Solution Brief

Symantec Cloud Workload Protection

Secure Your Public Cloud Deployments and Reduce Risk

Executive Summary

Organizations are rapidly adopting public cloud services such as Amazon Web Services (AWS) and Azure to increase business agility, relieve pressure on understaffed IT departments, and save money. The benefits of the public cloud can no longer be ignored as competitive pressures accelerate mainstream business adoption – in fact, while only about 25% of companies in 2015 used public Infrastructure-as-a-Service (IaaS) as the primary environment for at least one workload, that percentage is expected to rise to 37% in 2018[1]. However, relinquishing control over sensitive data can put companies at risk of failing a data security compliance audit, or worse, suffering the consequences of a data breach. For this reason, security concerns and increased risk remain the leading barriers to public cloud adoption.

For their part, public cloud providers generally guarantee security of their own underlying infrastructure, but will not guarantee security of customer data or protection against threats. This is known as the "shared responsibility" model. Companies attempting to "lift and shift" traditional data center security models to the public cloud soon discover that this can be a difficult and ineffective approach as cloud providers typically use proprietary infrastructure and orchestration tools. Clearly, if businesses are to continue to benefit from public cloud adoption, a simple and cost-effective way for enterprises to secure workloads and reduce risk is needed.

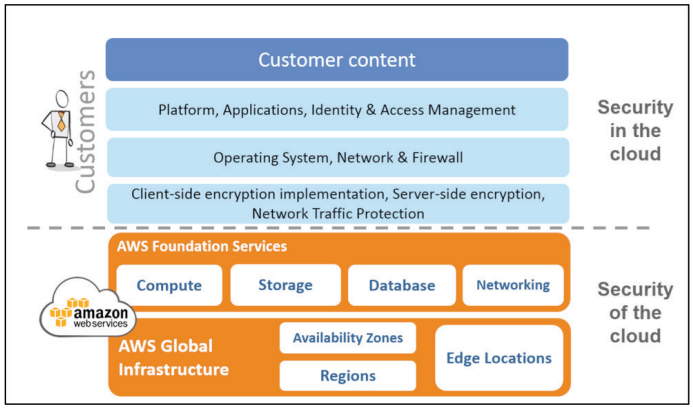

Figure 1: AWS Shared Responsibility Model

Introducing Symantec Cloud Workload Protection

Symantec Cloud Workload Protection (CWP) automates security for public cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and administrative burdens. Rapid discovery, visibility, and elastic protection of AWS and Azure workloads enable automated security policy enforcement to protect applications from unknown exploits.

Cloud-native integration allows DevOps to build security directly into application deployment workflows, while support for Chef and Puppet automates configuration, provisioning, and patching. Access to the Symantec Global Intelligence Network protects workloads against the latest global attacks and vulnerabilities, providing peace of mind for large enterprises and born-in-the-cloud businesses.

1. * McKinsey IT-as-a-Service (ITaaS) Cloud and Enterprise Cloud Infrastructure Survey, Sept. 2016

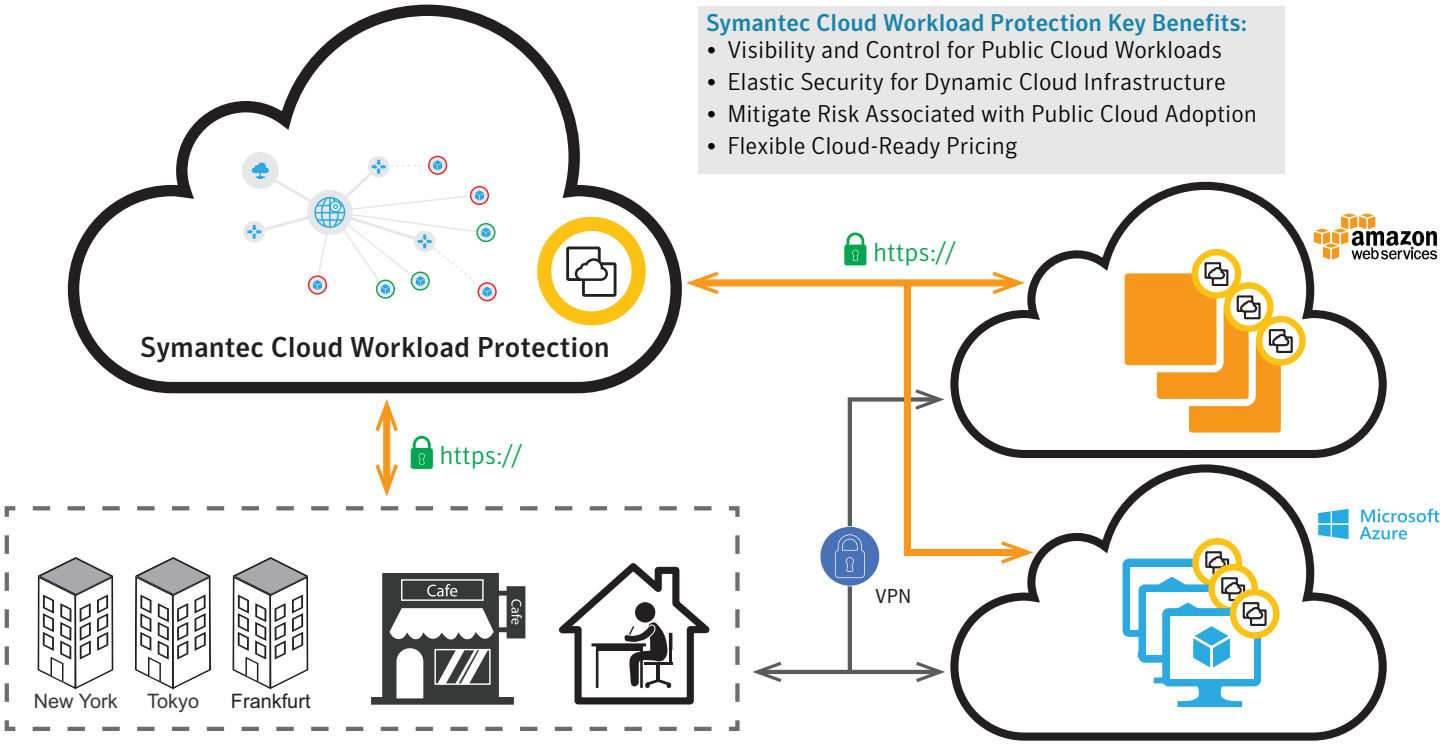

Figure 2: Automate Security for AWS and Azure Public Cloud Workloads

Visibility and Control for Public Cloud Workloads

You can't protect what you can't see. Unauthorized use of public cloud resources is a big challenge for organizations subject to strict data privacy rules, or concerned about leakage of sensitive information. Companies need an easy way to discover and control risky behavior, such as employees accidentally sharing intellectual property via "rogue" cloud-based applications, or DevOps running unprotected workloads on public cloud infrastructure.

Symantec Cloud Workload Protection automatically discovers and inventories all workloads running on AWS and Microsoft Azure public cloud platforms. Workloads are further profiled and categorized according to security risk; for example, do virtual instances have CWP agents installed? Have the right security policies been applied to them? Have workloads been attacked or compromised? All workloads and their security status are then displayed in a simple visual topology map. This makes it easy to see exactly where workloads are running, whether or not they are secure, and even apply corrective actions – all from a single pane-of-glass. CWP provides the following visibility and control features:

- Discovery of noncompliant or rogue workloads and servers
- Accurate compute, software inventory, and networking topology visualization across multiple public cloud service providers
- Security status and level of protection on every public cloud workload
- Continuous visibility into threat and vulnerability scores for public cloud deployments
- Visual topology map of all workloads and servers including security status and alerts on potential attacks
- View of AWS region, virtual private cloud, subnet, auto-scaling groups, security groups, and more

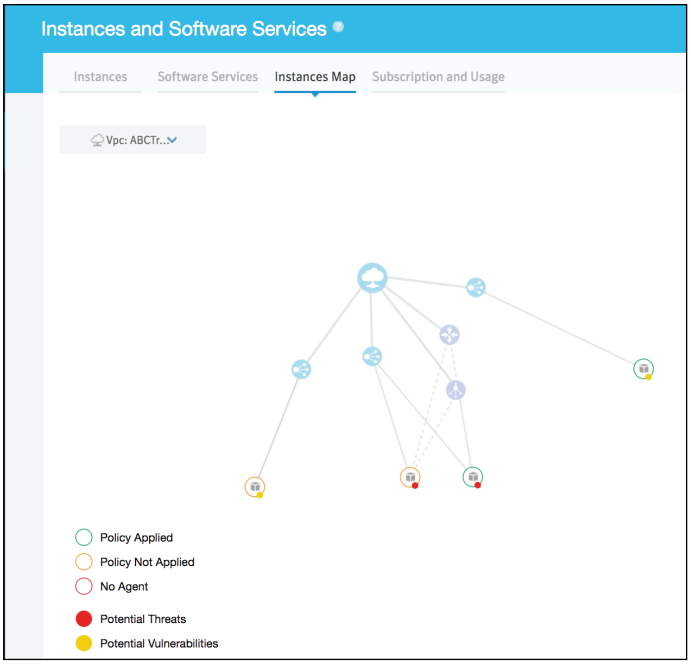

Figure 3: Discover, View, and Secure All Public Cloud Instances

Elastic Security for Dynamic Workloads

The shared responsibility model essentially shifts security responsibilities from public cloud providers to public cloud customers. Symantec Cloud Workload Protection provides an easy way for organizations to benefit from the public cloud while maintaining security and retaining audit controls. CWP is built from the ground up as a public cloud-native solution, leveraging years of Symantec server and virtual workload protection know-how. CWP provides the following security features:

- Cloud-native integration enables security that deploys and scales automatically with workloads based on intelligent and customizable rule sets
- Best-in-class segmentation of workload resources provides blocking at all stages of the attack chain
- Application isolation controls access to file, process, and network activities to lock down applications, operating systems, and configuration data
- Real-time file integrity and user activity monitoring can be configured to detect or actively prevent unauthorized activities and potential breach attempts
- Recommendation engine that continuously monitors for trigger points indicating recompilation of the protection services in place
- Out-of-the-box automated policy recommendations for LAMP Stack, Windows, and Oracle-based public cloud platforms

CWP automatically applies security and monitoring policies to all new workloads as they are spun up or spun down, for example in response to "bursting" or auto-scale events. Additionally, tight integration with AWS and Azure application programming interfaces (APIs) enables DevOps and SecDevOps to template security controls into application deployment workflows, delivering automatic workload protection.

Mitigate Risk Associated with Public Cloud Adoption

Enterprises are concerned that public cloud adoption might increase their risk of doing business. Therefore, increased risk, both real and perceived, remains the primary barrier to public cloud adoption. Fortunately, risk can be sufficiently mitigated by deploying strong security and monitoring controls along with sensitive public cloud workloads. CWP enables enterprises moving to the cloud, as well as "all-in-the-cloud" businesses to enjoy the cost savings and operational benefits of public cloud adoption. CWP provides the following features that help to mitigate risks associated with the public cloud:

- Context-aware workload monitoring enables recommendations for protection, and detects any changes that violate the specified security policies
- Intelligence from the Symantec Global Intelligence Network enables rapid response to both known and unknown threats and vulnerabilities based on installed software
- Click-through usability allows policies to be updated and applied from a single pane-of-glass to prevent known and unknown exploits
- Real-time monitoring of alerts and events provides security, SecDevOps, and audit teams with assurance that security controls are effective

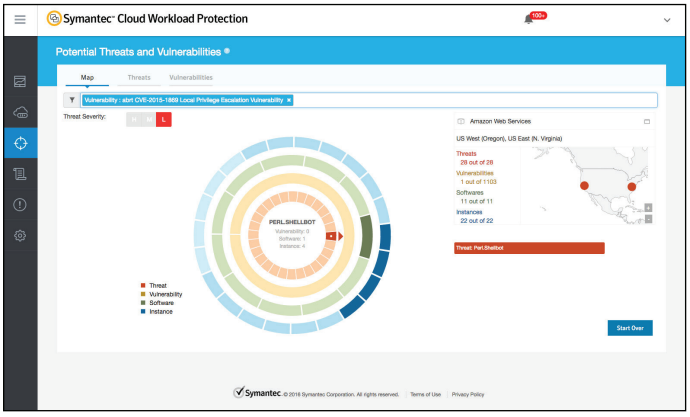

Figure 4: Understand and Control Public Cloud Risks

Symantec Global Intelligence Network

Symantec Cloud Workload Protection taps into the Symantec Global Intelligence Network, one of the world's premier civilian cyber defense threat intelligence services. The network continuously ingests threat information from more than 15,000 enterprises, 175 million consumer and enterprise endpoints, and 3,000 threat researchers and engineers. It also categorizes and analyzes threats posed daily by more than 1 billion previously unseen and uncategorized websites, and more than 2 billion emails sent and received by our customers. As a Symantec customer, you will benefit from the network effect of joining 90 percent of Fortune 500 companies. Symantec's security expertise minimizes false positives while giving you access to the world's most powerful analytical threat engine to keep you ahead of today's and tomorrow's fast-changing security threats. CWP uses Symantec DeepSight™ DataFeeds to provide actionable intelligence about malicious activity sources, emerging threats, and vulnerabilities on your public cloud deployments. Symantec DeepSight DataFeeds are derived from deep, proprietary analysis of billions of events from the Symantec Global Intelligence Network.

Flexible Cloud-Ready Pricing

Symantec Cloud Workload Protection offers two pricing models for flexible cost control:

Hourly

Metered pricing allows enterprises to pay only for the security they use:

- Customers are invoiced monthly and for hourly usage
- Payment in arrears enables scale-out security to keep pace with dynamic business demands

Annual Subscription

Customers can reduce monthly costs by purchasing an annual subscription to prepay for pre-determined usage:

- One annual subscription entitles Customer to protection of one (1) unnamed server for one (1) year
- Any overages are billed in arrears

Also, three service size options; small, medium, and large, are available to protect all sizes of public cloud application deployments - from website hosting to big data processing:

SUBSCRIPTION TYPE	SERVICE SIZE	CORES PER INSTANCE
Hourly	Large	4 or more
	Medium	2
	Small	1
Annual	Large	4 or more
	Medium	2
	Small	1

Figure 5: CWP Sizing

Symantec Cloud Workload Protection Unlocks Public Cloud Benefits for Business

From the advent of microprocessors, to the Internet, to mobile communications, and now cloud computing, major developments in technology continue to have a profound impact on business planning and operations. Ultimately, the pace of adoption of these new technologies can determine whether businesses thrive or eventually fall by the wayside. New technologies create opportunities to achieve disruptive advantages, and the public cloud is no exception, offering advantages that many companies can no longer ignore.

Every major technology shift presents major challenges in implementation and security. Companies that solve these problems first stand to benefit additionally from early mover advantages. Public cloud platform providers such as AWS and Microsoft Azure have largely solved implementation problems by offering cloud-compute resources as readily consumable, pay-as-you-go services. However, the shared responsibility model and lack of cloud-native solutions still present barriers to solving the public cloud security challenge.

Built to integrate natively with AWS and Azure IaaS environments, Symantec Cloud Workload Protection solves the biggest problem preventing companies from trusting security of workloads to the public cloud. By automating security for public cloud workloads, CWP provides an easy and cost-effective way for enterprises to secure mission critical applications and workloads, unlocking all of the benefits of public cloud adoption.

To learn more about Symantec Cloud Workload Protection, please visit us at **www.symantec.com**.

About Symantec

Symantec Corporation World Headquarters
350 Ellis Street Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com