



# WHAT IS MULTI-CLOUD? ITS OPPORTUNITIES AND NEW SECURITY CHALLENGES



## REWARDS AND RISKS OF CLOUD DIVERSIFICATION

Cloud providers today must be on cloud nine. In just a few short years, their market has exploded. It has transformed from a fringe platform utilized by courageous companies on technology's leading edge into a cloud-first, standard, go-to approach for running all sorts of business-critical systems. According to IDC, nearly 50% of IT infrastructure spend will be on private/public clouds by 2019.<sup>1</sup>

These days, that spend is being allocated to a greater variety of cloud services. According to RightScale, enterprises use an average of 1.8 Infrastructure-as-a-service (IaaS) clouds;<sup>2</sup> Okta found that companies averaged 13 Software-as-a-Service (SaaS) applications.<sup>3</sup>

As IT departments forge ahead with multi-cloud adoption, CISOs must remain accountable for applications and workloads protected by disparate cloud security implementations. CISOs can fret over their cloud provider SLAs, or they can take matters into their own hands with a fabric approach to multi-cloud security. An open standards-based fabric of integrated and adaptive security products offers end-to-end visibility and coordinated threat response, helping organizations make the most of their multi-cloud environments.

## TOP 5 PUBLIC IaaS PROVIDERS<sup>4</sup>

- AWS
- Microsoft Azure
- Google Cloud
- IBM
- Oracle Cloud

## TOP 10 SaaS APPLICATIONS BY MARKET SHARE<sup>5</sup>

- Salesforce
- Microsoft
- Adobe
- SAP
- ADP
- Google
- IBM
- Intuit
- Oracle
- Workday

## THE CURRENT STATE OF MULTI-CLOUD

An organization's multi-cloud environment may include any or all the following:

- Public and private clouds that provide Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) offerings
- Public and private clouds that host Software-as-a-Service (SaaS) applications
- Hybrid clouds that combine on-premises data centers with public or private cloud services

Companies are becoming increasingly comfortable with multiple clouds. One survey of enterprises with at least 1,000 employees found that 85% of respondents' organizations are using either hybrid clouds (58%), multiple public clouds (20%), or multiple private clouds (7%).<sup>6</sup> According to research from Fortinet, organizations now use a median of 62 different cloud applications, which accounts for roughly one-third of their applications.<sup>7</sup>

This enthusiastic adoption belies a potentially bumpy road ahead for CISOs.

### INHERENT CHALLENGES OF MULTI-CLOUD ADOPTION

Migration to the cloud has always been motivated by the need for greater cost-efficiency, resiliency, and easier scalability. Multiple clouds offer the additional advantage of resiliency across service providers and avoidance of vendor lock-in.

Tempering these advantages, however, are several security concerns:

**Burgeoning attack surface.** If migration to one cloud expands the attack surface, multiple clouds further magnify it (see *Figure 1*). How can an organization scale protection to accommodate growth and fluctuations in multi-cloud workloads?

**Threat containment.** When workloads are distributed across multiple clouds, threats are more readily propagated to places outside the organization's control. Segmentation is a typical best practice for containing threats, but how can security staff segment users and applications across on-premises, IaaS, and SaaS environments?

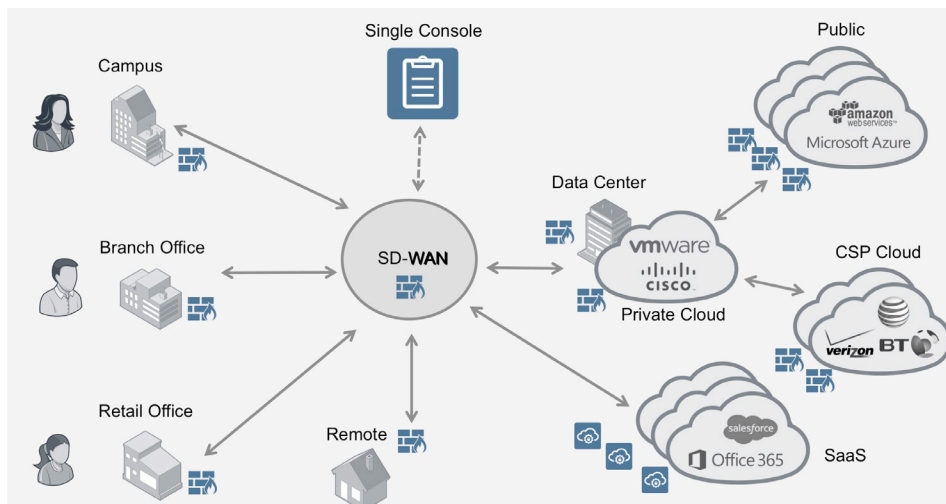


FIGURE 1. THE EXPANDED ATTACK SURFACE OF A MULTI-CLOUD ENVIRONMENT.

**Accountability.** Each cloud provider is responsible only for infrastructure or applications that it hosts. With data—and attack vectors—flowing rapidly between the organization and its various clouds, how can CISOs ascertain the source of an attack? Finger-pointing amongst providers is likely to ensue, but ultimately, it is the CISO who must answer to company leaders and shareholders.

85% of enterprises run multiple clouds

## WHY CLOUD SECURITY, AS USUAL, DOESN'T WORK IN MULTI-CLOUD

Every cloud provider worth its salt is deeply invested in the security of its customers' applications and infrastructure. Each provider will argue for the relative advantages of its own cloud security features. What multi-cloud adopters will experience, however, is a multiplicity of disparate security technologies, platforms, and management tools. For the corporate security team, this presents a few challenges:

**Poor visibility.** Because CISOs must be accountable for the entire portfolio of corporate applications and data assets, they must be able to assess the security of the portfolio in its entirety. Certainly, they have visibility into each cloud through cloud-specific portals, but they cannot see threats across all the clouds (which typically do not communicate with one another), nor can they immediately assess the impact of threats in one cloud on their entire organization.

**Lack of coordination.** With multi-cloud environments resembling a hub-and-spoke model, CISOs have a hard time reaching into all their clouds at once to detect and respond to threats. Without integration between security functions and centralized orchestration, they cannot mount a coordinated response to mitigate the impact.<sup>8</sup>

**High TCO, reactive security.** Undoubtedly, CISOs are doing everything they can, but in a multi-cloud environment, they are likely accruing much higher costs to consolidate their security posture than they did with a single cloud. Time is of the essence, too. In this era of zero-day threats and shrinking intrusion-to-breach windows, organizations don't have the luxury of spending hours matching and aggregating data from different cloud management portals or comparing signals from different clouds and then deciding on appropriate actions.

## THE FUTURE OF MULTI-CLOUD SECURITY: A FABRIC APPROACH

Meeting the challenges of a multi-cloud environment requires a more holistic approach that puts control back into the hands of the corporate security team. What's needed is a comprehensive suite of threat prevention, detection, and mitigation tools that integrates with all the major cloud services and can be managed within the enterprise from a single pane of glass.

This may sound like a platform solution. But it isn't. A platform is simply a loosely federated set of products. A security fabric is not a product, but rather an architectural approach based on open standards and protocols, which integrates different security devices—including security platforms—into a single security system that spans the multi-cloud network. Rather than following the hub-and-spoke structure of the multi-cloud network, the fabric creates a meshed security network in which all the security functions can communicate amongst themselves and with a central management console.

Not only does a security fabric provide end-to-end-visibility but it also enables end-to-end reach. Security staff can manage and prioritize patching, quickly identify and stop intrusions no matter where they happen, and mitigate their impact on the rest of the network. Finally, the centrally managed security fabric enables comprehensive incident analysis and gives CISOs a clear picture of their entire organization's security posture, which they can confidently take to the boardroom.



- <sup>1</sup> “Growth in Cloud IT Infrastructure Spending Will Accelerate in 2017 Driven by Public Cloud Datacenters and On-Premises Private Cloud Environments,” IDC, January 13, 2017.
- <sup>2</sup> “[RightScale 2017 State of the Cloud Report](#),” RightScale, 2017.
- <sup>3</sup> Chris Burt, “Slack May be Sexier, but Office 365 Most Used Cloud-based Business App,” WHIR, March 29, 2016.
- <sup>4</sup> “[RightScale 2017 State of the Cloud Report](#),” RightScale, 2017.
- <sup>5</sup> “[Microsoft Leads in SaaS Market; Salesforce, Adobe, Oracle and SAP Follow](#),” Synergy Research Group, August 31, 2017.
- <sup>6</sup> “[RightScale 2017 State of the Cloud Report](#),” accessed November 29, 2017.
- <sup>7</sup> “[Fortinet Threat Landscape Report Q3 2017](#),” accessed November 29, 2017.
- <sup>8</sup> Matthew Pley, “[Securing the Multi-Cloud: It’s Harder Than It Looks](#),” SDxCentral, November 17, 2017.



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199555  
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
Tel: +1.954.368.9990