radware

SECURING THE GAPS IN PUBLIC CLOUDS:
UNDERSTAND THE CLOUD SHARED RESPONSIBILITY MODEL

Hosting applications and data in public clouds is a proven way for enterprises to be nimbler with network operations, improve the customer experience and reduce costs. As more data transitions to the cloud with the adoption of contactless payments and remote work initiatives, organizations are increasingly relying on cloud service providers (CSPs) to not only host but also secure their data. About one-third of companies say they rely on CSPs to secure their digital assets, according to Radware research.

The issue with that approach is that every public cloud provider utilizes different hardware and software security policies, methods and mechanisms, creating a challenge for enterprises to maintain standard policies and configurations across all infrastructures. Plus, CSPs generally only meet basic security standards for their platforms because they want to standardize how they monitor and mitigate threats across their entire customer base.

CSPs subscribe to the shared responsibility model: a practice where the service provider is responsible for securing the cloud infrastructure and the associated environment, leaving the aspects of securing application, workloads and data hosted on the cloud to the customer. The failure of customers to fully understand and adhere to the shared responsibility model is responsible for the majority of public cloud data breaches. According to Gartner, "through 2022, at least 95% of cloud security failures will be the customer's fault."

MANAGING EXPECTATIONS

Many customers fail to realize that the responsibility of protecting their applications and customer data in the cloud is a shared responsibility. In its simplest terms, the cloud shared responsibility model denotes that CSPs are responsible for the security and availability of the cloud and customers are responsible for securing the data they put in the cloud. Depending on the type of deployment—IaaS, PaaS, or SaaS—customer responsibilities will be determined.

[1] C-Suite Perspectives: Accelerated Cloud Migration But Lagging Security

- **Infrastructure-as-a-Service (IaaS)**
  Designed to provide the highest degree of flexibility and management control to customers, IaaS services also place more security responsibilities on customers.
  For example, when customers deploy an instance of Amazon EC2, the customer is the one who manages the guest operating system, any applications they install on these instances and the configuration of provided firewalls on these instances. They are also responsible for overseeing data, classifying assets, and implementing the proper permissions for identity and access management.

- **Platform-as-a-Service (PaaS)**
  In PaaS, more of the heavy lifting is passed over to CSPs. While customers focus on deploying and managing applications (as well as managing data, assets, and permissions), CSPs take control of operating the underlying infrastructure, including guest operating systems.

- **Software-as-a-Service (SaaS)**
  Of the three deployment options, SaaS places the most responsibility on the CSP. With the CSP managing the entire infrastructure as well as the applications, customers are only responsible for managing data, as well as user access/identity permissions.

Responsibility	On-Premise	IaaS	PaaS	SaaS	FaaS
Data classification, access and accountability	🔴	🔴	🔴	🔴	🔴
Client and end-point protection	🔴	🔴	🔴	◐	◐
Identity and access management	🔴	🔴	◐	◐	◐
Application-level controls	🔴	🔴	◐	◐	◐
Compute, network and storage instances	🔴	◐	🔵	🔵	🔵
Host infrastructure	🔴	◐	🔵	🔵	🔵
Physical security	🔴	🔵	🔵	🔵	🔵

🔴 Cloud Customer 🔵 Cloud Provider

Source:
1. Microsoft Azure, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
2. Amazon Web Services, https://aws.amazon.com/compliance/shared-responsibility-model

HOW TO UPHOLD YOUR END OF THE BARGAIN

Before diving into the granular details, assess your organization's overall cyber hygiene. Measure your organization's cloud security posture against industry benchmarks and best practices, such as the Center for Internet Security. In addition, take guidance from your CSP. Cloud vendors such as Amazon and Microsoft provide detailed guidelines of security responsibilities for customers.

Keep one critical detail in mind: understanding these responsibilities is an evolutionary process because CSPs are constantly evolving. CSPs add new services that come with new configuration and security tools to manage those services. While native security tools can be convenient, they typically don't provide enterprise-grade security that covers all your organization's configuration needs. To overcome these platform-specific limitations, consider implementing third-party cloud security services, workload protection and access management solutions to provide your organization with holistic, 360-degree visibility and protection of your cloud-based assets.

Lastly, here are nine key considerations your security team should always be evaluating as you continue to migrate to the public cloud:

1. **Changes in network topologies and configurations** that are due to the shift of applications to public cloud environments.

2. **Challenges in adapting application to cloud-native architectures.** Keep in mind that the majority of applications being moved to public clouds were not developed with the infrastructure requirements of public clouds in mind.

3. **Changes to cloud workloads.** The evolution of cloud workloads has resulted in an array of new workload management policies to keep these environments secure from misconfigurations and excessive permissions.

4. **Sophistication of data access/authentication methods and shadow IT.** This has resulted in security gaps due to increasingly sophisticated compliance management, asset configurations and poor visibility for network security teams.

5. Remote operations and workforce possibly resulting in **non-compliance for key regulations such as HIPAA and GDPR**. Federal laws and regulations such as these present challenges to businesses when replicating office environments to remote operations.

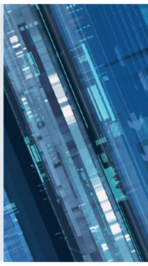
6. **Management of distributed assets.** Ensuring visibility and a strong security posture of data across heterogeneous environments (on-premise, virtual, hybrid and public cloud) is incredibly difficult.

7. **Management of third-party interfaces.** Third-party integrations and APIs add a new level of complexity to data protection policies.

8. **Inconsistencies in third-party data access.** This is primarily due to a lack of proper governance mechanisms around the access and privilege to public clouds, which can vary from one public cloud platform to the next.

9. **Overall lack of consistent security posture and policy enforcement.** Constantly evolving workloads can render an organization's security policies obsolete.

Learn Why Multi-Faceted Protection Is Critical For Today's Cloud Environments



About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.