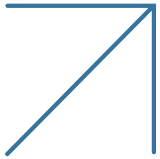


Consistent Cross-Cloud Web Application Protection



Modern organizations run their web applications across multiple environments, deployed across on-premise, private public cloud platforms. The result is a patchwork of application security tools that require either disparate tools with limited security and no central management or external cloud services that add latency and complexity. Radware SecurePath™ offers a unique application protection architecture specifically developed for hybrid environments and the public cloud by providing comprehensive protection against application, bot and API vulnerabilities, centralized cross-cloud management, and no added latency or complexity to multiple environments or cloud deployments.



STATE-OF-THE-ART PROTECTION
Comprehensive, cross-cloud protection with industry-leading WAF, bot management, API, and web application DDoS protection all-in-one



REDUCES LATENCY
Simple, API-based deployment reduces latency and increases uptime



NO TRAFFIC REDIRECTION
No need for DNS routing changes; traffic goes straight to the application server



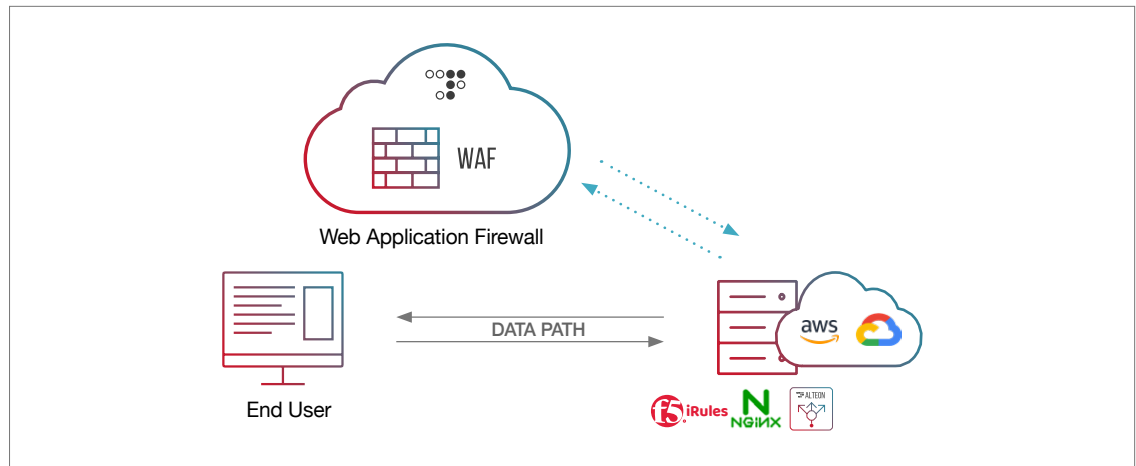
NO CERTIFICATE SHARING
Use the application's native SSL certificates. No need to share keys

Simple, API-Based, Out-Of-Path Deployment

Radware SecurePath™ is uniquely architected for application protection across on-prem, and public, private and hybrid cloud environments. Radware's solution is deployed out-of-path of cloud applications to minimize interruption and impact. An API-based software detector monitors application traffic to the origin server. The detector communicates with Radware's WAF engine, which processes its findings and alerts against any malicious traffic. Host transactions are blocked only when malicious traffic is detected.

Figure 1

API-based out-of-path architecture enhances performance and reduces complexity



State-Of-The-Art Application Security

Radware provides the industry's leading web application security based on a positive security approach. Unlike outdated security tools, which rely on static, manually-defined security policies, Radware uses behavioral-based machine-learning algorithms which learn customer behavior patterns and automatically create custom-tailored security policies to protect them. This enables Radware to provide a higher level of security with fewer false positives.



Comprehensive Protection Against Attacks

Radware's Cloud Application Protection Services offer comprehensive protection against an array of application attack vectors by combining Radware's web application firewall, bot management, API protection solution, and layer 7 DDoS protection into a single platform. This enables organizations to protect cloud applications against any threat.



Consistent Cross-Cloud Security

Radware supports an organization's cloud migration process by enabling it to protect applications deployed in any environment, including on-premise data centers, private cloud and public cloud platforms. This allows organizations to migrate applications between environments while maintaining consistent, cross-platform security with centralized management, reporting and analytics.



Frictionless, Zero Latency Deployment

Radware's solution is designed to be as unintrusive as possible. Radware's out-of-path solution does not introduce any latency, does not require DNS routing changes, and does not impact customer communications. In addition, it can use an application's original SSL certificate so an organization doesn't have to maintain multiple sets of SSL keys (or share them with third parties.)

