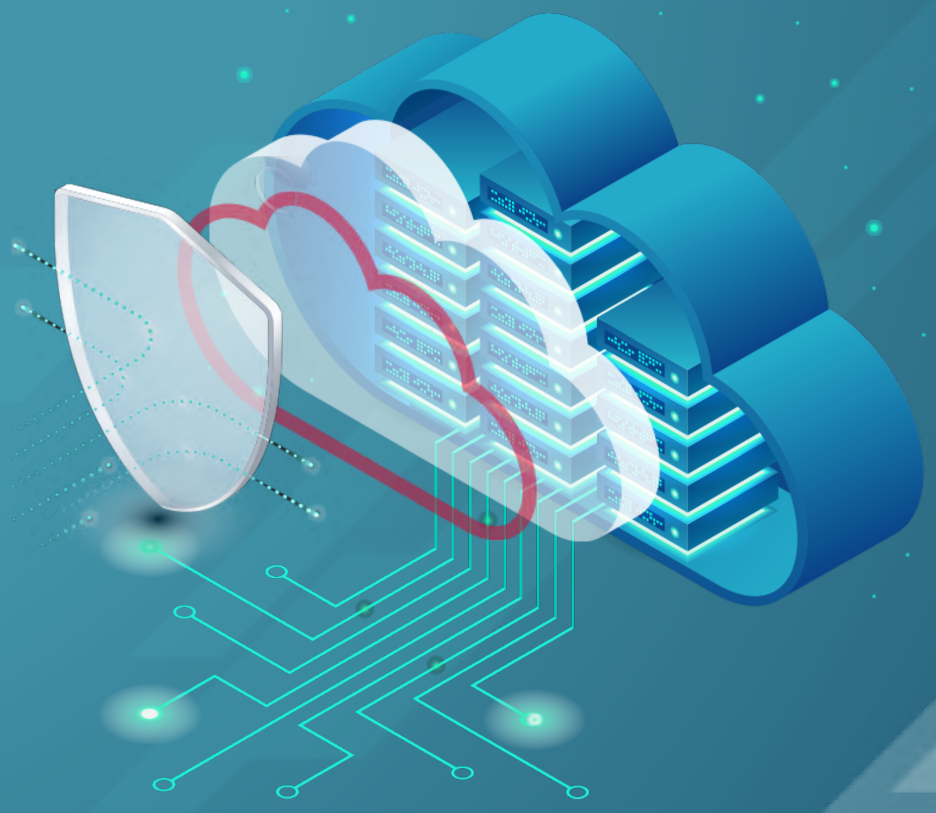
Web Application Security in a Digitally Connected World



radware | Microsoft Azure

Member of

Microsoft Intelligent Security Association

Microsoft

Microsoft Intelligent Security Association comprises a select group of premium security vendors like **Radware** who each contribute-to and benefit-from various Microsoft security products in order to improve the protection and usability of their products for mutual customers in Azure.

Why Radware?

Radware is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. Our solutions have been recognized by Gartner, IDC, Forrester Research and Frost & Sullivan for helping organizations protect sensitive data, build trust with consumers, and grow their businesses through a secure customer experience.

Keeping Modern Applications Secure

The State of Application Security

Today, applications are not just web-based. Web or mobile, homegrown or open-source, premise-based or cloud-hosted, monolithic or microservice applications, APIs and (in the latest architectures) even individual functions must be synchronized and supervised, as they all create, modify and process our data.

New technologies and frameworks bring new challenges to the application development life cycle. Serverless architecture, containers and the Kubernetes ecosystem are getting traction, boosting agility and efficiency and reducing time to market for new applications, features and services.

In cloud-native apps, the focus is on continuous integration and deployment, which makes it difficult for security teams to identify and mitigate risks.

Traditional security tools can’t match the sheer velocity, scale and dynamics of cloud-native applications.

The Application Threat Landscape

Application vulnerabilities are now the fastest-growing cybersecurity threat to organizations, according to a year-over-year comparison of Radware's annual Global Application & Network Security Report.

Applications, and the APIs they leverage, must be protected against an expanding variety of attack methods. In addition, DevOps and Agile development practices mean that applications are in a state of constant flux, and security policies must adapt to keep pace.

Web application security solutions must be smarter and address a broad spectrum of vulnerability exploitation scenarios. On top of protecting the application from these common vulnerabilities, they have to protect APIs and mitigate denial-of-service (DoS) attacks, manage bot traffic and make a distinction between legitimate bots (search engines, for instance) and bad ones, like botnets, web scrapers and more.

According to Radware's The State of Web Application Security report, only 33% of organizations say that their WAF mitigates all types of web application attacks.

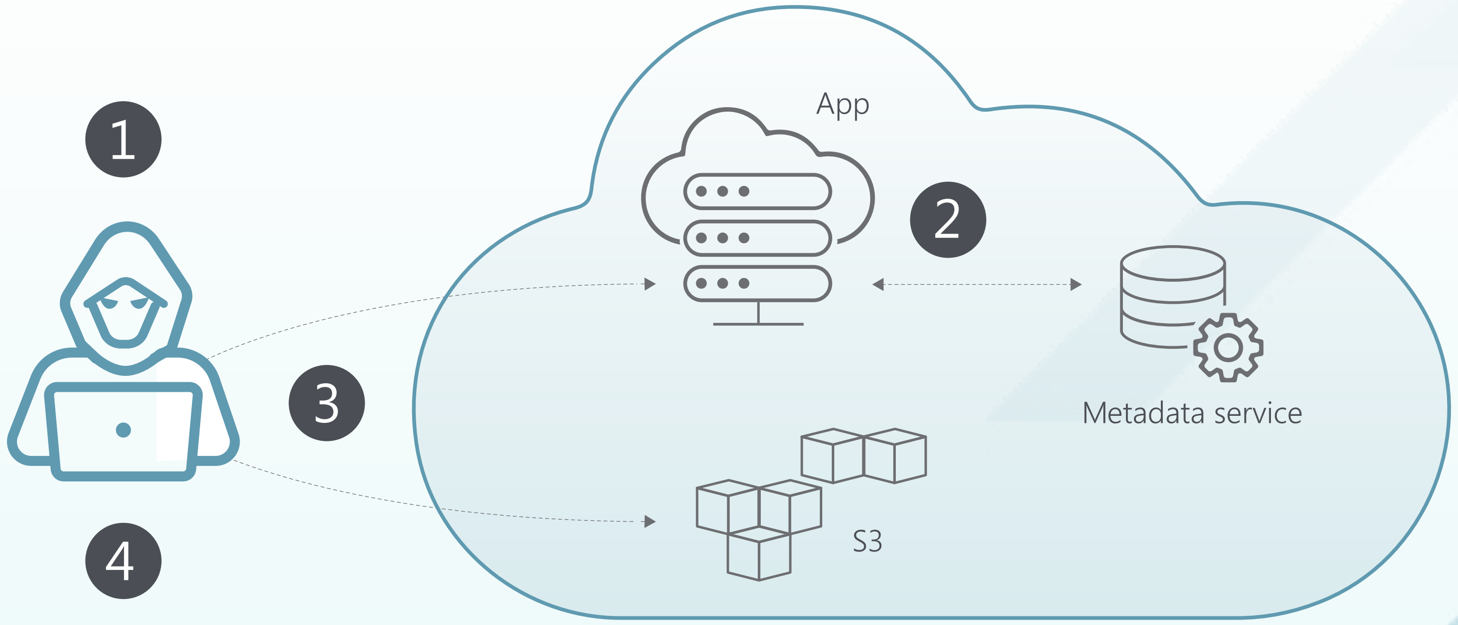
A Cloud-Native Application Breach Timeline

1. **A point of access is compromised.** This could be achieved in several ways, including a spear-phishing attack to steal legitimate credentials or a zero-day vulnerability (a weakness that you have not yet identified, but the attacker has already found and exploited).

2. **The attacker fortifies access, so the original break-in tactic is not needed every time.** One way they do this is by creating API access keys with full administrative access. Reconnaissance is then easy.

3. **The attacker searches for the most valuable data,** mapping out what permissions are granted and what actions this role allows.

4. **The attacker now exploits access at will** and could duplicate and exfiltrate the master user database and expose it to the outside world with public permissions, sell private data or even sell access to your systems to other criminals. Your data is now the attacker's candy store.



Encrypting data is no longer enough to stop hackers.

Hackers continue to use injections, cross-site scripting (XSS) and a few old techniques such as cross-site request forgery (CSRF), remote file inclusion/local file inclusion (RFI/LFI) and session hijacking to exploit these vulnerabilities and gain unauthorized access to sensitive information. Protection is becoming more complex because attacks come through trusted sources such as a content delivery network (CDN), encrypted traffic or application programming interfaces (APIs) of systems and services that we integrate with.

Threat actors, like automated bots, behave like real users and bypass challenges such as CAPTCHA, IP-based detection and others, making it even harder to secure and optimize the user experience.

Most common application attacks in the last 12 months[1]

50%	Encrypted web attacks (SSL/TLS based)
46%	Data security breaches
39%	Web scraping
34%	HTTP/Layer 7 distributed denial-of-service (DDoS) attacks
34%	API manipulations
34%	SQL injections
32%	Cross-site scripting
24%	Credential stuffing/credential cracking
11%	None of these/no attacks experienced

[1] Percentage of survey respondents to Radware's second annual global survey for web application security who indicated how often their organizations' applications or web servers are attacked. Most said that attacks happened weekly, and at least a quarter of the organizations reported attacks on a daily basis. Radware Research — The State of Web Application Security.

Five Biggest Challenges to Keeping Modern Applications Secure

CHALLENGE 1

Protection Beyond Fundamental Application Protection

The OWASP Top 10 list provides a starting point for ensuring protection from the most common and virulent threats—application misconfigurations that can lead to vulnerabilities, and detection tactics and mitigations. This list serves as an industry benchmark for the application security community and defines the basic capabilities required from a WAF to protect from common attacks like injections, cross-site scripting, cross-site request forgery, session hijacking and others.

There are innumerous ways to exploit these vulnerabilities, and WAFs should be able to protect beyond the OWASP Top 10 for security effectiveness.

Vulnerability protection is just the beginning. Advanced threats mean that application security solutions must do much more.

CHALLENGE 2

Bot Management and Protection

According to Radware's annual bot management report, almost 60% of internet traffic is bot-generated, half of which is attributed to "bad" traffic. Organizations invest to increase network capacity, ultimately accommodating fictitious demand.

Bot-generated attacks targeting web application infrastructure are increasing in both volume and scope, with the list of attack vectors growing in support of a variety of objectives.

Among the most common:

- Web attacks, such as SQL injections and Cross-Site Request Forgery (CSRF)
- Web scraping
- Application DDoS, brute-force attacks on login pages for password cracking, comment spammers, clickjacking and fraud.

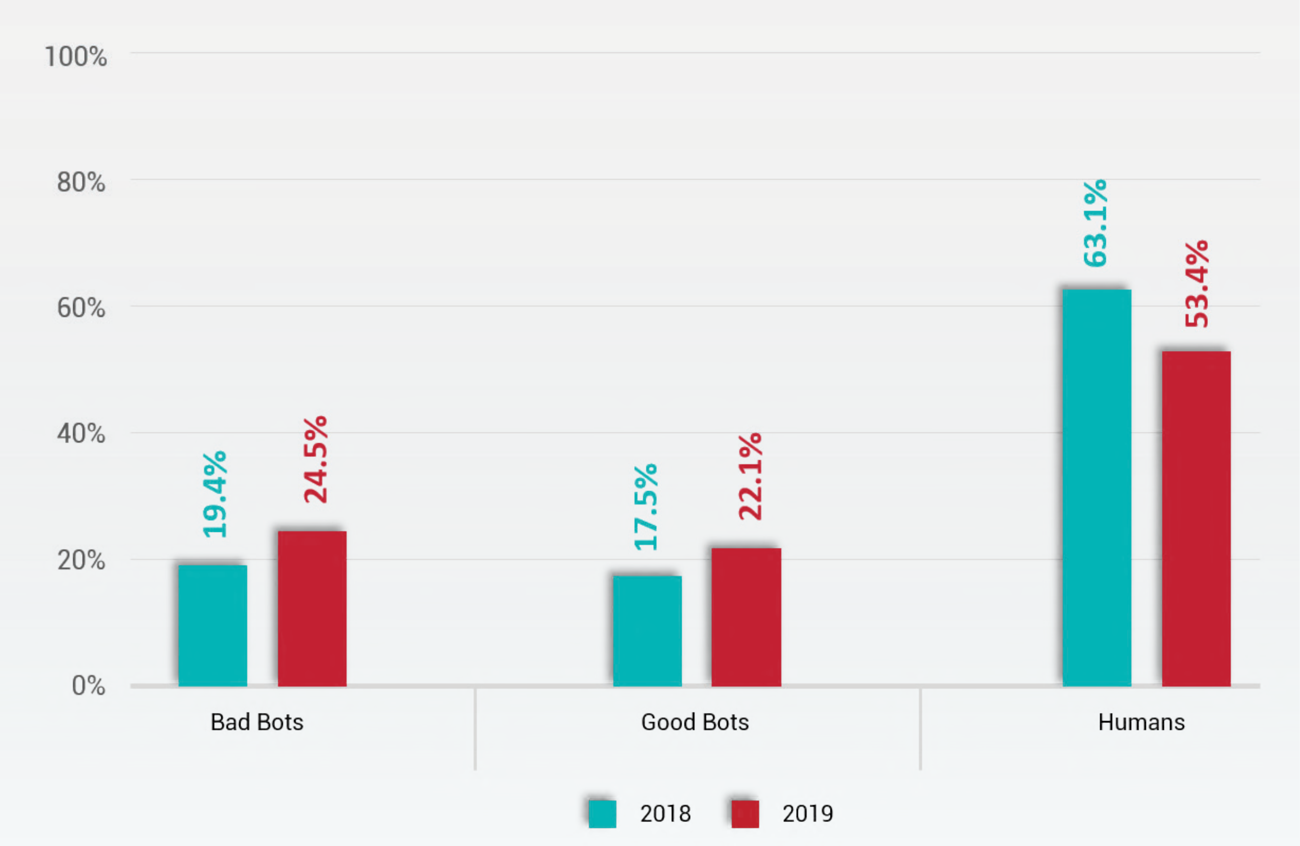
Some bot-generated attacks are static; others are dynamic over time.

Simple, script-based bots are not much of a challenge to detect and block. The same cannot be said of more advanced bots. Those based on headless browser technology, such as PhantomJS, dramatically complicate the detection process by mimicking user behavior, passing challenges (such as CAPTCHA) and serving up dynamic IP addresses.

One of the most important weapons in the bot battle is IP-agnostic bot detection. Successful detection of attack source requires correlation across sessions. That is because bot-generated traffic may seem harmless—even legitimate—at a discrete, HTTP transaction level.

However, the continuous nature of these attacks makes them a clear risk.

Accurate distinction between human traffic and bot-based traffic, and between "good" bots (like search engines and price comparison services) and "bad" bots, can translate into substantial savings and an uptick in customer experience.

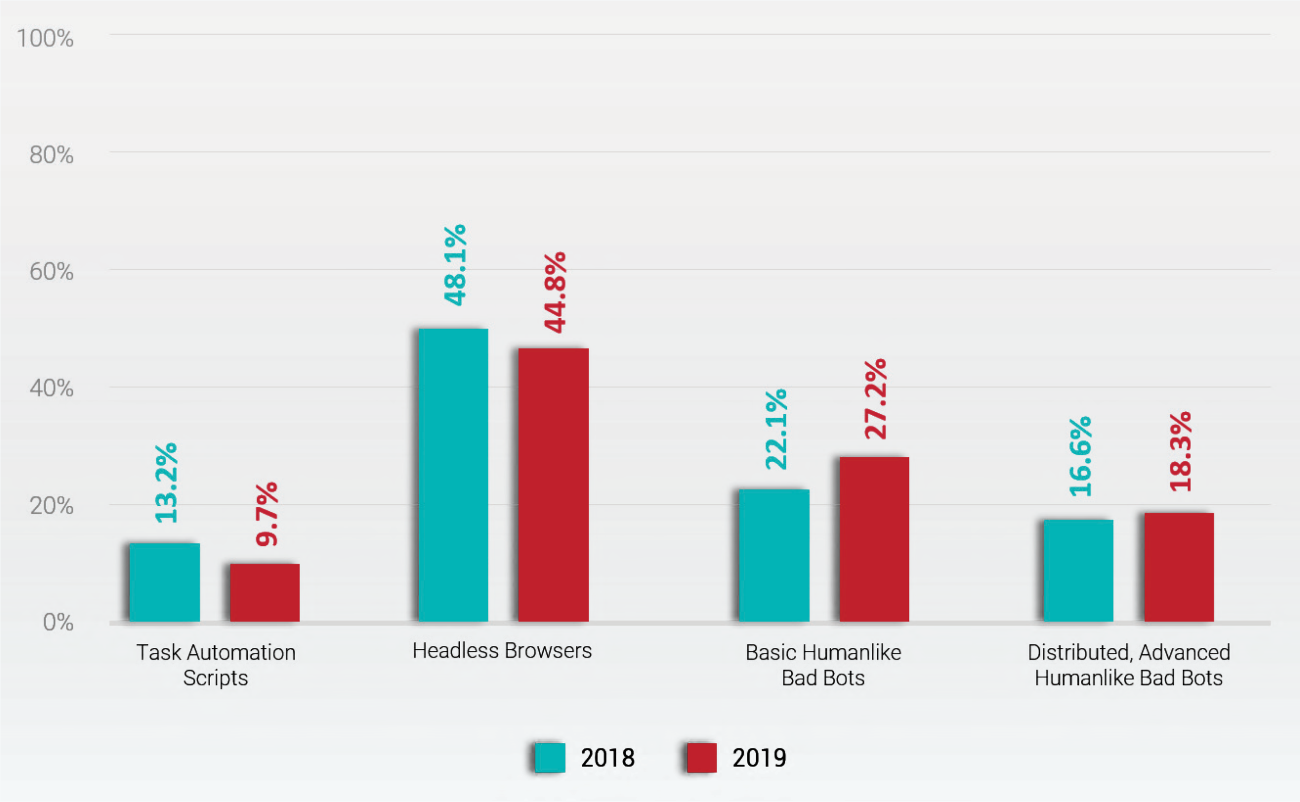


Distribution of Internet Traffic

In 2019, overall bot traffic grew 24% in comparison to 2018. Bad bot traffic accounted for a quarter (24.5%) of the total traffic.

In Q4 when more people shop online, bad bot traffic spiked to 29.3% of the total internet traffic.

Radware Research — The Big Bad Bot Problem



The Increasing Sophistication of Bad Bots

In 2018, the third and fourth generations of bad bots accounted for 22.1% and 16.6% of internet traffic, respectively. In 2019, the number reached 27.2% and 18.3%, respectively.

Radware Research — The Big Bad Bot Problem

CHALLENGE 3

Securing APIs

Many applications gather information and data from services that they interact with via APIs. When transferring sensitive data via APIs, more than 50% of organizations neither inspect nor protect APIs to detect cyber-attacks. Common API use cases are:

- IoT integration
- Machine-to-machine communication
- Serverless environments
- Mobile applications and event-driven applications

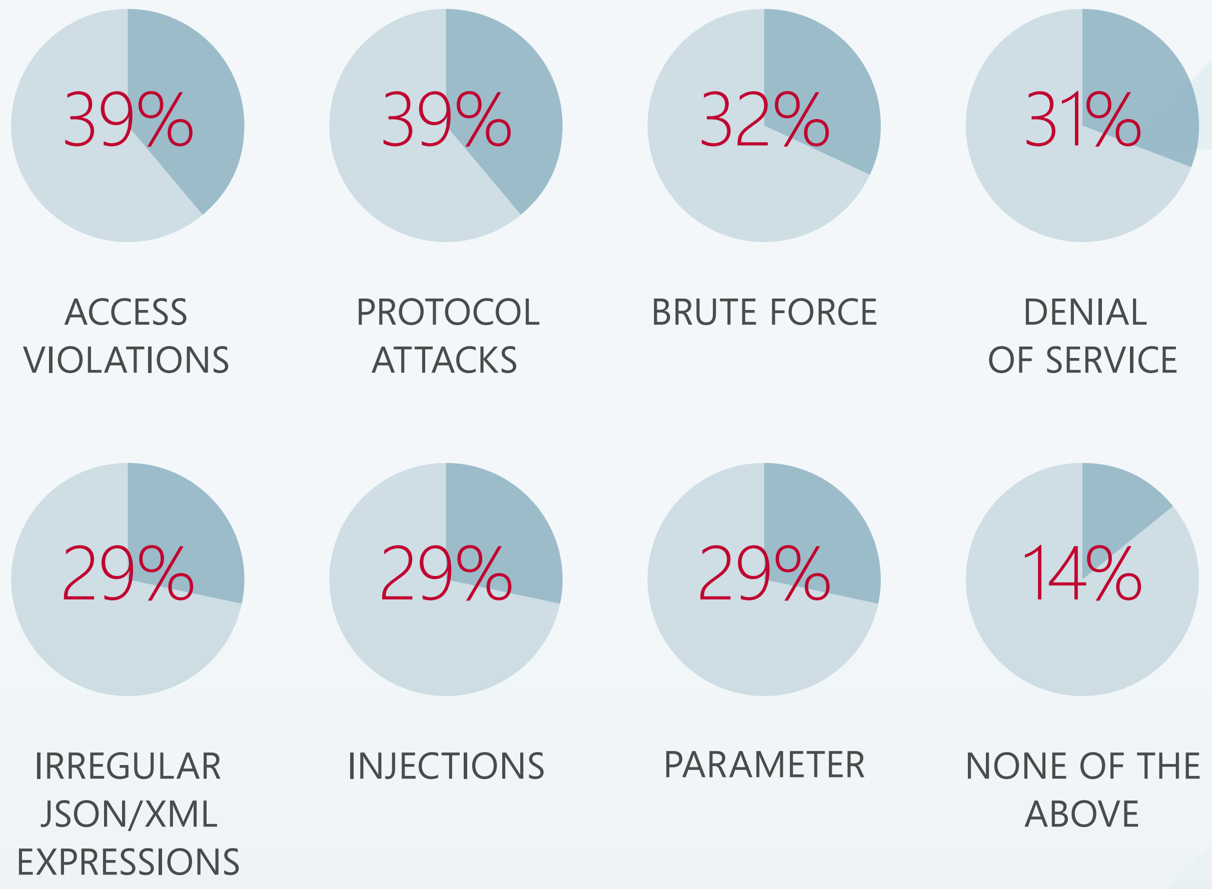
API vulnerabilities are similar to those of applications and include injections, protocol attacks, parameter manipulations, invalidated redirects and bot-generated attacks.

Dedicated API gateways evolved to secure the interoperability of application services that interact via APIs. However, they do not provide the end-to-end application security that a WAF can, with the necessary security controls such as HTTP parsing, Layer 7 ACL management, parsing and validation of JSON/XML payload and schema enforcement, and full coverage of the OWASP Top 10 vulnerabilities.

This is accomplished by extracting and inspecting key API values using both positive and negative models.

7 Common Attacks Against APIs

Access violations and protocol attacks led the list among organizations that have experienced API attackes in the past 12 months.



The Ever-Evolving Threats

Attackers constantly develop effective techniques to cause harm.

91%	49%	29%	26%
APPLICATION LAYER	RECURRING BURSTS	IoT BOTNETS	ENCRYPTED DDoS ATTACKS

49% IMPACT THE INFRASTRUCTURE

CHALLENGE 4

Denial of Service Attacks

Different types of application-layer DoS attacks are still very effective at taking down application services. Examples of attacks include HTTP/S Floods, low and slow attacks (Slowloris, LOIC, Torshammer), dynamic IP attacks, buffer overflow, Brute Force attacks and more.

Driven largely by IoT botnets, application-layer attacks have become the preferred DDoS attack vector.

CHALLENGE 5

Continuous Security

In DevOps, agility is often valued at the expense of security. Agile development and rollout methodologies result in applications being continuously modified and updated.

In such a fluid environment, it is difficult to frequently update security policies to safeguard sensitive data without creating a high number of false positives. It is a task beyond the abilities of any security expert, as the error rate and additional operational costs imposed can be enormous.

Machine learning security solutions are key, as they can map application resources, analyze possible threats and create and optimize security policies in real time.

Five Characteristics that Make Radware Cloud WAF-as-a-Service for Microsoft Azure the Right Choice

Member of
Microsoft Intelligent Security Association
Microsoft

1. Fully Managed WAF Service

TWO MINDS ARE BETTER THAN ONE

Cyberattacks are increasing in severity and complexity, making it difficult for organizations to stay ahead of the evolving threat landscape. Radware Cloud WAF-as-a-Service for Azure is fully managed and monitored globally with 24x7 proactive security services provided by Radware security experts to ensure service availability.

Unlike other WAF instances, products or services available in the Azure Marketplace, Radware's Emergency Response Team (ERT) assumes full responsibility for configuring and updating security policies, as well as detecting, alerting and mitigating attacks. A group of security experts are available 24x7 to provide proactive security support services for customers facing an array of application- and network-layer attacks, such as injections, remote scripting, unauthorized access and DoS attacks.

Powered by Radware's Threat Research Center, ERT engineers combat common and emerging attacks on a daily basis, providing customers with industry-leading expertise, best practices and a deep knowledge of threats, attack tools, intelligence and mitigation technologies.

2. Coverage Beyond OWASP Top 10

THE WIDEST WEB APPLICATION SECURITY COVERAGE

Radware's Cloud WAF-as-a-Service for Azure offers automated protection policies for individual applications and APIs based on rapid learning mechanisms, providing complete OWASP Top 10 coverage and beyond, including advanced fingerprinting technology to detect and mitigate sophisticated bots and market-leading DDoS protection.

3. Comprehensive and Accurate Security Coverage

POSITIVE + NEGATIVE = ZERO-DAY PROTECTION

Radware's Cloud WAF-as-a-Service offering delivers comprehensive and accurate security coverage of known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP top-10 threats, including injections, cross site scripting (XSS), broken authentication, leakage of sensitive information and session management. It offers security coverage for additional attacks and threats beyond the OWASP Top 10 list such as Web Application Security Consortium (WASC) threats.

By effectively providing defenses against known and unknown attacks and attackers, Radware improves and maximizes web application security.

The most effective security coverage with minimal impact on legitimate traffic is made possible by Radware's combination of negative (defining what's forbidden and accepting the rest) and positive (defining what is allowed and rejecting the rest) security models. Combining the two models allows granular and accurate policy definitions, thereby avoiding false positives and false negatives.

The negative security model protection is based on up-to-date signatures against known vulnerabilities which provide the most accurate detection and blocking technology of web application vulnerability exploits. The positive security model is useful in stopping zero-day attacks. The positive security rules and mechanisms allow definition of value types and value ranges for all client side inputs, included encoded inputs and within structured formats as XMLs and JSONs.

4. Learn and Protect:

AUTO-POLICY GENERATION AND API SECURITY

DevOps and agile development practices are great for creating new applications quickly and efficiently. Unfortunately, the fluidity of these environments also creates a bevy of unintended security risks. Radware's WAF technology incorporates machine-learning algorithms to keep web assets protected always, even while applications constantly change and threats rapidly evolve, assuring web security is future proof.

The Auto Policy Generation mechanism provides the best tool for automatically generating security policy for the secured Web application.

The Auto Policy Generation module will automatically utilize the required security filter, create security filter rules and switch the security filters into active mode. These operations would normally require many manual refinements. Building a security policy usually demands intensive work on the part of the administrator, while still leaving a system potentially open to attack due to inherent human error.

By leveraging machine-learning algorithms, Auto Policy Generation is designed to secure a web application as automatically as possible with little or limited user interaction. There are different attributes of the secured application, the environment needs that impact the process of policy generation.

The system automatically discovers the structure of a web application, while at the same time, Auto Policy Generation sets the relevant security filters, analyzes traffic properties from the application environment and builds a dynamic security profile according to which the Auto Policy Generation module automatically builds and deploys the security policy.

5. Protecting from Bad Bots:

GRAB THE BOT BY ITS SOURCE

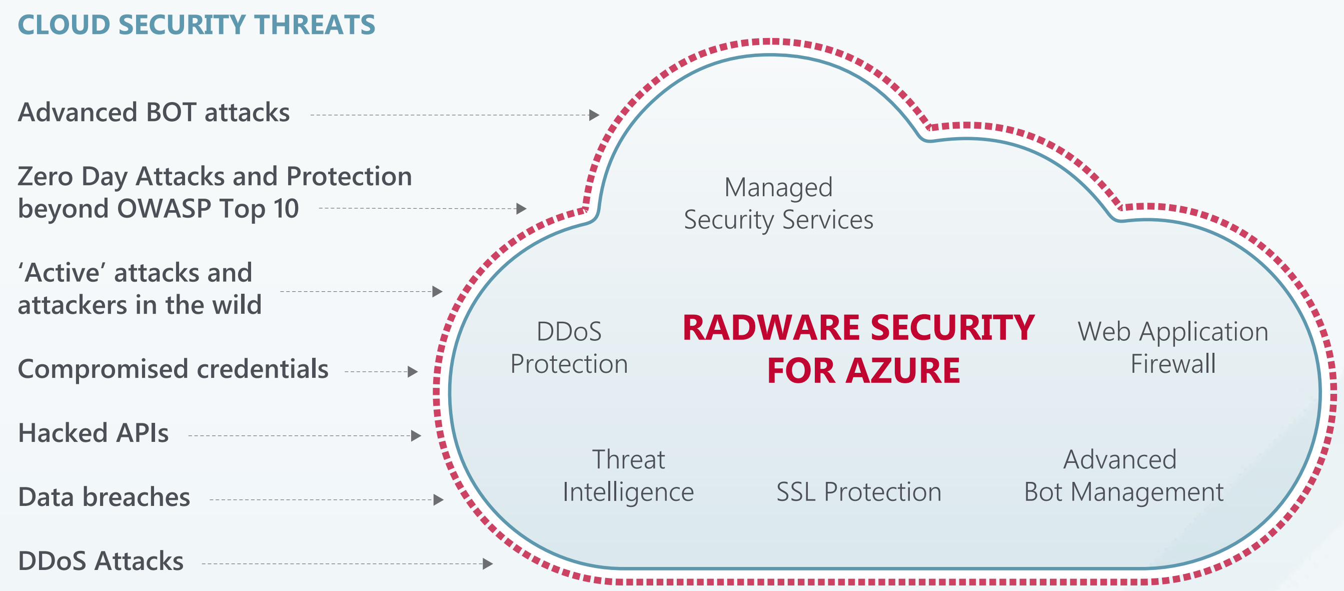
Bots, crawlers and spammers, using new techniques to disguise malicious traffic, can exhaust resources and scrape sensitive information from websites or cloud-based assets. Radware's WAF technology leverages a unique combination of intent encoding, intent and adaptive learning techniques and device reputation algorithms to employ IP-agnostic device fingerprinting methods for bot detection and blocking.

Bots can accelerate business processes and perform tedious tasks; however, malicious bots are using new techniques to take over accounts, steal data and scrape sensitive information from websites or cloud-based assets.

Radware's WAF technology leverages a unique combination of device fingerprinting, activity tracking, event correlation and violation scoring to employ IP-agnostic methods for bot detection and blocking with high accuracy. IP-agnostic fingerprinting and intent-based deep behavioral analysis enable precise bot activity tracking over time and development of IP-agnostic device reputation profiles to identify, blacklist and automatically block the bots used for attacks, regardless of the IP they hide behind.

Complete Protection Against Cloud Security Threats

FULLY MANAGED WAF-AS-A-SERVICE



CLOUD SECURITY THREATS

Advanced BOT attacks

Zero Day Attacks and Protection beyond OWASP Top 10

'Active' attacks and attackers in the wild

Compromised credentials

Hacked APIs

Data breaches

DDoS Attacks

Managed Security Services

DDoS Protection

RADWARE SECURITY FOR AZURE

Web Application Firewall

Threat Intelligence

SSL Protection

Advanced Bot Management

Radware provides the most comprehensive fully managed security service in Azure—a complete suite of protection that offers:

Security Services delivered within Azure regions globally providing automated and frictionless deployment at Azure scale. 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.

Protection from DDoS attacks on the network and application layers, volumetric, non-volumetric, SSL attacks and Advanced BOT attacks.

A Web Application Firewall for application security that provides protection against the OWASP Top 10 threats and beyond; while preventing zero-day web attacks using both a negative signature-based security model and positive security model with automatic security policy generation and continuously adaptive security policies.

Advanced bot management solution, using semi-supervised machine learning to protect against new generations of bots that simulate human behavior and get past traditional bot defenses.

Sophisticated security analytics capabilities, which analyze user behavior and provide granular insight into user and attacker activities, so you always know what is happening within your applications across a distributed environment.

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 application.

Neutralize the Application Threat

Successful organizations must establish and use repeatable processes and security controls, and application managers need to take charge of the application life cycle. The organization needs to have an application security program in place that effectively coordinates all facets of its infrastructure.

To that end, be sure that any application security solution that your company evaluates not only meets your existing security needs but also is flexible enough to adapt to future infrastructure environments and attack vectors. Make sure that it fulfills these six key criteria:

1. Application security solutions must encompass not only web and mobile apps but also APIs.

2. Include a bot management solution to overcome the most sophisticated bot-based attacks.

3. Mitigating DDoS attacks is an essential and integrated part of application security solutions.

4. A future-proof solution should protect containerized applications and serverless functions and integrate with automation, provisioning and orchestration tools.

5. To keep up with DevOps/agile development practices, security solutions should be able to update security policies automatically and in real time.

6. A fully managed service should be considered to remove complexity and minimize resource utilization.

Radware partners with Microsoft Azure to provide adaptive application security protection through its security offerings that go beyond signature-based protection and blacklisted IP addresses, to provide hassle-free, automated protection for today’s dynamic landscape.

Providing protection for web applications is a core part of Radware's security offering. Through its ICSA Labs certified Web Application Firewall and its Enterprise-grade WAF-as-a-Service, Radware offers full application security protection including OWASP Top-10 coverage, advanced attack protection and Zero-day attack protection that automatically adapts your protections to evolving threats and protected assets. Web assets are always protected, even while applications constantly change and threats rapidly evolve, assuring web security is future proof.

Radware Security offers the only WAF that provides complete web application security with the ability to block attacks at the perimeter and ensuring fast, reliable and secure delivery of mission-critical web applications.

Learn more about Radware Security for Azure and WAF-as-a-Service solution.

LEARN MORE TODAY

radware | Microsoft Azure

Member of

Microsoft Intelligent Security Association

Microsoft