Public Cloud Security: Myths vs. Facts

Approximately 38 percent of workloads are now on a public cloud, and public cloud services usage has registered approximately 18 percent growth*. As public cloud migrations have rapidly accelerated, so too have misunderstandings and myths surrounding public cloud security.

Statista Research 2021

This infographic details **the most common public cloud security myths** and the truth behind them.

1

Cloud security slows down innovation

Public cloud can accelerate innovation, time-to-value, and quality control. Security is an integral part of any software, but it's often neglected during the software development process. Embedding security into the software development life cycle (SDLC) through automation is a better approach rather than manual processes because:

1. The cost of remediating a security vulnerability post-production is much higher compared to addressing it in the earlier stages of the SDLC.
2. Embedding guardrails enables organizations to mitigate risk and ensure cloud deployments are secure and compliant without impacting the speed of development. Automation makes sure security becomes part of SDLC seamlessly without impeding innovation.

Public clouds are not secure

2

This is a common and prevalent misconception. Cloud providers have invested massively in the security of their platforms, and though public cloud does experience security incidents, 99 percent of them are customer-caused, with misconfigurations, excessive permissions, and other misuses of public cloud services being the main culprits, according to Gartner. Organizations need to understand the concept of the shared responsibility model to secure cloud environments, as shared responsibility varies greatly by provider and service type.

3

All workloads are the same and need the same security

Cloud workload security best practices vary depending on the type of cloud services, such as IaaS, PaaS, SaaS, and serverless. Each cloud model offers specific features and functionalities, and it is crucial for organization to distinguish, understand and remediate risk and security issues for various Workloads.

Cloud security and on-premises security are equally challenging

4

With no on-premises servers and partial responsibility shifted to cloud service providers, cloud workload security might seem like a more straightforward task than securing on-site workloads. Given the unique and dynamic nature of cloud environments, in reality, securing cloud workloads is often a far more complicated process than securing on-premises workloads.

For example:

- New features and functionalities are added regularly by CSPs, making it more difficult to protect against misconfigurations, vulnerabilities, and compliance risks.
- Rapid-release cycles employed by development and DevOps teams make it challenging for security and risk management teams to keep up with the changes and gain control over these deployments.
- Dynamic, ephemeral workloads mean that security must be automated rather than manual as automation eliminates human error and security incident response delays.

To learn more, read this blog: Preventing Cloud Security Breaches

5

Security is the responsibility of the cloud service provider

Cloud service providers won't be intimately familiar with every organization's line of business, so it is ultimately the organization's responsibility to verify that their data, applications, and resources are secured. It is essential to understand the shared responsibility model in which the cloud tenant is the ultimate custodian of their data, apps, etc., and is therefore responsible for safeguarding it.

Public cloud storage buckets are secure by default

6

Organizations assume that storage buckets such as AWS S3 are inherently secure simply because it runs on AWS. AWS S3 buckets are private and can only be accessed by those who have been granted access. So, yes, they are secure. However, many incidents highlight how many S3 buckets have been misconfigured and left open to public access. Although most cloud storage services have built-in security features, the configuration of these features and services, and the protection of stored data ultimately lies with the organization.

For more information, read: How to Find Externally Exposed Sensitive Cloud Data

7

SaaS applications don't need security

Many business-critical SaaS apps like Microsoft 365 contain sensitive data and information. Organizations are still responsible for SaaS application configuration to maintain security. It is crucial for organizations to continuously monitor and detect misconfigurations, incorrect permissions, and data exposure, as users are able to interact with files and data, including sharing and configuring access. This flexibility can lead to challenges with security, compliance, and uniform security policy enforcement. Without strong configuration practices in place, organizations are vulnerable to risk factors that can expose data and open the door for cyberattacks and abuse of privileges and resources.

Read more: Why You Need SaaS Security Posture Management (SSPM) for Microsoft 365

The cloud is a great place to innovate, but managing security risk, sensitive data, access permissions, and compliance within a complex cloud-based environment can be challenging. Hence, it is essential to separate fact from fiction when it comes to public cloud security.

Fortunately, Zscaler is here to help solve your public cloud security challenges. **Get in touch** with us today to start your cloud security transformation journey.