Continuous Delivery Without Continued Vulnerability

Web application development is becoming more complex, rapid and more vulnerable than ever before. The Radware Cloud WAF Service provides the industry's best web application security by using a positive security model based on machine-learning technologies to provide comprehensive protection coverage against OWASP Top 10 threats and other vulnerabilities. Radware's Cloud WAF Service provides dynamic security policies with automatic false-positive correction, built-in DDoS protection, integrated bot mitigation and many other features to help protect organizations against the risk of data loss.

COMPLETE PROTECTION

Radware provides the industry's best web application protection based on a positive security model for full coverage against OWASP TOP-10 threats and more

FASTER TIME TO SECURITY

Radware's advanced automation technologies instantly detect attacks, respond on-the-fly and reduce exposure for organizations

REDUCED OVERHEAD

Radware's automated WAF defenses and expert managed services take the burden off IT teams and provide better security with lower overhead

SINGLE PANE OF GLASS

Radware offers an integrated security solution which provides multi-vector web application protection with centralized management and reporting

SC AWARDS 2017 WINNER Honored in the U.S.

ICSA labs An Independent Division of Verizon Business

NSS LABS SECURITY RECOMMENDED

Cloud Computing 2017

How Radware Keeps You Agile and Secure

Automatic Traffic Learning

Radware uses advanced machine-learning algorithms that analyze traffic, learn what constitutes legitimate behavior and automatically block malicious activity

Application Mapping

Radware automatically maps protected applications, detects code changes whenever new features are added or modified, and identifies potential vulnerabilities

Adaptive Policies

Radware continuously adapts security policies to optimize coverage to applications' threat profile to maximize security coverage and reduce false positives

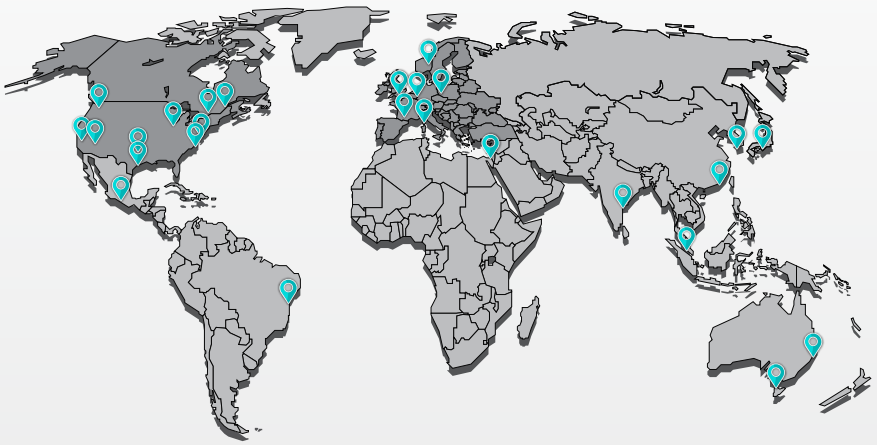
The Only Cloud WAF for Full PCI Compliance

Radware Cloud WAF Service is the only cloud WAF service which fully implements all 10 recommended security mechanisms of PCI-DSS Requirement 6.6, including enforcing a Positive Security Model and implementing Data Leakage Prevention (DLP) controls. Radware's Cloud WAF is also PCI-DSS certified and based on NSS Labs and ICSA Labs certified technology, meaning customers can deploy Radware's Cloud WAF Service with full confidence for maximal compliance.

PCI DSS COMPLIANT

Global Presence, Right Next to Your Origin Server

Radware's Cloud WAF Service is based on a global network of distributed WAF Points of Presence (PoPs), making sure that you are always protected from the closest point to your origin server. Radware's Cloud WAF PoPs are located at major traffic hubs with connections to Tier 1 ISPs, ensuring low latency and minimal impact on web application performance.



Service Features of Radware Cloud WAF Service

Complete Protection against OWASP TOP-10 Threats

- Based on a positive security model which uses advanced behavioral-analysis technologies to detect malicious threats
- Built-in DDoS protection to stop both network- and application-layer DDoS attacks
- Bot mitigation using advanced IP-agnostic device fingerprinting to identify malicious bots based on unique device characteristics
- Data leakage prevention mechanisms to automatically mask sensitive user data such as Personally Identifiable Information (PII)

Increased Agility for Continuous Delivery

- Fully-managed security service by Radware's expert Emergency Response Team (ERT), one of the industry's largest and most experienced security teams
- Dedicated Technical Account Manager (TAM) who serves as a focal point for all issues, including configuration, integration, upgrades and attack mitigation
- Continuously adaptive policies that automatically map applications, detect changes in them and dynamically deploy the optimal security policy
- Automatic false-positive correction using powerful machine-learning algorithms that identify legitimate application behavior

Flexibility in Deployment

- Support for high-capacity SSL traffic to ensure full SSL availability from the nearest PoP, even during peak times
- Global CDN service based on anycast-based routing and massive capacity of 30+ Tbps across 100+ PoPs
- Advanced load-balancing capabilities, including both local and global site load balancing (GSLB), site-failover, high-availability and health monitoring
- Extensive compliance and certifications capabilities, unparalleled by any rival, including industry-specific certifications such as PCI and HIPAA, as well as cloud security standards such as ISO 27001, ISO 27017, ISO 27018, ISO 27032 and others

Easy Management & Control

- Rich centralized dashboard to display threats and manage configuration
- Granular alerting capabilities to make sure that you're the first to know if something happens
- Easy-to-read executive reports with concise incident details
- Centralized reporting for both WAF and DDoS protection

©2018 Radware Ltd. All rights reserved. Radware and all other Radware product and service names are registered trademarks or trademarks of Radware in the U.S. and other countries. All other trademarks and names are property of their respective owners. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications. For more details please see: https://www.radware.com/LegalNotice/