Solution Showcase

Securing Hybrid Clouds with Symantec Cloud Workload Protection

Date: March 2018 **Author:** Doug Cahill, Senior Analyst

Abstract: The broad adoption of cloud services is changing the fundamental complexion of the data center, requiring new methodologies of operation that are equally impactful. For most, the transition to the cloud is driven by a business need for greater agility, resulting in a hybrid IT approach to managing hybrid clouds. The rate at which public cloud services are being adopted has created a gap between the extent to which organizations use infrastructure-as-a-service (IaaS) for business-critical applications and the readiness to secure these environments. Fundamental differences in cloud infrastructure and the shift to DevOps methodologies to manage it creates a need to first understand what is different about the cloud. Public cloud infrastructure also presents an opportunity for cyber adversaries by creating multiple vectors via which malware can be introduced. Symantec's Cloud Workload Protection (CWP) and Cloud Workload Protection for Storage are cloud-delivered solutions that protect both cloud-resident and on-premises workloads as well as cloud-resident object stores from compromise with an operationally efficient implementation.

Cloud Security Foundations

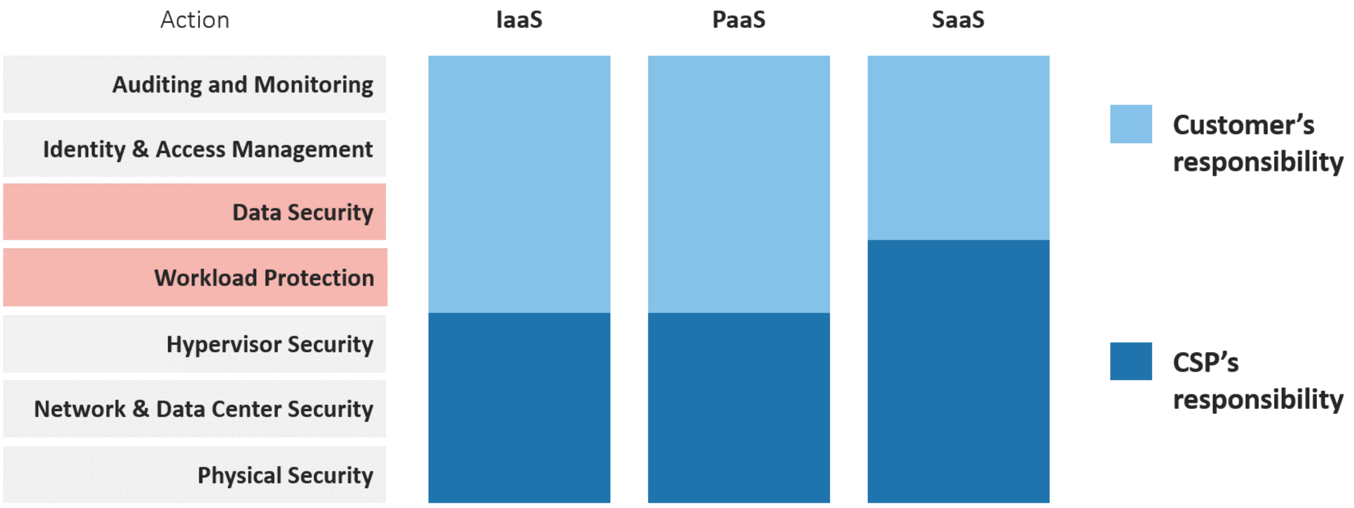
The broad adoption of cloud services, including SaaS applications and infrastructure platform services, is resulting in more business-critical assets being cloud-delivered and cloud-resident, creating, for many organizations, a cloud security imperative. Further complicating securing the use of public cloud services is the use of multiple clouds. According to research conducted by ESG, 81% of organizations using public cloud infrastructure services are doing so by subscribing to services from more than one cloud service providers (CSP).[1] Effectively securing a hybrid cloud environment comprised of multiple cloud services and customer managed infrastructure requires an understanding of cloud security foundations.

Cloud Security Is a Shared Responsibility

For many organizations, securing their transition to the cloud starts by grounding a strategy to do so in an understanding of the shared responsibility model that depicts the division of security responsibility between the customer and the cloud service provider (see Figure 1).

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Figure 1. Shared Responsibility Security Model



Source: Enterprise Strategy Group

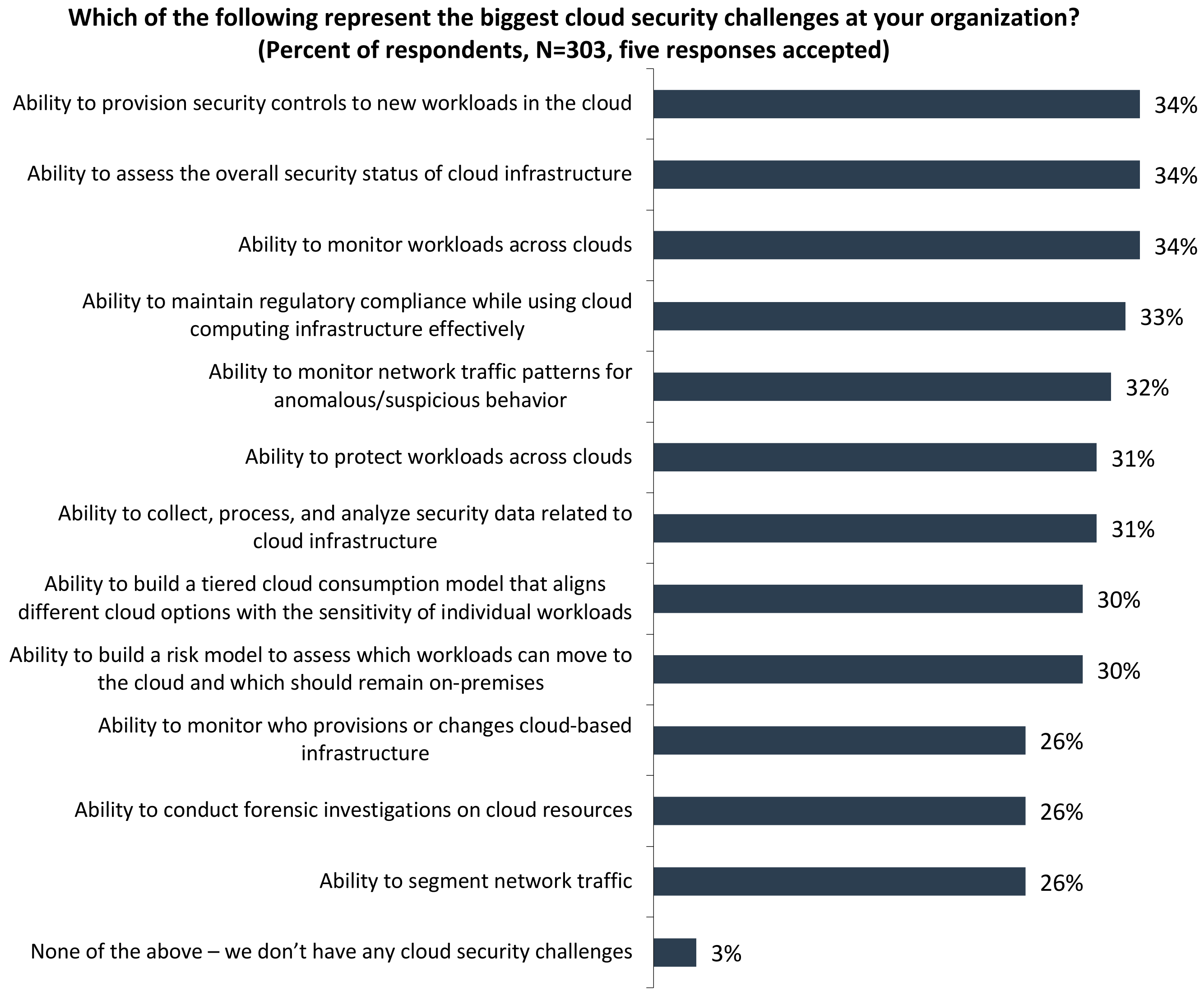
While the CSP is responsible for securing physical access to data centers, to the network, and up to the hypervisors hosting virtual machines, customers are responsible for securing their application workloads and cloud-resident data assets. Major CSPs meet and maintain compliance with a variety of industry regulations and certifications, including PCI-DSS and SOX, but customers still need to apply policies, processes, and controls to address their own compliance requirements.

Hybrid Clouds Have Physical and Virtual Perimeters

While perimeter defenses still play an important role in hybrid clouds, those same controls in a physical form factor cannot be applied in the public cloud due to the lack of physical access to the network layer. DMZs and firewalls still define the physical element of the on-premises side of a hybrid cloud, while workloads and configuration settings that govern access to object stores and other cloud services are the virtual perimeters of the public cloud portion of hybrid environments. As a result, the biggest cloud security challenges cited by participants in ESG research are indicative of the challenges of maintaining a consistent security posture across the disparate elements of hybrid clouds (see Figure 2).[2]

[2] Source: ESG Research Report, *The State of Cloud Security in the Enterprise,* October 2016.

Figure 2. Biggest Cloud Security Challenges



Source: Enterprise Strategy Group

Temporal Instances

The fact that cloud workloads in an auto-scaling group are temporal in that they are provisioned and de-provisioned automatically based on the compute needs of the application further contributes to an amorphous network perimeter. Cloud-resident workloads have other attributes that differ from their on-premises virtualized and bare-metal server brethren, including the use of server tags and instance IDs instead of names and IP addresses as naming conventions.

Immutable Infrastructure

Cloud workloads are often described as representing a form of immutable infrastructure since production servers are not updated, but rather replaced with workloads of a new configuration via automated cutover processes that do not interrupt application availability. Such an approach has security implications for how vulnerabilities are patched and configuration holes closed.

The Speed of DevOps

The cloud is more than a technology paradigm shift; it is also a change in how infrastructure is managed. While the DevOps methodology of automating the continuous testing, integration, and delivery of workloads and other cloud services addresses the agility demands of the business, the speed inherent in doing so can seem antithetical to security.

New Vectors and Targets for Malware Infections

The expansion of the attack surface creates a set of vectors and targets that organizations need to protect. Threats include malware that will attempt to move laterally to cloud-resident assets, necessitating the need for anti-malware protection for workloads, containers, and object stores. Vectors via which adversaries can introduce malware include:

- Workload instances and containers with software and/or configuration vulnerabilities.
- DevOps CI/CD automation and orchestration tools representing an insertion point.
- Business-to-consumer applications, which are often hosted on public cloud platforms and exposed to a range of users.
- Serverless (e.g., AWS Lambda) function calls, which could facilitate lateral movement.

ESG research reveals that organizations are aware of the threat that malware poses to their cloud-resident footprint, with 33% of respondents selecting malware prevention as one of the security controls for which their organization's spending has increased, or is expected to increase, specifically due to their use of public cloud infrastructure, making it the most-cited response.[3]

Essential Hybrid Cloud Security Best Practices

Securing these dimensions of public cloud infrastructure platforms, along with existing on-premises servers that together comprise hybrid cloud environments, requires a solution that enables the implementation of the following visibility and control best practices.

Gain Horizontal Visibility to Reduce the Attack Surface Area

The dimensions of the attack surface in a hybrid cloud include server types and infrastructure platforms comprised of virtual machine instances, object stores, application containers, bare metal servers, and a heterogeneous mix of operating systems. As such, a hybrid cloud security solution must be able to discover and secure any combination thereof across multiple IaaS platforms, private clouds, and data centers. Comprehensive platform coverage enables gaining centralized visibility of vulnerabilities that should be discovered and remediated in test environments before deployment to production. Vulnerabilities in this context include both software—operating system and application—and the configurations of server workloads and object stores, including access control settings.

Implement Integrity Monitoring and Controls

After gaining visibility into the attack surface area and reducing it by addressing vulnerabilities, organizations should seek to enforce steady-state workload configurations and detect any deviations that could be indicative of an intrusion. Because immutable infrastructure is just that, unchanging, production workloads should be monitored for unauthorized changes that may be indicative of a compromise.

[3] ESG Research, *Trends in Hybrid Cloud Security: Minding the Gap*, November 2018.

Detect and Prevent Threats Across Cloud Services and On-Premises Servers

Threat detection across a hybrid cloud is also a multidimensional concept. Threat types include exploits that will take advantage of vulnerabilities and malware that may be resident in an object store, on a server-attached file system, or attempting to move laterally. As such, multiple technologies need to be applied across the assets of a hybrid cloud, including intrusion detection and prevention (IDS/IPS) and anti-malware controls. Anti-malware engines should employ a variety of detection technologies to prevent known and unknown file and file-less malware before and during execution.

Employ Host-based Firewalls and Monitor Network Traffic

To protect against inbound threats such as distributed-denial-of-service (DDoS) attacks and to detect nefarious outbound communications, including those to a remote command-and-control server, a workload-centric approach requires implementing host-based firewall rules to govern inter-workload network traffic. Such rules help protect applications comprised of workloads that span the cloud and on-premises infrastructure and ensure that when a jump or bastion host is in use, other workloads are not externally facing and subject to port scanning.

Leverage a DevSecOps Approach to Automate Security

The automation of infrastructure via the continuous integration and continuous delivery (CI/CD) of code is an opportunity to integrate security controls and apply best practices further upstream in the application delivery process. To do so, infrastructure managers should apply security controls via script-level integration with their CI/CD tools and leverage workload tags so that the right policy is automatically assigned at instantiation, enabling the DevSecOps use cases such as discovering vulnerabilities in test and applying preventative controls in production.

Gain Operational Efficiencies from a Cloud-native Implementation

Security-as-a-service as a form of software-as-a-service provides appreciable benefits, including eliminating the need to deploy and manage on-premises management servers, enabling these services to automatically scale as the organization's use of cloud services scales up and down, and providing a centralized control plane across disparate environments. Cloud-delivered security services will also align the economic model of security with the cloud services it protects with similar metered, usage-based pricing.

Introducing Symantec Cloud Workload Protection (CWP) and Cloud Workload Protection for Storage

Symantec Cloud Workload Protection (CWP) and CWP for Storage, available separately or as a bundle, enable the implementation of these best practices to protect object stores and workloads deployed across hybrid clouds against compromise via the following capabilities:

Centralized Management via Coverage Across the Dimensions of Hybrid Clouds

Symantec Cloud Workload Protection supports a range of operating systems running on virtual machines, bare metal servers, and containers deployed on-premises, in private clouds, and in public cloud infrastructure platforms including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Symantec's Cloud Bridge connector allows customers to import security policies from Symantec's Data Center Security (DCS) server security product into CWP for the centralized definition and application of security policies across heterogeneous hybrid clouds.

Visibility via Discovery and Visualization

CWP discovers public cloud workloads, including containers, and presents them visually in a topological mapping so customers can understand the relationship between workloads. Tags are read to identify a workload's role and location so that the topological rendering can be employed to visualize the following:

- The region in which a workload is located.
- Membership in virtual private clouds (VPCs), type of subnets (public vs. private), and auto-scaling groups.

CWP for Storage extends visibility into AWS S3 storage buckets by discovering S3 buckets associated with AWS account(s), enabling the ability to securely scan for malware and identify misconfigured and publicly exposed S3 buckets as discussed below.

Contextual Configuration and Software Vulnerability and Exploit Detection and Remediation Across Cloud Services

With an inventory of operating systems and applications in hand from the discovery phase, Cloud Workload Protection correlates the Common Platform Enumeration (CPE) and Common Vulnerabilities and Exposures (CVE) dictionaries to determine whether known vulnerabilities exist in current workload stacks. CWP also references Symantec's Global Intelligence Network and DeepSight threat intelligence services to determine whether known exploits for discovered vulnerabilities put these workloads at risk, enabling customers to remediate as needed.

Because weak configuration settings also create vulnerabilities, CWP for Storage assesses AWS S3 access control settings and alerts on those S3 buckets whose settings leave them open to public access and thus at risk of data loss. CWP for Storage can also be configured to generate events to identify public objects in non-public buckets.

Malware Detection and Prevention

Both CWP and CWP for Storage employ the latest anti-malware engine from the Symantec Endpoint Protection (SEP) platform to detect and prevent new and unknown file and file-less malware. Both CWP products protect against known malware based on reputation, unknown malware via multiple techniques including machine learning, and file-less malware by analyzing the behavior of an attack chain. CWP for Storage scans selected areas of S3 buckets for objects that may include embedded malicious software. These scans are performed within a customer's virtual private cloud (VPC), ensuring that customer data does not leave their data center. CWP and CWP for Storage both offer remediation capabilities that can be triggered upon the detection of malware including, for example, quarantining such malicious files and objects.

Workload Lockdown via Integrity Control and Monitoring

The isolation of authorized applications restricts which system resources those applications are allowed to access, including authorized areas of the file systems. CWP provides prebuilt policies referencing Center for Internet Security (CIS) benchmarks for the "known good" configurations of common operating system and application stacks. This approach to workload lockdown to prevent unauthorized change is augmented by file integrity monitoring (FIM) and user activity monitoring to support both security and compliance use cases.

Inter-workload Network Controls and Monitoring via Host-based Firewall Rules

CWP provides a policy lexicon to control inter-server workloads communication across hybrid clouds, eliminating the need to rely on disparate host-based firewalls for this purpose and enabling the centralized consistency of policy.

Cloud-native Implementation

CWP is offered as a native SaaS service providing centralized visibility and control across hybrid clouds. The CWP SaaS service is elastic in that it automatically scales and offers metered pricing so that customers pay for what they use. Customers can deploy CWP as part of an Amazon Machine Instance (AMI) and Azure VM extension. Symantec's CWP also supports tags so that when CWP agents are installed with new instances, the appropriate protection policy is assigned.

The Bigger Truth

The strategic imperative to leverage cloud services to expedite the delivery of new applications has created a gap between the broad-based adoption of infrastructure-as-a-service and the implementation of cloud-ready cybersecurity policies, processes, and technologies. As this dynamic results in more cloud-resident corporate assets being exposed to intrusions and compromise, organizations must close the gap with security solutions that are designed for hybrid clouds. Such offerings must not only be effective in mitigating security risks and supporting compliance requirements, but must also be implemented for efficiency. The use of multiple disparate controls to secure hybrid environments is simply not operationally sustainable. Fortunately, the cloud as a delivery platform and the CI/CD methodology of DevOps offer the constructs to automate security across on-premises and cloud-resident workloads and services. By being purpose-built for hybrid cloud environments, Symantec's Cloud Workload Protection (CWP) and CWP for Storage meet these requirements, enabling the implementation of essential hybrid cloud security best practices so organizations can cloud safely.