Symantec

Solution Brief

CloudSOC CASB Security for Amazon Web Services

Protect your Amazon Web Services from misconfigurations, misuse, attacks, threats, and data loss with an industry-leading cloud access security broker.

- Are you monitoring your AWS for misconfigurations or unsanctioned instances?
- Do you log and analyze admin and user behavior, identifying risky actions?
- Do you ensure your confidential data is secure and private?
- Are you safeguarding instances against malware and advanced attacks?

DID YOU KNOW?

In 2018:

AWS was one of the top 5 apps used for business enablement.

13% of the 758M cloud-stored documents were broadly shared and at high risk of exposure.

Average cost per company of a data breach in the cloud: 2.8M

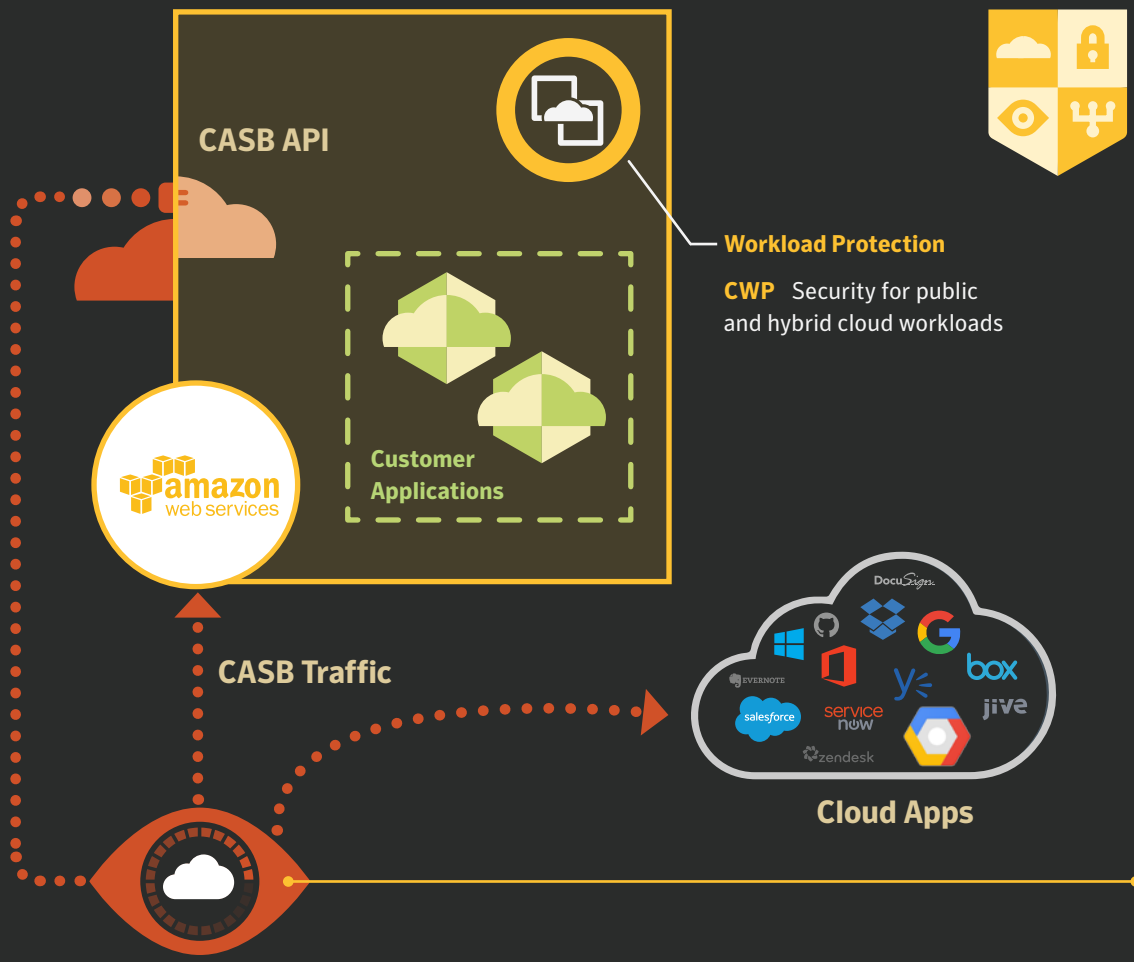
Sources: Symantec 2018 Shadow Data Report

S3 bucket misconfigurations were responsible for millions of PHI, PCI, and PII records exposed.

Source: Security Boulevard, Sept 2018

Symantec IaaS Security

Get continuous visibility and control over identity and access to systems, settings, and content based on granular contextual event attributes using multi-channel CASB functions leveraging both API integration and inline traffic inspection, as well as other tools such as Cloud Workload Protection and Secure Access Cloud.



Cloud Access Security Broker, CASB

- **Monitor, log, and analyze user and admin activity**
- **Enforce access controls to prevent misconfigurations**
- **Detect and remediate risky exposures in S3 buckets**
- **Defend S3 storage from advanced malware and ATPs**
- **Detect compromised accounts with User Behavior Analytics**
- **Detect and restrict misuse and "Shadow" AWS instances**

Integrated Cyber Defense

CloudSOC is an integral part of the Symantec Integrated Cyber Defense Platform, which delivers multi-channel protection across cloud, web, email, and endpoints —backed by the Symantec Global Intelligence Network.

Data Loss Prevention
Industry-leading DLP helps protect sensitive data from loss with comprehensive detection and unified policies.

Malware Protection
Advanced malware defense using reputation, machine learning, behavior analysis and virtual machine-aware sandboxing.

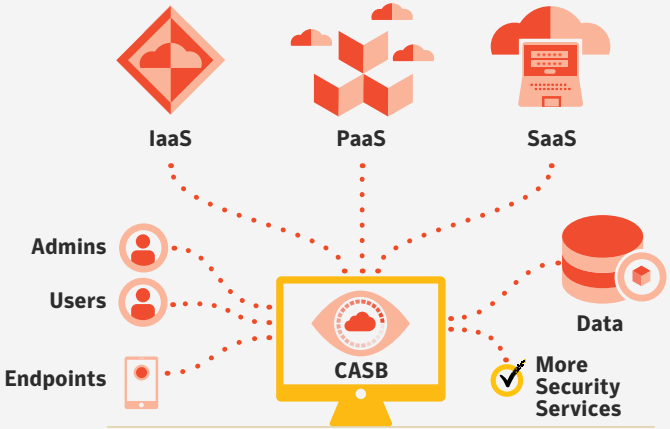
User Authentication
The Secure Access Cloud provides highly secure, granular access management for enterprise applications deployed in IaaS clouds or on-premises. Symantec VIP offers MFA based on real-time threat risks.

Encryption
Information Centric Encryption (ICE) enables end-to-end digital rights management.

Compliance
Verify cloud security posture against compliance and governance control guidelines.

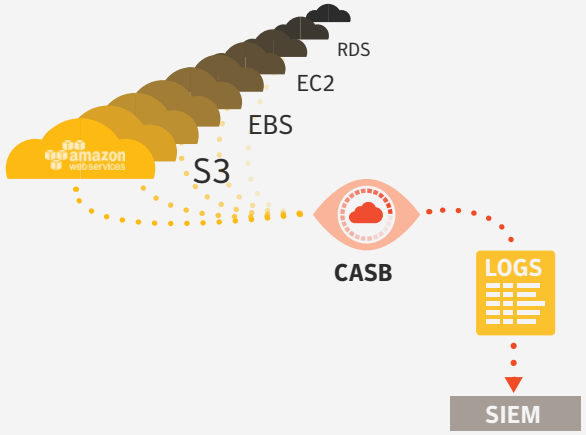
Symantec

Protect your users, data, and accounts in AWS with industry-leading security



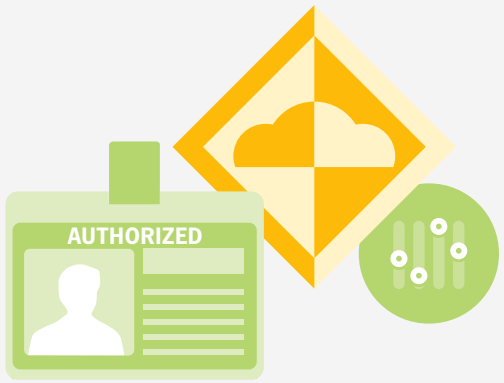
Symantec CloudSOC CASB helps you protect sanctioned and unsanctioned use of AWS with admin monitoring and logging, access controls, configuration monitoring and control, and user behavior analytics (UBA). CloudSOC provides exposure analysis, DLP scanning, and threat protection for S3 Buckets. Get visibility and control over access to systems, settings, and content based on granular contextual event attributes using multi-channel CASB functions leveraging both API integration and inline traffic inspection. CloudSOC enables you to detect and respond to security issues for your IaaS, PaaS, and SaaS cloud apps and infra-structure, including AWS, all in one platform.

Monitor, log, and investigate activity in AWS



Monitor the creation of new instances and log user and administrator activity across AWS Cloudtrail services, including EC2, EBS, S3, RDS, etc. with a customizable AWS dashboard. Access a complete audit trail of activity for your AWS and other cloud services in CloudSOC with visualization trees, so you can easily investigate and analyze security incidents to correlate events across cloud apps and accounts to discover what really happened. Get the big picture backed by granular detail in intuitive dashboards with powerful search and graphical reporting, or export detailed incident logs to your SIEM for analysis. Leverage customizable reports to provide critical insights to compliance, IT, and other stakeholders (like a Cloud Center of Excellence) when a security incident occurs.

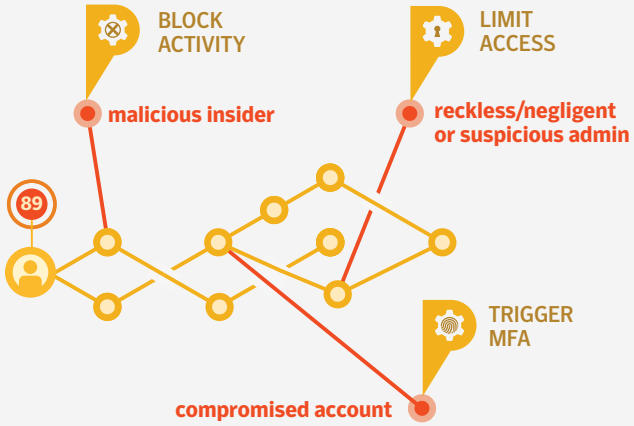
Safeguard against risky changes and privileged misuse



Remediate and prevent shadow AWS instances and unauthorized changes. Enforce access controls. Confirm that users creating instances or making administrative changes are authorized with change management. Automate protective controls over changes to AWS with policies to:

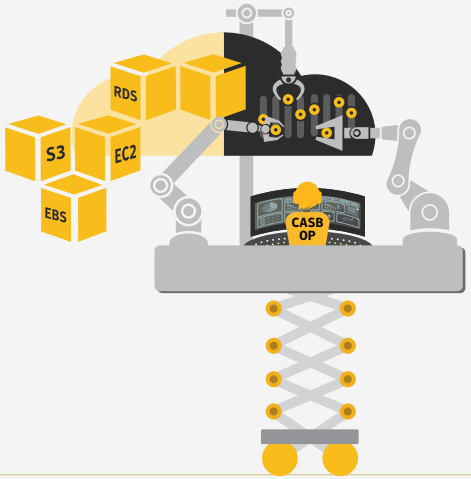
- Monitor creation and termination of instances,
- Control uploads of sensitive data,
- Restrict access based on location, endpoint attribute, or user ThreatScore™,
- Limit permitted user actions based on AD attributes,
- Prevent DevOps from working on unsanctioned accounts, etc.

Detect malicious insiders and compromised accounts



Discover attacks and malicious usage indicating a compromised user account or malicious insider with data science-driven UBA that automatically learns normal activity patterns for teams and individuals to help identify abnormal and potentially dangerous activity such as brute force attacks, malware upload, repeated attempts to change security settings, uploads of sensitive data, or instances of termination. A machine-learning system automatically assigns a dynamic ThreatScore to users and admins to allow you to quickly detect sources and activities of concern, with a simple policy-building tool to automate responses such as blocking further activity, limiting access, or requiring further user authentication - and initiate escalation where needed.

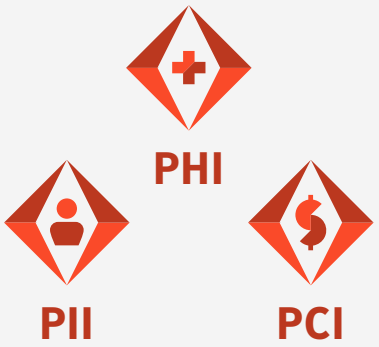
Monitor and control security configurations



Use CloudSOC to remediate and prevent data exposure or loss by auditing and correcting public S3 Buckets settings. Monitor and control S3 access and requests. Detect and enforce configuration controls over unsanctioned instances or unsanctioned changes to existing instances. Continuously monitor group, role, and security settings, and enforce controls over configuration settings and changes that could compromise security. Automate configuration controls over your AWS infrastructure with policies to:

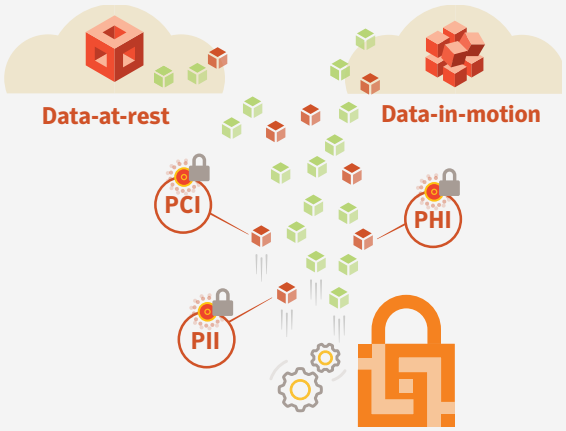
- Block or remediate changes to security groups,
- Confirm that MFA is enabled for root accounts,
- Monitor creation and changes to instances and S3 buckets,
- Correct misconfiguration.

Keep your S3 Buckets and your confidential data secure



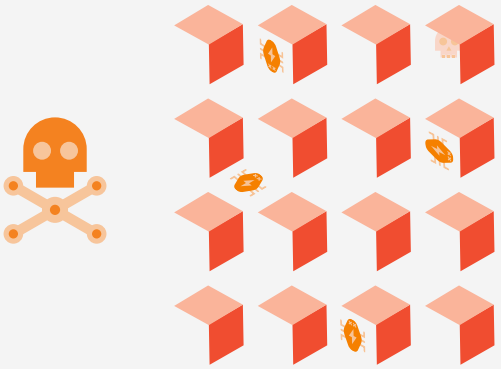
Monitor S3 Bucket configurations and track sensitive data in S3 Buckets using data science-powered DLP to automatically classify sensitive and compliance related data such as Personally Identifiable Information (PII), Payment Card Information (PCI), and Private Healthcare Information (PHI) and more - even source code. Prevent future data exposures or loss with content-aware and context-aware cloud DLP policies to track and control what sensitive data can be stored, accessed, and shared. Use ContentIQ™ DLP in CloudSOC to apply consistent DLP policies across all your cloud apps and services including AWS. or leverage integrated Symantec DLP to extend centralized enterprise-wide DLP policies and work flows to AWS.

Keep data private with automated encryption and digital rights management



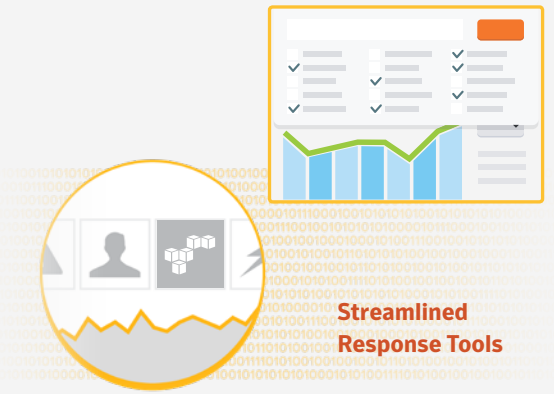
Ensure that confidential and sensitive data stays private by automating encryption controls using CloudSOC policies. Set layered protections in place to enforce DLP-driven encryption over data-at-rest in AWS and transactions with sanctioned and unsanctioned AWS instances that contain data-in-motion. CloudSOC flexibility enables you to use your preferred encryption approach—from Symantec Information Centric Encryption to native AWS encryption to third-party encryption solutions, such as SafeNet by Gemalto.

Defend AWS storage against advanced malware threats



Continuously scan S3 Bucket content to detect malware threats in your AWS storage. CloudSOC integrates with industry-leading Symantec threat protection to help you detect and quarantine advanced malware in your AWS storage using machine learning, behavioral and static analysis, file reputation insight, and virtual-machine aware cloud sandboxing.

Always know the state of your security with intuitive dashboards and reports



Easily keep track of the current state of your AWS installation security through an intuitive user interface that provides default and fully customizable dashboards. Gain deep insights into AWS and other cloud activity through detailed pivot tables, charts, and graphs. Role-based access controls provide administrators just the right level of visibility and control. Management, compliance officers, and other stakeholders can be kept informed with regularly scheduled, customizable reports. Create automatic event escalations of issues or violations with any email-initiated ticketing system.

About CloudSOC

The Data Science Powered™ Symantec CloudSOC CASB platform empowers companies to confidently employ cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC CASB 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 aids in investigation of historical account activity for post-incident analysis. CloudSOC provides cloud access security broker protection for a wide range of Saas, PaaS, and laaS solutions.

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.

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

CloudSOCforAWS_en_v6