White Paper

Five Considerations for Securing Hybrid Clouds

By Doug Cahill, ESG Senior Analyst

May 2016

This ESG White Paper was commissioned by Intel Security and is distributed under license from ESG.

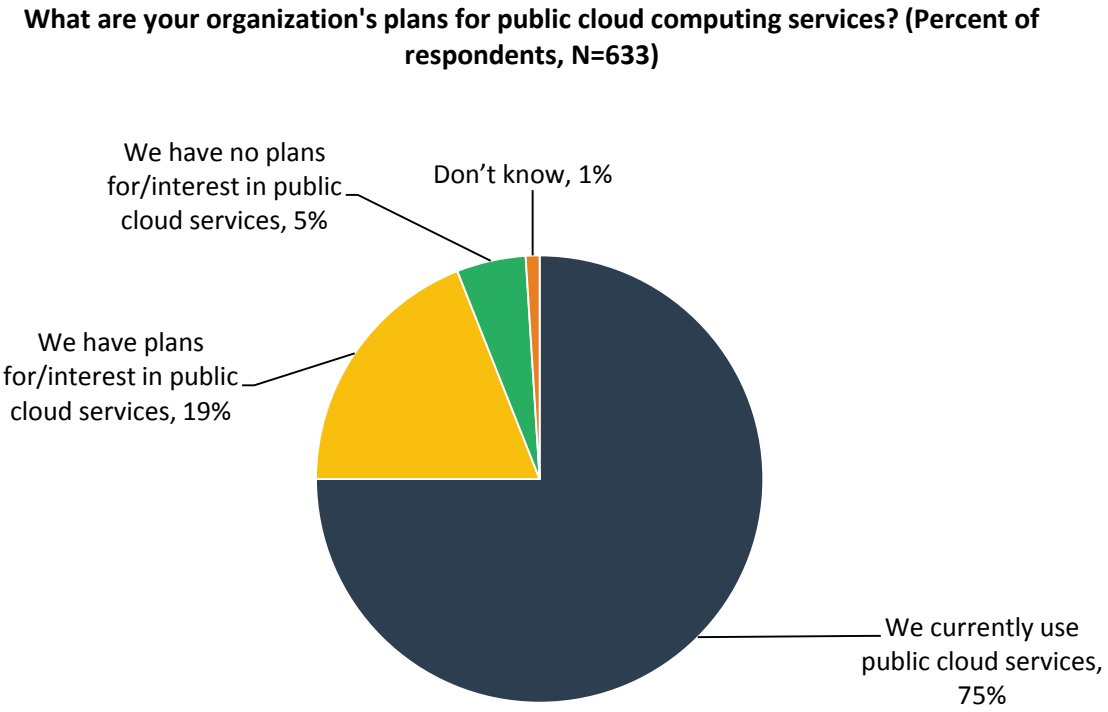
Contents

Hybrid Clouds: The Transformation of the Data Center

The Journey to the Cloud

Nearly all organizations are using some type of cloud services with many adopting a "cloud first" approach where all new IT projects, be they infrastructure or new applications, are deployed in the cloud. Indeed, three-quarters of the midmarket and enterprise organizations that participated in ESG's annual IT spending intentions survey currently use public cloud services in some capacity (see Figure 1).[1]

Figure 1. Usage Plans for Cloud Computing Services



Source: Enterprise Strategy Group, 2016

While the need to leverage the agility of cloud applications and on-demand infrastructure is essential for competitive advantage, if not parity, in today's go-fast world, so too is mitigating the associated risks and costs. New infrastructure models represent an opportunity to incorporate security best practices as an integrated element of a DevOps methodology so that security can be as agile as the cloud itself. Many security best practices are still applicable, but need to be applied relative to the attributes that make the cloud different, both technically and with respect to methodologies for how elastic infrastructures of the cloud are managed. The objective of this paper is to offer some considerations for organizations planning their journey to the cloud so they can move fast, safely. But before discussing such best practices, a look at the different types of cloud infrastructure is in order.

The New Normal: Multidimensional Hybrid Clouds

Hybrid cloud is a trendy term, and as is often the case with major IT trends, the words used to define it have gotten mixed up with a variety of technical concepts, obscuring the reason why we should care in the first place. If we start by

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

considering hybrid clouds as the mixed use of traditional IT infrastructure, public clouds, and private clouds, then those terms also need to be defined. Public clouds can be thought of as multi-tenant third-party infrastructure services, such as compute and storage that are available on demand via a set of APIs. Private clouds typically refer to a customer-managed, single-tenant infrastructure environment that is also API-driven, such as a virtual private cloud (VPC). A common thread across private and public clouds is the notion that they are software-defined so that resources can be automatically provisioned, and decommissioned, via automation systems. Racking and stacking of physical equipment is the absolute antithesis of the software-defined world of cloud computing.

One way to think about hybrid clouds is to consider the benefit of arbitrating data location and application tier across clouds to leverage the intrinsic benefit of each respective environment. A fairly basic, yet common hybrid cloud example is the use of local storage for online and near-line requirements, and cloud resident storage for offline and archiving purposes. A somewhat more sophisticated example is an application in which the database tier is deployed in an on-premises, customer-managed data center, or private cloud, and the web-based user interface tier deployed in a public cloud. Such an architecture allows for keeping data sets on-premises, and under direct customer control, while taking advantage of the auto-scaling capabilities and content delivery network of a public cloud platform for the web-based front-end. And to some, a hybrid cloud simply means that their journey to the cloud includes deploying a few workloads in the cloud—first for dev and test, and then for a new application. Whatever variation best describes an organization's own hybrid cloud, these multiple dimensions represent the new normal of the modern data center.

This new normal is not, however, exclusive to legitimate use by commercial and public sector entities. The agility and rapid application development environments provided by the cloud are attractive to malware writers just as they are to those developing business applications. The cloud also provides hosting for command and control servers as well as those executing a distributed denial of service (DDOS) attack. And SaaS applications, specifically sharing and collaboration platforms, have been used for the distribution of malware.

Before diving into best practices for securing hybrid clouds, organizations must understand what aspects of the cloud, specifically infrastructure-as-a-service (IaaS), are different from traditional data centers.

What's Different about Infrastructure-as-a-service (IaaS)?

There are some notable difference between traditional data centers and infrastructure delivered as a service, be it as a public cloud or a customer-managed private cloud.

- For IaaS, security is a responsibility shared with the cloud service provider (CSP). Customers and CSPs share the responsibility of securing the stack from the physical to the virtual. The CSP is responsible for physical data center security, from building access, through the network and server hardware, all the way up to the hypervisor hosting virtual machines. Given this demarcation line, the customer is responsible for the workload (i.e., the operating system and application) and, most importantly, their data. Customer responsibility for the data tier has legal liability as well as regulatory compliance implications such that customers must be attentive to sensitive data types such as personal health information (PHI) and other forms of personally identifiable information (PII) stored in their cloud accounts.

- The shifting network perimeter requires a workload-centric orientation. Perimeter defenses are still critical in a hybrid cloud, but that perimeter is less well defined than in a traditional data center where firewalls and DMZs are the definitive mark of the perimeter. Auto-provisioned workloads create their own perimeter, with some being externally facing and others being internally facing in that they only communicate with other workloads.

- Cloud-resident server workloads are highly dynamic. Just as fast as workload instances are provisioned to meet the resource requirements of an application, they are deprovisioned when demand diminishes. As such, server

workloads in the context of such auto-scaling groups are temporal or transient, each with a new and unique instance ID. Server naming conventions no longer apply with sets of key:value name pair tags used as the central construct for ease of management and to enable automation.

The concept of temporal workloads is also relevant to how workload configurations are managed in an on-demand cloud computing environment. Cloud-resident workloads in production are not updated nor patched, but rather they are simply replaced with new instances with a new configuration such as a patch (an attribute of the cloud sometimes referred to as immutable infrastructure) via automation services.

- DevOps employs API-driven automation for continuous delivery. DevOps can be thought as the yin to the agile software development methodology yang. Together, these methodologies make the agility of the cloud a reality by constantly iterating on software development via continuous integration, testing, delivery, and monitoring. The speed at which DevOps happens can result in the proliferation of insecure workload configurations expanding an organization's attack surface area. But DevOps also represents an opportunity to incorporate security best practices into the way in which hybrid clouds are increasingly being managed.

Securing Hybrid Clouds: Five Considerations

1. Gain constant visibility via continuous monitoring. The truism of "you can't secure what you can't see" is especially relevant in an elastic infrastructure where server workloads literally come and go. The other aspect of the cloud visibility gap is below the workload—that part of the stack for which the CSP is responsible, and into which, with some exceptions, customers lack visibility.

   Since a hybrid cloud is made up of disparate infrastructures, the first step to gaining better visibility is to inventory all of the elements, including physical and software-defined networks, workloads, automation servers, directory services, and more, because collectively they represent an organization's attack surface area. Special attention should be paid to those assets that are control points such as firewalls, proxies, and automation and directory service servers. The next step is to monitor activity, including the communication between workloads, to establish a baseline of what is normal. With the context of an inventory and standard behavior patterns, a hybrid cloud infrastructure should be continuously monitored to detect anomalous activities and to verify authorized access to services.

2. Employ a workload-centric security model. On-premises data centers have traditionally been protected with a network-centric security model to detect attacks moving laterally and prevent data from being exfiltrated. Since hybrid clouds are a combination of customer and third-party managed infrastructure, a workload-centric model should be added to the mix to both close the visibility gap and allow for applying policy-based controls.

   Integrity monitoring of workload system activity such as netflow traffic, process trees, file system changes, and more can detect anomalous events that could be indicative of a compromise. This intra-workload monitoring should be augmented with inter-workload monitoring—for example, tracking how workloads in a tiered application communicate with one another in order to ensure that workloads that are not supposed to be externally facing are not communicating with remote IP. And coupling these activities with threat intelligence will help detect communication with known-bad IP addresses such as that of a command and control server.

3. Leverage automation for operational efficiency. IT staffs, especially the security team, are already overburdened and thus need automation for operational efficiency. In many ways, securing hybrid clouds is an opportunity to gain efficiencies while also improving the business' security posture by incorporating security into how code is

delivered and workloads are provisioned. The DevOps methodology of automating continuous integration, testing, and delivery can be extended to include security in a few simple ways:

- As part of the automated continuous testing phase, vulnerability scanning should be conducted in the test environment and, if required, workload configurations must be updated with the latest patches in the automation platform so all new production workloads are current, reducing the risk of exploits. In production, the risk of zero-day exploits can be lessened with virtual patching by applying intrusion detection controls.
- By leveraging workload tags, security controls with the appropriate policies can be automatically applied to all new workloads—providing visibility and control from the moment the instance is provisioned.

These are examples of how the security and infrastructure management teams can collaborate to move security controls to the front of the line vis-à-vis automation.

4. **Apply the right control to the right assets.** With an inventory of assets across a hybrid cloud in hand, customers should then map out which security controls are most appropriate to secure each respective system.
   - Automation servers, for example, are core infrastructure elements in a hybrid cloud that, if compromised, provide attackers with not only access to a customer's infrastructure, but also the ability to change configurations. As such, controls such as requiring multi-factor authentication for access and default-deny application whitelisting can help greatly to maintain the integrity of these systems.
   - Jump or bastion hosts are meant to reduce the attack surface area by being the externally facing server which proxies Internet access for other servers in the application stack. If this one server gets owned, however, hackers have nearly unfettered access to move laterally to other servers and data assets. In addition to locking these servers down, all inbound and outbound traffic should be monitored to ensure that no one jumped the jump host.
   - The use of anomaly-based intrusion detection for more dynamic servers will help avoid possible identity compromises.
5. **Employ an integrated security solution for breadth and depth.** Finally, security teams should look for a solution that provides both coverage and controls. Hybrid clouds are heterogeneous by definition so cross-platform support for multiple operating systems is important to eliminate the need for multiple products. Products that aggregate multiple security functions into a single platform provide the feature depth to also reduce the number of tools required to secure a hybrid cloud. Reducing the complexity of securing hybrid clouds with solutions designed to work together versus a series of point tools from multiple vendors is a "better together" use case that the yields operational efficiencies all organizations seek.

Requirements for Hybrid Cloud Security Solutions

To put these best practices in action, organizations should consider solutions that are purpose-built for these workload-centric and highly dynamic environments based on the following requirements:

- **Flexibility** so customers can choose between software-as-a-service (SaaS), on-premises, and customer-managed cloud-resident deployment options for the control plane.
- **Support for tagging** to enable automated policy assignment for new workloads.
- **Integrity monitoring and control** functionality to detect configuration drift in the members of an auto-scaling group and for workload hardening.
- **Vulnerability scanning** to enable automating known exploit vectors in a test environment so all production workloads are current.
- **Anomaly-based intrusion detection** with built-in rules applied by server type so normal behavior is learned and baselined, and anomalous activity can be flagged.
- **An open architecture** is essential for API-driven software-defined infrastructures and should include both northbound and southbound interfaces, which allow for alert propagation and use of threat intelligence data such as signatures and known-bad IPs and URLs.

The Bigger Truth

Leveraging the agility of the cloud is a strategic imperative for nearly all businesses, resulting in hybrid clouds becoming the new normal of the modern data center. And as hybrid clouds become increasingly multidimensional by virtue of being comprised of disparate infrastructures, securing these complicated environments requires both an understanding of what makes them different and the use of solutions designed for the job. The best practices to do so are many of the same employed to secure traditional data centers but with an emphasis on automation which represents an opportunity to increase operational efficiency while keeping pace with highly dynamic cloud infrastructures. With these considerations in mind, it is possible to go fast safely in the cloud.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188