SOLUTION BRIEF

Seclore and Symantec Data-Centric Security Solution

Discovery, classification, protection, and tracking on-prem, across cloud applications, and beyond.

Executive Summary

Seclore and Symantec have renewed their longstanding partnership to deliver industry-leading security. By seamlessly Integrating Symantec DLP Cloud with Seclore Data-Centric Security, enterprises now have full control and visibility over data throughout the entire lifecycle to better protect their sensitive information and ensure compliance.

Challenge

Sensitive data is the lifeblood of most organizations, however, fending off sophisticated cyber threats and preventing the misuse of that data remains increasingly difficult. The challenge is keeping data safe, accessible, and shareable across a multitude of local and remote environments — each with their own security controls and access protocols. Adding to this challenge are cloud migrations, regulatory requirements, and the legitimate business need to share sensitive data with third parties.

Joint Solution

Symantec (Broadcom) and Seclore have partnered to deliver an industry-leading solution that solves these challenges. By seamlessly integrating Symantec DLP Cloud with Seclore Data-Centric Security, enterprises now have access to comprehensive discovery and data-centric protection for sensitive information in endpoint, network, email, cloud repository, and third-party applications. With security, compliance, and privacy rules embedded with the data itself, enterprises can adopt uniform access and usage policies instead of a fragmented patchwork of application and environment-based standards. Now security and compliance teams can better protect and track their most sensitive data anywhere it goes.

Joint Solution Components

- Seclore Data-Centric Security
- Symantec DLP Cloud

Joint Solution Benefits

- Automatically protect sensitive data and ensure security policies are consistently applied across endpoint, cloud, on-prem, and third-party applications.
- Accurately discover and classify sensitive digital assets to ensure appropriate protection and usage controls are enforced throughout the entire data lifecycle.
- Get complete file-level visibility and insights to quickly identify unauthorized attempts to access, demonstrate compliance, and revoke access if necessary.
- Protect regulated data such as Personally Identifiable Information (PII), Payment Card Industry (PCI), and Protected Health Information (PHI), Intellectual property (IP), and sensitive business documents or emails.

Joint Solution Components

Seclore Data-Centric Security - Seclore integrates seamlessly with Symantec DLP (Data Loss Prevention) Cloud to automatically discover, classify, protect, and track sensitive data. Seclore adds persistent classification, encryption, granular access controls, dynamic watermarking, and visibility, giving enterprises complete control over data no matter how and where it is shared.

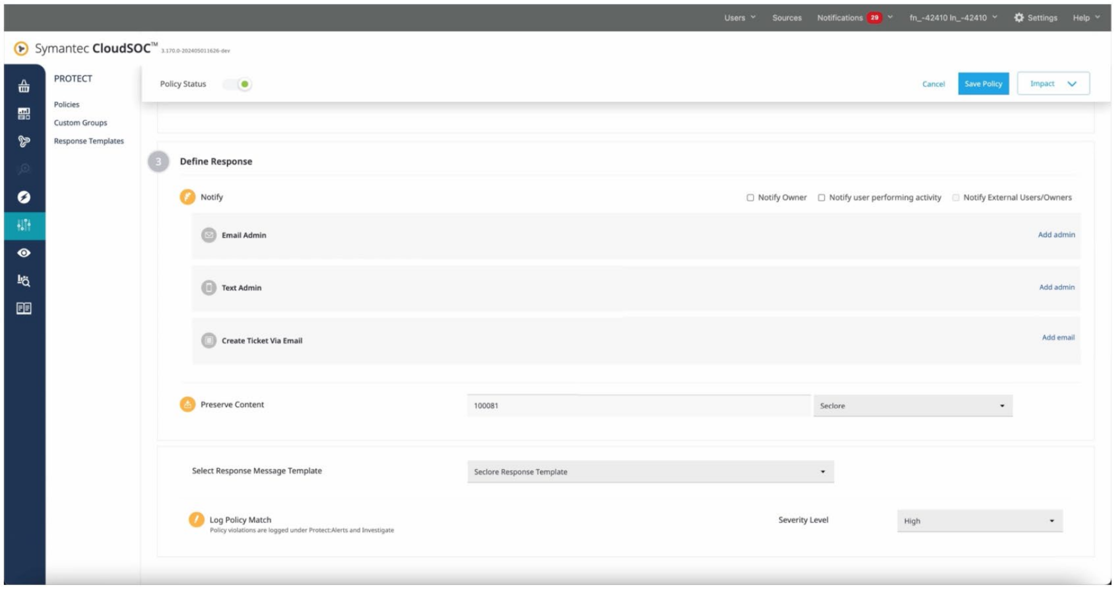
Symantec DLP Cloud provides comprehensive discovery, monitoring, and protection capabilities that empower customers with broad visibility and security in their enterprise cloud environments. It also automates the classification of Personally Identifiable Information (PII), Payment Card Industry (PCI), Protected Health Information (PHI), and other regulated data flowing in and out of the cloud. This continuous monitoring helps organizations safeguard data across cloud apps, maintain compliance across SaaS and IaaS, and quickly respond to security incidents.

Symantec DLP - Seclore has integrated seamlessly with Symantec's on-premises DLP solution for over ten years to automatically discover, classify, protect, and track sensitive data. Seclore extends DLP protection by adding persistent classification, encryption, granular access control, watermarking, and visibility to data anywhere it is shared. This mature integration also enables Symantec DLP to discover sensitive information within Seclore-protected data.

Joint Solution Integration

The Seclore and Symantec joint solutions operate harmoniously to protect sensitive data and keep organizations secure and compliant.

Example Use Case - Symantec DLP Cloud discovers sensitive data in a cloud environment and applies a "confidential" classification label that automatically triggers Seclore to add encryption, access-controls, and tracking. (Figure 1). Seclore applies different access-control rules based on the threat risk associated with each classification label.



Policy Status

3 Define Response

Notify ☐ Notify Owner ☐ Notify user performing activity ☐ Notify External Users/Owners

Email Admin

Text Admin

Create Ticket Via Email

Preserve Content: 100081 | Seclore

Select Response Message Template: Seclore Response Template

Log Policy Match
Policy violations are logged under Protect:Alerts and Investigate

Severity Level: High

Figure 1: Edit a policy to apply Seclore file protection

Symantec obtains this information from Seclore via its API, and can apply policies based on labels such as:

1. Confidential
2. Internal Use Only
3. Public

Summary

While on-prem, hybrid-cloud, and remote-first environments have many benefits, security and privacy professionals are challenged to find solutions that provide the level of protection and compliance enterprises need. The Symantec and Seclore partnership empowers organizations to embrace flexible hybrid environments while effectively safeguarding their most sensitive data. The combination of Symantec DLP Cloud and Seclore Data-Centric Security accomplishes this through persistent classification, encryption, granular access control, watermarking, and visibility across all sanctioned and unsanctioned environments so organizations can share data fearlessly.

SECLORE™

www.seclore.com