Symantec

DATA SHEET

Symantec Cloud Workload Protection & CWP for Storage

At a Glance

Cloud Workload Protection

Automatic Discovery and Protection of Workloads

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

Single Console to Protect Multi-cloud and Hybrid Cloud Environments

- Single console helps to protect workloads across multiple public clouds, private clouds, and physical on-premises data centers
- Anti-malware scanning using industry-leading SEP technologies helps to block threats including ransomware
- Application control and 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
- Real-time user activity and process monitoring identifies suspicious behaviors
- Protection and monitoring for Docker containers

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

CWP for Storage

Protects Cloud Storage Against Threats and Discovers Sensitive Data

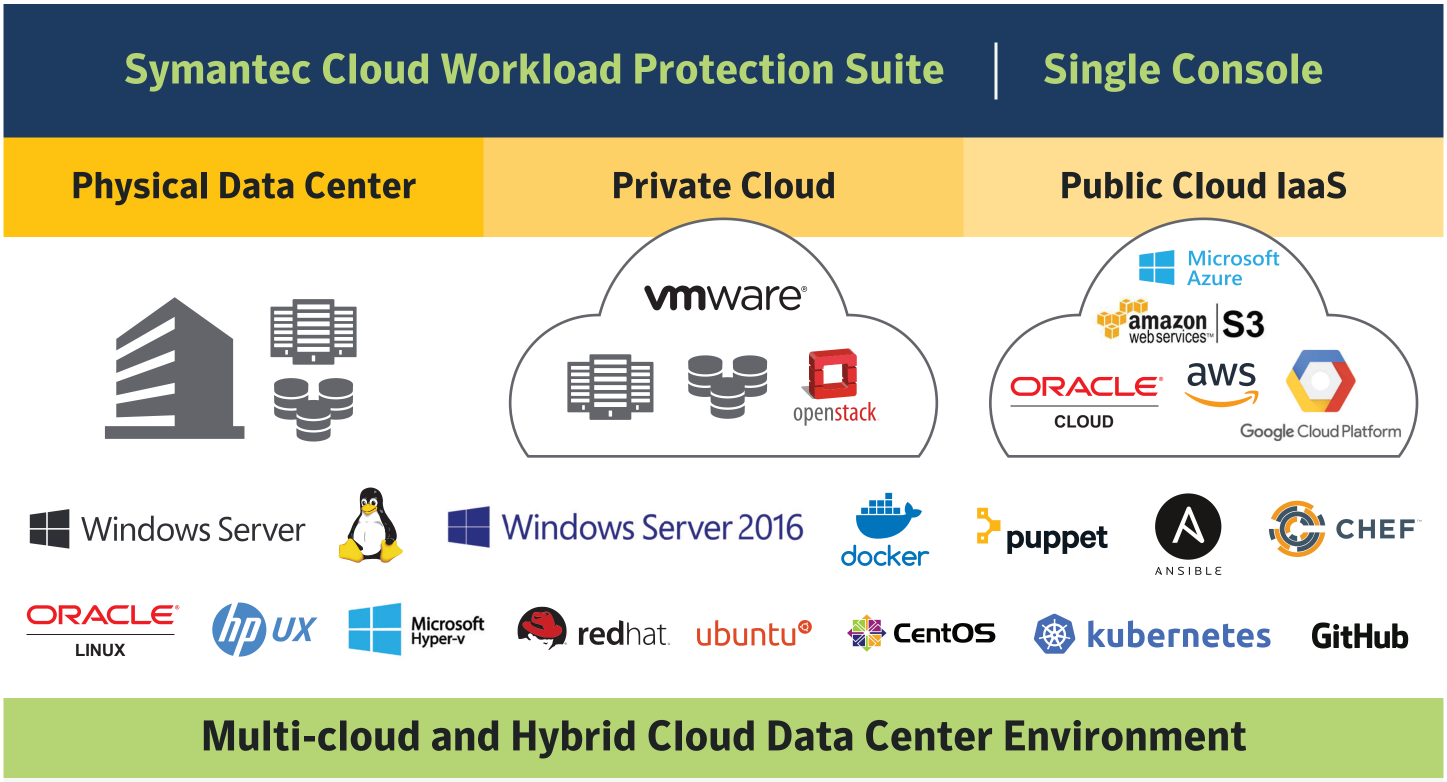
- Automatic discovery and scanning of Amazon S3 buckets
- Uses SEP anti-malware technologies including reputation analysis and advanced machine learning to remediate threats
- Alerts when S3 buckets are misconfigured or exposed to the public internet to protect against data breaches
- Apply Symantec DLP policy to data stored in Amazon S3 buckets to discover and tag sensitive information
- Data never leaves the protected environment during malware or DLP scanning
- Create custom alerts based on events and view results and security posture in a single intuitive dashboard
- Industry-first solution for in-tenant anti-malware and DLP scanning of cloud storage

Challenge: How Can I Protect Our Cloud Compute Instances?

As competition intensifies, enterprises are rapidly adopting public cloud services such as Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI) to increase business agility, relieve pressure on understaffed IT departments, and reduce costs. According to ESG, "39% of midmarket and enterprise organizations take a cloud-first approach to new application deployments, up from 29% in 2018[1]" Public cloud providers may offer security certifications for their own underlying infrastructure (up to the hypervisor level), however they require enterprises to take responsibility for securing workloads, along with any embedded vulnerabilities, against exploits and data breach attempts. Adding further complexity, most enterprises are using multiple public clouds (multi-cloud), or a combination of public cloud, private cloud, and on-premises infrastructure (hybrid cloud) to deliver applications and services to their employees and customers.

Enterprises migrating workloads to public cloud platforms quickly discover that a "lift and shift" approach to security does not work. To protect cloud workloads, security solutions must integrate with DevOps practices that are central to efficient development and deployment of applications in the cloud. Additionally, "cloud-native" API interoperability is required to ensure that security scales rapidly and responds quickly to alerts and attacks.

[1] ESG Research Report, 2019 Technology Spending Intentions Survey



Symantec Cloud Workload Protection Suite | Single Console

Physical Data Center

Private Cloud

Public Cloud IaaS

Multi-cloud and Hybrid Cloud Data Center Environment

Cloud Workload Protection Key Benefits:

- Auto-discovery, visibility, and protection of cloud workloads
- Robust security across multi-cloud and hybrid cloud environments
- Elastic, cloud-native protection from a single management console
- Industry-leading SEP anti-malware scanning

CWP for Storage Key Benefits:

- Automatic protection of Amazon S3 buckets
- Data remains protected during anti-malware and DLP scanning
- Alerts when buckets are misconfigured or publicly accessible
- Apply DLP policies and tagging to sensitive data in the cloud

aws partner network

Advanced
Technology Partner

Security Competency
SaaS Partner

Solution: Symantec Cloud Workload Protection

Symantec Cloud Workload Protection (CWP) allows enterprises to secure their critical workloads wherever they are – public clouds, private clouds, and physical on-premises data centers – all from a single centralized console. CWP automates workload security, providing discovery, visibility, and protection against advanced malware and threats. Automatic identification of workload security postures and software services, including visibility into infrastructure changes and flow logs, enables automatic policy recommendations and deployment.

CWP provides multi-layered protection for cloud compute instances including anti-malware scanning using industry-leading SEP technologies, application control and isolation to help 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. Docker containers are also supported.

Cloud-native integration with public cloud platform APIs allows CWP to both share and consume information in real-time, along with any changes to cloud infrastructure and security settings. For example, CWP consumes information from Amazon Cloud Trail, and shares information with AWS Security Hub. CWP receives the latest threat intelligence from the Symantec Global Intelligence Network (GIN).

Public cloud API integration also enables DevOps practitioners to build security directly into service deployment workflows, ensuring that applications are protected, and that security scales automatically with dynamic cloud infrastructure. Flexible pay-for-use and annual subscription pricing models support agile business planning.

The CWP cloud console can also be used to manage Symantec Data Center Security (DCS) agents on virtualized and physical on-premises servers.

Challenge: How Can I Protect Our Cloud Storage?

Many applications and services running on AWS utilize Amazon S3 buckets for storage. Over time, buckets can become contaminated with malware or misconfigured, leaving data vulnerable to breach events and corruption. Many industry regulations stipulate that sensitive information must be continuously protected wherever it is stored, even in the cloud. A solution is needed to discover and scan cloud storage for malware to prevent threats from spreading to adjacent storage, applications, or users, and to ensure that buckets are not publicly exposed or compromised.

Solution: CWP for Storage

Symantec Cloud Workload Protection for Storage helps to protect Amazon 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.

And now with DLP integration, you can apply the same DLP policies used on-premises to information stored in Amazon S3 buckets. When sensitive information is discovered, AWS tags can be applied to objects as needed for further actions in time.

CWP Features

Protect Your Hybrid Cloud Workloads from a Single Console

Auto-Discovery and Visibility

- Visibility of workloads deployed across AWS, Microsoft Azure, Oracle Cloud Infrastructure 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

- Real-time, on-demand, and scheduled scanning helps block 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
- Unparalleled protection powered by Symantec Global Intelligence Network, with 175 million endpoints secured

CWP for Storage Features

Scan Your Amazon S3 Buckets for Malware and Prevent Data Breaches

Keep Your S3 Buckets Free of Malware

- Automatic, scheduled, and on-demand scanning of Amazon S3 buckets helps to keep threats from spreading
- Discovers known and unknown threats using Symantec's antimalware suite of technologies including advanced machine learning and reputation analysis
- Helps to protect against data breaches by discovering and alerting when S3 buckets are misconfigured or exposed to the public internet

Apply DLP Policy to Your S3 Buckets

- Leverages Symantec's proven DLP technology for sensitive data detection
- Detects sensitive data and creates AWS Tags as needed for further actions in time
- Deployment for both anti-malware and DLP services is done through a single cloud formation template

Secure Data Assessment

- Anti-malware and DLP scanning occurs entirely inside of the customers VPC, ensuring that sensitive data stays secure
- Alerts when buckets are publicly accessible and allows configuration of custom alerts based on events generated

Built for the Cloud

- Scanning results, alerts, events, and intuitive dashboards are available in the single CWP cloud console
- Automatic protection of S3 buckets minimizes DevOps and administrative workloads
- Scanning infrastructure scales elastically for cost optimization

CWP Specifications

Public cloud platform support:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)

Automated policy recommendations included for:

LAMP Stack –

- OS: Amazon Linux, RedHat, CentOS, Ubuntu, Oracle Enterprise Linux
- Applications: Apache, Tomcat, PHP, Postgres SQL, MySQL, Oracle RDBMS, Docker, NGINX, MongoDB

Windows –

- OS: Win 2008 R2, 2012 R2, 2016
- Applications: IIS, SQL Server

CWP for Storage Specifications

Public cloud storage support:

- Amazon S3

Symantec Global Intelligence Network

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.

Contact an Account Manager for more information.

Connection™
we solve IT™

1.800.800.0014
www.connection.com/microsoft/azure

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.

Symantec™
350 Ellis St., Mountain View, CA 94043 USA

Copyright ©2019 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.