Application Delivery with Integrated Cloud WAF Service

Many organizations still need to deploy and protect certain mission-critical applications on-premise. For organizations with limited resources, in-house application protection may leave applications exposed to cyberattacks, while using a fully-managed, cloud WAF service can result in added latency and a suboptimal experience.

Radware's Alteon ADC solution with SecurePath™ provides the best of both options: an integrated, fully-managed Cloud WAF service integrated with Alteon's ADC functionality, requiring no traffic redirection or SSL certificate sharing. It provides state-of-the-art security against application, bot and API vulnerabilities and a visibility/management console.

The Best of Both Worlds
On-premise application delivery and a managed security solution without the complexity of application protection management or traffic redirection

State-of-The-Art Protection
Comprehensive, cross-cloud security with industry-leading WAF, bot and API security

No Traffic Redirection
No need for DNS routing changes; traffic goes straight to the application server, increasing uptime and with no added latency

No Certificate Sharing
Use the application's native SSL certificates; no need to share SSL keys

Simple, Out-of-Path Deployment

Radware Alteon with SecurePath™ plugin delivers a comprehensive solution that provides application delivery and protection for various on-premise scenarios. SecurePath is a plug-in embedded in Alteon ADC for out-of-path communication with Radware's Cloud WAF Service. It analyzes data sent to it and communicates back to Alteon which traffic is legitimate or malicious and which transaction should be blocked, reported, or allowed to pass. Alteon Integrated Cloud WAF enables both monitoring and active protection. Its out-of-path architecture ensures it never becomes a point of failure and provides full control to minimize interruption and maximize the quality of experience.

The SecurePath architecture provides separate management of the ADC functions from the application protection managed services, enabling clear demarcation points between the infrastructure and security teams.

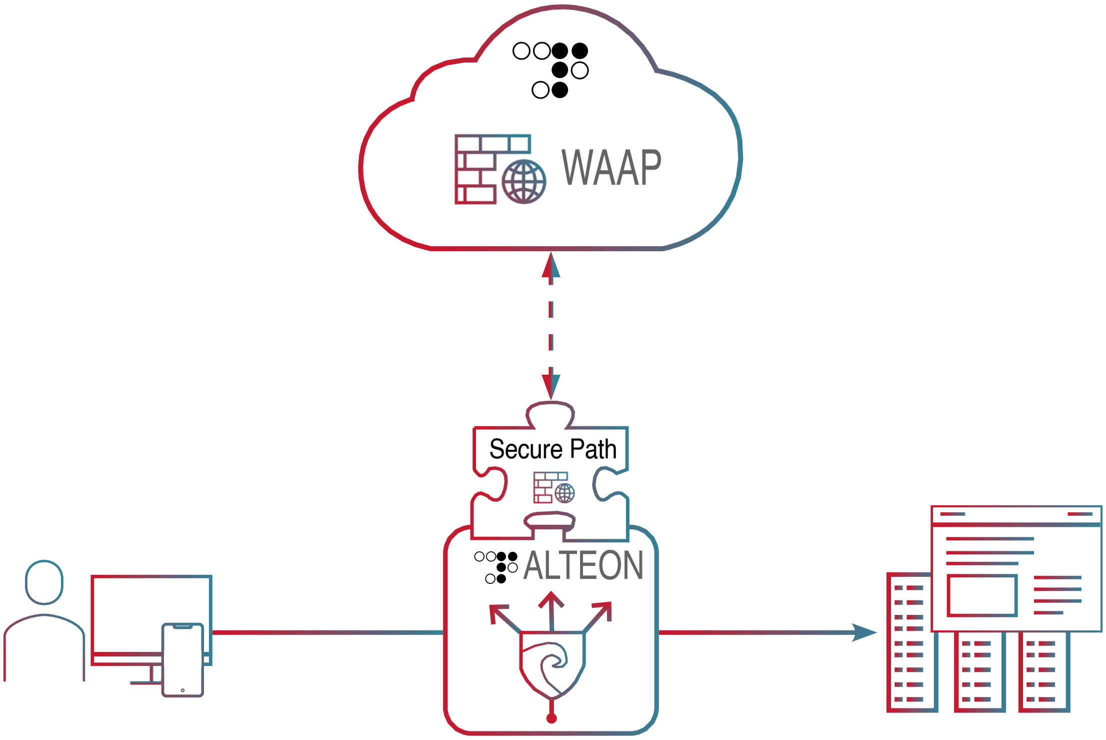

Figure 1

Integrated & managed application protection 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 model. Unlike outdated security tools, which rely on static, manually-defined security policies, Radware uses behavioral-based, machine-learning algorithms to understand customer behavior patterns and then automatically creates 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 security platform offers comprehensive security against an array of application attack vectors by combining Radware's web application firewall, bot management, API security solution and Layer-7 DDoS protection into a single solution. 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 3rd-parties).