Application Security for Any Cloud

The Radware SecurePath™ architecture is uniquely designed for protecting today's multi-cloud application environments while maintaining consistent, high-grade and comprehensive protection for applications regardless of where they are deployed.

Radware's new API-based architecture was designed to optimally protect applications deployed across any data center or cloud environment – whether on-premise, private cloud or public cloud – while improving security, uptime and performance.

Multi-Cloud Is the New Normal

Organizations are no longer migrating to the cloud; they're already there. According to IBM's report "State of the Multi-Cloud," 96% of organizations deploy at least one public cloud environment.

However, this strategic change in the market has given way to a new paradigm shift: the rise of the multi-cloud. According to IBM's report, 60% of companies now run at least two or more public cloud environments, and 30% run three or more. This means that a majority of companies today fall into the multi-cloud category.

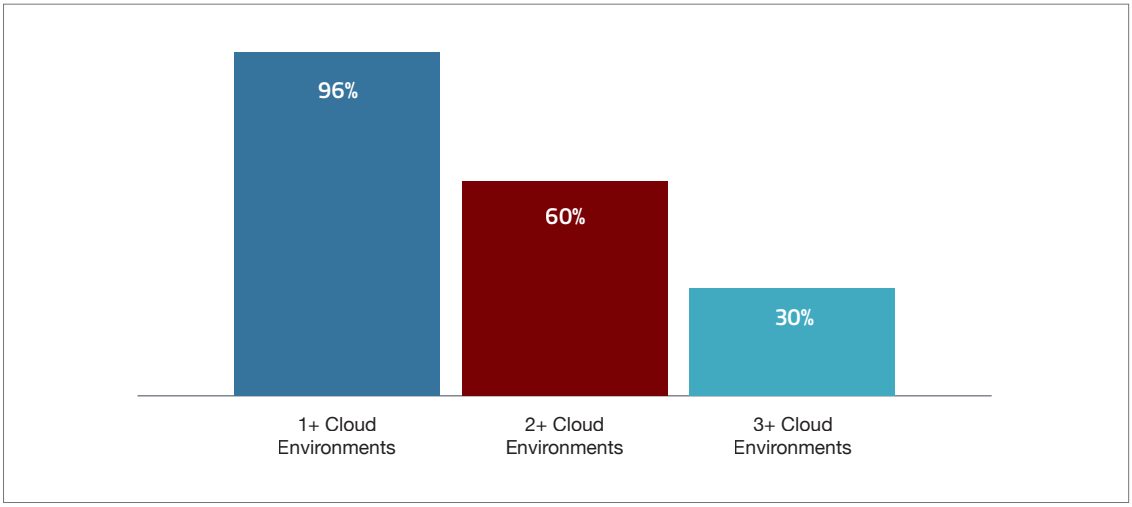
Adding to the complexity, about one in three companies runs applications in private cloud environments. The result is that most organizations run applications in

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.

Figure 1

Percentage of companies with one or more cloud environments



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, which 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.

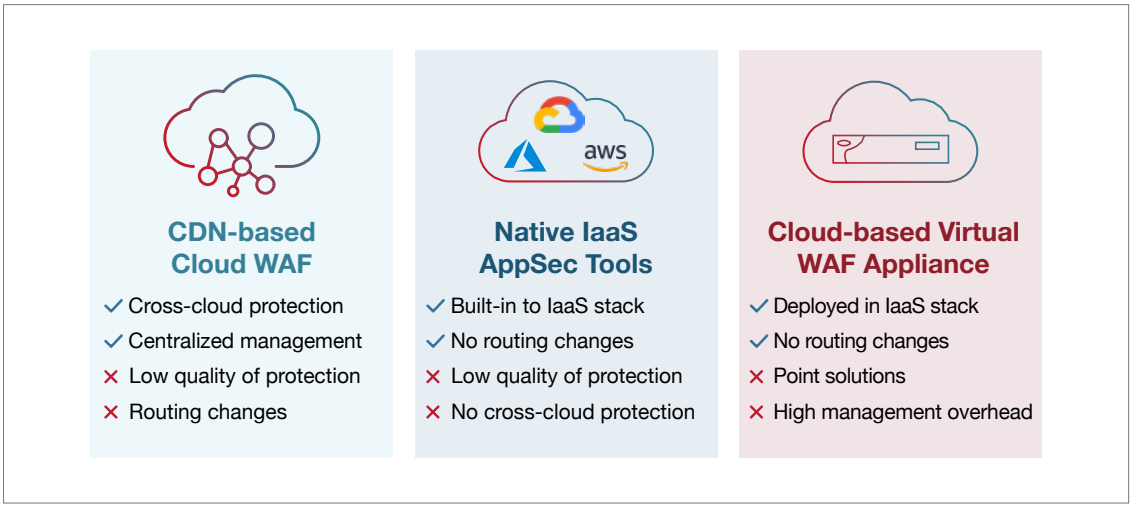
Each of these tools has its own merits and drawbacks:

- **CDN-based cloud WAF services:** These services provide cross-cloud protection and centralized control, but as a separate cloud network external to the public cloud environment, and they also require DNS routing changes, add latency and another point of inline processing, and require sharing SSL keys.
- **Native security tools of IaaS vendors:** These tools are convenient to implement and built directly into the IaaS stack, but they usually provide a low level of security and have no cross-cloud capabilities for the protection of other public cloud, private cloud or on-premise environments.

- **WAF virtual appliances:** These provide a high level of protection (depending on the vendor), but they require high operations and management overhead and usually are point solutions, requiring additional (external) tools for bot, API, and distributed denial-of-service (DDoS) protection. Moreover, they usually lack centralized, cross-environment management, and making the solution fault tolerant and scalable adds more complexity.

Figure 2

Existing tools provide partial coverage



As a result, there are key challenges in securing web applications across hybrid environments:

- **Quality of security:** Most cloud-based security solutions are based on a "negative" security model, using static, manually defined security policies.
- **Varying levels of protection:** Maintaining the same level of protection across platforms is difficult, as each solution has different levels of security.
- **Inconsistent security policies:** Security policies between different environments are incompatible and inconsistent with each other.
- **Point of failure:** Inline WAF deployments invariably add another point of failure to the system. If they go down, all communication to the server is blocked.
- **Increased latency:** Going through third-party cloud networks, external to the public cloud environment, adds traffic hops.
- **Tight coupling between security and delivery:** Most cloud-based WAFs require tight coupling between a CDN and security, reducing operational agility and flexibility.
- **SSL certificate sharing:** Existing tools require the application's SSL certificate, adding management overhead and violating user privacy.
- **Fragmented logging and reporting:** It's difficult to get a view of the threats across platforms.
- **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.

Radware SecurePath™ Architecture

To overcome the challenges of multi-cloud application security, Radware's application security architecture is specifically architected for multi-cloud and hybrid cloud environments to provide comprehensive, consistent and frictionless application protection regardless of where the application is deployed and without interfering with existing business and development processes.

The Radware SecurePath™ architecture provides a number of key advantages that address the challenges of multi-cloud and hybrid-cloud application protection:

- **State-of-the-art security:** Radware provides industry-leading application security based on advanced behavior-based machine-learning algorithms across multiple security modules, including WAF, bot manager, API protection, level -7 DDoS protection, threat intelligence and more.
- **Deployment flexibility:** Radware offers multiple deployment types (either cloud-based inline or API-based out-of-path deployment), and customers can choose whichever architecture they prefer for every application based on their preferred business or technical considerations.
- **Wide variety of supported platforms:** Radware provides native integrators into a variety of common cloud tools and DevOps frameworks, to enable frictionless integration into any environment.
- **Single, centralized application security portal:** Security for all applications, wherever they are, can be managed with full security protections (WAF, bot, API, and so on).

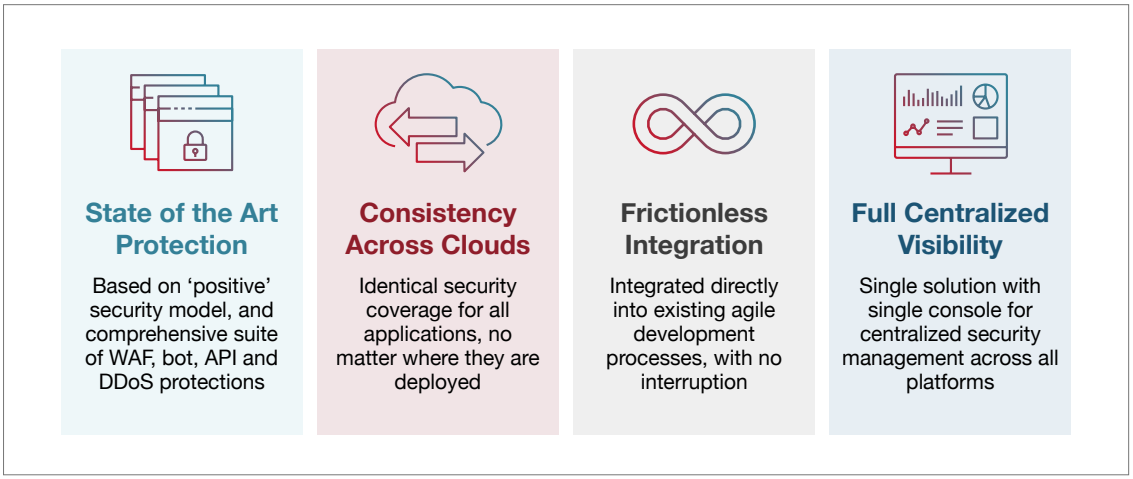


Figure 3

Advantages
Key benefits of Radware's application security architecture

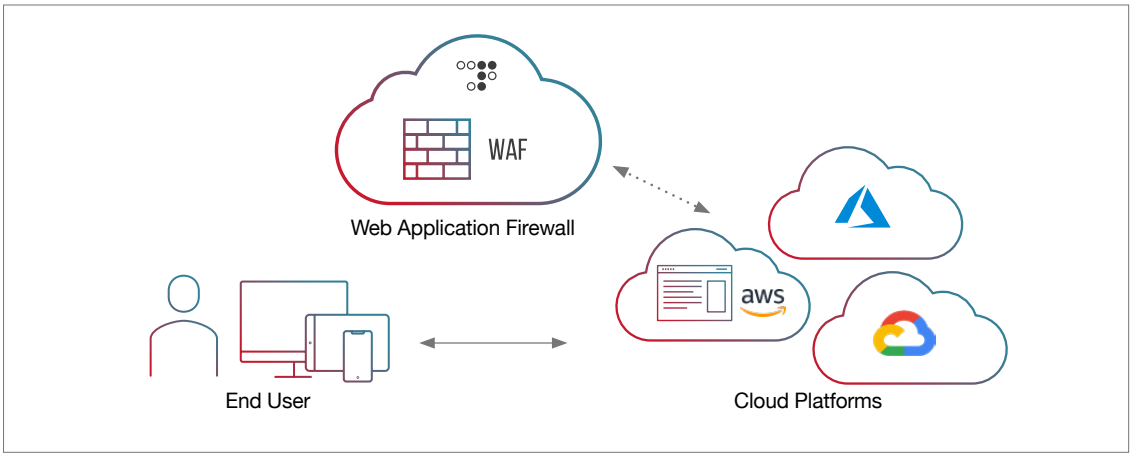
Unique API-Based Architecture

Radware can address these challenges of cross-cloud application protection because the Radware SecurePath™ architecture is uniquely architected for application protection across public, private and hybrid cloud environments.

Radware's solution is deployed as an API-based solution, out of the path of cloud applications to minimize interruption and impact. A software detector monitors application traffic to the origin server. The detector communicates with Radware's analysis engine, which processes its findings and alerts against any malicious traffic. Host transactions are blocked only when malicious traffic is detected.

Figure 4

Radware's API-based architecture



This approach provides several key advantages:

- **No routing changes:** Domain Name System (DNS) and Border Gateway Protocol (BGP) routing changes are not required.
- **No SSL certificate sharing:** Sharing with third-party vendors is not required.
- **Reduced latency:** Requests go from the client directly to the application server without any interruptions, and customers have full control over latency.
- **Increased uptime:** Inline components inherently add a point of failure in the system. As an out-of-path solution, in the event of an outage, the customer won't be impacted.

Application Security as an Enabler for Cloud Migration

By enhancing the level of application security and reducing the level of complexity in managing it, Radware helps organizations in their cloud journey by making application security an enabler for cloud and cross-cloud migration.

Radware removes the key burdens to the process of cross-cloud application security and provides the key capabilities needed for true cross-cloud protection:

- **Consistent security across clouds:** Security coverage for applications is the same, regardless of where the application is deployed.
- **Comprehensive security coverage:** Applications are protected against web application attack vectors, minimizing the risk of a data breach.
- **Centralized visibility for applications:** A single solution with single management allows centralized security management for all applications across platforms.
- **Protection for every environment:** Agnostic to the underlying platform, protection is allowed on premise, in private clouds, in the public cloud, using microservices and more.
- **Easier migration process:** Organizations can migrate applications between platforms without having to worry about losing the quality of security.
- **Customer confidentiality:** There is no need to share SSL keys with third-party vendors, thereby preserving customer confidentiality and meeting compliance requirements.
- **Frictionless deployment:** Security can be integrated directly into existing agile development processes with minimal interruption to DevOps.

Better Security than with Traditional Tools

Radware's approach helps organizations overcome the gaps of traditional application security tools when it comes to hybrid-cloud application security, allowing for better application security with less management overhead:

- **Better protection:** Whereas CDN-based WAF cloud services, as well as IaaS providers' native WAF tools, are based on a "negative" security model with limited security coverage, Radware's solution is based on a combination of "negative" and "positive" security models, allowing for full protection against both known and unknown threats.
- **Coverage against attack vectors:** While the native tools of IaaS hosting providers, as well as WAF virtual appliances, are point solutions that do not provide comprehensive protection against all attack vectors, Radware's solution is a fully fledged application security platform providing protection against WAF, bot, API and DDoS attacks.
- **Centralized management:** Using multiple security tools with multiple management systems creates additional management overhead and interrupts agile development processes. Radware provides full, centralized visibility for all security modules on all applications across platforms from within a single dashboard.

- **Fully managed security service:** Radware's solution is, by default, a fully managed security service, taking the burden off organizations and offloading it to a dedicated team of experts.
- **No routing changes:** Unlike CDN-based WAF services, which require that DNS entries be changes to route all application traffic through their network, Radware's solution is an out-of-path solution that does not require any routing changes.
- **No latency:** Unlike CDN-based WAF services, which route application traffic through third-party CDN networks, thereby adding extra "hops" and additional latency, Radware's solution does not add any latency to customer communications.
- **Enhanced uptime:** Whereas other types of WAF defenses (CDN-based, virtual appliance, IaaS native tools) require that all traffic be routed through them, Radware's solution is deployed out of path, so, in the unlikely event of service interruption, customers won't be impacted.
- **No SSL certificate sharing:** Radware's solution does not require the SSL certificate to be shared with the security vendor, thereby maintaining customer privacy and meeting regulatory requirements.