SHIELDX

ShieldX Return

STATS

Gartner and growth of multicloud: Market Insight: How Tech CEOs Can Position and Promote Services in the New World of Hybrid Cloud and Multicloud, September 2018:

- Hybrid cloud is the foundation of digital business. The market size for cloud is growing exponentially and is projected to reach $317 billion by 2022.
- The number of cloud managed service providers (MSPs) will triple to peak in 2020, then experience massive consolidation through 2023.
- By 2020, 75% of organizations will have deployed a multicloud or hybrid cloud model for their IT needs.
- Gartner expects cloud adoption rates among organizations to jump from 68% in 2017 to 80% in 2018
- Insecure Cloud Services Will Continue To Hemorrhage Sensitive Data: During the last few years, we have seen a number of large data leaks due to misconfigured cloud services such as MongoDB and Amazon's Simple Storage Service (S3). In Q3 of 2017 alone, major companies such as Time Warner, Verizon, and Viacom experienced this type of data leak — losing encryption keys, customer account details, and other sensitive data. [3] While third parties were directly responsible for the loss of customer data in both the Time Warner and Verizon situations, it's important to recognize whose name ends up in the press when shared customer data is lost.[4]

THE PROBLEM

The cloud exponentially increases complexity: Digital transformation, the cloud, and the advent of DevOps, speed up business and drive innovation, but for network and security operations teams, it means a significant increase in workload. The resultant increase in change requests spans complex multi-vendor, multi-technology, and hybrid cloud environments. With limited resources and manual processes, it is difficult for IT organizations to keep up with demand and document change.

Misconfiguration is deadly

- IBM: One of the key points was the skyrocketing rate of poorly-configured cloud infrastructure. The report estimated that breaches related to bad configuration jumped by 424%, accounting for nearly 70% of compromised records over the year. [2]
- Firewalls, for example, are frequently misconfigured by their users. Policies can be left too broad, effectively leaving the network permanently exposed. Test systems may not be properly firewalled from production systems; and the basic principal of least privilege is not always enforced.
- Gartner: Through 2022, 80% of successful attacks on serverless PaaS will have a root cause of misconfiguration or the use of known vulnerable code due to immature tools and processes.

Misconfigurations are a major contributor to breaches and other security flaws in the cloud. The skyrocketing rate of poorly-configured cloud infrastructure is THE major source of breaches. Bad configuration jumped by 424%, accounting for nearly 70% of compromised records over the year. Computing Cloud Review 2018 noted that 86% of organizations cite data breaches and loss as the primary reason they hesitate to adopt the cloud.[1] A simple misconfiguration, even a failure to set a single option in a company's cloud service, can create a major security risk. And the threat of misconfiguration will only grow exponentially with the growth of multi cloud environments. By 2020, 75% of organizations will have deployed a multicloud or hybrid cloud model for their IT needs.

THE SOLUTION

The ShieldX Elastic Security Platform dynamically scales to deliver comprehensive and consistent controls to protect data centers, cloud infrastructure, applications and data no matter where they are or where they go to make the cloud more secure than on-premise deployments. Our frictionless approach combines agentless technology with the ShieldX Adaptive Intention Engine which autonomously translates and enforces intention into a set of comprehensive controls and policies—including micro-segmentation, firewall, IPS and more—making security the easiest thing you do in the cloud.

SHIELDX IMPACT

- ShieldX's forward-thinking method of protecting the cloud led us to an improvement in our security effectiveness and we've already seen a reduction in our operation costs. As we continue to replace dated, ineffective investments with the ShieldX Elastic Security Platform, we experienced a 30 percent overall reduction in cost.

- ShieldX makes the cloud safer than on-prem deployments. That is because that the number-one cause of security incidents today is human error, and those errors are often a result of very complex security structures. ShieldX makes it a lot easier and a lot simpler to define your policies and define your rules, and that greatly reduces the opportunity for user error.

What to do about it: You must be proactive in managing your digital risk. You need to have visibility into how your admins configure publicly facing services. While this may be accomplished through periodic red team exercises or internal auditing, Forrester recommends working with a digital risk monitoring (DRM) company to monitor your infrastructure externally in real time.[7]

1 https://www.computing.co.uk/ctg/news/3030593/computing-cloud-review-2018
2 https://www.htbridge.com/blog/OWASP-security-misconfiguration.html
3 https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018/-/E-RES137206?objectid=RES137206#endnote9
4 https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018/-/E-RES137206?objectid=RES137206#endnote10
5 https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018/-/E-RES137206?objectid=RES137206#endnote11
6 https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018/-/E-RES137206?objectid=RES137206#endnote12
7 https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018/-/E-RES137206?objectid=RES137206#endnote13

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

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

November 2018