Solution Brief

Citrix Web Application Firewall - Proven, Robust Security for your Web Applications

NIST reports that 92% of reported vulnerabilities are in applications rather than in networks. As a result, attacks are becoming more sophisticated as they shift to the application and with hackers getting more creative. CISOs and SecOps teams feel like they are always one step behind. They are looking for a proven, robust solution that is easy to deploy and will protect their applications today and, cater for the rapid evolution of their applications in the future.

Citrix Application Delivery Controller (ADC) provides comprehensive and integrated Layer 3–7 security, including an integrated web application firewall (WAF) to protect your applications. The WAF employs an advanced security model to protect your applications from known and unknown attacks and evolves your security to fend off cyber threats. It offers operational and security consistency across your hybrid multi-cloud environments. Integrations with vulnerability scanning tools enable faster deployments and the integrated nature of the WAF means that traffic can be inspected in a single pass, with fewer devices to manage for faster enforcement, less complexity and a lower TCO. Citrix ADM offers deep visibility and uses machine learning to aid troubleshooting and remediation of issues.

Proven Robust Security

Citrix WAF provides proven, robust security to all your applications types wherever you choose to deploy them. Deployed by many thousands of customers around the globe, the WAF is a mature product, constantly evolving to enhance protection and security performance.

- NSS Labs recommended: In the latest tests by NSS Labs, Citrix WAF blocked 100% of all the attacks and was recommended with the best price-performance of all devices.
- PCI-DSS Compliance: Citrix WAF is used by many customers to ensure they meet their compliance requirements for their payment card transactions.

Protect from Known and Unknown Attacks

Attacks that you've seen before are relatively easy to defend against but threats are constantly evolving and you need to protect against new vulnerabilities. The Citrix WAF employs a hybrid security model to protect your applications from all types of known and unknown attacks.

- **Signatures:** Incoming requests are checked against signatures to detect known attacks quickly and efficiently.
- **Zero-day attacks:** Citrix WAF employs a positive security model that mitigates unknown attacks by monitoring user interactions and learning your application behavior. It also uses AI/ML to detect behavior-based attacks including business logic abuse and Layer 7 DDoS.
- **OWASP top 10:** Protect your applications from all of the attack types highlighted as the most critical security risk by OWASP.

Easier Deployment and Simple to Keep Up To Date

Citrix has made its WAF easier to purchase and deploy than many other vendors. This simplicity enables you to get up and running quickly so that your applications are protected.

- **No additional devices:** Citrix ADC has all the security functionality in a single Premium license. There are no other devices, licenses or services to deploy and manage.
- **Scanning tool integration:** Citrix WAF integrates with the leading vulnerability scanning tools - Rapid 7, IBM, Qualys, White Hat - so you can convert scan results into WAF configurations to set up protections quickly and easily.
- **Dynamic profiling:** It uses a positive security model and automates the deployment of learned rules exceptions to ensure that as your applications change your WAF security will adjust automatically.
- **Portable rules:** A single code base across all Citrix ADC form factors means that defined rules are portable across deployments. You can migrate applications dev/test into production more quickly.
- **Single license:** Citrix ADC offers a single license approach, which includes security features like WAF, bot mitigation and API protection, which brings simplicity and reduces TCO.

Actionable Insights for Faster Remediation

Citrix ADM collates security data from your entire Citrix ADC estate and provides actionable security insight for your applications. Intuitive dashboard highlights anomalies and the interactive nature lets you troubleshoot quickly for faster remediation.

- **Single pane of glass:** Citrix ADM provides holistic visibility of your application security posture from a single point. It is a single tool that spans across all your deployment environments and application types.
- **Violations:** Quickly see the type and volume of attacks on your applications wherever they reside. Drill down into specific applications or attacks to spot issues.
- **Applications:** See immediately, which of your applications are most at risk and prioritize your remediation accordingly.

Flexible and Simple Deployment Options for Multi-Cloud

Citrix WAF is available as part of the Citrix ADC offering and is included with the premium edition license. Citrix ADC is available in multiple form factors and in the major public clouds (AWS, Azure, GCP) to suit your requirements. The single code base across the whole Citrix ADC portfolio enables you to maintain operational consistency across your deployments and applications. This, single license approach, which includes security features including WAF, bot mitigation and API protection, brings simplicity and reduces TCO.

Keeping it simple lets you keep it secure.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States