Symantec® on AWS

Symantec® Cloud Workload Protection: Elastic Security for AWS Workloads

Challenges

Enterprises are rapidly migrating critical workloads to Amazon Web Services (AWS) to increase business agility, reduce costs, and focus scarce resources on core initiatives instead of data center management.

While the benefits of the public cloud cannot be ignored, many businesses find that relinquishing control of sensitive assets can increase their threat exposure and the risk of an expensive data breach. Many organizations attempt to “lift and shift” traditional on-premises security solutions to the public cloud, only to discover that they do not transition or function effectively.

In many cases, this is because organizations do not recognize the need for security solutions to embrace the modern operational practices that are central to efficient cloud operations and application deployment—namely, the continuous delivery flows of DevOps practitioners.

Operating in a cloud environment also requires that you ensure workload visibility and control are not limited, and presents a need to devise effective ways to automate security agent deployment and policy enforcement

The Symantec Cloud Workload Protection Solution

Symantec Cloud Workload Protection (CWP) provides instant visibility and rapid protection for all of your public cloud workloads. This automated, elastic, cloud-delivered solution protects AWS instances, easing DevOps and administrative burdens while enabling security policy enforcement to block advanced and unknown exploits.

Cloud-native integration allows DevOps to build security directly into application deployment workflows for seamless protection. In addition, access to the Symantec Global Intelligence Network provides actionable, up-to-date information on the latest global attacks and vulnerabilities.

ASSESS

Discover, View, and Secure All Public Cloud Instances

DETECT

Insight into Advanced Threats and Vulnerabilities

BLOCK

Protection that Scales Automatically in Dynamic Environments

Key Benefits

AUTOMATIC DISCOVERY AND VISIBILITY

Discover and map the blind spots in your cloud environment:

- Continuous visibility of workloads across AWS regions
- Automatic discovery of software services on workloads
- Automatic identification of workload security postures
- Real-time visibility into infrastructure changes

ROBUST SECURITY ACROSS CLOUD REGIONS

Protect workloads against advanced attacks and zero-day threats:

- Unique application isolation blocks exploits targeting known and unknown vulnerabilities
- OS hardening stops zero-day threats
- Real-time file integrity monitoring (RT-FIM) prevents unauthorized changes

ELASTIC, CLOUD-NATIVE PROTECTION

Cloud workloads can rapidly scale up or down. CWP scales automatically with dynamic cloud infrastructures and provides:

- Context sensitive security recommendations
- Flexible cloud-ready pricing
- Security that expands when capacity spikes, and scales back when workloads are retired

CustomerOne on CWP

Through their CustomerOne program, Symantec uses Cloud Workload Protection (CWP) to secure customer utilization of AWS-delivered products and services. Cloud Workload Protection provides automatic discovery, visibility, and security for all Symantec workloads in AWS, enabling developers to be as productive as possible while adhering to strict security policies.

Symantec on AWS

Whether “all-in” on the AWS Cloud, or preferring a hybrid data center approach, Symantec Cloud Workload Protection provides discovery, visibility, and advanced threat protection for your AWS workloads, wherever they are, allowing you to focus on what matters most - your business.

Getting Started

Learn more about how Cloud Workload Protection can keep your AWS cloud environment safe today:

Symantec Cloud Workload Protection on AWS

Last Updated: May 2017