radware

Challenges in Application Security (And Why Your On-Prem WAF is No Longer Enough)

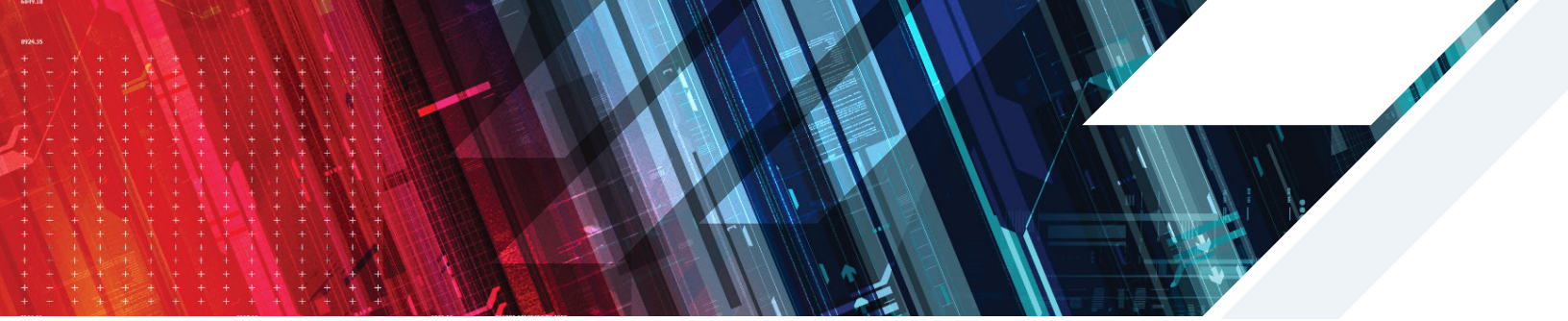


Table of Contents

Overview

Applications are at the core of most organizations, responsible for internal-, partner- and customer-facing business. It's crucial that these organizations understand the importance of their protection, as the application threat landscape is changing with more frequent, sophisticated and intense attack vectors. At the same time, application development and deployment are evolving to a point where traditional web application firewall (WAF) solutions are no longer effective, requiring a completely different approach to application protection.

The Application Threat Landscape

According to Radware's threat analysis hub, the number of blocked malicious events by Radware's cloud WAF service increased by 392% (year over year, 2022 vs 2021). In the same period, there was also an increase of 105% of bad bot transaction. Over 50% of organizations also reported that they have experienced multiple vectors of attacks on a monthly basis or more frequently (see figure 1).

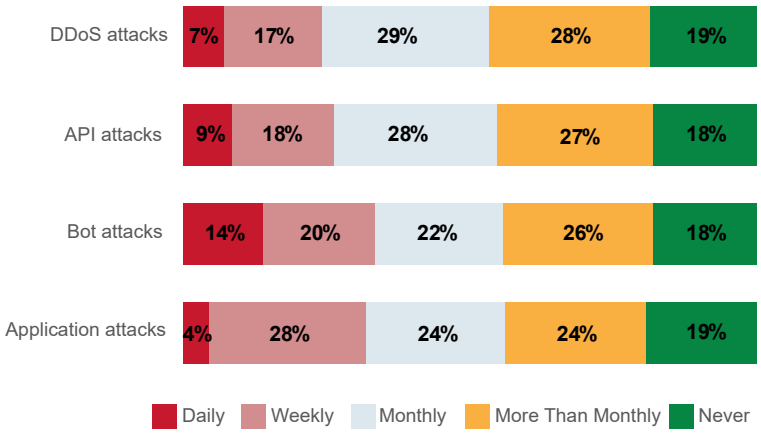


Figure 1:

Frequency of attacks

(Source: Radware Application Protection in a Multi-Cloud World, 2022)

One immediate conclusion is that protecting applications takes a combination of different solutions to cover all attack vectors. This includes using WAFs for application vulnerabilities, API protection, bot management and DDoS protection with layer 7 DDoS protection abilities. It should also be noted that these solutions will only be as good as the application protection experts who operate them.

In 2022 alone, we saw all sorts of organizations vulnerable to application-level attacks—from large service providers to big e-commerce brands and large software vendors. With a fair assumption that those organizations have top notch application protection solutions in place, it is becoming clear that attack sophistication is on the rise, challenging every CISO's teams.

The application development and deployment aspect

Historically, applications were monolithic and deployed only in a private datacenter. Today, they are deployed across multiple environments, such as traditional datacenters, private clouds and public clouds. The architecture of these applications is also changing. Although the vast majority was previously based on one monolithic application code base, today's applications use a micro-services architecture with many integrated third-party services. They rely extensively on APIs to communicate between micro-services and third-party services. Moreover, many of the applications rely on running code in the client-side browser, making the clients' devices part of the application.

With this evolving architecture, protecting applications requires a different approach than relying on the traditional on-prem WAF, even if it can be deployed in your various cloud environments.

Shortage in security experts and skills

The recent 2022 (*ISC*)² Cybersecurity Workforce Study & Survey by Gaper ISSA/ESG showed that 70% of organization are facing skill shortages in their cybersecurity teams and a high burnout rate in existing teams due to the high workload. The same survey showed that there are over 3 million open cybersecurity positions worldwide, including 400,000 in the US.

Challenges and Requirements in Managing Application Protection

Considering these obstacles, it only makes sense to reconsider whether or not a self-managed on-prem WAF is still the right tool to provide adequate application protection. The following are some of the challenges that an on-prem WAF faces in the current application and threat landscape.

Management overhead: With an increasing number of applications and deployment happening in more environments than ever before, the management overhead of protecting those applications is becoming impossible to handle.

Shortage in cyber experts: As the amount of threat vectors and attack sophistication continues to grow, the level of expertise required to manage it all is also increasing. Unfortunately, the number and skill level of application protection experts has not caught up. This gap creates a challenge for many organizations to maintain high-quality protection technology for their applications.

Quality of protection: A WAF is only as good as the security policies it is configured with. An on-prem WAF can only generate security policies based on the local application it protects, which can be extremely limited. Moreover, optimizing this protection and covering BOT and API domains requires ML/AI based algorithms which are not available on on-prem WAF devices.

Protecting all application surfaces: As the application architecture changes, protecting just the application server in one environment is no longer enough. The new application architecture introduces many locations through which it can be accessed—and they all need protection (e.g., server, cloud, third-party APIs, client). Old school on-prem WAF can't provide protection on all those application access points.

Agility and scalability: Rolling out a new application service is a labor-intensive task. Ensuring that the service doesn't break the application (and yet effectively protects it) consumes even more resources. This impacts the agility of the organization. Moreover, because application protection is a compute-intensive function, it also poses a challenge in the ability to scale it.

Why Your On-Prem WAF is No Longer Relevant

Traditional on prem WAF made a lot of sense when all your applications were deployed in your private datacenter and a WAF was all you needed to protect your applications. However, this is no longer the case. Here are several considerations that show why on prem self-managed WAF is no longer relevant, and why a managed cloud WAF service is the best option for organizations.

Management overhead

To effectively protect applications, there are many rules and signatures that need to be configured and tuned. This is a tedious process which can often create false positives that break the application and hurt the business.

Moreover, the application threat landscape requires integration of multiple solutions and technologies to provide good enough coverage against all threat vectors like WAF, bot management, API protection, layer 7 DDoS protection and more. This increases the level of complexity of on-prem/self-managed solutions, and directly increases the management overhead. Combined with the fact that there are more applications to protect, the management overhead is just too big for most organizations to handle.

On the other hand, a fully managed cloud WAF service is led by application protection experts that can provide more accurate signatures that both better protect the application and are also less likely to create false positives.

Radware's cloud WAF service incorporates algorithms to automate policy generation for positive security rules and only allows transactions that adhere to those rules. They do this without increasing the management overhead. With other machine learning algorithms, Radware's cloud WAF analyzes logs and automatically identifies remaining false positives before eliminating them at a click of a button. The service also includes all solutions required to protect against all threat vectors, including API protection, bot management, DDoS protection, analytics and forensic tools.

The result of replacing a self-managed on-prem WAF with a fully managed cloud WAF is the elimination of management overhead both for onboarding and ongoing maintenance of application protection services.

Shortage in cyber experts and quality of protection

We've already seen how organizations are struggling to fill their cybersecurity positions. Combining this challenge with the management overhead directly impacts two critical issues that organizations can't afford to compromise on:

- With too few application experts, application protection service onboarding is often measured in weeks, slowing down the business dramatically.
- With so many application protection domains to master and too few experts to master them all, in many cases the result is a compromised quality of protection.

A cloud WAF service managed by experts eliminates these bottlenecks. It enables onboarding new application protection services in a matter of hours instead of weeks, while ensuring the quality of protection is not compromised no matter the domain of protection (i.e., API, BOT, DDoS, WAF).

Quality of protection

The level of quality of protection an on-prem WAF can provide is limited by design due to a few factors:

- It can only learn from traffic on the local applications it protects, and it doesn't have the insights that can be generated from the thousands of applications a cloud WAF provider protects.
- Continuously optimizing security policies and protection requires AI-based automation (e.g. identifying false positives and refining policies accordingly). The amount of compute required to do that is not available for on-prem WAF solutions.
- Effective BOT protection and API protection (e.g., API discovery) also require compute-intensive AI algorithms, which can't run on on-prem devices and thus limit the quality of protection in those domains.

A cloud WAF service oversees thousands of applications and can learn and automatically generate signatures to protect against attacks it identifies on one application-for all of the applications it protects.

The amount of compute resources on a cloud WAF service are much bigger than those available on an on-prem device. Because of this, they're allowed to run many advanced AI algorithms and automate the optimization of security policies of applications. They can also automate detailed API discovery (often more accurate than self-documented APIs) and better identify BOT traffic.

The result is a much better quality of protection with a much wider attack vector coverage and automated security policy adaptability to application changes.

Protecting all application surfaces

An on-prem WAF is a device (or virtual device) that sits in-line in front of the application and protects its servers. However, with application components that run on the client side (e.g., scripts that communicate with third-party data providers from the client's browser), a different type of protection is also required to cover the client side—something that the standard WAF can't do.

Attackers can easily implant third-party libraries in the application. The browser will later run these on the client side and communicate sensitive information with the hackers' servers without the on-prem WAF ever seeing or protecting against this breach.

Radware's Cloud WAF service also offers a client-side protection module, which runs on each client's browser. It analyzes the communication to and from that browser, identifies unauthorized application communication and then reports and blocks it.

Agility and scalability

All application protection functions, namely WAFs, are compute intensive. Should a certain application exceed its typical capacity needs, it will have significant impact on the compute resources it requires to protect it. In many cases this will create bottlenecks which will require time, money and a lot of human resources to solve with an on-prem WAF.

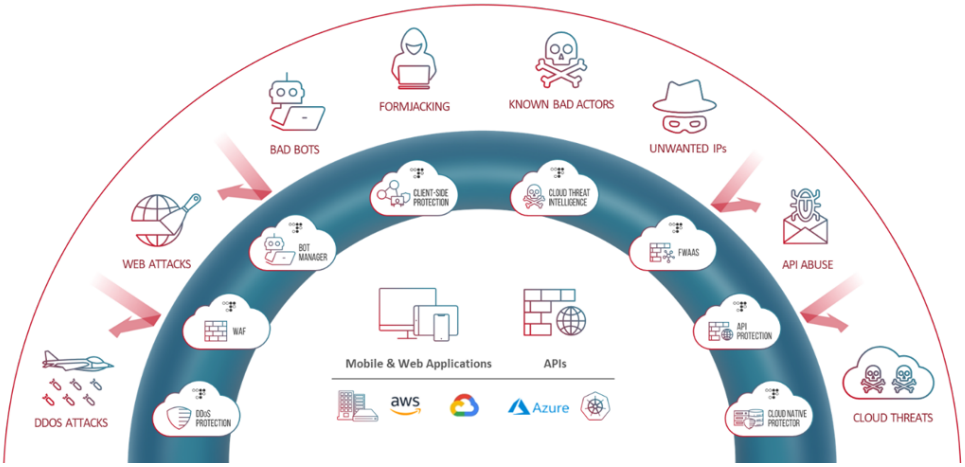
An on-prem WAF can only provide protection to local applications. It can't protect applications deployed on other private and public cloud environments. For those, most organizations need to use a different localized WAF solution (e.g., on AWS – use the AWS WAF), with different technology and inconsistent security policies and capabilities.

Using a cloud WAF service eliminates this problem completely. Increasing the capacity of a service is as simple as adding capacity to the service subscription, requiring no physical changes and no time from your expert. The addition of services like API discovery and protection, bot management and layer 7 DDoS is seamless in a cloud WAF service.

A cloud WAF can provide coverage for any application regardless of where it is deployed: private datacenter, private cloud or public cloud. Even for applications that can't divert traffic to Radware cloud WAF, Radware Secure Path plug in (deployable in various clouds and ADC solutions) can provide Radware's cloud WAF service in out of-path mode, including both attack detection and blocking.

Radware's Cloud WAF Service: A Comprehensive and Frictionless Application Protection Service

Easily manage and seamlessly scale your application security as you grow your business, evolve your application architecture and expand your cloud environments and services. The one-stop-shop comprising Radware's protection services keeps you protected against threat vectors as your business grows and applications evolve, while eliminating management overhead and enabling the fastest time to protection.



State-Of-The-Art Application Protection as a Service

Web Application Firewall

Radware's adaptive and automated WAF protects against web application attacks, hacking and other vulnerabilities. The WAF technology uses a positive security model that automatically learns the behavior patterns of legitimate user activities, automatically builds security policies tailored to allow those activities and blocks any action that deviates from these patterns of legitimate behavior.

Radware's combination of negative and positive security models provides a complete level of protection against OWASP Top 10 threats and zero-day attacks that WAFs based on negative security models cannot stop.

API Protection

A dedicated, end-to-end API protection fully automated solution ensures the security of apps, APIs, development platforms and infrastructure. It maps the API attack surface by leveraging an automated deep discovery algorithm to discover APIs endpoints and their full structure and generate tailored security policies to detect and block API-focused attacks in real time. It also uses a combination of access controls, data leakage prevention, bot management and DoS mitigation tools to protect against the growing array of API security threats listed in the OWASP API Security Top 10.

Bot Manager

Radware's industry-leading bot management and mitigation solution can accurately detect and distinguish between human traffic, good bots and bad bots, and ensure comprehensive protection of web applications, mobile apps and APIs from automated threats and bots.

It provides precise bot management across web, mobile and API traffic by combining behavioral modeling for granular intent analysis, collective bot intelligence and fingerprinting of browsers, devices and machines. It protects against all OWASP 21 automated threats, including account takeover, credential stuffing, brute force, denial of inventory, DDoS, ad and payment fraud, and web scraping.

Application DDoS Protection

Industry-leading application-layer (L7) protects against DDoS attacks. It is based on Radware's unique behavioral approach that distinguishes between legitimate and malicious traffic, automatically protecting against zero-day attacks. With unique hybrid, always-on and on-demand cloud DDoS service deployment options, Radware's Cloud DDoS Protection Service provides best-in-class security against a wide variety of threats, including HTTP Floods, HTTP bombs, low-and-slow assaults, and brute-force attacks.

Client-Side Protection

Advanced client-side protection ensures the protection of end users' data when interacting with any third-party services in the application supply chain. Easily block requests to suspicious third-party services in your supply chain and adhere to data security compliance standards. Protect against client-side attacks coming from third-party JavaScript services (formjacking, skimming/magecart), and automatically and continuously discover all third-party services in your supply chain with detailed activity tracking. Also, get alerts and threat level assessment according to multiple indicators, including script source and destination domain. Prevent data leakage by blocking unknown destinations or legitimate destinations with illegitimate parameters, as well as DOM-based XSS. Lastly, Radware Client-Side Protection's unique surgical enforcement capabilities block only nefarious scripts and don't stand in the way of vital JavaScript services.

ERT Active Attackers Feed

Radware ERT Active Attackers Feed serves as your very own network intelligence agency. It enhances the protection of applications and data centers by introducing a preemptive protective layer on top of Radware's attack mitigation solutions. The feed supplies Radware devices and Radware cloud security services with a list of attackers that were recently involved in a security incident, such as a DDoS attack, an application attack, an intrusion, or a scanning attack. This enables the platform or service to preemptively block known attackers before they come anywhere near your assets and initiate an attack.

In-Depth Visibility and Control

Radware gives you security and development dashboards with actionable analytics, automation and customized controls. This allows you to be aware of threats to your apps at all times and make educated decisions for application development.

Summary

Protecting applications with a self-managed on-prem WAF is no longer a valid option. The associated management overhead combined with the shortage of cybersecurity experts creates both unacceptable bottlenecks as well as compromised quality of protection. With the evolving application architecture, on-prem WAFs are simply incapable of providing one consistent solution for all applications in all the environments they are deployed in.

Radware's Cloud WAF addresses these gaps and challenges, providing best-of-suite application protection with complete coverage of a wide range of attack vectors, deployable in hours instead of minutes. This is achieved thanks to the experienced Emergency Response Team (ERT)—a group of experienced application protection experts— as well as AI-based algorithms that automate and constantly optimize security policies. Combined with SecurePath, it provides flexible deployment options for any scenario—even when traffic can't be diverted or SSL keys can't be shared. Radware's cloud WAF service provides a higher quality of protection while eliminating the management overhead and increasing any organization's agility.

RW1167 3.16.2023