CloudSOC™
CASB for IaaS

Symantec

Symantec CloudSOC safeguards your organization so you can embrace IaaS with confidence.

Safeguard your data

Organizations store and share sensitive corporate content in AWS, Azure and other sanctioned IaaS storage. Secure this data against accidental exposure or malicious data breach.

Protect against threats

IaaS misconfigurations errors are common and leave cloud services exposed to public access or misuse. Bad actors and malware target these accounts for attack. Protect your organization against the impact of a compromised cloud account.

Achieve regulatory compliance

Regulations require risk analysis, monitoring, data privacy and documented systems to maintain a compliant security posture. Manual auditing is unreliable. Manage your cloud security posture and ensure compliance across IaaS deployments.

Respond to security incidents

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

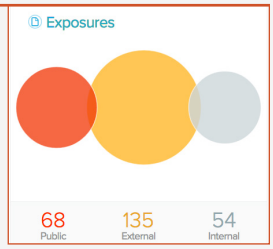
CASB for IaaS

Classify sensitive data

Automatically classify and track sensitive data in cloud apps with machine learning-based ContentIQ™ for highly accurate identification of compliance-related data, confidential data, and data in custom forms.

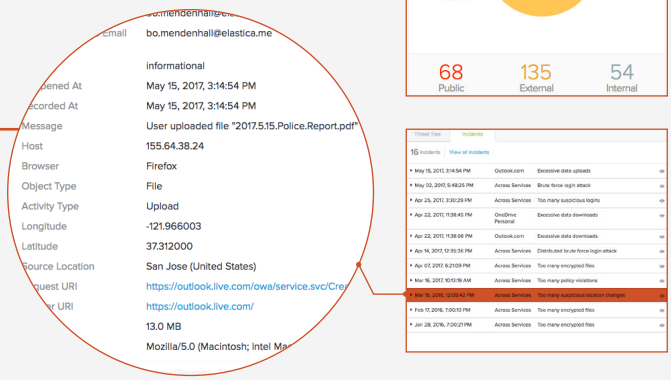
Identify and remediate risky exposures

Prevent and reduce risk of data exposure with policies that can block, coach, alert, encrypt, unshare, and otherwise safeguard data in the cloud. Use ContentIQ DLP in CloudSOC or extend your Symantec Enterprise DLP to protect data in cloud apps.



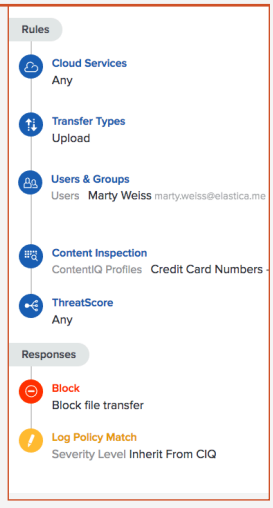
Track user activity in granular detail

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 both sanctioned and unsanctioned apps and preventative controls with this in-line capability.



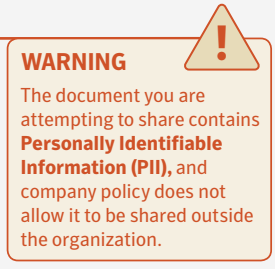
Enforce granular policies to safeguard data

Prevent data breach with automatic controls to encrypt, block, unshare, or trigger adaptive multifactor authentication for sensitive data. Get granular with policy controls defined by action, object type, data classification, user, ThreatScore™, app and more.



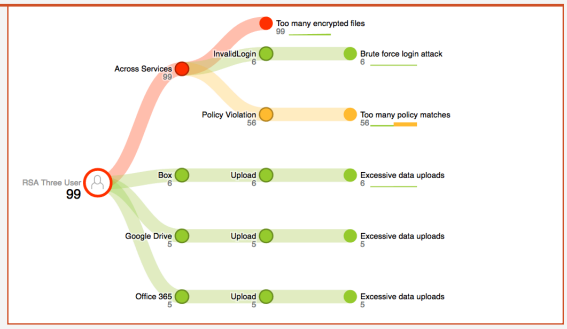
Coach users on appropriate cloud use

Automatically alert users when they have attempted high risk behavior and inform them of security response actions.



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.



Symantec

CASB for IaaS *(cont.)*

Detect and mitigate malware in the cloud

Defend your organization from malware in cloud accounts with industry-leading Symantec advanced protection complete with file Insight reputation, anti-malware, file analysis, and sandboxing in the cloud.

Comply with regulations and benchmarks

Achieve compliance with cloud security posture management (CSPM) in integrated Symantec Cloud Workload Assurance. Continuously monitor and assess your risks with out-of-the-box policies that map IaaS configurations to government regulations, industry standards, and best practice frameworks such as CIS, PCI, HIPAA, and more. Use data security capabilities to identify, monitor, encrypt and control access to regulated types of data. Keep your data in your geography with regional data centers.

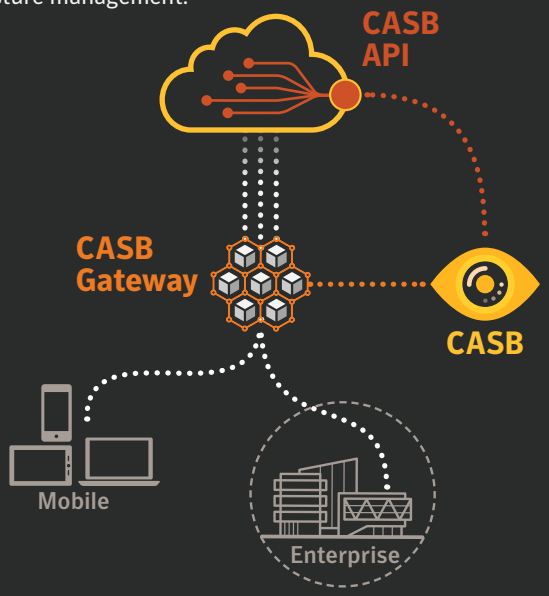
SSN PII FERPA PHI PCI GLBA

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 IaaS 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 deliver highly accurate monitoring and policy control built on machine learning and delivered through intuitive easy-to-use dashboards. CloudSOC offers integrated Cloud Workload Assurance for cloud security posture management.



E10 CASB for IaaS

Protects sanctioned corporate accounts with API-based, app-specific Securlet

E20 CASB for IaaS

Protects sanctioned corporate accounts with API-based, service-specific Securlet

Secures service-specific traffic with any accounts with CASB Gateway service-specific Gatelet

Available for: Amazon Web Services, Microsoft Azure

E30 CASB Gateway available for monitoring and control over custom apps in IaaS

Symantec

Key Features

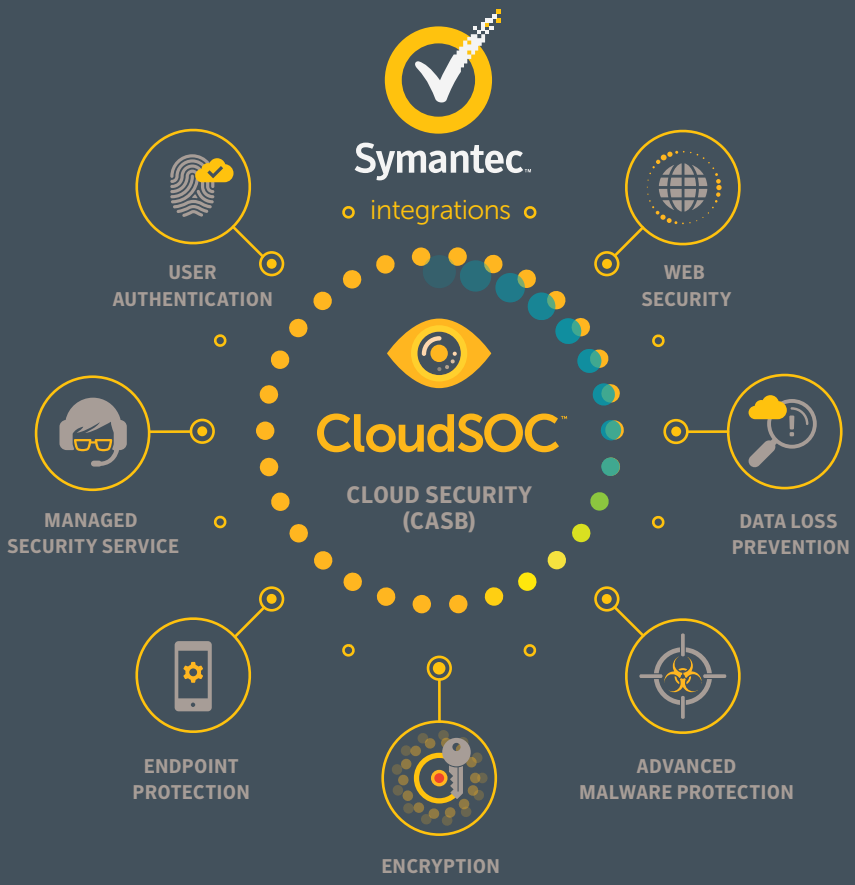
Comprehensive App Coverage	Monitors and controls use of sanctioned SaaS and IaaS platforms including custom apps on AWS, Azure, Google Cloud Platform and more through API integrations and in-line traffic analysis.
ContentIQ™ DLP	Automatically identifies sensitive data such as PII, PCI, PHI, source code, and more that is at risk through user activity and enables policy controls to prevent data loss. Leverages machine-learning, custom and predefined dictionaries, and learned custom form profiles for highly accurate results.
StreamIQ™ Activity Monitoring	Extracts events in cloud apps and from real-time cloud application traffic and delivers granular data including user, action, app, file, data, device, and more. Unique data science-powered technology enables this deep visibility into transactions with any cloud application.
User-Centric ThreatScore™	CloudSOC User Behavior Analytics (UBA) leverages intelligence from StreamIQ and machine learning to automatically maintain individualized user profiles, map user activity, and compile a live user ThreatScore.
Policy Enforcement	Enforces granular, context-aware policies based on ThreatScore 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 historical 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 to suit your organization. Leverage unified authentication, integrated endpoint options, proxy chaining, shared intelligence, unified policy management, and more between CloudSOC and integrated Symantec DLP, authentication, encryption, threat protection, endpoint and secure web gateway solutions.

Specifications

Usability and Management
Management dashboards to monitor users, policies, threats, services, violations, locations
Service-specific dashboards
Customizable dashboards with customizable widgets
Easy online 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, etc.)
LDAP-based User Directories (Active Directory, UnboundID, Open Directory, etc.)
Mobile app support, Symantec Endpoint Protection Mobile, 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
Content types: FERPA, GLBA, HIPAA, PCI, PII, Business, Computing, Cryptographic Keys, Design, Encryption, Engineering, Health, Legal, Source Code. Machine learning classifies custom form types.
File classification: Animation, communication, database, publishing, encapsulated, and executable file types.
Blacklist and whitelist content profiles
Integrated Symantec DLP
Encryption and DRM: Symantec Information Centric Encryption powered by PGP, Cloud Data Protection, SafeNet
Threat Detection
Dashboard views of riskiest users, incidents, services, location, severity
Threat Map visualization of risky user actions and ThreatScores
User activity summaries and detailed logs
Integrated Symantec advanced threat protection with file reputation, advanced anti-malware, and cloud sandboxing
Policy Enforcement
Granular policy controls based on UBA-based ThreatScore, service, action, user, date, time, risk, browser, device, location, object, 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, source
Activity log summaries: services, action, user, date, time, risk
Granular log data: services, actions, user, date, time, risk, browser, policy, location, object, content, URL, and device details
SIEM export formats: CEF, CSV, LEEF

Get better security with less complexity

Deploy a cloud security solution that integrates with your existing security infrastructure. A Symantec solution with CloudSOC provides greater security coverage, reduces operational complexity, and provides an optimal user experience.



For more info on Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems, visit **go.symantec.com/casb**

About CloudSOC

Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of 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.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

symantec.com +1 650-527-8000