WHY LEGACY SECURITY ARCHITECTURES ARE INADEQUATE IN A MULTI-CLOUD WORLD

CONTENTS

EXECUTIVE SUMMARY

Cloud services are a pillar of a digital transformation, but they have also become a thorn in the side of many security architects. As data and applications that were once behind the enterprise firewall began roaming free—on smartphones, between Internet-of-Things (IoT) devices, and in the cloud—the threat landscape expanded rapidly. Security architects scrambled to adjust their technologies, policies, and procedures. But just when they thought they had a handle on securing their cloud-connected enterprises, new business imperatives indicated that one cloud wasn't enough.

Modern enterprises operate in a multi-cloud world, where the threat landscape has reached a new level of complexity. Security teams are juggling a hodgepodge of policies, threat reports, and management tools. When each cloud operates in its own silo, the security architect has even more difficulty supporting the CISO or CIO with a coherent, defensible security posture.

MULTI-CLOUD CHANGES THE SECURITY EQUATION

As complicated as it may be to manage, cloud diversification makes good business sense. Increased application availability, improved performance, and avoidance of vendor lock-in are among the reasons organizations subscribe to multiple clouds. And they are doing so in droves. One survey of enterprises with at least 1,000 employees found that 81% of respondents' organizations are using either hybrid clouds, multiple public clouds, or multiple private clouds.[1] Public cloud services may include Infrastructure- or Platform-as-a-Service (IaaS/PaaS, such as AWS) or Software-as-a-Service (SaaS, such as Salesforce or Office 365) hosted either in public or service providers' private clouds.

Much of the multi-cloud diversification is coming from the adoption of SaaS, either for new application deployments or to offload applications from the enterprise network. According to research from Fortinet, organizations now use a median of 62 different cloud applications, accounting for roughly one-third of their applications.[2]

Consider, however, how a multi-cloud environment affects cybersecurity. For one, siloed clouds create gaps in security and limit visibility into vulnerabilities and threats. Second, as the multi-cloud environment expands, the threat landscape expands with it. With more applications, greater data volumes, and more endpoints to manage, security teams are finding it exponentially more difficult to keep up with accelerating threats, scale security coverage, and comply with evolving security standards and regulations. In a recent survey of organizations with multi-cloud deployments, 7 of 10 respondents cited security as their top concern.[3]

At the root of this problem are security architectures that were designed for a single data center or cloud. Now stretched beyond their limits, they are no longer effective or operationally efficient. Organizations that don't retool their security architectures for multi-cloud operations face a range of risks and liabilities, which are unpacked and explained in the rest of this eBook.

[1] "RightScale 2018 State of the Cloud Report," accessed April 16, 2018.
[2] "Fortinet Threat Landscape Report Q3 2017," accessed April 5, 2018.
[3] "New Global Research Reveals Keys to Unlocking Successful Multi-Cloud Adoption," VMware press release, December 12, 2017.

01 CLOUD SILOS IMPAIR VISIBILITY AND RESPONSE

The security team is tasked with protecting the entire portfolio of corporate applications and data assets. Although they have visibility into each cloud through the cloud provider's portal, they usually do not have a consolidated view into threats across all the clouds (which typically do not communicate with one another). Likewise, they cannot immediately assess the potential impact on their entire organization of threats in one isolated cloud.

One 2017 study revealed that it takes organizations 191 days, on average, to detect a data breach and 66 days to contain it.[4] The study also found that access to cloud-based applications and data increases the time required to deal with data breaches. This is a logical consequence of not having efficient means to consolidate threat intelligence and vulnerability data across the enterprise.

When a threat is detected in one cloud, staff must scramble to analyze logs and corroborate threat information with other clouds and the data center. An environment replete with disparate tools and manual processes sets up the security team to fight a losing battle against accelerating threats.

[4] "2017 Cost of Data Breach Study," Ponemon Institute LLC, June 2017.

02 ADMINISTRATIVE BURDEN BECOMES UNSUSTAINABLE

Most enterprises do not create multi-cloud environments all at once. Rather, they subscribe to cloud services one at a time. Each cloud service comes with its own security provisions and management tools. This creates several administrative headaches:

Staffing. Not only must security staff learn how to use each of these tools, but team leads face the challenges of allocating and training staff as services are added and cloud providers update their tools.

Compliance. As compliance demands pile up after each new wave of breaches, enterprise security teams may look to their various cloud service providers (particularly SaaS providers) to track and report on activity in the clouds. But cloud services operate on a shared responsibility model. Providers commit to secure their own applications, but enterprise security teams must ensure that cloud security provisions meet corporate standards. Security teams must also ensure compliance when regulated data traverses multiple cloud boundaries.

Integration. With each cloud application evolving and operating autonomously, it is up to the enterprise security team to disseminate changes in corporate security policy across all clouds and to integrate enterprise security technologies with those of each cloud provider. Short-staffed teams may outsource integration tasks, but in doing so, this merely shifts the costs elsewhere. It also fails to account for the cost and time associated with managing the third-party provider.

Security experts overburdened with these tasks have little time to take a strategic perspective, to ensure that the security architecture supports a long-term view of the threat landscape—specific to the cloud—and the digital transformation of the business.

03 SECURITY COVERAGE LAGS BEHIND CLOUD APP DEPLOYMENT

Much of the value of cloud services lies in enabling organizations to deploy and scale applications quickly. A line-of-business manager can deploy an application in the cloud and move information off-site in minutes. Compounding the problem, configuration changes occur rapidly. With the adoption of DevOps, organizations now roll out new software updates quickly. IaaS cloud providers have shortened the development cycle, so new releases arrive every few minutes—in some cases, even every few seconds.

Ensuring watertight security coverage with such accelerated deployment is hard enough with a single cloud, especially if security provisioning is not automated. Multiple clouds multiply the problem.

The result is a painful trade-off for IT and security executives. While waiting for security to catch up, they must either throttle back on application deployment and cede competitive advantage, or they must move ahead and hope that nothing bad happens. Few security architects will want to answer to a CIO or CISO in this predicament.

04 HUMANS CAN'T KEEP UP WITH SOPHISTICATED THREATS

In today's tight security labor market, enterprises are lucky if they can recruit enough talented and experienced staff. Yet even the best and the brightest security experts can't keep up with threats that have exploded in volume, velocity, and sophistication—unless they have the right technology in the right architecture.

Several flaws may limit the ability of a security architecture to respond at the speed of automated cyber threats:

The security solutions are based on point products or platforms. Point-product architectures often evolve organically, as architects specify best-of-breed technology for each new security challenge that arises. The problem is that what happens on one device may stay on that device unless a human manually shares the information. Consequently, some security architects have opted for security platforms, which seem to promise an integrated approach. Unfortunately, these platforms are really a loosely federated set of products that operate in a hub-and-spoke fashion, with all messaging flowing through a central point. The inherent latency in this model allows an unacceptable level of damage to occur before it can be remediated.

They lack automation and multi-cloud orchestration. With today's automated and intelligent threats, manual, reactive response is quickly becoming an indefensible strategy. Lacking automated, proactive threat protection, staff have no clear priorities for threat response, chasing too many low-level threats while allowing potentially devastating threats to go undetected and uncontained.

Threat intelligence is an add-on. Though it is widely available, threat intelligence is not very useful if it comes too late, it isn't shared across the entire enterprise, or it cannot be acted on quickly enough. To be consistently effective, threat intelligence cannot simply be used in conjunction with, or applied to, threat protection technologies. It must be part of the architecture.

CONCLUSION

As enterprise networks blossom into multi-cloud environments to support digital transformation, enterprise security architectures must transform with them. Security executives are demanding solutions that adapt to the current threat landscape and changes in the attack surface; enable centralized and automated control; and empower the security team to protect sensitive information.

To meet these demands, security architects need to design architectures that eliminate information silos, provide transparency across the system landscape, easily support new tools, automate routine tasks, quickly respond to threats, and improve detection and remediation. Only with such a security architecture can a company transform multi-cloud security from a potential business inhibitor into a business enabler.

FORTINET®

www.fortinet.com

175400-0-A-EN