Symantec Cloud Workload Protection

on Amazon Web Services

INTRODUCTION

Each year, an increasing number of organizations choose to migrate to the cloud for many reasons. Among the most common are increased business agility, automation of repetitive, manual tasks, and the opportunity to reduce costs. Cloud adoption also presents the need to recognize security as a shared responsibility between the organization choosing to migrate and the cloud services provider.

Organizations face challenges when formulating and implementing a security strategy for their cloud environment, and, in many cases, the inability to devise a secure, effective solution presents a barrier to cloud migration. The fact that traditional, security strategies and practices (the ones employed in on-premises data centers) do not transition well to the cloud is one of the more common challenges organizations must overcome, but additional issues often arise once companies have begun the migration process and cloud operations.

Lack of visibility into the entire cloud environment presents numerous problems for Chief Information Security Officers and Security Analysts, who require a solution that will make it easy for them to discover everything that is running on their cloud, and a method to ensure that what is running is secure. In short, they need clear visibility into workload security posture and status, along with monitoring and logging capabilities. Moving to the cloud also sees many organizations begin to employ DevOps practices, with continuous application deployment workflows being one of the core tenets.

As a result, organizations moving to the cloud must find a security solution that provides them complete visibility of workloads across their entire environment, and automatically identifies and controls unauthorized and unknown workloads and applications. Cloud security solutions must also be elastic to properly function within the dynamic cloud infrastructure, while mitigating the risks associated with cloud adoption.

This eBook presents some of the details, features, and benefits of the automated Symantec Cloud Workload Protection (CWP) security solution on Amazon Web Services (AWS).

SYMANTEC CLOUD WORKLOAD PROTECTION ON AMAZON WEB SERVICES

Optimized for use on AWS, **CWP can help your organization securely migrate your legacy applications to the cloud, deploy new cloud-native applications and services, and augment your on-premises data center requirements** with AWS to reliably enhance your hybrid cloud infrastructure. Applications utilized on the cloud are dynamic and automated, and they require a flexible, modern security solution.

INCREASE VISIBILITY

You can't protect what you can't see. CWP provides instant visibility and rapid protection for all of your AWS 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 INTEGRATION

Cloud-native integration allows DevOps to build security directly into application deployment workflows for seamless protection. With CWP, you are able to discover, view, and secure all AWS workloads and instances, and gain insights into emerging advanced threats and vulnerabilities with protection that scales automatically in the dynamic AWS Cloud.

AUTOMATED DISCOVERY

CWP's automatic discovery of software services on your AWS workloads, combined with the continuous visibility into your entire cloud environment, makes it easy for you to find and map the blind spots that exist in your cloud environment. These capabilities, along with the automated identification of workload security postures and real-time visibility into infrastructure changes, help to ensure your AWS environment remains secure.

ELASTIC, SCALABLE, CLOUD SECURITY

The elastic, cloud-native protection that CWP delivers enables automated scalability with your cloud workloads and infrastructure by providing context sensitive security recommendations, as well as a solution that expands when capacity spikes and scales back when workloads are reduced or retired. A library of pre-configured security policies are available for a wide range of workload types, and support for Docker ensures that container deployments remain secure.

PROTECT YOUR ENTIRE AWS ENVIRONMENT

The robust security that CWP offers is available across all of the AWS regions your cloud environment may extend to, protecting your workloads against zero-day threats and cyberattacks with a unique application isolation capability that blocks attempts to exploit both known and unknown vulnerabilities. CWP also delivers OS hardening and real-time file integrity monitoring (RT-FIM) to prevent unauthorized changes throughout your AWS Cloud presence.

PROTECT HYBRID CLOUD WORKLOADS

CWP delivers additional value by providing the capability to manage workload security across your entire hybrid cloud from a single console. Now you can manage your on-premises Symantec Data Center Security (DCS) assets from the CWP console. Simply import your existing DCS security policies into CWP to manage your DCS-protected physical or virtual servers from the cloud. The ability to manage security of all hybrid cloud workloads enables you to maintain security while simplifying your transition to AWS.

SYMANTEC GLOBAL INTELLIGENCE NETWORK

In addition, CWP also accesses the Symantec Global Intelligence Network (GIN) to provide actionable, up-to-date information on the latest global attacks and vulnerabilities. GIN is based on information gathered from Symantec customers worldwide, and categorizes and analyzes threats posed by previously unseen and uncategorized websites, as well as emails sent and received by Symantec customers.

CWP ON AWS: PROTECTION IN PARTNERSHIP

CWP on AWS is the result of a partnership that blends Symantec's knowledge, with the breadth and depth of AWS services, and presents a unique opportunity for your organization to secure your cloud environment. Symantec is an AWS Advanced Technology Partner.

CWP IS AVAILABLE ON AWS IN TWO PRICING MODELS

HOURLY

Metered pricing allows your organization to pay only for the CWP security it uses, and you are invoiced for your hourly usage on a monthly basis. Payment in arrears allows security to be scaled out so you can keep pace with dynamic business demands.

ANNUALLY

You also have the option to reduce monthly costs by purchasing an annual subscription for CWP, in effect prepaying for pre-determined usage. One annual subscription provides protection for one instance for one year, with any overages billed in arrears.

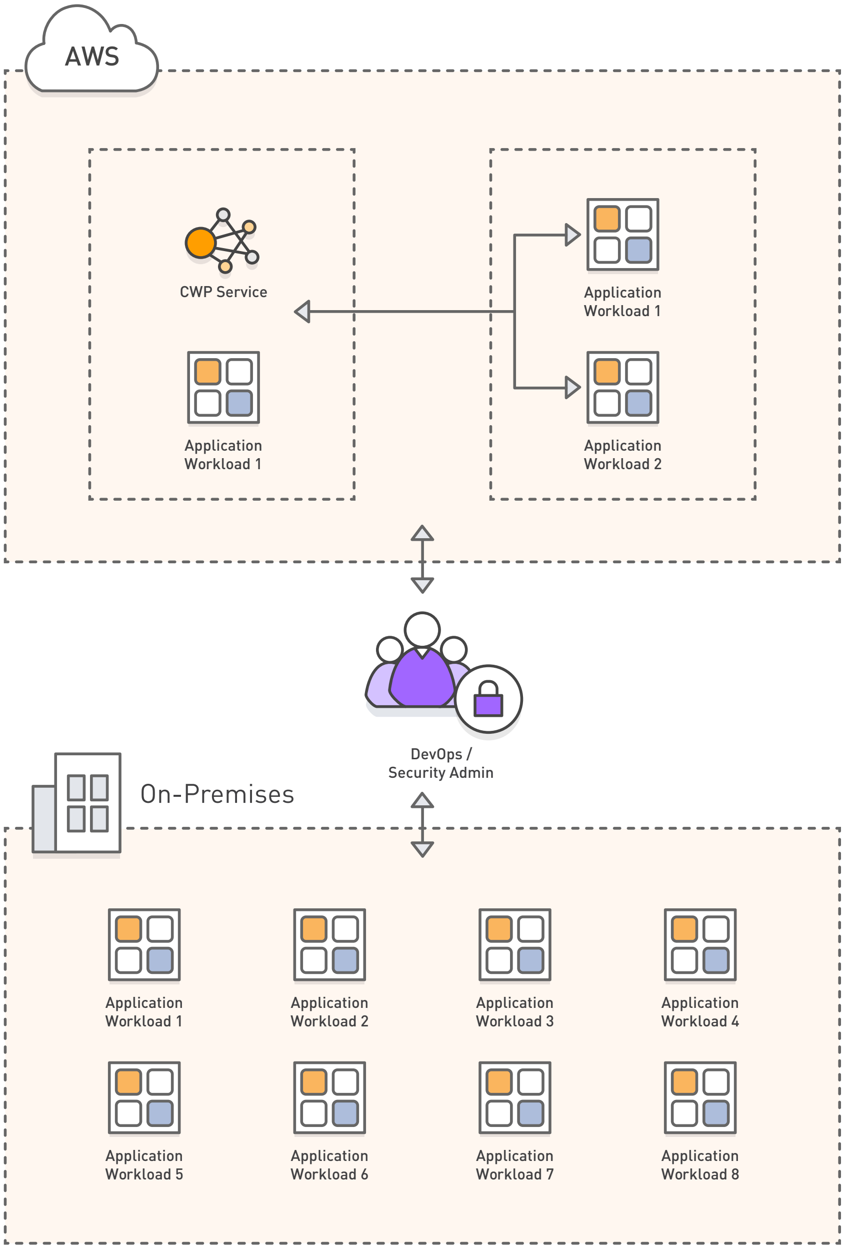
SYMANTEC CLOUD WORKLOAD PROTECTION DIAGRAM

CWP ON AWS PROVIDES:

Protection of all workloads from a single cloud-based console

Automatic discovery and visibility of public workloads

Elastic, cloud-native protection that scales seamlessly



USE CASES

SECURE CLOUD MIGRATION

GAIN VISIBILITY TO MORE RAPIDLY IDENTIFY THREATS

SECURE CLOUD AND ON-PREMISES ENVIRONMENTS WITH CWP

CHALLENGE

Transitioning your existing security products and strategies from your on-premises data center to the AWS Cloud.

Limited visibility and control of your AWS workloads.

Automated security agent deployment and policy enforcement.

SOLUTION

CWP delivers constant monitoring and protection of your AWS environment against zero-day threats and the exploitation of vulnerabilities. The unique isolation of applications targets both known and unknown vulnerabilities to block attempts at said exploitation. In addition, OS hardening in CWP protects you from zero-day threats on AWS, while real-time file integrity monitoring prevents unauthorized changes.

You need to know what your organization is running on AWS, and the automatic discovery and visibility of your AWS workloads that CWP delivers helps to quickly find and view software services on workloads across all of the AWS regions you operate in. CWP also instantly and automatically identifies AWS workload security postures, providing real-time visibility into infrastructure changes and the ability to shut down rogue instances to reduce your potential attack surface.

Your AWS environment needs security that integrates natively with AWS APIs. CWP provides cloud-native security that scales automatically with your dynamic AWS cloud infrastructure, while enabling DevOps to build security directly into service deployment workflows.

CUSTOMER CASE: LIFELOCK

LIFELOCK, an identity theft protection company, decided to migrate their on-premises workloads to AWS and needed a solution that provides the same enterprise-class security and monitoring that their identity protection customers have come to expect. In addition, LifeLock required a solution that provides the flexibility and scalability that allows their DevOps teams to maintain their continuous workflow and development practices without having to worry about manual configuration or deployment of security.

LifeLock chose CWP to secure their AWS environment because it automated their security, enabling continuous monitoring and protection of all cloud workloads. CWP provides rapid discovery, visibility, and strong protection that blocks both known and unknown exploits to derail advanced attacks that could potentially disrupt LifeLock operations or exfiltrate customer data.

CWP's cloud-native integration with AWS APIs allows LifeLock's DevOps team to build security directly into application deployment workflows for elastic protection that scales seamlessly with their growing business. A single cloud-based console simplifies management and security policy deployment, reducing LifeLock's administrative burdens and overhead, while allowing them to take advantage of the breadth and depth of AWS services.

AWS Cloud networks can be built and configured on demand by any developer. This is a big transformation from traditional data center operation. LifeLock needed to ensure that network controls are properly applied, and that workloads are appropriately isolated from one another. Additionally, LifeLock needed automatic enforcement of security policies on new servers so they weren't left exposed. CWP was developed to automate security on cloud workloads, and applies it seamlessly so that LifeLock developers can continue their work at maximum efficiency.

GET STARTED

Whether your organization is “all-in” on the AWS Cloud, or is using 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. By extending the proven expertise of Symantec CWP to your organization’s AWS-based workloads and instances, you will realize the benefit of knowing that your customer and corporate data is protected.

Built to integrate natively with AWS infrastructure as a service (IaaS) environments, Symantec Cloud Workload Protection solves the biggest problem preventing companies from trusting security of workloads to the cloud. By automating security for AWS workloads, CWP provides an easy and cost-effective way for your organization to secure mission critical applications and instances, unlocking all of the benefits of cloud adoption.

To learn more about CWP on AWS, contact Symantec or your AWS Sales Representative.

AWS SERVICES USED BY CWP

TO RUN SYMANTEC CWP ON AWS:

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon CloudWatch

AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

AWS CloudFormation Templates

AWS Identity and Access Management (AWS IAM)

Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Queue (Amazon SQS)

TO ENHANCE THE CAPABILITIES OF SYMANTEC CWP ON AWS:

Amazon Route 53

AWS Elastic Load Balancer

ElastiCache

AWS Lambda

Amazon Kinesis

AWS Key Management Service (AWS KMS)

ADDITIONAL RESOURCES:

AWS Featured Partner

Symantec in AWS Marketplace

About Symantec on AWS

Symantec Cloud Workload Protection

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 or connect with us on Facebook, Twitter, and LinkedIn.

ABOUT AMAZON WEB SERVICES

For 10 years, Amazon Web Services (AWS)

has been the world's most comprehensive and broadly adopted cloud platform. AWS offers more than 90 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world monthly — including the fastest growing startups, largest enterprises, and leading government agencies — to power their infrastructure, make them more agile, and lower costs.

To learn more about AWS, visit aws.amazon.com