Enterprise Strategy Group by TechTarget

SHOWCASE

SEPTEMBER 2023

Overcoming Application Security Challenges With Managed WAF

John Grady, Principal Analyst

Abstract: As web applications have become more important, security challenges have continued to mount. Security teams have more on their plate than ever yet continue to struggle with a problematic shortage of skills. At the same time, application security tools can be expensive, difficult to deploy, and ineffective to use. A managed web application firewall (WAF) can help security teams navigate these issues and improve the organization's application security posture. Fortra Managed WAF offers customers an end-to-end, continuously managed WAF that provides protection against known exploits, emerging threats, zero-day exploits, bots, and large-scale DDoS attacks for both web applications and API endpoints.

Challenges Securing Web Applications Persist

Applications have become critical for businesses of all sizes and types to connect with customers, enable partners, and ultimately drive revenue. To support this reality, there has been a significant focus on innovation to enable better agility, scalability, and efficiency. Yet, as is often the case, IT teams move more quickly than security teams can keep pace with. Therefore, it is unsurprising that research from TechTarget's Enterprise Strategy Group found that 55% of those surveyed said securing their organization's web applications has become more difficult than it was 2 years ago.[1]

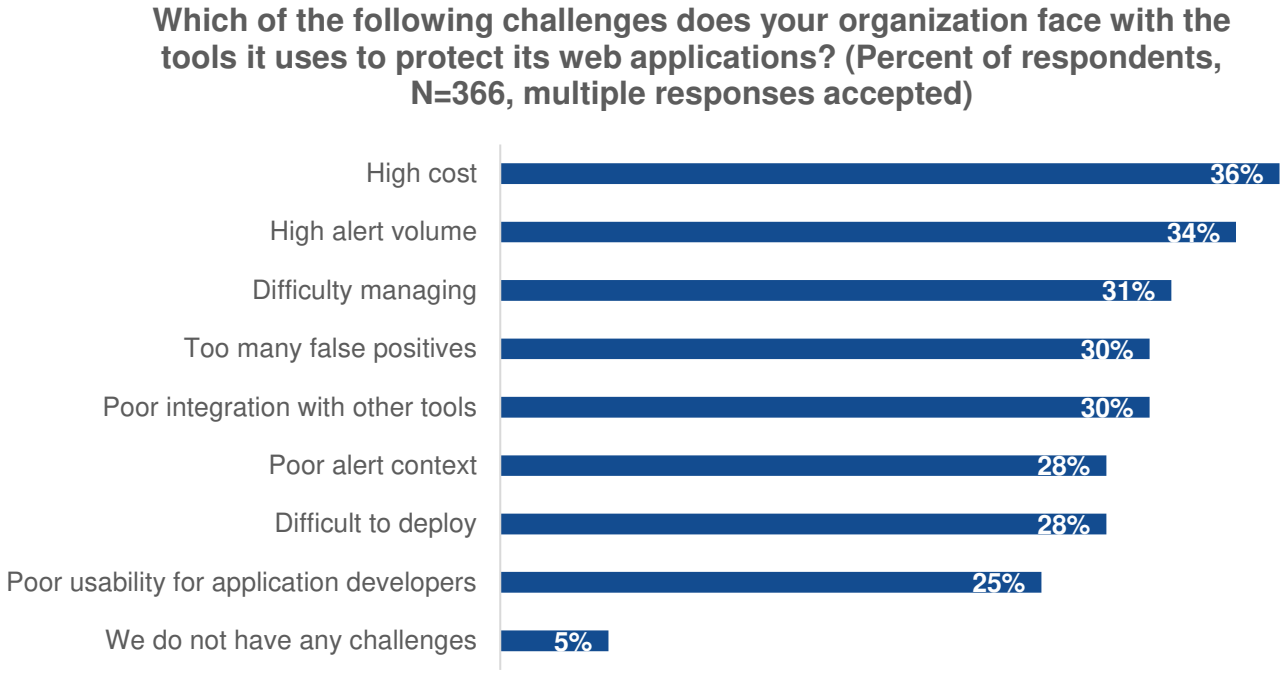
There are a variety of challenges cited that lead to this difficulty. Some of the most significant include:

- **Scale**. 15% of respondents said they supported at least 200 public facing web applications, but 45% anticipated having at least 200 public facing applications over the next 24 months.
- **Architecture**. Similarly, 28% said most or all of their applications use APIs, while 57% expect most or all of their applications to use APIs over the next 24 months.
- **Skills**. 30% say they don't have enough application security skills and/or personnel.

While there are a variety of tools that can be used to protect web applications, the WAF remains a prominent component of many organizations' web application security strategies. In fact, 72% of research respondents indicated their organization uses a WAF. Yet the solutions security teams use to protect these applications present their own set of issues and often make the problem worse (see Figure 1).

[1] Source: Enterprise Strategy Group Complete Survey Results, *Trends in Modern Application Protection*, July 2022. All data from this report. All research references and charts in this showcase are from this survey results set.

Figure 1. Application Security Tool Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As seen in Figure 1, deployment, management, and efficacy were prominently mentioned in a variety of ways. For instance, 28% of respondents cited difficulty deploying web application security tools as a challenge their organization faces, while 31% responded that they had difficulty managing tools and 30% mentioned poor integration with other tools. On the efficacy front, 28% noted the poor alert context their tools provide, while 30% and 34% cited false positives and high alert volume as challenges, respectively.

This research paints a picture of common application security challenges. Even when organizations deploy tools to protect applications, provisioning appliances and tuning policies while maintaining application availability can be difficult. Applications are dynamic, and even when policies are correctly configured initially, they often need to be modified over time. Poor integration with bot management and API security tools may leave the door open for attackers, who are increasingly targeting web application front ends and the APIs that connect application components. Furthermore, if the efficacy of tools is low due to false positives and poor alerts, especially with web application firewalls, many organizations elect to run them in detect-only mode to avoid blocking legitimate traffic. All these factors lead to increased cost, which is the most commonly cited challenge organizations face with application security tools, whether procurement or operational.

The Benefits of a Managed WAF

Utilizing a managed web application firewall is one of the most direct ways to overcome many of these web application security challenges. Managed offerings can help security teams close the skills gap without having to hire their own practitioners. Enterprise Strategy Group research backs up this idea. When asked what their organization will do over the next 12-18 months to implement and optimize their web application and API protection strategies, 44% said they plan to work with managed service providers to manage web application and API protection tools.

By leveraging third-party experts to help deploy and tune the WAF, security teams can reduce their time to value and have more confidence shifting from detect to prevent mode quickly. Beyond deploying and tuning early on, managed services provide continuous monitoring and ongoing management, which are critical to help security teams maintain the solution and respond to alerts when they do occur.

While managed services are important and can help overcome some technology limitations, the capabilities of the solution itself are equally important. A managed WAF must be able to:

- Block known OWASP Top-10 and unknown exploits against web applications.
- Use robust threat intelligence to defend against zero-day attacks and emerging exploits.
- Protect against both common and advanced API attacks, which have become favored threat vectors of attackers as API usage has exploded.
- Prevent automated attacks from bots, including those targeting customer accounts and credentials.
- Defend against both low-and-slow Layer 7 denial-of-service (DoS) attacks and large-scale distributed denial-of-service (DDoS) attacks measuring terabits per second.

Fortra Managed Web Application Firewall

Fortra helps customers protect web applications and APIs via its Managed Web Application Firewall. The solution is designed and managed to maintain uptime, secure sensitive data, and minimize the risks that come with the utilization of web applications and APIs.

Fortra Managed Services support begins prior to deployment, runs through configuration, and includes 24/7 monitoring after blocking mode is enabled. A typical deployment begins with a kickoff call to confirm the project scope and plan the deployment. During deployment, Fortra engineers are available to support any required network changes and to validate the deployment. Additionally, Fortra Security Operations Center (SOC) experts create policies and configure the WAF to run in detect mode. Fortra analysts then review logs and tune the WAF as necessary to ensure false positives are removed and the security profile is optimized. With customer approval, and once Fortra SOC analysts are confident that policies are correctly tuned, the WAF is transitioned to blocking mode. After this is completed, the Fortra SOC continues to monitor managed WAFs 24/7.

Fortra Managed WAF provides a variety of capabilities beyond expert analysts to ensure customers are well protected from a variety of threats. These capabilities include:

- **Emerging threat and zero-day protection.** By combining Fortra's advanced threat protections, machine learning, anomaly detections, positive security policies, blacklists of emerging threat actor IPs, and managed security policy optimization, customers are protected against lesser-known and unknown attacks.
    - Virtual patching maintains security between patch windows by achieving the security outcomes of a patch without having to follow a change management or patch testing process. Fortra will create and apply the virtual patch. This covers known exploits targeting the top 100 web applications, customer-specific web applications (subject to request), and emerging threats.
- **Adaptive trust-based policies.** To help minimize false positives and improve WAF outcomes for highly dynamic websites, adaptive trust-based policies use an advanced tiered signature model in combination with dynamically set connection trust scores based on client activity. This model applies increasingly strict blocking controls to connections that violate the initial controls or are known to be malicious based on activity observed in other protected environments across Fortra's customer base and broad security offerings.
- **Bot management.** Bot management capabilities on Fortra Managed WAF protect against automated attacks and unwanted data scraping bots using session anomaly detection and CAPTCHA enforcement. This helps security teams protect against denial-of-service attacks, credential stuffing, fraudulent checkout, and other automated attacks, while maintaining the ability to allow benign web crawlers (such as Google). Relatedly,

credential attack protection and session anomaly detection ensure that customer accounts and information are protected:

  - Credential attack protection prevents automated unauthorized activity (such as brute force password guessing) through controls such as CAPTCHA, rate limiting, and outright blocking.
  - Session anomaly detection uses advanced machine learning models to build baselines of normal user behavior or normal API usage along with challenge, slow down, or block traffic that is characterized as anomalous.

- **DDoS mitigation.** For deployments on AWS and Microsoft Azure, Fortra Managed WAF detects unexpectedly high volumes of traffic and challenges clients using a non-interactive JavaScript challenge or CAPTCHA to detect automated, malicious activity. This capability is delivered in partnership with AWS, providing the scalability to defend against large-scale DDoS attacks, but without Fortra customers having to manually intervene or manage multiple vendor relationships.
- **API protection**. Fortra Managed WAF supports discovering and managing protection of API endpoints through API definition files. The service protects API endpoints through positive endpoint policies, enforcing the API definition and session anomaly detection along with anti-automation controls to counter volumetric and sequential attack patterns.

Conclusion

Security teams have a lot on their plate, and as the speed and scale of application development has increased, many struggle to keep pace. At the same time, the criticality of web applications to the business makes ensuring strong security an imperative. While many of today's web application firewalls offer an array of protections for not only OWASP Top-10 risks, but also bots, APIs, and DDoS attacks, the cost, complexity, and inaccuracy of these tools can cause more problems than they solve. Offloading the management of WAFs can provide some relief to beleaguered security teams, leveraging third-party experts to help deploy and tune the WAF, but only if these solutions still have the technical capabilities to protect modern application environments.

Fortra Managed WAF checks both these boxes. The solution offers enterprise-grade security capabilities, coupled with expert support from planning to deployment to continuous monitoring. Through this combination, customers can more effectively and efficiently maintain uptime, secure sensitive data, and limit application vulnerabilities across all their web applications and APIs.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com