Advanced Protection for Web Applications on AWS

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

Table of Contents

Executive Overview 3

Enhancing 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 10

WAF Deployment Options 11

Evaluating WaaS Solutions: Checklist 13

FORTINET | aws

Executive Overview

As companies migrate business-critical applications from their on-premises infrastructure 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. Plus, simply repurposing existing on-premises security tools does not address the challenges of the current threat environment.

Instead, organizations require security solutions designed specifically for internet-facing applications—namely, web application firewalls (WAFs). 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.

83%

of enterprise workloads will be in the cloud by 2020.[1]

Enhancing Security in the Cloud

When organizations deploy web applications in the cloud, their risk profile changes. For one thing, the public cloud has no security perimeter, so every new application increases the number of possible entry points and thereby the attack surface. Making matters worse, the volume and velocity of threats continue to grow. For example, unique exploits increased by 5% in the last quarter of 2018, and data shows that criminals are getting smarter and more efficient by 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, up 20% from 2015.[3]

As they evaluate the 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.

Accuracy

False positives divert valuable staff time and, in large numbers, can mask true threat situations. WAF solutions that meet core business issues integrate machine learning (ML) to improve their ability to identify incoming threats accurately with minimal human oversight.

In 2018, misconfigurations were the cause of 70% of cloud data breaches, a 424% increase over the previous year.[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, application programming interface (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 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—2017
A1: 2017-Injection
A2: 2017-Broken Authentication
A3: 2017-Sensitive Data Exposure
A4: 2017-XML External Entities (XXE)
A5: 2017-Broken Access Control
A6: 2017-Security Misconfiguration
A7: 2017-Cross-Site Scripting (XSS)
A8: 2017-Insecure Deserialization
A9: 2017-Using Components with Known Vulnerabilities
A10: 2017-Insufficient Logging and Monitoring

Figure 1. OWASP Top 10 security risks for web applications.

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 trends in attack signatures, IP reputation, antivirus, and sandboxing.

In a recent survey, 48% of executives believe that DDoS attack threats have increased year over year.[8]

Requirement 3: Low Total Cost of Ownership

Among the deployment options, WAF-as-a-Service (WaaS) offers the most cost-effective solution for many enterprises. In this model, the cloud provider supplies the hardware and software components, virtually eliminating the need for capital investments (CapEx) and the operating costs (OpEx) associated with platform maintenance.

The AWS global infrastructure includes 22 AWS Regions and AWS GovCloud (US), geographic entities physically isolated from each other. Organizations can take advantage of this global infrastructure by choosing a WaaS hosted in the same AWS Region as the applications it protects. This strategy reduces latency and reduces data transfer costs significantly—namely, the organization pays only for data traffic to the WaaS, while the WaaS provider handles the outbound fees.

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.[9]

WAF Deployment Options

While AWS offers its customers a WAF on a pay-per-usage basis, Fortinet offers Managed Rules to enhance it or FortiWeb that provides comprehensive enterprise-grade security that many business-critical applications require. This gives DevOps and security decision-makers 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. The provider automatically updates the rules as new vulnerabilities and bad actors emerge, keeping security policies up to date.

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.

WAF-as-a-Service

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

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]

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.[11]

Evaluating WaaS Solutions: Checklist

When evaluating and comparing WaaS 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 Cloud WAF-as-a-Service 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 www.fortiweb-cloud.com.

[1] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[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] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

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

[7] "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," OWASP, accessed July 13, 2019.

[8] "Q1, 2019 Cyber Threats & Trends Report," Neustar, April 17, 2019.

[9] "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," OWASP, accessed July 13, 2019.

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

[11] Ibid.

www.fortinet.com

431437-A-0-EN

August 21, 2019 4:16 AM

eb-advanced-protection-for-web-applications-on-aws-V1