

## Why Radware Security for Azure?

Radware Security for Azure is a fully managed security service jointly developed with Microsoft Azure. The service integrates the Azure DDoS service with Radware’s cloud-delivered WAF technology, bot management capabilities, security analytics, threat detection and real-time security feeds in a single security portal. Radware Security for Azure provides the industry’s most complete web application security solution, protecting applications against hacking, malicious bots, API exposure, DDoS attacks and other vulnerabilities.

Member of  
**Microsoft Intelligent Security Association**



### FULLY MANAGED SECURITY SERVICE

24x7 access to WAF experts who build, proactively monitor and fine-tune WAF policies against known and emerging threats in real time



### PROTECTION FOR EVERY THREAT SURFACE

A fully integrated security suite based on Radware’s WAF, Bot Manager and threat intelligence feeds combined with application and volumetric DDoS protection



### INSTANT APP DEPLOYMENT WITH OPTIMIZED SECURITY

Unique auto-policy generation technology designed to secure a web application automatically with little or limited user interaction

## Radware Security Solution Components



**Global Azure Region Deployment** — Radware’s security suite is delivered within Azure regions, providing automated and frictionless deployment at Azure scale sets. Running within Azure regions provides ultra-low latency based on Azure’s global network with data residing in Azure regions to maintain customer data residency requirements.



**Web Application Firewall** — A WAF delivered within Azure for protection against OWASP Top 10 threats and zero-day web attacks using both a negative (signature-based) and positive security model with automatic security policy generation and adaptive security policies



**Bot Detection and Defense** — Advanced bot management solution using semisupervised machine learning to protect against new generations of bots that simulate human behavior and get past traditional bot defenses



**Security Analytics** — Sophisticated security analytic capabilities that analyze user behavior and provide granular insight into user and attacker behavior, so your organization knows what is happening within your applications



**Threat Intelligence** — Integrated with Radware’s threat intelligence and active attacker feeds, providing the latest real-time data on your risk profile — stopping attacks and attackers before they target your applications

**Radware is a market leader in application availability and cybersecurity solutions for virtual, cloud and software-defined data centers.**

**Trusted and Proven** — Over 12,500 enterprise and carrier customers, including:

▶ 8 of the world’s top 12 stock exchanges

▶ 10 of the world’s top 20 commercial banks

▶ 5 of the world’s top 10 retailers

▶ All 10 of the world’s top 10 carriers

▶ 5 of the top 10 SaaS providers

## Industry Recognized

**Gartner™**  
Web Application  
Firewalls Magic  
Quadrant Visionary,  
September 2019

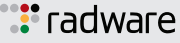

**Frost & Sullivan**  
2019 WAF & DDoS  
Vendor of the Year

**IDC**  
DDoS Prevention  
Solutions Leader,  
2019

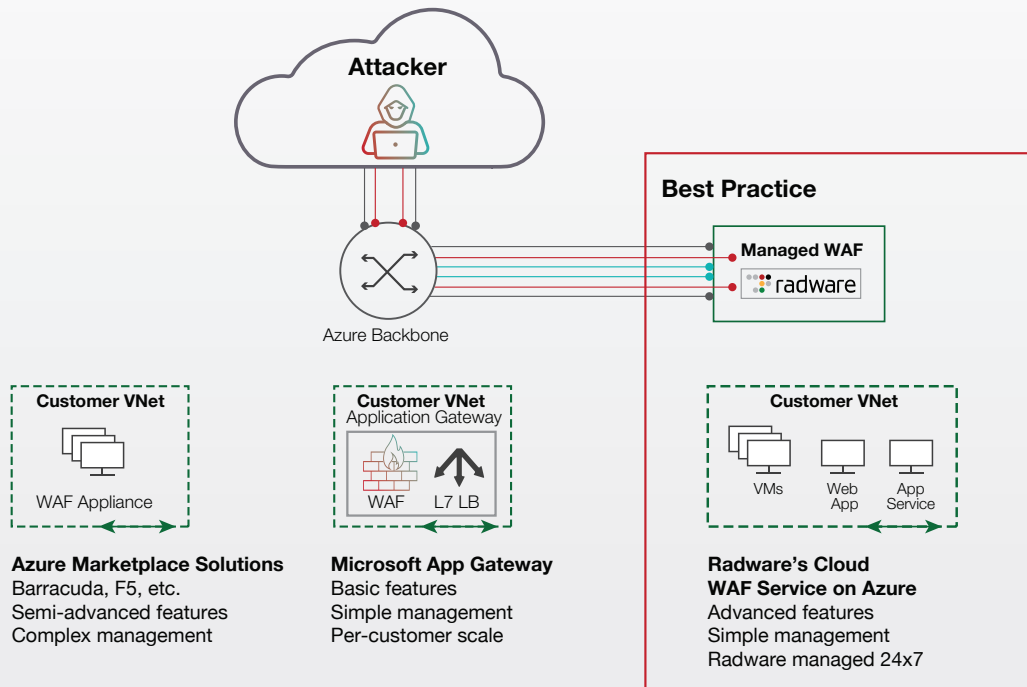
**Forrester™**  
2018 Web Application  
Firewalls Wave  
Strong Performer,  
2018 Bot Management  
Wave Leader

**Cloud Computing**  
2018 Winner  
Cloud Computing  
Product of the Year

## Competitive Feature Comparison

|   | Radware Security for Azure  | Azure Native WAF   | WAF as a Service on Azure | Azure-Based WAF Appliances |
|---|---|--|---------------------------|----------------------------|
|   |  |  |                           |                            |
| Deployed directly within Azure                        | ✓   | ✓  | ✓                         | ✓                          |
| Fully managed security service                        | ✓   | ✗  | ✗                         | ✗                          |
| Positive security model                               | ✓   | ✗  | ✗                         | Some solutions             |
| Automatic traffic learning and auto-policy generation | ✓   | ✗  | ✗                         | Some solutions             |
| Fast, low-touch deployment                            | ✓   | ✗  | ✓                         | ✗                          |
| Integrated threat intelligence                        | ✓   | ✗  | Some solutions            | ✗                          |
| Advanced bot management                               | ✓   | ✗  | Some solutions            | Some solutions             |

## Reference Architecture



## With Radware Security for Azure, You Can:

**Secure critical application workloads in Azure** with fully managed security services

**Use it in the cloud and on-premise**, with security services available in data centers and private and public cloud environments in Azure

**Use the *only* Azure-based managed security suite** operating within Azure regions to provide ultra-low latency and simplified regulatory compliance

---

### Target Industries:

**Retail** organizations that must comply with payment card industry (PCI) regulations

**Financial services** that store sensitive customer financial data

**Healthcare organizations** that protect sensitive patient data

**SaaS/technology/entertainment/gaming/education affiliations** that protect online services and intellectual property

---

### Resources and Contacts:

[Get started](#) with more information, and schedule a demo

[Radware cloud WAF technology overview](#)

[Radware Security for Azure](#)

---

#### Radware Sales Connection:

E: [azurealliance@radware.com](mailto:azurealliance@radware.com)

#### Microsoft Alliance Contact:

Ricky Mehta, Program Manager

E: [ricky.mehta@radware.com](mailto:ricky.mehta@radware.com)

P: 530-305-5625

### About Radware

**Radware®** (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit [www.radware.com](http://www.radware.com).

Radware encourages you to join our community and follow us on: [Facebook](#), [LinkedIn](#), [Radware Blog](#), [Twitter](#), [YouTube](#), Radware Mobile for [iOS](#) and [Android](#), and our security center [DDoSWarriors.com](http://DDoSWarriors.com) that provides a comprehensive analysis of DDoS attack tools, trends and threats.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2020 Radware Ltd. All rights reserved. Any Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are the property of their respective owners.