment, but over the last few years made significant strides towards migrating processes and data to the cloud. Today they are supporting around 5,000 users across the network.

The client's leadership team knows the importance of data security and data loss prevention (DLP) but focuses most of their time and energy on their core health insurance business. As a result, the client prefers third parties to manage its DLP program and help it comply with HIPAA and other regulations, as well as audit compliance, such as SOC 2.

The client had used Symantec for data security and DLP, but when it implemented Microsoft Office 365, it became evident that Symantec could not provide the required data visibility, particularly for Teams and OneDrive content.

CLIENT CHALLENGES

The client needed to improve overall awareness of PHI/PII among both internal and external users. Internal users included human resources (HR) staff, the finance department, and specific business units. External users included medical practices, other health insurance companies, and outsourcing companies used for software development, system maintenance, and other outsourced administrative functions.

More particularly, the client needed to improve technical monitoring to streamline data analysis and improve incident detection and remediation. For example:

- Several of the policies introduced by a previous Managed Security Services provider turned out to be inefficient or plain out irrelevant and were only used to buff up remediation statistics. This put significant stress on the back-end database, leading to wasted storage and sluggish user experience in the DLP console.
- The client suffered from "incident fatigue." Single incidents often generated multiple alerts, draining human capital to manage the duplicates and refine multiple tools, which took focus away from more productive activities.
- Data security "vendor sprawl" also drained the client's internal resources. The client's mix of data security tools was not optimized for functionality, integration, or cost (e.g., three different tools all tried to block same type of PII).
- The client's incident reporting also seemed designed to boost "issues solved" scores without fully considering the content that was most relevant for DLP.

When the client decided to implement Microsoft Office—and run Microsoft DLP and Symantec DLP simultaneously—these issues multiplied. The client did not have the necessary Microsoft DLP expertise, did not know how to effectively integrate Microsoft DLP with Symantec, and urgently needed better control over the data that employees shared across Teams and OneDrive.

Also, the client had experienced uneven results with prior DLP providers whose approaches to managing DLP did not provide satisfactory personal service. The client wanted exceptionally responsive service and a deep, trusted relationship with a well-established data protection vendor.

Choosing a dedicated service provider with a long record of improving DLP processes, training personnel on PHI/PII, and managing complex data protection programs was paramount for the client.

WHY INFOLOCK

Infolock demonstrated technical and business expertise, such as:

- Hands-on experience with both Microsoft and Symantec DLP, including thousands of hours of creating and managing strategic DLP programs for large enterprises.
- DLP program design and planning, using the latest data security technology and a systematic roadmap to improve program maturity.
- Timely system administration and maintenance, including optimal distribution of agents across platforms and effective management of tool and system updates.
- Policy tuning and incident response, especially understanding issues and applying rules for a range of use cases to minimize false positives, while at the same time reducing number of escalated incidents in need for review by customer analysts.

Additionally, Infolock's reputation for strong client relationships was paramount in the client's decision to engage the company. Infolock focuses on client needs and outcomes, not reselling a particular solution, and provides clients with dedicated points of contact for responsive, personal support.

INFOLOCK'S SOLUTIONS

DLP Program Consolidation. Infolock integrated the client's Symantec and Microsoft DLP platforms to effectively manage Microsoft Outlook, Teams, and SharePoint data. Focal points included:

- Detailed Symantec/Microsoft tool comparisons (overlaps, conflicts, and complements).
- Engineering a third-party cloud data security solution to augment the Symantec/Microsoft DLP integration (i.e. automatically scanning Microsoft 365 data transfers, identifying and blocking most unauthorized PHI/PII uploads to the cloud, and creating a cloud quarantine function for systems out of scope for blocking).
- Simultaneous Symantec/Microsoft capability testing on controlled use cases.
- Microsoft's complex licensing and other setup requirements.
- Optimal system tuning to overcome Microsoft DLP limitations and rectify policy inconsistencies and enforcement issues, especially in Teams chat.

At a higher level, Infolock helped the client establish a DLP governance committee to provide effective structure and control over DLP policies.

Infolock helped the client create more disciplined processes, greater visibility of issues, and more relevant metrics for continuous data security improvement. For example, Infolock conducted quarterly and annual reviews, attributed specific costs to the avoidance of potential breaches, and assessed and tracked the client's DLP maturity compared to industry peers.

In addition, Infolock educated the client, demonstrating how process control and employee training improved awareness of how to treat PHI and PII.

On a more granular level, Infolock took over management of the client's day-to-day Tier 1 triage, assessing and mitigating potential data security issues. Highlights included:

- Building a dynamic playbook of remediation tactics so the client's internal resources would not be burdened by routine, repeated activities.
- Implementing an incident escalation procedure to make the best use of the client's time.
- Turning off policies that drained compute resources without generating value
- Focusing on effective automation to encrypt emails that contained PII/PHI as well as intellectual property.

DLP Maturity Levels

Infolock implemented a DLP maturity roadmap to measure and track the client's data security program over time. A DLP maturity score has three components: the effectiveness of DLP policies in detecting issues; the technical success of DLP controls; and the efficacy of internal-external engagement and collaboration on DLP incidents. The score is measured on a scale of 1 to 5, where 1 ("Ad Hoc") means disorganized and inefficient and 5 ("Optimized") means integrated, automated, continuous, and optimized.

Infolock measures DLP maturity levels annually to keep a pulse on the health and efficacy of the DLP system overtime.

THE RESULTS

In a time frame that exceeded expectations, Infolock successfully integrated the client's Symantec and Microsoft DLP platforms and engineered additional DLP solutions to maximize the efficiency and efficacy of the client's data security.

Quantitative Outcomes

Infolock achieved the following outcomes to ensure the client's DLP usage was maximized.

Through Infolock's planning, implementation expertise, and ongoing managed services, the client's DLP maturity score increased over 20%, from approximately 3.40 to 4.10, and has remained above a 4.0 threshold ever since. This improvement closed ex-filtration gaps and significantly reduced other data security risk vectors.

Infolock's policy management and proactive triage improved the client's incident detection and remediation to avert potential PHI and PII exposure. For example, Infolock reworked a policy to increase automatic email encryption by 700% for sensitive IP transfers.

Using a data breach valuation of $250 per record, based on IBM/Ponemon Institute research, Infolock has cumulatively prevented exposure of 28,000 sensitive data records with a potential loss value of $7 million.

By consolidating DLP tools, streamlining the client's data security tech stack, and introducing new policies and processes, Infolock has reduced DLP management costs by over $460,000 per year, the equivalent of 3.5 full-time employees.

By eliminating the need to find, train, and retain qualified data security employees, Infolock's outsourced services have saved the client another $200,000 in internal human resource costs.

Qualitative Outcomes

The client was especially concerned about the effectiveness of its Symantec-Microsoft integration. Infolock ensured a successful outcome by, among other things:

- Working directly with Microsoft to explore a wide range of tools for the most efficient DLP deployment and workflow.
- Creating a "single pane of glass" (which Microsoft could not provide) to satisfy all client use cases—without incurring any costs on additional tools.
- Testing extensively to address problematic Microsoft Teams use cases—and applying lessons learned to optimize an effective, hybrid Microsoft-Symantec approach.
- Educating users on how the integrated Microsoft-Symantec systems work together and impact the client.
- Successfully integrating a third-party Security orchestration, automation, and response (SOAR) solution to augment Microsoft DLP in the client's hybrid environment.
- Satisfying all client use cases to align DLP policies, stop sensitive data leakage, and close gaps between the Microsoft and Symantec DLP platforms.

The Bottom Line

Infolock's performance dashboards and reporting gave the client's management team a clearer picture of the value of DLP to help justify continued investments in data security. Infolock took the workload off of the client's InfoSec team, enabling them to focus on other priorities, and gave the client maximum value from all of their DLP tools. The client was extremely happy - and signed Infolock to a multi-year DLP management contract.

About Infolock

Founded in 2005, Infolock is the go-to data risk management advisory, consulting, and managed services firm for security conscious organizations. With a programmatic approach, Infolock expertly manages the complex data risks of its clients, enabling organizations to achieve their strategic business objectives. Named among the "Fastest Growing Companies" on Inc. Magazine's "Inc. 5000" list, Infolock developed DataRAMP™, a data risk management framework which empowers organizations to understand and manage data risk in the same manner as other organizational risks, such as financial, competitive, and regulatory risk. Headquartered in Arlington, VA, Infolock serves customers in the financial services, healthcare, government, educational and other highly-regulated industries around the world.

2900 South Quincy Street Suite 330
Arlington, Virginia 22206

Web: www.infolock.com
Email: info@infolock.com

Local: (202) 600-7270
Toll free: (877) 610-5625