CloudSOC™ Gateway

Data Sheet

Symantec CloudSOC Gateway enables enterprises to continuously monitor and control the use of cloud apps.

Gain granular visibility & control

Gain deep visibility into user activity across a broad range of cloud apps and services, and enforce granular content and context-based policies.

Protect sanctioned, unsanctioned, and custom apps

Track and govern activity for both sanctioned and unsanctioned cloud apps, including custom apps and those not administered by the organization.

Enforce policies in real-time

Identify risky activity, malicious behavior or malware threats and block them in real-time.

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.

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.

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

About Symantec

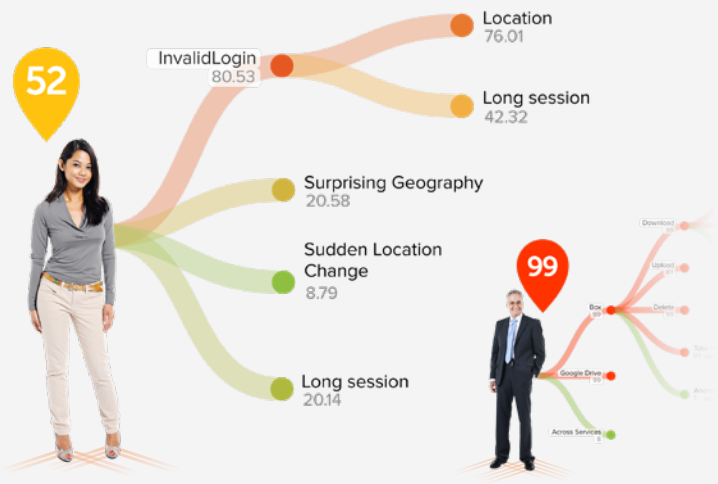
Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across 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.

CloudSOC Gateway

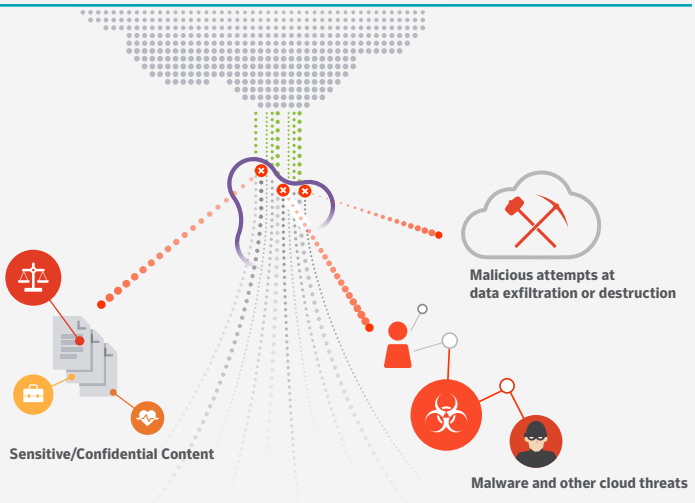
Identify risky behavior and high-risk users

View and prioritize threats based on user ThreatScore to quickly identify anomalous user behavior, such as account takeovers, data exfiltration and data destruction attempts. This data can be cross correlated with associated detailed logs to verify suspected breaches. If any users have been found to have been targeted by the attack, policies can be created to block those users from accessing the service to prevent data loss.



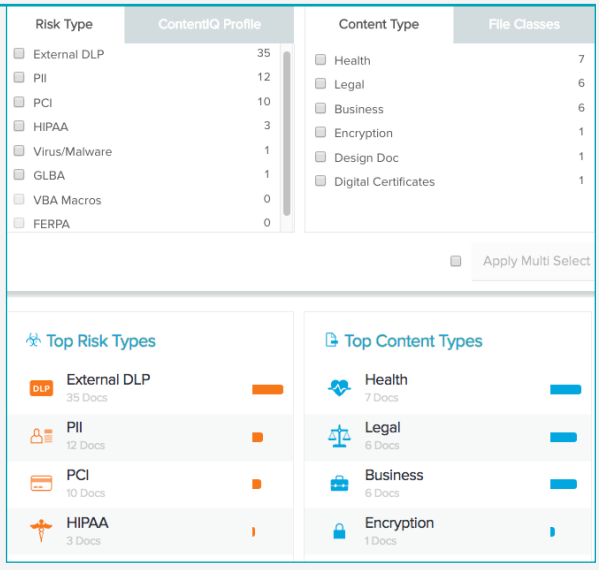
Continuously monitor to identify and protect sensitive data

ContentIQ™ technology can be leveraged to continuously monitor cloud app usage and detect sensitive content such as source code, design documents, or engineering documents that are being shared in the cloud. These events can trigger alerts for further investigation, or policies can be crafted to prevent unwarranted uploading and sharing of these documents.



Prevent compliance violations

ContentIQ identifies and classifies critical compliance related data such as personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) content then continuously monitors how that data is being uploaded, downloaded, or shared in cloud apps. Policies can be used to control how this data is handled. Any attempted compliance violations can be tracked for further follow-up.



Symantec.

CloudSOC Gateway *(cont.)*

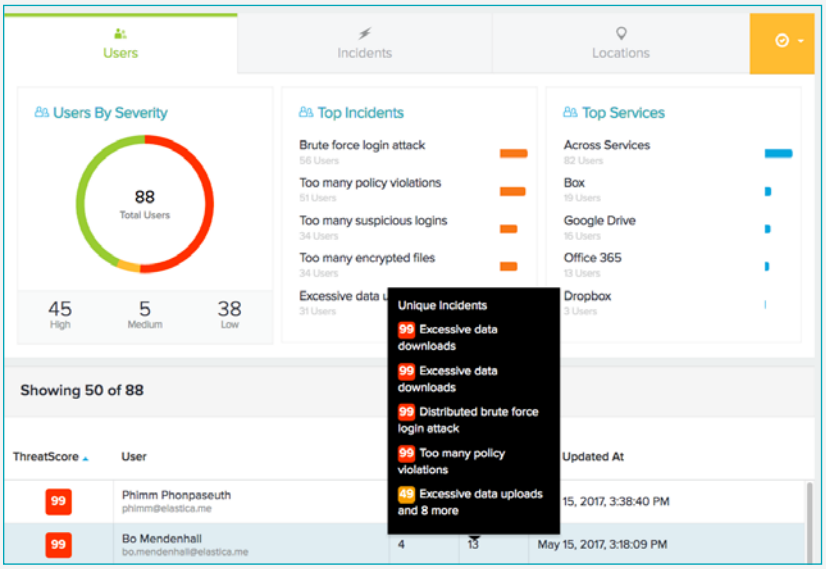
Perform post incident analyses on historical data

Quickly investigate areas of concern in cloud accounts. CloudSOC collects granular data on transactions using machine learning-assisted StreamIQ™ technology. You can then access historical data through intuitive search and filtering functions and analyze it via powerful data visualizations and consolidated log reports.

Extend your existing data protection investment to the cloud

Symantec offers several native integrations designed to extend your existing security investment to the cloud. These integrations add the ability to:

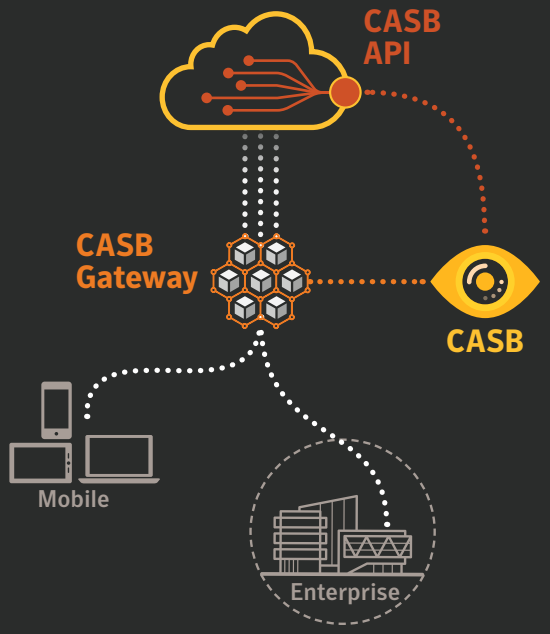
- Apply existing Symantec DLP policies and remediation workflows to content inspection in the cloud.
- Control user access to cloud apps based on dynamic UBA intelligence from CloudSOC.
- Tokenize or encrypt compliance related cloud data



Symantec.

How it Works

CloudSOC Gateway is a cloud-based transparent forward proxy that can perform user account activities without breaking cloud app functionality. Symantec's CloudSOC data science platform analyzes cloud traffic in real-time to identify threats, create and enforce policies, and support analysis of historical cloud activity.



Natively integrate CloudSOC Gateway with Symantec DLP, ICE, and VIP:

DLP
Extends on-premises DLP policies and workflows to the cloud

ICE
Tokenizes or encrypts compliance data without breaking cloud app functionality

VIP
Enables risk-based intelligent authentication for critical cloud app activities and content

ITSM
Enables incident response workflows

Key Features

Comprehensive App Coverage	Monitors use of SaaS, PaaS, and IaaS through in-line traffic analysis of any cloud app. Control transactions with both sanctioned and unsanctioned cloud apps and accounts.
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 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, including custom apps.
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	Real-time enforcement of granular 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, and secure web gateway solutions.

Specifications

Usability and Management
Management dashboards to monitor users, policies, threats, services, violations, locations
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, etc.)
LDAP-based User Directories (Active Directory, UnboundID, Open Directory, etc.)
Mobile app support, MDM platform interoperability, and SEP Mobile integration 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
File classification: animation, communication, database, publishing, encapsulated, executable
Blacklist and whitelist content profiles
Integrated Symantec DLP
Encryption and DRM: Symantec 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 Cynic 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, 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

Symc_DS_CloudSOC_Gateway_en_v3b

Symantec.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com