Symantec

DATA SHEET

Symantec Cloud Workload Protection & CWP for Storage

At a glance

Cloud Workload Protection

Automatic Discovery and Visibility of Public Cloud Workloads

- Continuous visibility of workloads deployed across AWS, Azure, and Google Cloud Platform (GCP)
- Automatic discovery of software services and workload security postures
- Real-time visibility into infrastructure changes

Apply Leading-edge Security across Hybrid Cloud Infrastructure

- Single console helps to protect workloads across public clouds, private clouds, and physical on-premises data centers
- Real-time anti-malware scanning using trusted SEP technologies OS hardening helps to block zero-day threats
- Unique application isolation helps to block exploits targeting known and unknown vulnerabilities
- OS hardening helps to block zero-day threats
- Real-time file integrity monitoring (RT-FIM) helps to prevent unauthorized system changes
- Protection and monitoring for Docker containers
- Real-time user activity and process monitoring identifies suspicious behaviors

Elastic, Cloud-native Protection

- Security scales automatically with dynamic cloud infrastructure
- Cloud-native integration with public cloud platforms enables DevOps to build security directly into service deployment workflows
- Flexible pay-for-use and annual subscription pricing models support agile business planning

Industry-leading SEP Real-time Anti-malware Scanning

- Real-time anti-malware scanning for compute instances and servers to help block malware-based attacks, including ransomware
- First cloud workload agent providing both anti-malware and hardening protections
- First cloud-native anti-malware offering in the industry for both compute and storage protection

CWP for Storage

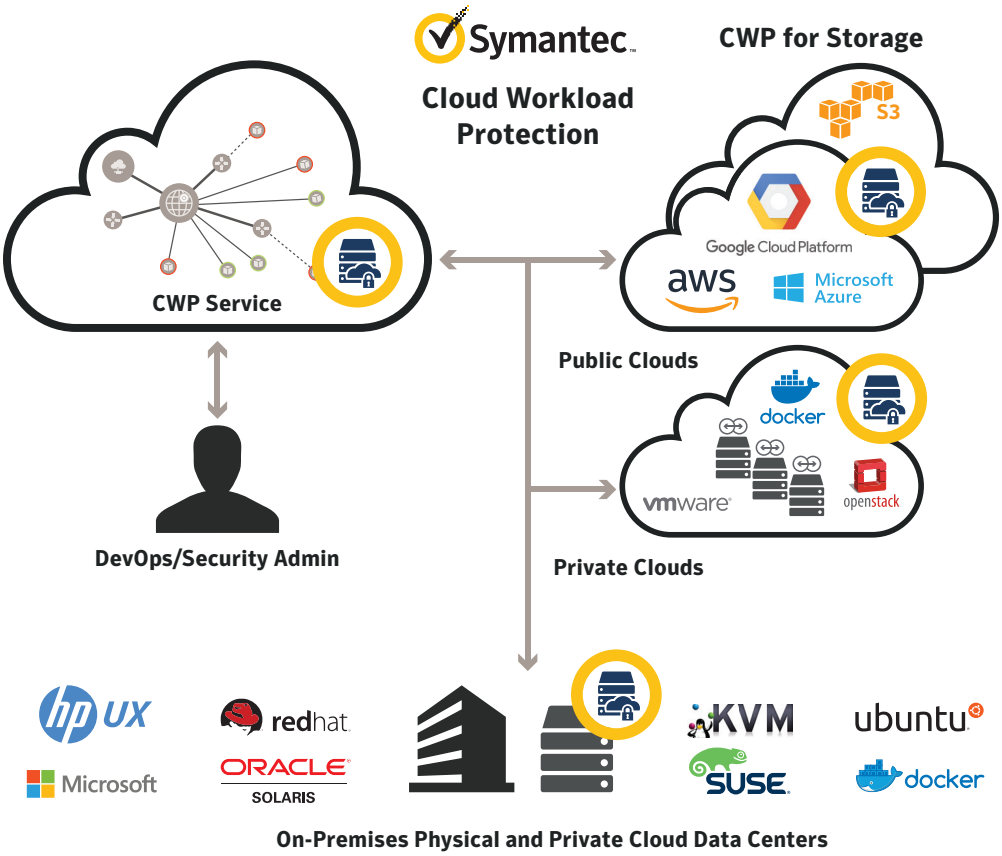
Keeps AWS S3 Buckets Free of Malware

- Automatic, scheduled, and on-demand scanning of AWS S3 buckets provide automatic threat protection
- Uses Symantec's suite of anti-malware technologies including reputation analysis and advanced machine learning
- Helps to protect against data breaches by discovering and alerting when S3 buckets are misconfigured or exposed to the public internet
- Anti-malware scanning occurs entirely inside of the customers VPC, ensuring that sensitive data is protected during assessment

Cloud Workload Security Challenges

As competition intensifies, enterprises are rapidly adopting public cloud services such as Amazon Web Services (AWS), Microsoft® Azure™, and Google Cloud Platform to increase business agility, relieve pressure on understaffed IT departments, and save money. Many public cloud providers offer security certifications for their own infrastructure, however the "shared responsibility" model of security means that customers are still responsible for protecting their workloads, along with any vulnerabilities, against exploits and data breach attempts. And, while some enterprises are choosing to go "all-in" with the public cloud, most businesses are choosing to pursue a "hybrid cloud" approach - using a combination of public cloud, private cloud, and on-premises resources and infrastructure to deliver applications and services to their employees and customers.

Further complicating security, when businesses begin migrating workloads, they quickly discover that a "lift and shift" approach to security fails in the public cloud. Modern operational practices must encompass the DevOps continuous delivery workflows that are central to efficient public cloud operations. Therefore to secure public deployments, enterprises need to purchase additional security solutions and hire additional operations personnel and security analysts to deploy policies, respond to alerts, and remediate threats.



On-Premises Physical and Private Cloud Data Centers

CWP Key Benefits:

- Auto-discovery and visibility of public cloud workloads
- Robust security across hybrid clouds
- Elastic, cloud-native protection
- Industry-leading SEP anti-malware scanning

CWP for Storage Key Benefits:

- Automatic protection of AWS S3 buckets
- Alert when buckets are publicly accessible
- Data remains inside VPC during scanning

aws partner network
Advanced Technology Partner
Security Competency
SaaS Partner

What enterprises need is a security solution that allows them to view, monitor, scan, and protect all of their workloads across the entire hybrid cloud from a single, efficient console.

Cloud Storage Security Challenges

Many applications and services running on AWS utilize S3 buckets for storage. Over time, storage can become contaminated with malware, ransomware, and other threats. Additionally, buckets can be misconfigured or left accessible to the public internet, leaving them vulnerable to a data breach event, and privacy regulations often require data to remain in the customers control at all times. A solution is needed to automatically scan buckets to keep them clean and free of malware while keeping sensitive data inside the VPC and not publicly accessible.

Symantec Cloud Workload Protection

Symantec Cloud Workload Protection (CWP) allows organizations to secure their critical workloads wherever they are – public clouds, private clouds, and physical on-premises data centers – all from a single intuitive console. CWP automates workload security, providing discovery, visibility, and protection against advanced threats. CWP's Cloud Bridge feature enables Symantec Data Center Security (DCS) customers to manage DCS agents on their virtualized and physical on-premises servers from the CWP console as well. Automatic and elastic cloud-native security for AWS, Azure, and Google Cloud Platform workloads, along with Docker container protection, enables business agility while integrating advanced protections into DevOps service workflows. Automatic identification of workload security postures and software services, including visibility into infrastructure changes, enables automatic policy recommendations and deployment.

CWP provides robust protection for hybrid cloud workloads including; Real-time Anti-malware scanning using industry-leading SEP technologies, unique Application Isolation that helps to block exploits targeting known and unknown vulnerabilities, OS Hardening that helps to stop zero-day threats, and Real-time File Integrity Monitoring (RT-FIM) that helps to prevent unauthorized system changes. In addition, CWP and CWP for Storage receive the latest threat and vulnerability information via the Symantec Global Intelligence Network (GIN). Powering one of the world's premier civilian cyber defense threat intelligence services, Symantec GIN continuously ingests threat information from more than 15,000 enterprises, 175 million endpoints (consumer and enterprise), and 3,000 threat researchers and engineers.

CWP for Storage

Symantec Cloud Workload Protection for Storage helps to protect AWS S3 buckets, enabling secure adoption of containers and serverless technologies such as AWS Lambda. Symantec's suite of anti-malware technologies, including advanced machine learning and reputation analysis, help to discover and remediate known and unknown threats to keep cloud storage clean. Automatic, scheduled, and on-demand scanning modes enable full-time protection to inspect files as they are uploaded, downloaded, or modified. Importantly, CWP for Storage helps to protect against data breaches by discovering and alerting when S3 buckets are misconfigured or exposed to the public internet. In addition, anti-malware scanning occurs entirely inside of the customers VPC, ensuring that sensitive data is protected during assessment and enabling compliance. S3 bucket security posture, alerts, and events are viewed in the single CWP console.

CWP Features

Protect Your Hybrid Cloud Workloads from a Single Console

Auto-Discovery and Visibility

- Visibility of workloads deployed across AWS, Microsoft Azure, and Google Cloud Platform
- Automatic discovery of software services on workloads
- Automatic identification of workload security postures
- Visibility into infrastructure changes

Robust Security across Hybrid Clouds

- Single console to protect workloads across public clouds, private clouds, and physical on-premises data centers
- Unique application isolation helps to block exploits targeting known and unknown vulnerabilities
- OS hardening helps to stop zero-day threats
- Real-time file integrity monitoring (RT-FIM) helps to prevent unauthorized system changes
- Real-time user activity and process monitoring identifies suspicious behaviors
- Protection and monitoring for Docker containers

Elastic, Cloud-native Protection

- Context sensitive, automated security policy deployment
- Infrastructure change tracker
- RESTful APIs for SIEM integration
- Security scales automatically with dynamic cloud infrastructure
- Cloud-native integration with public cloud platforms enables DevOps to build security directly into service deployment workflows
- Flexible pay-for-use and annual subscription pricing models support agile business planning

Industry-leading SEP Anti-malware Scanning

- Real-time, on-demand, and scheduled anti-malware scanning helps block malware-based attacks including ransomware and data exfiltration
- First cloud workload agent providing both anti-malware and hardening protections
- First cloud-native anti-malware offering in the industry for both compute and storage protection
- Leverages SEP hardening, reputation analysis, and advanced machine learning technologies to help discover and block unknown threats
- SEP anti-malware has received numerous awards and accolades from leading industry analysts and testing organizations

CWP for Storage Features

Scan Your AWS S3 Buckets for Malware and Prevent Data Breaches

Ensure Integrity of Data Stored on AWS S3

- Automatic, scheduled, and on-demand scanning of AWS S3 buckets
- Helps to protect against data breaches by discovering and alerting when S3 buckets are misconfigured or exposed to the public internet
- Anti-malware scanning occurs entirely inside of the customers VPC, ensuring that sensitive data is protected during assessment

Out-of-the-Box Security Policies

- Discovers and helps to block known and unknown threats using Symantec's anti-malware suite of technologies including advanced machine learning and reputation analysis
- Unparalleled protection powered by Symantec Global Intelligence Network, with 175 million endpoints secured

Seamless Integration and Scalability

- Automatic protection of S3 buckets minimizes DevOps and administrative workloads
- Enables secure adoption of containers and serverless AWS technologies such as Lambda
- Scanning infrastructure scales elastically for cost optimization

CWP Specifications

Public cloud platform support:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Automated policy recommendations included for:

LAMP Stack –

- OS: Amazon Linux, RedHat, CentOS, Ubuntu, Oracle Enterprise Linux
- Applications: Apache, Tomcat, PHP, Postgres, MySQL, Oracle

Windows –

- OS: Win 2008, 2012, 2016
- Applications: IIS, SQL Server

Additional Information Online

CWP supported platforms, kernels, and browsers

CWP supported software service discovery

CWP architecture and components

CWP getting started

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, 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 and LifeLock product suites to protect their digital lives at home and across 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, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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

19C205721_ds_Symantec_Cloud_Workload_Protection_EN