SOLUTION BRIEF

KEY FEATURES

- **Safeguard data across cloud apps, email, and the web:** Employees use email, the web, and sanctioned and unsanctioned cloud apps such as Office365 and Box to store and share sensitive corporate content. Secure it all against accidental exposure or malicious breach.
- **Respond to security incidents:** Security incidents happen. Rich, contextual data from CloudSOC helps you understand what, when, who, and how it happened, to respond quickly to security events in the cloud.
- **Gain deep transaction visibility, and control Shadow IT:** Risky transactions can slip under the radar in the cloud. Collect, view, and control them all—from sanctioned or unsanctioned apps, with options for managed and unmanaged devices—using this inline capability.
- **Protect against threats:** Bad actors and malware target cloud app accounts that are accessible directly from the Internet. Protect the organization against the impact of compromised cloud accounts.
- **Maintain regulatory compliance:** Governments and industries require risk analysis, monitoring, and documentation to maintain data privacy and security. Fulfill these requirements with a system that's effective and easy to use.
- **Trust the 10-time Gartner Magic Quadrant Leader for DLP:** Competing claims for suppliers' cloud solutions can be difficult to sort out. Symantec DLP is a proven solution that Gartner, Forrester, IDC, and other leading analysts recognize as a global market leader.
- **Monitor and prevent sensitive data going to generative AI apps:** Monitor and inspect data-in-motion to generative AI apps. Highlight any risks and compliance issues these may pose. Detect sensitive content with DLP policies and prevent data transfer going to these AI apps.

Symantec by Broadcom

Symantec® Data Loss Prevention Cloud Solution

Secure your most sensitive data with confidence across cloud apps, email and the web.

Establish a Secure Data-Centric Foundation in the Cloud

Companies are growing more distributed, driven by increases in cloud applications, direct to cloud traffic, remote work, and bring-your-own-device initiatives. Symantec® Data Loss Prevention (DLP) Cloud provides a single control point from which security teams can configure DLP policies that secure SaaS apps, control access to web destinations, and identify shadow IT.

Symantec DLP Cloud combines industry leading enterprise Data Loss Prevention (DLP) and Symantec CloudSOC® CASB. With it, you can extend current policies and robust detection to cloud applications, and use rich contextual data to manage all incidents directly from the DLP console. It delivers deep visibility into user activity and tracks and governs activity for both sanctioned and unsanctioned apps, including Box, Google Workspace (G Suite), and Office365.

By combining DLP Cloud and DLP Core packages, a single DLP policy can apply controls to data stored on endpoints, servers, file shares, databases, SharePoint, and more—protecting data on premises, in the cloud, and on the road.

Use Symantec DLP Cloud to build a solid, data-centric foundation that secures your most valuable assets across the cloud, email, and the web.

Solution Benefits

- Protect critical data with targeted controls and policies based on user risk and data sensitivity.
- Deliver deep visibility of user activity across thousands of cloud applications, email, and the web, including Shadow IT.
- Continuously monitor and protect sensitive data from potential breach.
- Identify, classify, and document compliance for PHI, PCI, PII, and other critical data.
- Monitor email and web channels in real time for immediate action toward prevention of accidental exposure or sharing.

Solution Differentiators

Protection of Sensitive Data Across Cloud Apps, Email, and the Web

Together, DLP and Cloud Access Security Broker (CASB) detect and protect against intrusions, threats, and data loss across your most important business apps, email, and the web.

Unified DLP Engine

CloudSOC uses a single DLP engine to detect and remediate on-premises and cloud based violations. It features built-in PII, PCI, and HIPAA policies, plus a Cloud Detection Service to create custom policies from the Symantec DLP Enforce console.

Compliance Enforcement DLP enforces cloud storage, sharing,

and access policies for HIPAA, PCI, PII, and other sensitive data. It automatically protects regulated data with integrated encryption and multifactor user authentication.

Flexible Deployment

CloudSOC deployment options include unified authentication, integrated endpoints, agentless solutions, integrated web security, proxy chaining, shared intelligence, unified policy management, and more. Integrations with Symantec DLP support authentication, encryption, threat protection, and secure web gateway solutions.

Centralized Policies and Granular Controls

A powerful policy engine delivers efficient, fine-grained control over how users and apps share, transfer, and use sensitive data. One policy can apply multiple detection methods for precision, compound matching conditions for accuracy, and group rules and exceptions for individualization. BYOD options extend real-time CASB restrictions to authorized users on unmanaged endpoints.

Safely Use Generative AI Apps in Your Organization

Allow the use of AI apps such as ChatGPT with real-time granular inspection of submitted data, and prevent sensitive data from going to these apps.

Visibility and Control Over Data In Use, At Rest, and In Motion DLP uses deep content inspection

and context analysis to provide a comprehensive understanding of the location, movement, and exposure of sensitive data, so you can prevent data leaks and exfiltration attempts.

Comprehensive App Coverage

DLP uses API integrations and inline traffic analysis to monitor and control use of sanctioned SaaS platforms. It provides risk scoring for over 37,000 apps using hundreds of security mechanisms, compliance certifications, and other metrics.

High-Speed Policy Enforcement

API-based inline policy enforcement uses ThreatScore, abnormal user behavior, threat detection, and content classification to prevent data exposures and quickly control access, sharing, or other app specific actions.

Powerful UEBA Detection and Machine Learning Risk Analysis

Symantec CloudSOC UEBA and machine learning capabilities connect the dots between violations, users, accounts, and assets to assign risk scores to users and incidents. Risk scores identify malicious insiders and outsiders, prioritize risks across multiple platforms, and categorize incidents tied to misaligned policies or user mistakes.

Continuous Monitoring of Risk and Adaptive Access Control

CloudSOC continuously monitors risks from data loss, unsanctioned applications, malware, device security posture, compromised accounts, and other sources. Adaptive access controls harness this data to protect information, with CASB enforcement of real time policies at its gateway to prevent exfiltration of sensitive data, block malicious content, and keep malicious or compromised users off cloud applications.

What's Included

Product	Details
CASB Audit	*Symantec CloudSOC Audit discovers and monitors every cloud app used across an organization, identifies their users, and highlights any risks and compliance issues they may pose. It provides visibility into Shadow IT, and blocks access to unapproved cloud services.*
CASB for SaaS and IaaS	*CloudSOC CASB for SaaS and CloudSOC CASB for IaaS are cloud-based services that provide visibility and control over user activities in cloud applications. They monitor and protect stored, transferred, and shared data. A complete list of supported cloud applications can be found in the CloudSOC online store; it includes Microsoft Office365, Google Workspace (G Suite), Box, Salesforce, and ServiceNow.*
CASB Gateway	*Symantec CloudSOC Gateway continuously monitors and controls the use of cloud apps to enforce policies, identify malicious or inappropriate data sharing, signal malware threats, respond to security incidents, and automate escalations. It offers deep visibility into user activity across thousands of cloud apps and services, and both tracks and governs the activity of sanctioned and unsanctioned cloud apps.*
DLP Cloud Detection Service for CASB	*Symantec DLP Cloud Detection Service inspects content extracted from cloud apps and web traffic and automatically enforces sensitive data policies. Cloud-to-cloud integration with Symantec CloudSOC protects data in motion and at rest across more than 100 sanctioned and unsanctioned cloud apps, including Office 365, Google Workspace (G Suite), Box, Dropbox, and Salesforce. The integration allows the extension of existing policies and robust detection to cloud applications, and incident management directly from the DLP console.*
DLP Cloud Detection Service for Cloud SWG	*DLP Cloud Detection Service for Cloud SWG integrates with Symantec Cloud Secure Web Gateway to monitor even encrypted web traffic for the protection of roaming and mobile users.*
DLP for Office365 and Gmail	*Symantec DLP Cloud Service for Email continuously monitors corporate email traffic, using built-in intelligence and advanced detection to minimize false positives. It protects against data leaks in real time with automated message modification or blocking to enforce downstream encryption or quarantine. For data shared with third parties, it can automatically enable identity-based encryption and digital rights for email bodies and attachments.*

DLP Cloud Bundle Add-Ons

Product	Details
Mirror Gateway	*Symantec CloudSOC Mirror Gateway is a superior solution for secure cloud access from unmanaged devices. It extends CASB controls to unmanaged devices or BYOD, giving them the same secure access to cloud apps as managed devices, with no need for an agent.*
CloudSOC Advanced Threat Protection	*Safeguard your organization in the cloud with industry-leading threat protection. CloudSOC secures your cloud accounts and transactions against malware with Symantec Advanced Threat Protection including file reputation intelligence, A/V scanning, and sandboxing technologies.*

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

DLP-Cloud-SB102 January 24, 2025