Symantec
A Division of Broadcom

Product Brief

CloudSOC CASB for SaaS

Safeguard the organization and embrace cloud apps with confidence.

Overview

The data-science-powered Symantec CloudSOC CASB platform helps companies use cloud applications and services with confidence while staying safe, secure, and compliant. A range of capabilities from CloudSOC deliver the full life cycle of cloud application security including auditing shadow IT, real-time detection of intrusions and threats, protection against data loss and compliance violations, and investigation of historical account activity for post-incident analysis.

Safeguard Data

Employees store and share sensitive corporate content in Office 365, Google, Box, Salesforce, and other sanctioned cloud applications. Secure this data against accidental exposure or malicious data breach.

Respond to Security Incidents

Security incidents happen. Get the what, when, who, and how information needed to respond quickly to a security event in the cloud.

Protect Against Threats

Cloud app accounts are often accessible directly from the Internet. Bad actors and malware target these accounts for attack. Protect the organization against the impact of a compromised cloud account.

Maintain Regulatory Compliance

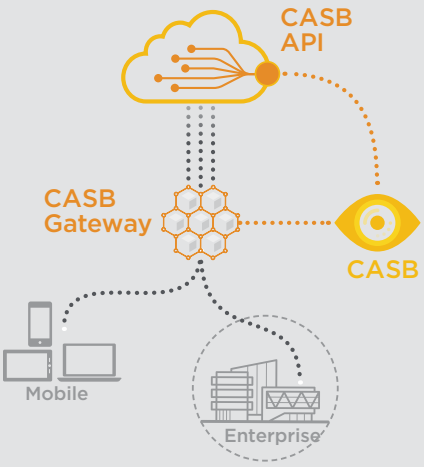
Government and industry regulations require risk analysis, monitoring, and documented systems to maintain data privacy and security. Fulfill these requirements with an easy-to-use system.

CASB for SaaS

Benefit	Details
Identify, Block, and Remediate Risky Exposures	Prevent data exposure and reduce risk of exposure with policies that can block, coach, alert, encrypt, unshare, and otherwise safeguard data in the cloud.
Track User Activity in Granular Detail	Detect transactions with the cloud in granular detail with data science-driven StreamIQ™ for fine-tuned visibility and policy control. Get visibility over transactions with any sanctioned or unsanctioned app with options for managed or unmanaged devices and preventative controls with this in-line capability.
Enforce Granular Policies to Safeguard Data	Prevent data breach with automatic controls via fast API and in-line enforcement to encrypt, block, unshare, or trigger adaptive multi-factor authentication for sensitive data. Get granular policy controls defined by action, data classification, user, ThreatScore™, and automate responses.
Secure Unmanaged Devices	CloudSOC provides broad BYOD options via the Mirror Gateway to provide real-time CASB security for users of unmanaged endpoints using an unlimited number of company-sanctioned cloud apps.
Protect Cloud Accounts with User Behavior Analytics	Detect risky user behavior and malicious activity such as brute force attacks or ransomware with user behavior analytics and a quantified user ThreatScore that can automatically trigger controls to block, quarantine, or alert on accounts with high-risk activity.
Detect and Mitigate Malware in the Cloud	Malware detection covers malicious file detection, sandboxing for conviction of unknown files and detection of malicious scripts.
Comply with Regulatory Requirements	Use data security capabilities in CloudSOC to identify, monitor, encrypt, and control access to PII, PHI, and other regulated types of data. Keep data in a geography with regional data centers. Control access to CloudSOC data with granular RBAC.
Investigate and Quickly Respond to Incidents	Identify security issues through visualizations of user, threat, policy, and service activity and easily connect actions to users, apps, and data. Use robust search and filter options to quickly find and review logs in context and enhance SIEM-led investigations with intelligence from CloudSOC.

How It Works

CASB for SaaS monitors data and activity in the cloud to secure data, protect against threats, and provide intelligence for incident response. CloudSOC monitors activity in the cloud via API-based Securlets and a CASB Gateway to delivers highly accurate monitoring and policy control built on machine learning and delivered through intuitive easy-to-use dashboards.



Available for: Office 365, G Suite, Box, Salesforce, ServiceNow, and Slack.

Key Features

Feature	Details
Comprehensive App Coverage	Monitors and controls use of sanctioned SaaS platforms such as Office 365, G Suite, Box, Salesforce, and more through extensive API integrations and in-line traffic analysis.
Unified DLP Engine	CloudSOC leverages the same world-class DLP engine for cloud-based and on-premises violation detection and remediation. CloudSOC offers built-in DLP Polices for PII, PCI, and HIPAA or a full Cloud Detection Service for custom policy creation via the Symantec DLP Enforce console.
StreamIQ™ Activity Monitoring	Extracts events from real-time cloud application traffic and delivers granular information including user, app, actions, file, data, device, and more. Unique data science-powered technology enables this deep visibility into transactions with nearly any cloud application.
User-Centric ThreatScore™	CloudSOC User Behavior Analytics (UBA) leverages intelligence from APIs via StreamIQ and machine learning to automatically maintain individualized user profiles, map user activity, and compile a live user ThreatScore.
High Speed Policy Enforcement	Fast API and in-line enforcement of granular policies based on ThreatScore, abnormal user behavior, threat detection, or content classification to prevent data exposures and control access, sharing, or other app-specific actions.
Incident Investigation	Intuitive, post-incident tools enable deep-dive analysis of cloud activity.
Advanced Visualizations	Zoom into desired information with easy-to-use filters, pivot views, free-form search, and actionable content.
Compliance Enforcement	Enforce policies governing how HIPAA, PCI, PII, and other sensitive data is stored, shared, and accessed in the cloud. Automatically protect regulated data with integrated encryption and multi-factor user authentication.
Ease of Deployment	CloudSOC offers a range of deployment options. Leverage unified authentication, integrated endpoint options, agentless solutions, integrated web security, proxy chaining, shared intelligence, unified policy management, and more between CloudSOC and integrated Symantec DLP, authentication, encryption, threat protection, and secure web gateway solutions.

Specifications

Specification	Details
Usability and Management	• Management dashboards to monitor users, policies, threats, services, violations, and locations.
App-Specific Dashboards	• Customizable dashboards with customizable widgets. • Easy online store activation for new apps.
RBAC	• Standard and custom reports.
Deployment, Access, and Control for Users and Devices	• SAML-based single sign-on solutions (Okta, Ping, ADFS, VIP, and so on). • LDAP-based User Directories (Active Directory, UnboundID, Open Directory, and so on). • Mobile app support and MDM platform interoperability to manage cloud traffic via IPSec VPN tunnels. • Device management and security posture checks with OPSWAT Gears host checking to management access from both company and personal devices.
Data Security and DLP	• Automatic classification content types: FERPA, GLBA, HIPAA, PCI, PII, Business, Computing, Cryptographic Keys, Design, Encryption, Engineering, Health, Legal, and Source Code. • Automatic file classification: Animation, communication, database, publishing, encapsulated, and executable. • Blacklist and whitelist content profiles, custom forms learning. • Integrated Symantec DLP
Threat Detection	• Dashboard views of riskiest users, incidents, services, location, and severity. • Threat Map visualization of risky user actions and ThreatScores. • User activity summaries and detailed logs. • Integrated Symantec threat protection with file reputation, malware detection, and cloud sandboxing.
Policy Enforcement	• Granular policy controls based on UBA-based ThreatScore, service, action, user, date, time, risk, browser, device, location, object, and content. • Pre-deployment policy impact analysis. • Policy-driven activity logs. • Policy actions: Admin and user notifications, multi-factor authentication, block, quarantine, logout, redirect, legal hold, and additional cloud app-specific actions for access monitoring and enforcement and control over data exposure, file sharing, and transfers.
Logs and Data	• Log-driven visualizations and graphs. • Boolean Search and granular filters: Servers, user, object, activity, severity, location, browser, platform, device, and source. • Activity log summaries: Services, action, user, date, time, and risk. • Granular log data: Services, actions, user, date, time, risk, browser, policy, location, object, content, URL, and device details. • SIEM export formats: CEF, CSV, and LEEF.
CloudSoc API	CloudSOC offers an API for events and incidents that are recorded by CloudSOC modules. The API facilitates an easy integration of CloudSOC with apps and tools like SIEM, SOAR, etc

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-CASB-SaaS-PB101 May 20, 2020