Data Sheet

CloudSOC™ Gateway

Symantec

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

Enforce policies in real-time

Identify malicious or inappropriate data sharing, malware threats, credential attacks and more, and react with policy response in real-time.

Gain granular visibility & control

Gain deep visibility into user activity across thousands of cloud apps and services, and enforce granular content and context-based policies. Rank risky behavior via user behavior analysis.

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, and automate escalations

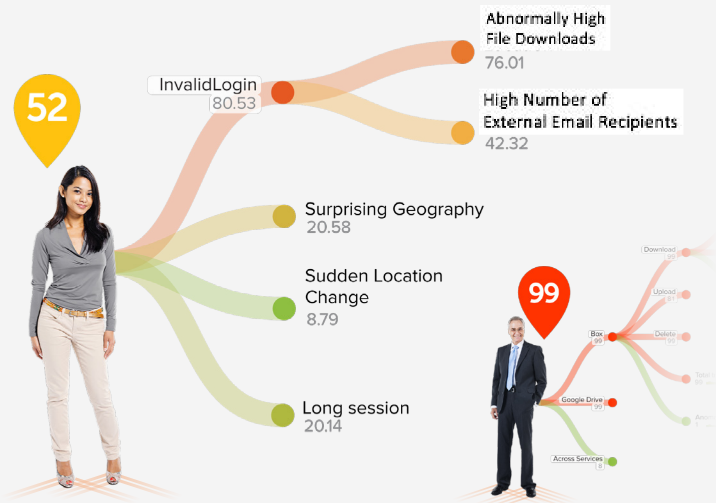
Protect sanctioned & unsanctioned apps

Track and govern activity for both sanctioned and unsanctioned cloud apps, including those not administered by the organization. Employ forward proxy, Gateway, or Mirror Gateway options to complete coverage for managed and unmanaged devices for any app.

CloudSOC Gateway

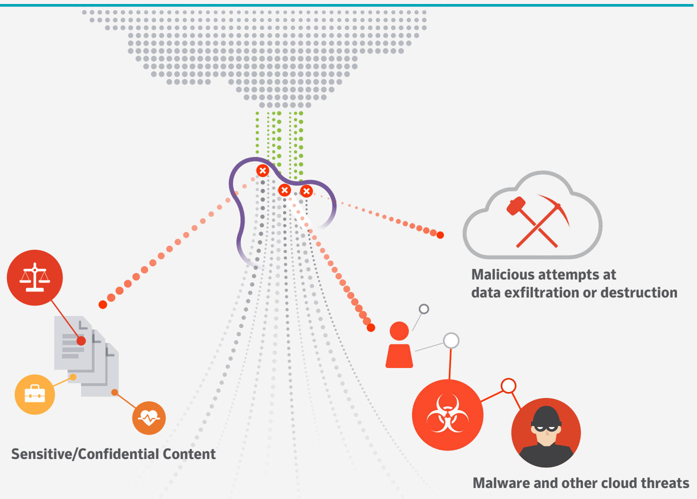
Identify risky behavior and high-risk users

View and prioritize threats based on a user behavior analytic (UBA) 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. For users targeted by the attack, policies can be created to block those credentials from accessing an sharing confidential data or service to prevent data loss.



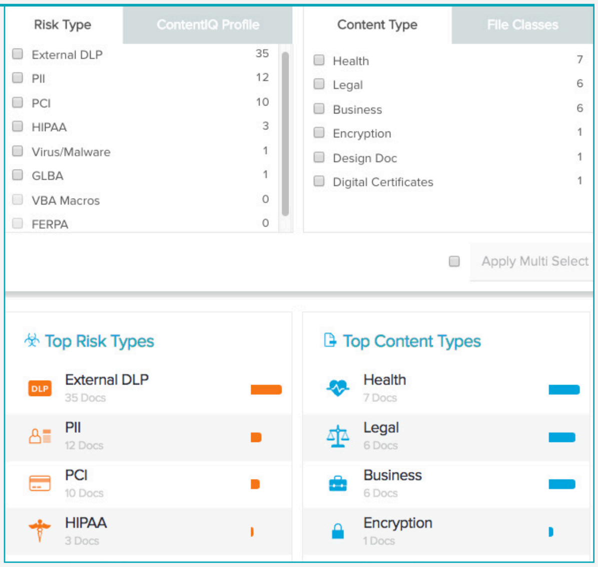
Continuously identify, monitor, and protect sensitive data

ContentIQ™ technology can be employed to continuously monitor and detect sensitive data such as source code, design documents, legal documents, or engineering documents that are being shared in the cloud. ContentIQ can apply DLP and automatically classify sensitive data types. DLP events trigger alerts for further investigation, or policies can be crafted to prevent unwarranted uploading and sharing of confidential data.


Malicious attempts at data exfiltration or destruction
Sensitive/Confidential Content
Malware and other cloud threats

Prevent compliance violations

ContentIQ enforces data loss prevention by identifying and classifying critical compliance-related data such as PHI, PCI, and PII, and 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 are recorded for further follow-up or investigation.



Risk Type	ContentIQ Profile
□ External DLP	35
□ PII	12
□ PCI	10
□ HIPAA	3
□ Virus/Malware	1
□ GLBA	1
□ VBA Macros	0
□ FERPA	0

Content Type	File Classes
□ Health	7
□ Legal	6
□ Business	6
□ Encryption	1
□ Design Doc	1
□ Digital Certificates	1

□ Apply Multi Select

Top Risk Types

- External DLP 35 Docs
- PII 12 Docs
- PCI 10 Docs
- HIPAA 3 Docs

Top Content Types

- Health 7 Docs
- Legal 6 Docs
- Business 6 Docs
- Encryption 1 Docs

CloudSOC Gateway *(cont.)*

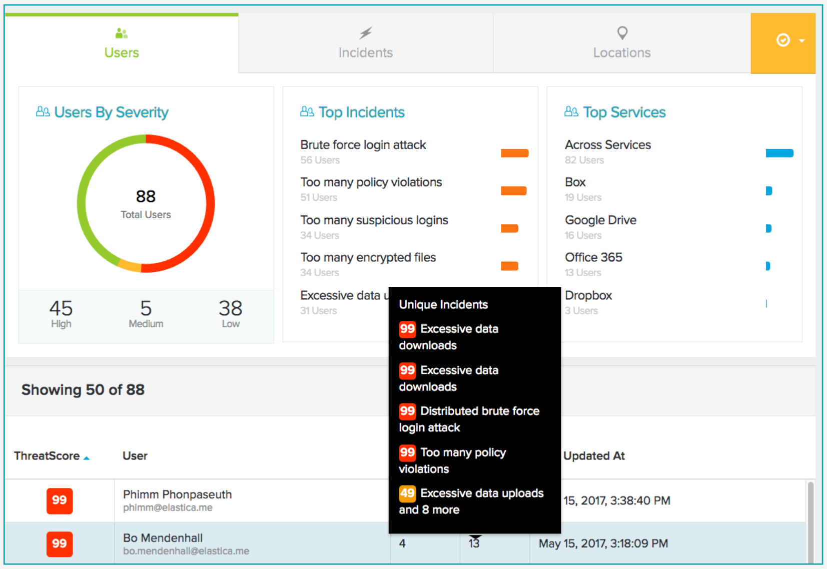
Perform post-incident analyses

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 on cloud actions and security incidents through intuitive search and filtering function, then analyze it via powerful data visualization 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 enterprise DLP policies and remediation workflows to the cloud.
- Implement quantified risk-based, adaptive user authentication to cloud apps based on UBA intelligence.
- Encrypt compliance-related cloud data and apply digital rights management.



Users By Severity

88 Total Users

45 High | 5 Medium | 38 Low

Top Incidents

Brute force login attack
56 Users

Too many policy violations
51 Users

Too many suspicious logins
34 Users

Too many encrypted files
34 Users

Excessive data u
31 Users

Top Services

Across Services
82 Users

Box
19 Users

Google Drive
16 Users

Office 365
13 Users

Dropbox
3 Users

Showing 50 of 88

ThreatScore	User			Updated At
99	Phimm Phonpaseuth phimm@elastica.me			15, 2017, 3:38:40 PM
99	Bo Mendenhall bo.mendenhall@elastica.me	4	13	May 15, 2017, 3:18:09 PM

Unique Incidents

99 Excessive data downloads

99 Excessive data downloads

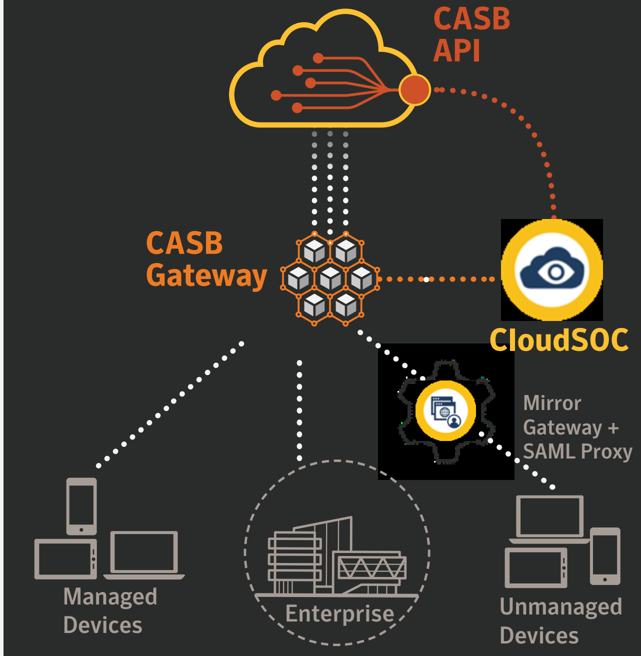
99 Distributed brute force login attack

99 Too many policy violations

49 Excessive data uploads and 8 more

How it Works

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



Natively Integrate CloudSOC Gateway with Symantec DLP, ICE, VIP, and WSS:

DLP

Extends on-premises DLP policies and workflows to the cloud

ICE

Encrypts compliance data without breaking cloud app functionality

VIP

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

WSS

Provides one-click integration to simplify app traffic management and access controls

Key Features

Comprehensive App Coverage	Monitors use of any application, SaaS, and IaaS platforms through in-line traffic analysis. Control transactions with both sanctioned and unsanctioned cloud apps and accounts, with options from managed and unmanaged devices.
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 data matching 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 nearly 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, 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 with simple visualizations allow 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. Employ 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, Symantec WSS, ICE 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 SEP integration, 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
- Agentless deployment using SAML and Mirror Gateway
- Single unified web and cloud security agent for devices

Data Security and DLP

- Content types: FERPA, GLBA, HIPAA, PCI, PII, Business, Computing, Cryptographic Keys, Design, Encryption, Engineering, Health, Legal, Source Code, and more
- File classification: Animation, communication, database, publishing, encapsulated, executable
- Blacklist and whitelist content profiles
- Integrated with Symantec DLP
- Encryption and DRM: Symantec ICE Encryption powered by PGP, SafeNet
- Highly accurate, automated data classification informed by over 300 million micro indicators for 1,000+ file types

Threat Detection

- Dashboard views of riskiest users, incidents, services, location, severity
- Threat Map visualization of risky user actions, behavior profiles, and ThreatScores
- User activity summaries and detailed logs
- Integrated Symantec threat protection with file reputation, URL reputation, malware detection, and cloud sandboxing

Policy Enforcement

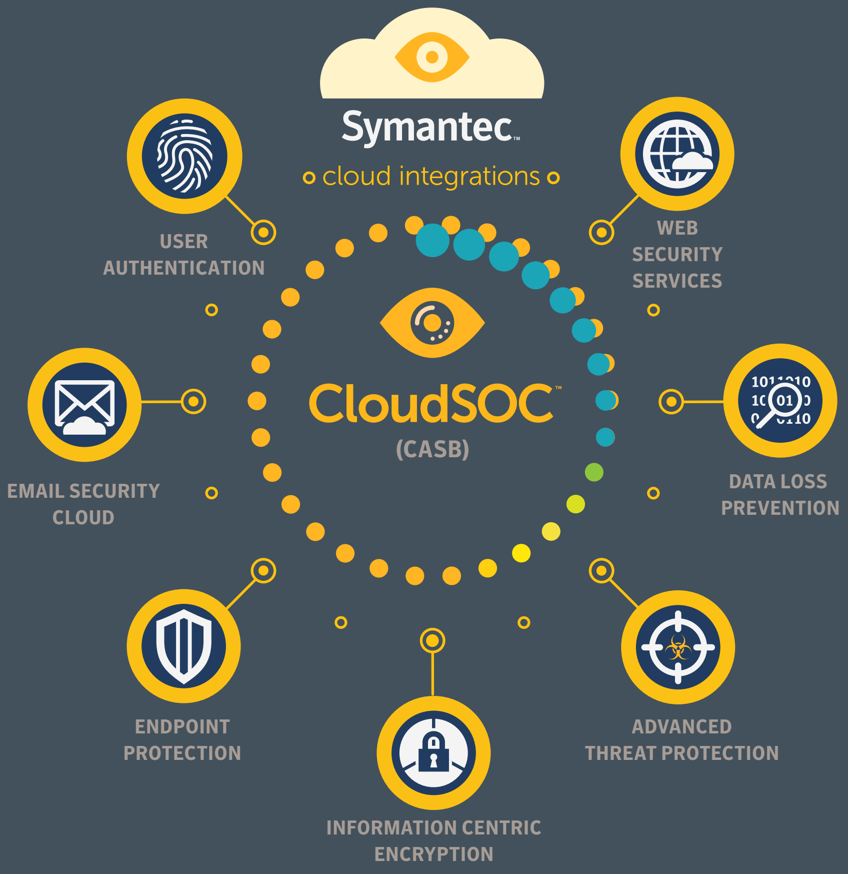
- Granular policy controls based on UBA-based ThreatScore, service, action, user, date, time, risk, browser, device, location, object, content
- Pre-deployment policy impact analysis
- Policy-driven activity logs
- Policy actions: admin and user notifications, multi-factor authentication, block, quarantine, 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, and API

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 lets companies to use cloud applications and services with confidence 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