WHITE PAPER

Why Security Architects Struggle to Manage Risk in Multi-cloud Environments

Lack of Skills, Integration, and Automation Lead to Multiple Security Gaps

Executive Summary

Cloud adoption is surging. Yet, enterprise security teams are challenged to protect the applications and data that now reside in multiple cloud environments. Risks are creeping in from many sources, from misconfiguration of cloud security controls to undetected cloud service usage and unscrupulous file storage. Without broad and deep visibility into all cloud assets, users, and activity, security teams are at a loss to defend their organizations' expanding attack surfaces. Manual cloud security control configuration processes are error-prone and do not scale. Disparate cloud-native tools impede threat protection and compliance. With a persisting shortage of cybersecurity skills, security architects must rethink their cloud management strategies.

Average global total cost of a data breach: **$3.86 million**

Annual business losses due to denial-of-service attacks and ransomware: **$2.3 million**

Introduction: Cloud Renders Perimeter Security Assumptions Obsolete

Enterprise networks no longer have clear perimeters. Previously, when networks were fully contained on-premises, the security team had a single point of control—all communications could be driven through a few Cat-5 cables and scrutinized by next-generation edge firewalls (NGFWs).

That single chokepoint has now disappeared, as enterprises operate in a multi-cloud world. As of this year, 84% of organizations have a multi-cloud strategy.[1] Overall, expenditures on public cloud services are expected to more than double between 2019 and 2023, from $229 billion to almost $500 billion globally.[2]

Obviously, where there is cloud sprawl, there is increased risk. Migrating workloads and data to multiple clouds creates new threat vectors. Notably, as the cloud platform control plane expands, it enlarges the attack surface. The risks of this expanded attack surface originate not only from external bad actors but also from the misconfiguration and unauthorized use of cloud APIs and UIs by developers and other internal users.

Another source of risk is the rapid pace at which cloud providers add service features. Amazon Web Services (AWS), for example, offers more than 140 services for compute, storage, networking, and myriad other data-related activities.[3] It takes only a few clicks for a user to add new cloud services. But it takes much more effort for enterprise security teams to ensure that the workloads using these services are protected.

Cloud security risks extend even to workloads that remain on-premises, as well as those 74% of applications that are migrated to the cloud but then brought back to the corporate data center.[4] The reason is that, in a multi-cloud world, all traffic effectively becomes web traffic, whether it is a front-end web application, web services middleware, or a mobile app with a web services-based back-end API. In this situation, security architects cannot look to their on-premises NGFWs as a sole source of enterprise threat information. They need to know what is going on in their cloud deployments.

Unclear Responsibilities Pose a Security Risk

The extent to which enterprise security teams are responsible for security of their cloud environments depends on the cloud deployment model. For example, in an Infrastructure-as-a Service (IaaS) environment, such as the AWS Amazon Elastic Compute Cloud (Amazon EC2), customers are responsible for all of the security configuration and management tasks, both for the operating system and for application software or utilities that the customer installs on the EC2 instances.[5] In a Software-as-a-Service (SaaS) cloud, such as Office 365 running on Microsoft Azure Cloud, the cloud provider is responsible for both network- and application-level controls. Customers handle data classification and accountability, and they share endpoint protection and identity and access management (IAM) responsibilities with the cloud provider.[6]

Still, many cloud customers remain unclear about who exactly is responsible for specific vulnerabilities or security events in their cloud deployments.[7] When that uncertainty spans multiple cloud services, asset and risk management confusion can envelop the entire organization.

Security architects are under pressure to resolve these uncertainties because, in the event of a breach, they and their CISOs or CSOs are accountable for any losses that result. Recent estimates have pegged the average total cost of cyber crime for a company at $13 million, with business losses due to distributed denial-of-service (DDoS) attacks and ransomware contributing $2.3 million yearly.[8]

Data breaches caused by cloud misconfigurations jumped 424% year over year, comprising 70% of all cloud data breaches.[13]

Configuration Mishaps Lead to Security Gaps

Even if cloud customers understand the shared responsibility model, it does not mean they can competently configure all the controls in the cloud environment. For AWS EC2 instances, customers must maintain up-to-date security patches for the operating system as well as any software or utilities that run on the instances. They also must configure the network firewalls on each virtual private cloud (VPC). Finally, they are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.[9]

But this is a challenge for many organizations due to the shortage of cybersecurity skills—a global gap estimated at nearly 3 million professionals.[10] Often, it is likely that the staff member tasked with configuring the cloud controls is not an expert on cloud security controls. Or they are familiar with one cloud provider, but not with any others that the organization uses. To assist those inexperienced in cloud security and to minimize configuration errors, security teams often use “golden” configuration templates, which eliminate the need for manual entry via web or command-line interfaces. Unfortunately, the templates themselves are prone to coding errors and may become obsolete. Worse, errors in templates are multiplied with reuse.

Another risky scenario is one in which security teams rely on preconfigured native cloud security services. For example, Azure DevOps Services comes with preconfigured security groups, with default permissions already assigned.[11] If the default permissions are not confirmed to be aligned with corporate IT security policies, they may open the door for cyber criminals to wreak havoc on the network. In fact, data breaches caused by cloud misconfigurations jumped 424% year over year, comprising 70% of all cloud data breaches.[12]

Malware and Data Leakage Hide in the Cloud

Security gaps crop up not only in the configuration of cloud services but also from inappropriate usage of the services. Specifically, with the movement to the cloud, disparate application teams are making decisions about data storage that may be in violation of corporate security policies or industry regulations.

Nearly two-thirds of security professionals list data loss and leakage in the cloud as a top security concern.[14] One way this can happen is when unsolicited datasets—which may contain malware—are stored haphazardly across cloud infrastructures and are not scanned—both on demand and on access for malware. In that case, undetected malicious code embedded in online data stores can spread to unsuspecting users or customers, creating new security incidents and even negative headlines. Online data stores may contain sensitive information, such as customer credit cards, drivers' licenses, or passport numbers, all of which may be stored online against company policy or in violation of compliance requirements. In sum, with more than half of breaches still taking months or longer to discover,[15] and an average cost of $148 per stolen record,[16] security architects cannot afford not to know about everything that resides in their clouds.

Lack of Visibility Hampers Cloud Security Efforts

Effectively discovering and remediating security gaps requires visibility into all the cloud environments in which the organization operates. Not only that, but it requires a consolidated view of all those environments and requires native integration into the management and security infrastructure of each cloud.

As with configuration templates, cloud providers seem to meet the need for cloud visibility and control with built-in tools such as Amazon Inspector (AWS) or Microsoft Cloud App Security (Azure). But each of these tools is focused on its own cloud platform. Because they function separately, these tools do not give enterprise security teams an easy way to view their entire multi-cloud services landscape.

Without a global view, teams cannot maintain an accurate and current inventory of all their cloud assets and resources, nor can they monitor changes in these resources over time.[17]

A lack of integration between cloud tools also hampers efforts to assess the multi-cloud security posture, which undermines both threat protection and compliance. To get the information they need, security teams are left to manually correlate information from the separate cloud tools. This is a waste of precious skills and may not enable enterprises to meet regulatory audit time constraints.

Underlying the challenges in accurate configuration and cloud security monitoring and management are human limitations in consistency, accuracy, and scale. Even without the severe cybersecurity skills shortage, human effort is no match for the explosive growth of the cloud attack surface and the increasingly artificial intelligence (AI)-driven threats that pervade cloud environments.

With more than half of breaches still taking months or longer to discover,[18] and an average cost of $148 per stolen record,[19] security architects cannot afford not to know what is going on in their clouds.

Stepping Up to Multi-cloud Security

Security architects are responsible for protecting the cloud environment (82% list cloud security as their direct responsibility).[20] But without a broad set of integrated and automated tools, they are struggling to reduce and prioritize risk. Avoiding cloud deployment is not a popular choice. A full 74% of enterprise security professionals reported moving applications or infrastructure into the cloud despite specific security concerns with the deployment.[21] So, it is up to the security architect to figure out how to do so securely.

[1] "RightScale 2019 State of the Cloud Report from Flexera," Flexera, January 2019.

[2] "Are CISOs Ready for Public Cloud Spending to Double?" The CISO Collective by Fortinet, August 5, 2019.

[3] "Overview of Amazon Web Services," AWS, July 2019.

[4] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, Q2 2019.

[5] "Shared Responsibility Model," AWS, accessed August 13, 2019.

[6] Frank Simorjay and Eric Tierling, "Shared Responsibilities for Cloud Computing," Microsoft, April 3, 2017.

[7] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, Q2 2019.

[8] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture/Ponemon Institute, 2019.

[9] "Shared Responsibility Model," AWS, accessed August 13, 2019.

[10] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)^2 Cybersecurity Workforce Study, 2018," (ISC)^2, accessed September 20, 2019.

[11] "Azure DevOps Services: About security and identity," Microsoft, June 1, 2019.

[12] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

[13] Ibid.

[14] "Data Loss, Leakage Top Cloud Security Concerns," Dark Reading, July 17, 2019.

[15] "2019 Data Breach Investigations Report," Verizon, May 2019.

[16] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, July 2018.

[17] Chris Purcell, "Is Multi-Cloud Sprawl Causing Your Money to Fly Away?" CIO, September 17, 2018.

[18] "2019 Data Breach Investigations Report," Verizon, May 2019.

[19] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, July 2018.

[20] "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, June 29, 2019.

[21] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, Q2 2019.

FORTINET

www.fortinet.com