9 Challenges To Securing Applications In Multi-Cloud Environments

The migration to the cloud has given way to a new architectural paradigm: the multi-cloud. According to the IBM report, "State of Multi-Cloud," 60% of companies now run at least two or more public cloud environments, and 30% run three or more.[1]

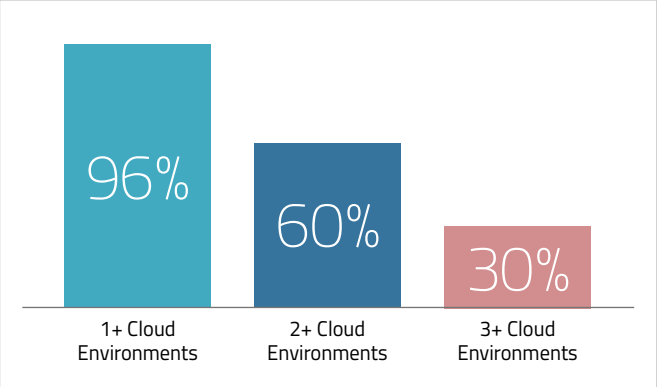

Figure 1

Number of Companies Running Various Cloud Environments

Adding to the complexity, about one in three companies runs applications in a private cloud environment. The result is that most organizations run applications in a combination of on-premise, private cloud, public cloud and multi-cloud settings, each with their own unique mix and choice of platforms.

This creates a challenging computing environment that must be managed and secured.

1. "*State of Multicloud: A CIO's Guide to the Underlying Dynamics Fueling Multicloud Strategies*", Turbonomic, an IBM Company, 2021.

Existing Application Security Solutions Lead to Security Silos

The problem is that there are no sufficient solutions that enable organizations to secure web applications across distributed environments in a consistent, high-quality and comprehensive manner.

Public cloud environments frequently have their own native protections that work only in their particular environment (but not on other platforms), while nonnative solutions often can provide cross-cloud protection but also add operational overhead and latency.

As a result, organizations are frequently forced to run multiple application security tools, each of which protects only a portion of their applications. It is not uncommon, for example, for organizations to use hardware web application firewall (WAF) appliances for their on-premise data centers, native WAF solutions of infrastructure-as-a-service (IaaS) providers to secure their cloud applications and WAF networks based on content delivery networks (CDNs) to protect their private cloud environments.

Each of these tools has its own merits and drawbacks:

- **CDN-based cloud WAF services** provide cross-cloud protection and centralized control but also require DNS routing changes, add latency and another point of failure and require sharing the SSL key.
- **Native security tools of IaaS vendors** are convenient to implement and built directly into the IaaS stack, but usually provide a low level of security and have no cross-cloud capabilities for protection of other public cloud, private cloud or on-premise environments.
- **WAF virtual appliances** can provide a high level of protection (depending on vendor) but require high operations and management overhead and usually are point solutions, requiring additional (external) tools for bot/API/DDoS protection. Moreover, they usually lack centralized, cross-environment management, and making the solution fault tolerant and scalable adds more complexity.
- **Hardware WAF appliances** are used traditionally to protect on-premise data centers but are irrelevant in cloud environments and obsolete in supporting cloud migration. While they can be deployed in High Availability (HA) modes, making such solutions fault tolerant and scalable adds more complexity.

Figure 2

Pros and Cons of Application Security Tools

CDN-based Cloud WAF

- ↗ Cross-cloud protection
- ↗ Centralized management
- ↘ Low quality of protection
- ↘ Routing changes

Native IaaS AppSec Tools

- ↗ Built-in to IaaS stack
- ↗ No routing changes
- ↘ Low quality of protection
- ↘ No cross-cloud protection

Cloud-based Virtual WAF Appliance

- ↗ Deployed in IaaS stack
- ↗ No routing changes
- ↘ Point solutions
- ↘ High management overhead

As a result, there are nine key challenges to consider when securing web applications across hybrid environments:

1. **Quality of security**: Most cloud-based security solutions are based on a "negative" security model, using static, manually defined security policies.
2. **Varying levels of protection:** Maintaining the same level of protection across platforms is difficult, as each solution has different levels of security.
3. **Inconsistent security policies:** Security policies between different environments are incompatible and inconsistent with each other.
4. **Point of failure:** In-line WAF deployments invariably add another point of failure to the system. If they go down, all communication to the server is blocked.
5. **Increased latency:** Going through third-party cloud networks that are external to the public cloud environment adds traffic hops.
6. **Tight coupling between security and delivery:** Most cloud-based WAFs require tight coupling between a CDN and security, reducing operational agility and flexibility.
7. **SSL certificate sharing:** Existing tools require the application's SSL certificate, adding management overhead and violating user privacy.
8. **Fragmented logging and reporting:** It's difficult to get a view of threats across platforms.
9. **No centralized management:** Security breaks into silos with disparate management, leading to an overhead nightmare of managing multiple security tools for each platform.

These disjointed security solutions often result in security silos for applications across different platforms, with inconsistent application security, varying levels of protection, fragmented logging and reporting and disparate management. The result is a degradation of application security and high operational overhead.

Learn Why Comprehensive Protection Across Multi-Cloud Environments Is Now Critical

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.