CISO's Guide to Multicloud Security

Multicloud is a network of services from more than one cloud provider and may include a mix of public infrastructure as a service (IaaS) across environments such as Amazon Web Services and Microsoft Azure. According to MarketsandMarkets, a B2B research company, more than 75% of businesses are planning to implement multicloud architectures within the next two years (2018–2019) for agility, flexibility and cost savings. But while the technologies across multicloud infrastructures have advanced quickly, cloud security technologies continue to lag. The challenge for Chief Information Security Officers (CISOs) is how to fit into this new world, and how to overcome the toughest cloud security challenges including:

- Visibility and monitoring across multiple clouds
- Ensuring uniform policy across all cloud instances
- Pressure on security teams to protect everything spanning on premise to multiple clouds
- Threat detection and containment across an expanded multicloud attack surface
- Scaling security in keeping with today's developer and business needs

Security teams have a choice: Figure out how to adapt security to today's business needs or try to retrofit existing security processes and toolsets. Many CISO's want to maintain the practices and toolsets that they have built over the years, but unfortunately traditional agent and network tools are not suited for the scale, automation, or the architectures of multicloud. Failure to automate and streamline provisioning across multiple clouds complicates IT's ability to deliver secure, agile services at the scale that organizations are demanding. As security teams struggle to keep up with threat containment across multicloud, it leads to initial compromises, which if undetected in application traffic (east-west) result in outages and more severe incidents. And, most importantly, security teams are hindered by the lack of a single tool that can provide both visibility and the enforcement of uniform security policies across multiple, cloud-specific architectures.

ADOPT A CLOUD-FIRST STRATEGY: TAKE AN AGILE APPROACH TO SECURITY

As CISOs look to embrace the world of multicloud, they may want to recast the toolsets that they use and adopt a new mindset and partner with their business and developer counterparts. Here are our recommendations on reinventing security while enhancing protection:

- ☐ Find ways to overcome common objections encountered during migration such as security compromises on performance and cost. CISOs that focus on tools that can elastically scale "out and in" will find themselves in favor with their developer counterparts.
- ☐ Focus on automated orchestration for ease of deployment and management and to integrate seamlessly with each cloud-specific architecture, for example, Microsoft Azure.
- ☐ Find ways to gain visibility across your datacenter and cloud so that security policy can be consistent across these environments. Visibility is a major point of distinction between single and multicloud security. It is challenging enough to coordinate threat management between the corporate network and a single private or public cloud. With applications running in and accessed through multiple clouds, the challenges multiply, so coordination and consistency are paramount to achieving a defensible security posture. And, in today's agile developer world, workloads need to migrate with ease from one environment to the next. Security profiles

should follow these workloads regardless of where they are housed. This requires having a security toolset that can discover workloads and auto-classify based on workload attributes.

- ☐ Micro-segmentation has become very popular as a way to ensure application-aware access control. Focus on toolsets that can help automate this process at scale and according to workload risk profiles. However, many incorrectly assume that micro-segmentation by access control alone will detect and prevent the lateral spread of threats in east-west traffic. Be prepared to leverage the full spectrum of security controls as a part of your micro-segmentation strategy, such as anti-malware, Data Loss prevention (DLP), Transport Layer Security (TLS) decryption and Deep Packet Inspection (DPI) through Layer 7 for lateral traffic inspection, and for threat prevention and containment.
- ☐ Public cloud providers typically employ a shared responsibility model where they secure the underlying infrastructure but customers are responsible for securing everything above the hypervisor in an IaaS model. Look for lightweight and non-intrusive security solutions that will complement the layers of protection spanning perimeter-based controls to anti-malware and DPI traffic inspection and threat control.
- ☐ Make sure that other business key stakeholders understand how the shared responsibility model works and be sure to review documentation from your cloud provider carefully. Upholding your responsibilities and ensuring that your cloud provider is fulfilling theirs may require that you monitor their logs and ensure they are meeting their compliance obligations.
- ☐ Choose your cloud vendors carefully. Have a thorough understanding of their security practices and posture to ensure they are not introducing unanticipated risks into your environment.

Cyber threats are dynamic, and attackers can quickly infiltrate cloud infrastructures causing major data loss, outage and related damages. Perimeter security is not sufficient alone and cannot offer the scalability and agility required by today's multicloud infrastructures. An additional layer of protection—defense in depth—is essential. Cloud is designed for flexibility, agility, and scale and security must operate using the same principles.

SHIELDX MAKES SECURITY THE EASIEST THING ENTERPRISES DO IN THE CLOUD.

Our cloud-native, network security platform elastically delivers a full stack of agentless security controls—IPS, firewall, malware prevention, microsegmentation, and more—to protect data centers, cloud infrastructure, applications, and data. Our driving philosophy is to bring cloud speed, scale, and orchestration into the hands of security professionals worldwide. Based on cloud agnostic microservices technology, ShieldX ensures that security teams understand and maintain vigilance over cloud operations and workflows by continuously translating a security's intention into controls as cloud infrastructure rapidly evolves. Today, customers including Alaska Airlines and IDT have saved millions of dollars by eliminating control sprawl and consolidating security processes to dramatically reduce tactical systems management.

SHIELDX

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

October 2018