

Advanced Protection for Web Applications and APIs on AWS

Web Application Firewalls Offer
Easy-to-manage, Cost-effective Security

Table of Contents

Executive Overview	3
Challenges of Security in the Cloud	5
Requirement 1: Easy To Deploy and Manage	6
Requirement 2: Advanced Threat Protection	8
Requirement 3: Low Total Cost of Ownership	11
WAF Deployment Options	12
Evaluating WAF Solutions: Checklist	13



Executive Overview

As companies migrate business-critical applications from their on-premises infrastructures to the cloud, they increase their exposure to known and unknown targeted attacks. Every new application deployed in the cloud expands the number of possible entry points and thereby the attack surface. Making matters worse, the volume and virulence of threats continue to grow, putting unprecedented pressure on organizations to deploy and manage multiple security solutions.

Enterprises that choose to host their applications on Amazon Web Services (AWS) often erroneously assume that they need not worry about security. What they need to understand is that AWS secures the infrastructure, while the customer is responsible for securing the application and data. Simply repurposing existing on-premises security tools does not address the challenges of the current threat environment. Basic web application firewall (WAF) solutions also may not cover the entire web application attack surface. For example, they may lack key features such as application programming interface (API) security, bot mitigation, or tools to reduce administrative overhead such as machine learning (ML).

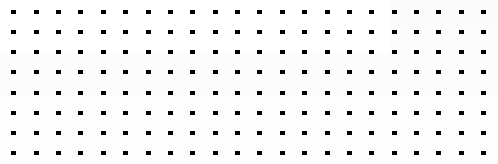

Instead, organizations require a WAF that delivers a full web application and API protection (WAAP) solution for internet-facing applications, including customer-facing websites, content management systems, and the APIs that support mobile applications. WAFs protect against external and internal attacks, monitor and control access to web applications, and collect information for compliance and analytics purposes. For maximum architectural flexibility, top-tier vendors offer WAFs in physical, virtual, and cloud-native form factors.





55%

of all cyberattacks targeted organizations' web applications in 2019, which is a substantial increase compared to the previous few years, when these types of attacks made up around 30% of the total number.¹



Challenges of Security in the Cloud

When organizations deploy web applications in the cloud, their risk profile changes. Web applications typically have exposure to the public internet, enabling user connections from unmanaged devices over networks that the organization does not control. To further complicate things, the attack surface evolves every time the organization updates applications, and when the organization begins supporting mobile applications via APIs, the attack surface expands further. Making matters worse, the volume and velocity of threats continue to grow with threat actors creating more sophisticated coded and targeted attacks.²

Many organizations adopt the DevOps model to enable their business to move fast. In doing so, DevOps teams frequently take on the responsibility for securing internet-facing applications using WAFs. However, DevOps personnel usually have neither the time nor the security expertise to take on WAF configuration and management without negatively impacting revenue-generating duties such as continuous delivery of new features. Hiring an additional security engineer can address these concerns, but the talent shortage makes this tactic difficult to implement. A leading professional organization predicts that unfilled cybersecurity jobs will reach 1.8 million by 2022.³

As they evaluate commercially available WAF solutions, organizations must consider all of the factors discussed above. To simplify the process, many decision-makers start by developing a set of organizational requirements for ease of use, advanced threat protection, and total cost of ownership (TCO).

Web applications constitute the #1 attack vector leading to a data breach.⁴



Requirement 1: Easy To Deploy and Manage

Firewall configuration constitutes one of the most important success factors for web application security. To avoid configuration errors and minimize the time drain on developers, DevOps teams need to assess WAFs based on ease of deployment, customizable security policies, and accuracy.

Ease of Use

Given the growing cybersecurity skills gap, security solutions must minimize the level of security expertise required for installation and operation. To achieve this goal, organizations should choose WAFs that are easy to deploy, configure, and manage. Key features that contribute to ease of use include setup wizards, predefined rules, and intuitive dashboards.

Customizable Policies

Once organizations have the WAF up and running, DevOps and security professionals need the ability to easily fine-tune firewall rules to reduce the operational overhead of security management and accommodate changes in the security landscape. A solution should include the ability to create reusable templates and to manage policies across multiple applications.

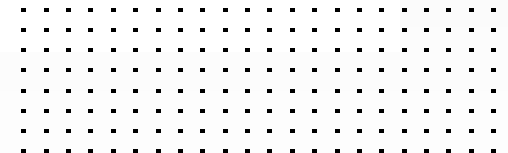
Accuracy

False positives divert valuable staff time, and in large numbers, can mask true threat situations. Worse, they can force an organization to go into monitor-only mode to avoid blocking time-sensitive transactions when legitimate users are blocked in error, opening the door to potential attackers. WAF solutions that integrate ML can significantly reduce false positives and improve the WAF's ability to identify incoming threats accurately with minimal human oversight.





The cost of web-based attacks is now an average of \$2.3 million annually for organizations.⁵



Requirement 2: Advanced Threat Protection

The threat landscape continues to escalate and diversify. For example, a recent survey finds that researchers uncover at least one new zero-day threat every week.⁶ When evaluating the protection capabilities of potential solutions, the key criteria include effectiveness, API protection, and security updates.

Security Effectiveness

The OWASP Top 10 represents a broad consensus on the most critical web application security threats. Organizations seeking to effectively protect web applications and address compliance requirements should choose solutions that defend against all the risks in the OWASP Top 10 list as well as unknown and zero-day exploits (Figure 1).⁷

OWASP Top 10

1	Injection
2	Broken Authentication
3	Sensitive Data Exposure
4	XML External Entities (XXE)
5	Broken Access Control
6	Security Misconfiguration
7	Cross-site Scripting (XSS)
8	Insecure Deserialization
9	Using Components With Known Vulnerabilities
10	Insufficient Logging and Monitoring

Figure 1: OWASP Top 10 list.



API Protection

Unprotected APIs constitute serious security vulnerabilities that allow attackers to exfiltrate data and launch distributed denial-of-service (DDoS) attacks. Here, comprehensive application security requires specialized security rules to protect APIs against malicious actors.

Security Updates

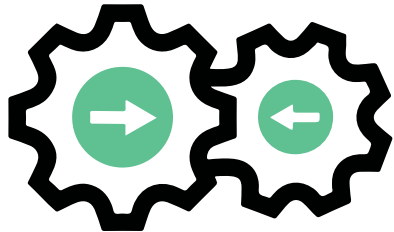
In addition to the above advanced protection capabilities, solutions must include a subscription to a threat research service to keep current on the latest attack signatures, IP reputation, antivirus, and sandboxing.

Advanced Analytics

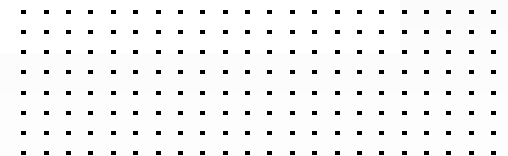
A solution must go beyond signatures and IP reputation and include advanced analytics to identify and block zero-day threats.

The OWASP Top 10 is based primarily on 40-plus data submissions from firms that specialize in application security, as well as industry surveys completed by over 500 individuals. The data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real-world applications and APIs. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact.⁸





**API abuses will become
the most-frequent attack
vector by 2022.⁹**



Requirement 3: Low Total Cost of Ownership

The AWS global infrastructure includes 24 AWS Regions, geographic entities physically isolated from each other. Organizations can take advantage of this global infrastructure by choosing a WAF solution hosted in the same AWS Region as the applications it protects. This strategy reduces latency and data transfer costs significantly, while simplifying deployment. But TCO isn't just about keeping CapEx and OpEx expenditures down—look for a solution that delivers the accuracy the security team needs to detect and block threats without overwhelming false positives.

Organizations using SaaS models such as WAF-as-a-Service spend 21% less on IT as a percentage of revenue and 16% less on IT on a per-user basis than those that embrace an on-premises application model.¹⁰



WAF Deployment Options

While AWS offers its customers a basic WAF on a pay-per-usage basis, the AWS solution alone cannot provide the enterprise-grade security that many business-critical applications require. Instead, DevOps and security decision-makers should look for a WAF with a range of deployment options that enable them to meet ease-of-use, advanced threat protection, and low TCO requirements.

Managed Rules for AWS WAF

Offered by third-party security vendors, managed rule packages enable users to quickly and easily establish more robust security controls on top of the AWS WAF without adding management or architectural complexity. The provider automatically updates the rules as new vulnerabilities and bad actors emerge, keeping security policies up to date.

[Fortinet managed rulesets for AWS WAF](#) are based on FortiWeb WAF security service signatures, and are updated on a regular basis to include the latest threat information from FortiGuard Labs.

WAF-as-a-Virtual Machine

WAF delivered as a virtual machine (VM) protects applications running on platforms such as VMware,

Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, and Docker. WAF VMs offer the same features as hardware-based WAFs but with the flexibility to meet the demands of dynamic application hosting environments. By deploying VMs, customers can address specific architectural and compliance requirements such as FedRAMP.

[FortiWeb VM](#) includes the same capabilities as FortiWeb hardware-based appliances, with the flexibility to deploy instances as needed to meet the demands of dynamic application hosting environments.

WAF-as-a-Service

WAF-as-a-Service (WAFaaS) allows organizations to provide advanced threat protection in a form factor that is easy to deploy and manage. The WAFaaS provider maintains the security infrastructure, freeing DevOps staff to focus on high-value tasks that drive innovation and generate additional revenues. WAFaaS includes all the functionality of the hardware and virtual WAF formats and offers regional hosting options that can reduce transfer costs and latency.

[FortiWeb Cloud](#) is a WAFaaS offering and delivers FortiWeb capabilities with no software or infrastructure to maintain.



Evaluating WAF Solutions: Checklist

When evaluating and comparing WAF solutions for their AWS-hosted web applications, DevOps leaders can use the following checklist:

Deployment

- Implemented as cloud-native solution on AWS
- Includes predefined configurations
- Deploys in minutes using predefined set of policies

Manageability

- Scales easily to accommodate changing security requirements
- Supports regional hosting to reduce costs and streamline compliance
- Offers flexible, on-demand pricing

Efficacy

- Protects against OWASP Top 10 and zero-day exploits
- Provides access to advanced configuration options
- Includes customized WAF rules
- Provides API security
- Includes subscription to threat research service

FortiWeb protects public cloud-hosted web applications from advanced threats—the OWASP Top 10, zero-day threats, and other application-layer attacks. For more information, visit [Fortinet.com](https://www.fortinet.com).



¹ James Coker, "[Substantial Rise in Attacks on Orgs' Web Apps Last Year](#)," Infosecurity Magazine, August 7, 2020.

² "[Quarterly Threat Landscape Report: Q4 2018](#)," Fortinet, February 2019.

³ "[Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher](#)," (ISC)², June 7, 2017.

⁴ "[2019 Data Breach Investigations Report: Summary of Findings](#)," Verizon, accessed July 2, 2019.

⁵ Kelly Bissell, et al., "[Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection](#)," Ponemon Institute and Accenture, 2019.

⁶ "[Quarterly Threat Landscape Report: Q4 2018](#)," Fortinet, February 2019.

⁷ "[OWASP Top 10](#)," OWASP, accessed December 1, 2020.

⁸ Ibid.

⁹ Maria Korolov, "[What you need to know about the new OWASP API Security Top 10 list](#)," CSO, November 14, 2019.

¹⁰ "[Cloud Users Enjoy Significant Savings](#)," Computer Economics, accessed July 13, 2019.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.