Symantec

Solution Brief

Security for IaaS
CloudSOC is the cornerstone for tactical defense

Protect your Amazon Web Services, Azure environments, and Google Cloud Platform with the industry's most complete solution for IaaS security.

- Are you able to secure and monitor the access of your DevOps teams to your cloud datacenter?
- Do you log and analyze admin and user behavior to both identify possible credential compromise, and mitigate high risk or unsanctioned activity?
- Are you monitoring your IaaS deployments for misconfiguration, unsanctioned instances, and compliance posture?
- Do you ensure your confidential data is secure and private, and safeguarding against malware and advanced attacks?

DID YOU KNOW?

On public IaaS platforms:

Stolen Credentials represent the **most common lateral attack movement** through the network.[1]

2/3 of All Organizations have risky user behavior. [2]

[1] *Source: 2018 Symantec Internet Security Threat Report*

[2] *Source: Symantec 2018 Shadow Data Report*

amazon web services

Google Cloud

Microsoft Azure

Symantec Security for AWS, Azure and GCP

CWP DevSecOps

IaaS Environment

Cloud Workload Protection

Cloud Workload Protection Platform (CWPP)

- Auto-discovery and security
- Anti-malware and real-time file integrity management
- App isolation and control

CWP for Storage

- Anti-malware scanning
- Public exposure alerts
- DLP detection & remediation

CloudSOC™ InfoSec

CASB for IaaS

Cloud Access Security Broker (CASB)

- User monitoring and control
- UEBA account protection
- Discover shadow accounts
- Prevent misconfiguration
- Policy enforcement
- DLP for storage
- Advanced Malware Protection for storage

* *Integrates with* ***CASB for SaaS***

Cloud Workload Assurance

Cloud Security Posture Management (CSPM)

- Auto-discovery of resources
- Monitor configuration risks
- Compliance assurance

Secure Access Cloud

Zero-trust access to corporate applications deployed in cloud or on-premises

- Simplify remote access for infrastructure
- Enhanced trust SaaS
- Application-level visibility and control

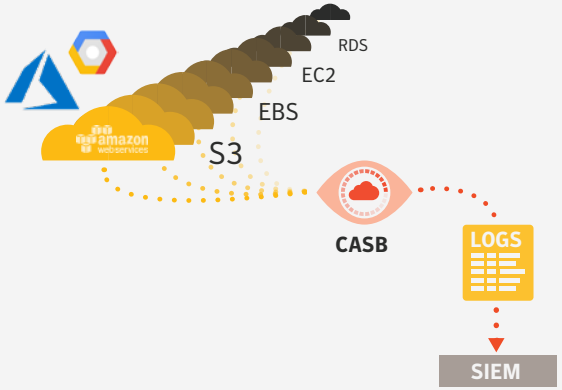
Integrated Cyber Defense

Unify cloud and on-premises security to provide advanced threat protection and information protection across all endpoints, networks, email and cloud applications.

Symantec helps you detect and respond to security issues within your IaaS, PaaS, and SaaS environments; including AWS, Azure, and Google Cloud; with integrated security solutions.

Get visibility and control over identity an access to platforms, settings, and content, based on granular context and event attributes using multi-channel cloud security functions using API integration, agents, and in line traffic inspection. Symantec Security for IaaS offers administrator monitoring and logging, OS hardening, access control, configuration monitoring and control, user and entity behavior analytics (UEBA), exposure analysis, DLP, threat protection, plus compliance analysis and remediation.

Monitor, log, and investigate activity



With the click of a button, users can instantly procure and provision IaaS instances, many of which are spun up outside the view of IT, and which house sensitive data. Get visibility into sanctioned and unsanctioned IaaS usage with Symantec CloudSOC. Monitor the creation of new IaaS instances, and log user and administrator activities across AWS CloudTrail services, including EC2, EBS, S3 and RDS, all from a customizable dashboard. Access a complete audit trail of activity for AWS and other cloud services and apps, where you can easily investigate, analyze and correlate security events across cloud apps and accounts to discover what really happened. Get the big picture backed by granular details using intuitive dash boards with powerful search and data visualization. Integrate cloud with other network security by exporting detailed incident logs to your SIEMs. Provide critical insights about security incidents to internal stakeholders—including Audit and Compliance—using customizable reports from CloudSOC.

Secure and harden workloads

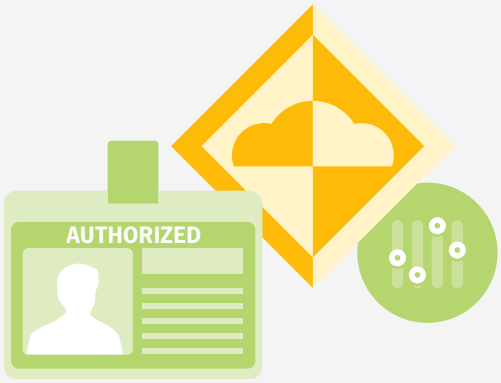
Organizations are rapidly migrating data center workloads to IaaS providers including AWS, Azure, and Google Cloud Platform for business agility, IT modernization, and cost savings. While cloud providers secure the underlying infrastructure, customers are responsible for securing their workloads, containers, and storage. Symantec Cloud Workload Protection automatically discovers and protects IaaS workloads with OS hardening, real-time file integrity monitoring, anti-malware, and application control to help block attacks and prevent data breaches or ransomware. Native integration with public cloud APIs allow DevOps personnel to incorporate security best practices into their agile workflows to deploy secure, immutable applications and services essential to compliance. A single Cloud Workload Protection console enables control and security of enterprise workloads, containers, and storage across multiple IaaS public and private clouds, and even traditional on-premises data center environments.

Secured the access to workloads

Provides granular authorization to corporate resources deployed in IaaS clouds or on-premises based on the contexts of user, device, and workload, offering full visibility and control over the user's actions to create a Zero-Trust access method for enterprises. Eliminate the inbound network connections created by VPNs and NGFWs, effectively cloaking corporate applications and making them invisible to would-be attackers and malicious users while preventing network-based attacks and lateral movement.

No agent is needed on the endpoint device; SAC can be deployed within minutes and removes the complexity and cost of maintaining appliances and endpoint agents.

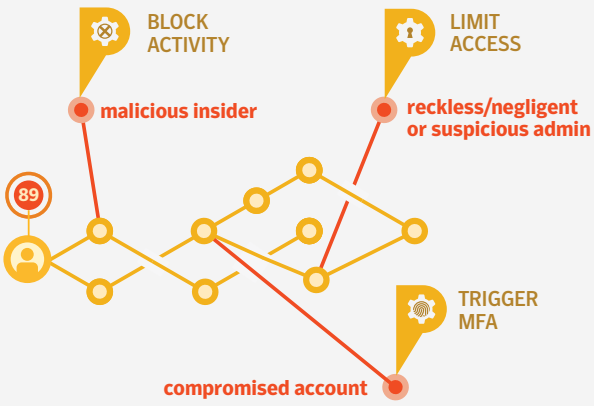
Safeguard versus privileged misuse



Remediate and prevent shadow IaaS instances and unauthorized changes. Enforce access controls. Confirm users creating instances or making administrative changes are authorized. Automate protective controls over changes to IaaS environments via CloudSOC policies to:

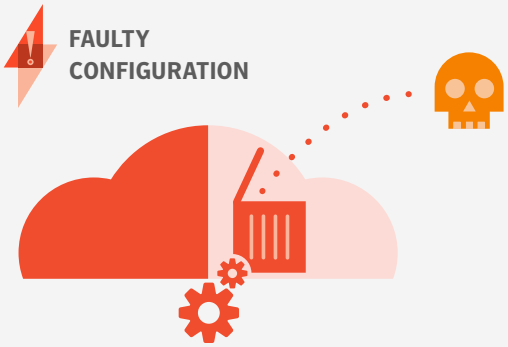
- Monitor creation and termination of instances
- Control uploads of sensitive data
- Restrict access based on location, endpoint attribute, or user ThreatScore™
- Limit permitted user actions based on AD attributes
- Report on compliance and enforce policy
- Prevent DevOps from working on unsanctioned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

Detect malicious insiders and compromised accounts



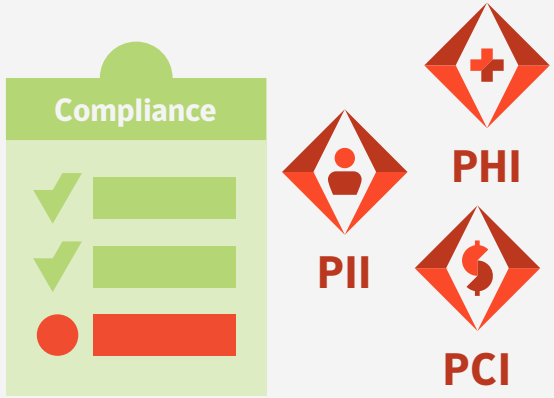
Discover attacks and malicious usage indicating privileged misuse, a compromised user account or malicious insider with data science driven UEBA that automatically learns normal activity patterns and identifies abnormal and potentially dangerous activity such as brute force attacks, attempts to change security settings, upload sensitive data, or terminate instances. Machine learning within in CloudSOC automatically assigns a dynamic ThreatScore to users and admins to report sources and activities of concern. With ThreatScore, you can automate policy-based responses such as blocking further activity, limiting access, or requiring further user authentication. A ThreatMap gives you are view of risky user activities across IaaS, PaaS, and SaaS apps to diagnose attack patterns visually. Complex sequence detectors identify multi-stage attacks involving multiple apps and actions.

Identify and control misconfigurations



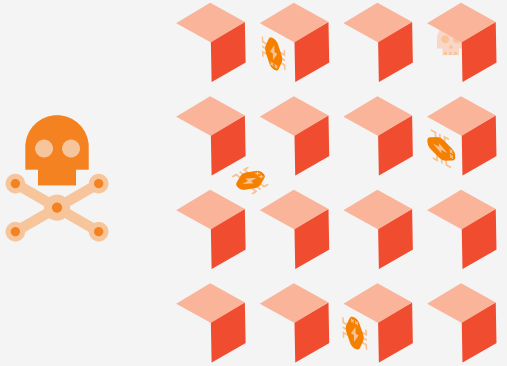
Configuration errors in cloud storage services are exposing massive amounts of corporate data to the public Internet and leaving the door wide open to hackers. With Symantec cloud security solutions you can monitor and control siloed IaaS environments for faulty resource configurations that expose your organization to malicious attacks and data breaches from a centralized control point. Cloud Workload Assurance service, integrated with Symantec CloudSOC and Symantec Cloud Workload Protection, identifies and fixes exploitable misconfigurations through automated discovery of cloud resources and remediation of failed security checks across your AWS and Azure environments. Cloud Workload Protection performs OS hardening while CloudSOC tracks admin activities for high risk configuration changes.

Keep confidential data secure meet compliance standards



Configuration errors in cloud storage services are exposing massive amounts of corporate data to the public Internet and leaving the door wide open to hackers. Avoid embarrassing and costly breaches with unparalleled data protection for cloud storage from Symantec cloud security. Monitor and track confidential data in Amazon S3, Azure Storage, and custom apps with content scanning that automatically classifies document types an ientifies regulated data, intellectual property, and any other type of sensitive information. Prevent leaks with data loss prevention policies that monitor and secure what data can be stored, accessed, and shared on AWS and Azure. Ensure personal data stays private with automated encryption controls for Amazon S3.

Defend storage against advanced malware threats



Attackers are using advanced techniques to exploit and abuse cloud services, looking for weak links that can provide a clear path to data or opportunities to use your IaaS resources for their purposes. Automatically detect and remediate malware threats lurking in your AWS S3 storage buckets with powerful anti-malware scanning and quarantine action from Symantec cloud security. Immediately identify and alert when any S3 buckets are infected. Prevent the proliferation of malware, and protect against data destruction or breaches with industry-leading threat protection that leverages reputation analysis, machine learning, behavioral analysis, and cloud sandboxing.

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, detection of intrusions and threats, detection of high risk user actions, protection against data loss and compliance violations, and investigation of historical account activity for post-incident analysis. CloudSOC provides cloud access security broker protection for sanctioned and unsanctioned IaaS, PaaS, and SaaS use. CloudSOC integrates with Symantec Cloud Workload Assurance (CSPM), Data Loss Protection, Secure Web Gateways, User Authentication, Encryption, Advanced Threat Protection, Endpoint Protection, Global Intelligence Network and more to offer a CASB 2.0 Integrated Cyber Defense solution.

go.symantec.com/casb

About Cloud Workload Protection

Symantec Cloud Workload Protection (CWP) Suite enables secure adoption of cloud IaaS platforms with workload protection, storage protection, and cloud security posture management. CWP discovers and secures workloads across AWS, Azure, and Google Cloud Platform, as well as private cloud and on-premises environments. CWP for Storage discovers and scans Amazon S3 storage for malware and threats with cloud-native integration that allows DevOps to build security into CICD pipelines. Cloud Workload Assurance reduces risk by benchmarking security controls in AWS and Azure against industry and compliance standards including CIS, CSA, PCI, HIPAA, and more. A single console unifies visibility, security policy and posture, and vulnerability reporting.

go.symantec.com/cwp

About Secure Access Cloud

SAC provides an agentless, cloud-delivered service that secures access at the application-level to corporate resources deployed in IaaS clouds or on-premises using Zero Trust Access principles and Software-Defined Perimeter (SDP) architecture. SAC provides true point-to-point connectivity and cloaks all resources on the network, fully isolating data centers from end-users and the Internet. Unlike the broad network access legacy of VPNs and NGFWs, the network-level attack surface is entirely removed, leaving no room for lateral movement and network-based threats.

SAC provides additional protection of the corporate resources by implementing continuous contextual (user, device and resource-based) authorization and granular activity controls for enterprise applications, whether deployed in IaaS clouds or on-premises data center environments.

https://www.symantec.com/solutions/zero-trust-ecosystem

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**

security-for-iaas-cloudsoc-cwp-sac-en.pdf