SOLUTION BRIEF

Seclore and Symantec Data-Centric Security Solution

Discover, classify, protect, and monitor your enterprise's sensitive data with unified orchestration.

Joint Solution Components

- Seclore Data-Centric Security
- Symantec DLP Cloud
- Symantec CloudSOC CASB

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 and emails.

Executive Summary

Seclore and Symantec have created a longstanding partnership to deliver industry-leading data-centric security. Symantec CloudSOC CASB and Symantec Endpoint DLP both integrate with Seclore's Data-Centric Security platform enabling enterprises to have full control and visibility over data throughout the entire lifecycle to better protect 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 CloudSOC CASB and Endpoint DLP with Seclore Data-centric Security Platform, enterprises now have access to comprehensive discovery and data-centric security for sensitive information in endpoint, network, email, cloud repository, and third-party applications. With security, compliance, and privacy rules embedded in the data itself, enterprises can adopt uniform data-centric 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 - Seclore is a holistic data-centric security platform that empowers security and other teams to protect their most sensitive data with persistent encryption, granular access control, and tracking that gives enterprises complete control everywhere their data is shared or stored.

Symantec CloudSOC CASB (Cloud Access Security Broker) - Symantec CloudSOC CASB provides comprehensive discovery, monitoring, and protection capabilities that give customers broad visibility and security in their enterprise cloud environments. It also includes automating 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 (Data-Loss Prevention) - Symantec DLP provides comprehensive protection and visibility for network, file-share, databases, and other endpoints. It can also automate discovery and classification for Personally Identifiable Information (PII), Payment Card Industry (PCI), Protected Health Information (PHI), and other regulated data flowing in and out of these environments.

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 CloudSOC CASB and Endpoint DLP discovers sensitive data in a cloud environment, and user devices respectively 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.

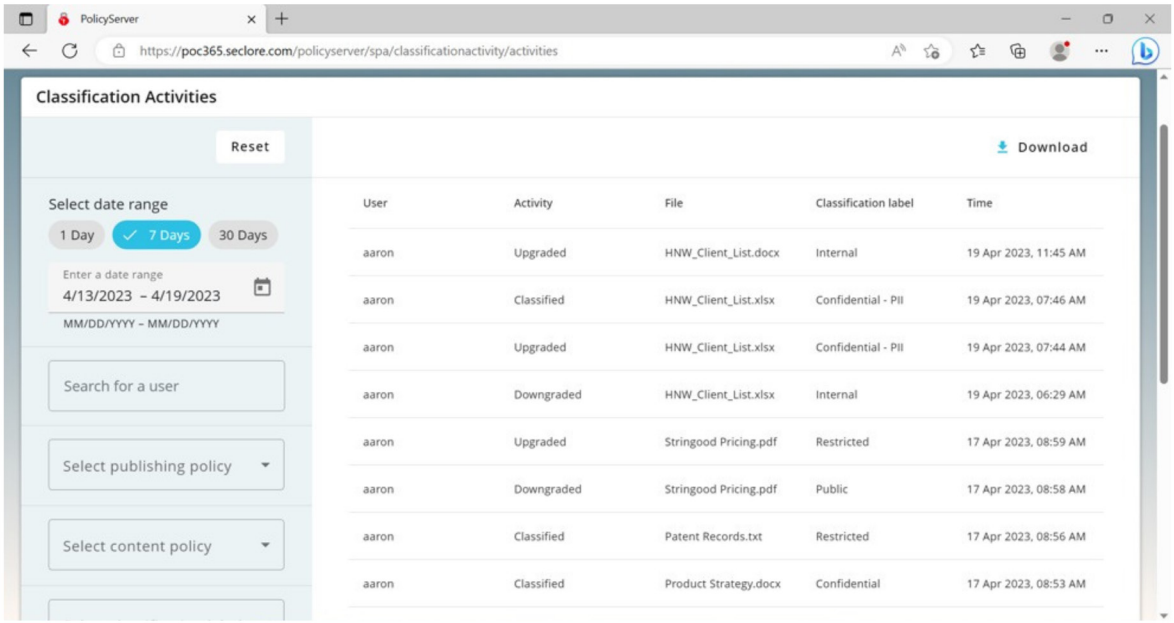

Figure 1: Edit access-control rule profiles in Seclore

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 empower organizations to embrace flexible hybrid environments while effectively safeguarding their most sensitive data. The combination of Symantec CloudSOC DLP, Endpoint DLP and Seclore 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™