Symantec™

CloudSOC™
CASB for SaaS

Data Sheet

Symantec CloudSOC CASB for SaaS safeguards your organization so you can embrace cloud apps with confidence.

Safeguard your data

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

Protect against threats

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

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.

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.

About CloudSOC

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.

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

About Symantec

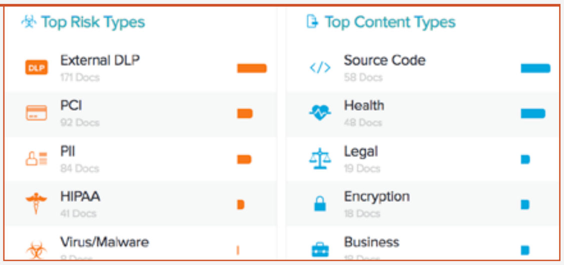
Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across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

CASB for SaaS

Classify sensitive data

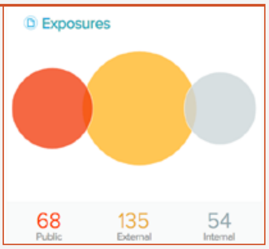
Automatically classify and track sensitive data in cloud apps with machine learning-based ContentIQ™ DLP for highly-accurate identification of compliance-related data, confidential data, and data in custom forms.



Top Risk Types		Top Content Types	
External DLP	171 Docs	Source Code	58 Docs
PCI	92 Docs	Health	48 Docs
PII	84 Docs	Legal	19 Docs
HIPAA	41 Docs	Encryption	18 Docs
Virus/Malware	8 Docs	Business	18 Docs

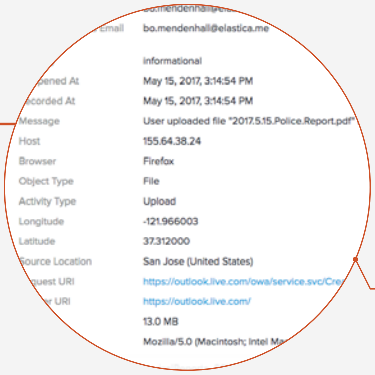
Identify, block, and remediate risky exposures

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

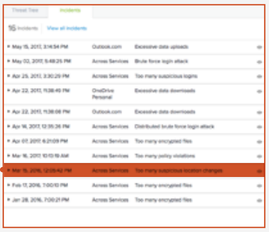


Track user activity in granular detail

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 any sanctioned or unsanctioned app with options for managed or unmanaged devices and preventative controls with this in-line capability.



Email	bo.mendenhall@elastica.me
	informational
pened At	May 15, 2017, 3:14:54 PM
ecorded At	May 15, 2017, 3:14:54 PM
Message	User uploaded file "2017.5.15.Police.Report.pdf"
Host	155.64.38.24
Browser	Firefox
Object Type	File
Activity Type	Upload
Longitude	-121.966003
Latitude	37.312000
Source Location	San Jose (United States)
quest URI	https://outlook.live.com/owa/service.svc/Cre
r URI	https://outlook.live.com/
	13.0 MB
	Mozilla/5.0 (Macintosh; Intel Ma



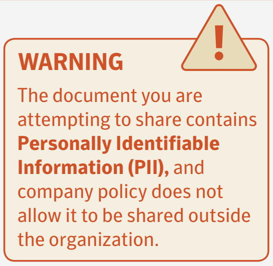
Threat Tree Incidents

16 Incidents | View all incidents

May 15, 2017, 3:14:54 PM	Outlook.com	Excessive data uploads
May 03, 2017, 5:48:25 PM	Across Services	Brute force login attack
Apr 25, 2017, 3:30:29 PM	Across Services	Too many suspicious logins
Apr 22, 2017, 11:38:40 PM	OneDrive Personal	Excessive data downloads
Apr 22, 2017, 11:38:08 PM	Outlook.com	Excessive data downloads
Apr 18, 2017, 12:35:26 PM	Across Services	Distributed brute force login attack
Apr 07, 2017, 6:21:09 PM	Across Services	Too many encrypted files
Mar 16, 2017, 10:10:18 AM	Across Services	Too many policy violations
Mar 15, 2016, 12:05:42 PM	Across Services	Too many suspicious location changes
Feb 17, 2016, 7:00:10 PM	Across Services	Too many encrypted files
Jan 28, 2016, 7:00:21 PM	Across Services	Too many encrypted files

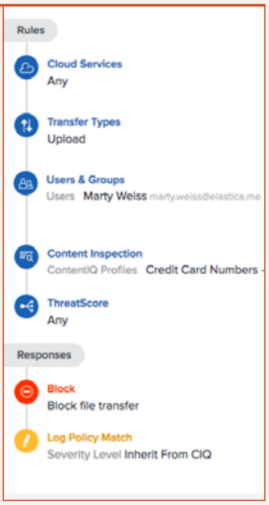
Enforce granular policies to safeguard data

Prevent data breach with automatic controls via fast API and in-line enforcement to encrypt, block, unshare, or trigger adaptive multifactor authentication for sensitive data. Get granular policy controls defined by action, data classification, user, ThreatScore™, and automate responses.



WARNING

The document you are attempting to share contains **Personally Identifiable Information (PII),** and company policy does not allow it to be shared outside the organization.



Rules

Cloud Services
Any

Transfer Types
Upload

Users & Groups
Users Marty Weiss marty.weiss@elastica.me

Content Inspection
ContentIQ Profiles Credit Card Numbers

ThreatScore
Any

Responses

Block
Block file transfer

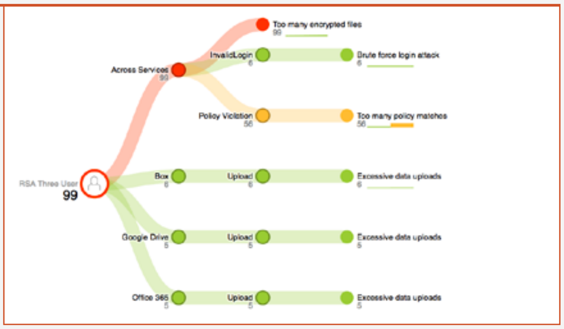
Log Policy Match
Severity Level Inherit From CIQ

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.



Symantec.

CASB for SaaS *(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, URL reputation, and cloud sandboxing.

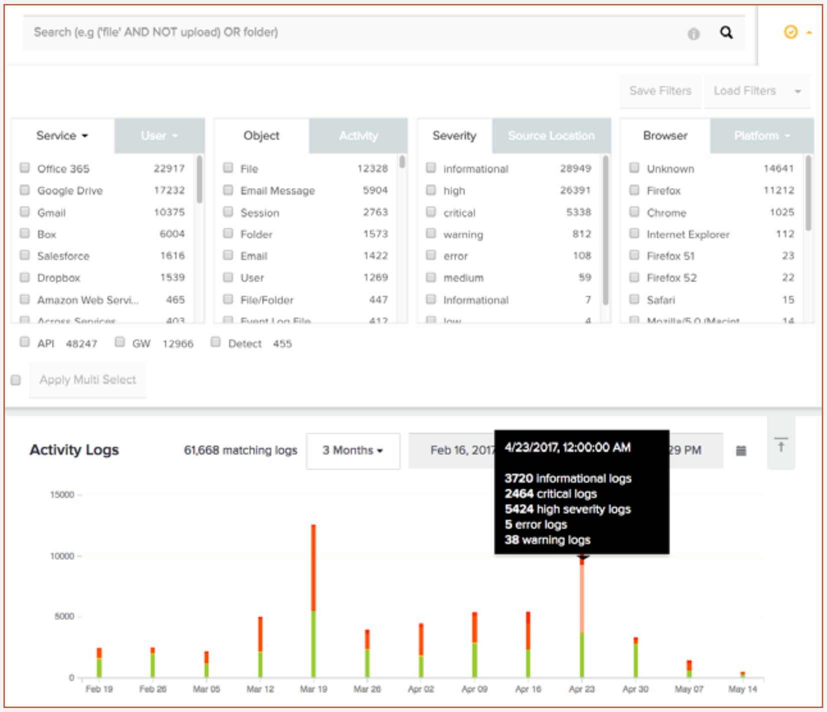
Comply with regulatory requirements

Use data security capabilities in CloudSOC to identify, monitor, encrypt and control access to PII, PHI, and other regulated types of data. Keep your data in your geography with regional data centers. Control access to CloudSOC data with granular RBAC.

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.



Search (e.g ('file' AND NOT upload) OR folder)

Service ▾		User ▾
□ Office 365	22917	
□ Google Drive	17232	
□ Gmail	10375	
□ Box	6004	
□ Salesforce	1616	
□ Dropbox	1539	
□ Amazon Web Servi...	465	
□ Across Services	403	

Object		Activity
□ File	12328	
□ Email Message	5904	
□ Session	2763	
□ Folder	1573	
□ Email	1422	
□ User	1269	
□ File/Folder	447	
□ Event Log File	412	

Severity		Source Location
□ informational	28949	
□ high	26391	
□ critical	5338	
□ warning	812	
□ error	108	
□ medium	59	
□ Informational	7	
□ low	4	

Browser		Platform ▾
□ Unknown	14641	
□ Firefox	11212	
□ Chrome	1025	
□ Internet Explorer	112	
□ Firefox 51	23	
□ Firefox 52	22	
□ Safari	15	
□ Mozilla/5.0 (Macint	14	

□ API 48247 □ GW 12966 □ Detect 455

□ Apply Multi Select

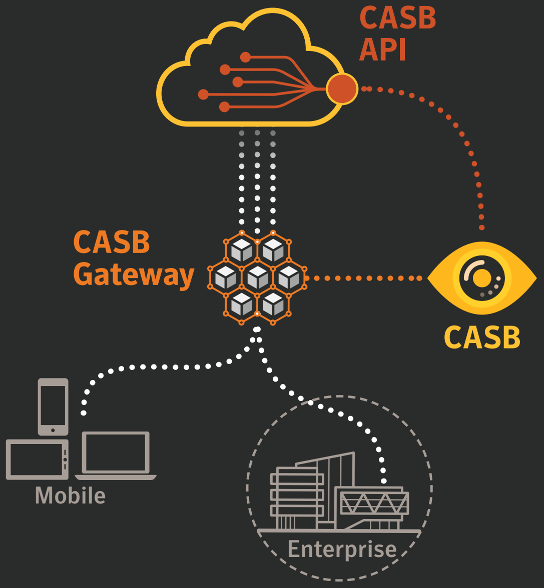
Activity Logs 61,668 matching logs 3 Months ▾ Feb 16, 2017 … 29 PM

4/23/2017, 12:00:00 AM

3720 informational logs
2464 critical logs
5424 high severity logs
5 error logs
38 warning logs

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.



Advanced CASB for SaaS (E10)

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

Premium CASB for SaaS (E20)

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

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

Available for: Office 365, Box, Dropbox, Salesforce, GitHub, Jive, DocuSign, ServiceNow, Workday, Yammer, Slack, Cisco Webex Teams, Facebook Workplace, GitHub.

Also available for Amazon Web Services, Google G-suite, Microsoft Azure laaS.

Key Features

Comprehensive App Coverage	Monitors and controls use of sanctioned SaaS platforms such as Office 365, G-Suite, Box, Dropbox, Salesforce, and more through extensive 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 data-matching results.
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 to suit your organization. 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

Usability and Management

- Management dashboards to monitor users, policies, threats, services, violations, 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, etc.)
- LDAP-based User Directories (Active Directory, UnboundID, Open Directory, etc.)
- 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, Source Code
- Automatic file classification: animation, communication, database, publishing, encapsulated, executable
- Blacklist and whitelist content profiles, custom forms learning
- 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 threat protection with file reputation, malware detection, and cloud sandboxingw

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