aws marketplace

Security ebook Series

How to improve your security posture with a web application firewall

Enterprise protection for inspecting incoming network traffic

Application-level security that's evolving in step with the internet

The internet continues to provide new, innovative services that are increasingly relied upon, every day. While security protocols have been in place since the dawn of the internet, we now engage online in a dramatically different fashion, and our digital defenses are evolving in step to secure the applications that power that experience. Ensuring that they run reliably, and their users stay protected, has never been so important to so many people.

At one point, a firewall that only permitted ports 80 and 443 access to a web server was considered sufficient. But with all the additional 'noise' present in today's online environment, port number assignments aren't enough—we need to monitor and restrict which traffic types reach our applications. And these security controls need to operate without slowing down processing speeds.

Realizing the need to upgrade traditional firewalls, security teams debuted a new wave of devices—including web application firewalls (WAFs)—that intelligently inspect the traffic's protocol and content to decide if it's legitimate.

In this ebook, you'll learn how to protect business-critical web applications against malicious traffic, and help improve your compliance posture using a WAF that you can deploy, configure, and align to your enterprise's business processes and security policies.

Protecting applications begins with controlling their traffic

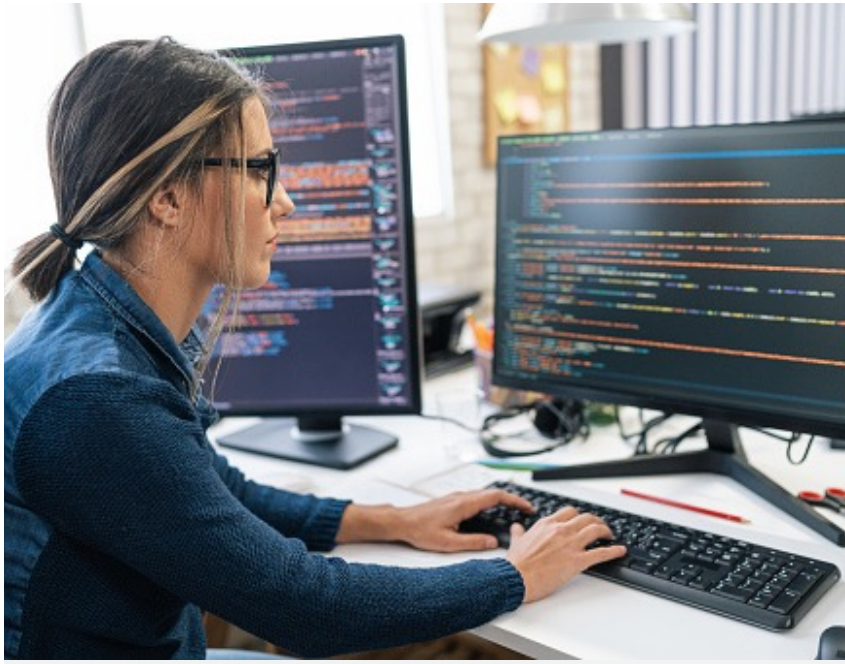
A WAF is a physical or virtualized appliance or Software as a Service (SaaS) solution designed to protect web-facing applications by ensuring that they only receive expected requests.

A WAF inspects and filters traffic between a web application and the clients using it. Most WAFs have foundational capabilities to create rules based on factors like IP source, regular expression matching for data in the URL, inspection of request headers, and verification that an HTTP request is valid.

To help customers shield their applications, modern WAFs often have rules that align with the Open Web Application Security Project (OWASP) list of common risks (see sidebar). A WAF may also provide functionality to block or allow access from geographical regions, help verify the difference between a real person and a bot, and even integrate with machine learning to help detect anomalous behavior that might indicate a threat before a security event even happens. This technology can deliver important benefits including meeting compliance requirements, eliminating invalid requests, and helping teams implement a defense-in-depth security strategy.

Why use a web application firewall

WAF inspects HTTP requests, looking at each individual request and deciding whether or not to permit it based on a broad range of factors. These factors include if the request is protocol compliant, if a specific value is present in the HTTP header, and if there are signs of common patterns of abuse.



The types of risks a WAF can help prevent are centered on the OWASP Top 10, as well as web application–specific traffic.[1] At a glance, these include:

1. Broken access control
2. Cryptographic failures
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

[1] The OWASP Top 10 is a regularly updated list of the 10 most common and impactful web application vulnerabilities and risks, and it's compiled based on real-world analytics and input from the community.

How to realize the full benefits of WAFs

A WAF is a security tool that requires a certain degree of specialized expertise if enterprises are to get the most benefit from it. Optimized configuration of a WAF requires familiarity with business processes, operations, and applications. Legitimate concerns about issues like false positives make fine-tuning a WAF essential.

The extended capabilities of modern WAFs are sometimes overlooked. Their simplified, cloud-based rule management and application programming interface (API) functionality can enable integration with other security tools and services to create a global, network-layer block of threats. The technical expertise required to programmatically interact with a cloud-native service at scale is complex and may fall outside of an internal IT department's skill set. But this shouldn't deter organizations from unlocking the full range of features that a WAF can provide.

Cloud-based WAFs, whether offered by a cloud service provider or a third-party provider, have management APIs that allow dynamic updates and configuration changes. These changes can be made and managed using custom-written code, a provided software development kit (SDK), or infrastructure-as-code services like AWS CloudFormation or HashiCorp Terraform. This means that security teams can couple changes to a WAF to changes in a new or existing application workloads through the same release pipeline that will update the application itself.

A WAF—or at the very least its policies—can be developed from the ground up to support the application. Additionally, security teams can adjust rules and policies to support the application as it changes. This helps ensure that stale rules don't linger and unintentionally impact application performance.

Deploy an AWS-native WAF in just a few clicks

AWS WAF can help protect web applications or APIs against common web exploits and bots by:

- Enhancing protection against layer-7 distributed denial of service (DDoS) events
- Integrating with AWS Shield Advanced for advance notifications and customized support
- Addressing the OWASP Top 10 security risks
- Strengthening your application's defenses against automated bots.

Customers can get started quickly using a pre-configured set of rules managed by AWS or AWS Marketplace Sellers. AWS WAF can be deployed on Amazon CloudFront, Application Load Balancer, Amazon API Gateway, or AWS AppSync.

Smithfield regains cost-effective, agile ownership of its IT infrastructure and data with Barracuda

Founded in 1936, **Smithfield Foods** is a $14 billion global food processor—the world's largest pork processor and hog producer. The company is based in Smithfield, VA, with facilities across the US and Europe and with 52,000 employees worldwide.

The Challenge

Smithfield wanted to migrate all external-facing websites and applications to AWS while maintaining security against cyberthreats. Previously, it had relied upon outsourcing companies to host and manage its data center operations. But as its needs evolved, it required less costly solutions that were also more agile and gave Smithfield more ownership of its IT infrastructure and data.

The Solution

Smithfield chose Barracuda Web Application Firewall to provide the needed controls, as well as to extend and standardize security across its properties. For Smithfield, being able to configure and provision directly through the AWS Marketplace made it very convenient.

The Results

Barracuda helped Smithfield's cloud migration project proceed smoothly, completing deployment and configuration in a single day. Barracuda Web Application Firewall provides Smithfield with security across their internet- and public-facing applications.

> "The Barracuda Web Application Firewall provides the controls we need, but also has a very easy user interface, even for people without a strong technical background."
>
> — Jeff Thomas, Chief Technology Officer, Smithfield Foods

Barracuda security solutions are engineered for AWS and designed to support your cloud journey. As part of the shared security responsibility model, Barracuda products complement existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, providing enhanced security against cyberattacks and advanced threats. Barracuda solutions are well architected and pre-qualified by AWS. Learn more

Zoosk prevents account takeovers and romance fraud with Cequence

Zoosk is a leading online dating company that personalizes the dating experience to help singles find the person and relationship that's just right for them. Zoosk's Behavioral Matchmaking technology is constantly learning from the actions of over 35 million members to deliver better matches in real time.

The Challenge

Bad actors had targeted legitimate users for fraud—about 90% of the attacks targeted the mobile application APIs—costing an average $12K per successful attempt. Zoosk needed to safeguard its brand and reputation from damage caused by bad actors, as well as protect all exposed APIs and web-based account login and registration applications with consistent security.

The Solution

Zoosk replaced its existing automated attack-prevention solution with the Cequence Application Security Platform with Bot Defense, which complements native AWS security. CQAI, the foundation of the platform, uses machine learning to automatically discover and analyze Zoosk web, mobile, and API-based applications, detect automated attacks, and block malicious ones using a lightweight module that is deployed inline.

The Results

With Cequence Security deployed, Zoosk has prevented account takeovers and romance scams, which increased user confidence. Zoosk has also reduced infrastructure costs and improved productivity among its application team, as well as maintained its brand and reputation.

> "Cequence has virtually eliminated romance scams associated with automated account takeovers and fake account creation attacks targeting our mobile app APIs. Their agentless approach bakes security into our development workflow, allowing us to securely deploy new application updates every two weeks."
>
> — Conor Callahan, Technical Lead of Platform and Infrastructure, Zoosk

Cequence Security protects organizations' APIs to minimize theft, fraud, and business disruption with the only solution that addresses all phases of the API protection lifecycle. The Cequence Unified API Protection (UAP) solution provides runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology leveraging a distributed, container-based architecture that supports cloud and hybrid deployment scenarios. Learn more

Are you protected against the most common cyberattacks?

A well-tuned and properly implemented WAF helps solve security, compliance, and due diligence use cases for organizations around the globe. By using a WAF, organizations can help control the risk to their organization, protect workloads, enhance logging capabilities, and substantially increase their security posture.

As you read in the Smithfield and Zoosk case studies, a WAF can help organizations increase the security of their applications. Find help to extend the reach and impact of your security strategy by exploring more solutions from AWS Marketplace sellers.

What is AWS Marketplace?

AWS Marketplace makes it simple to find, try, buy, deploy, and manage software that runs on AWS.

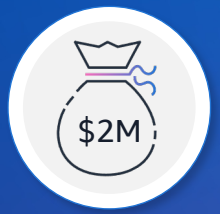
Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

Why AWS Marketplace?

Security teams use AWS-native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security footprint.

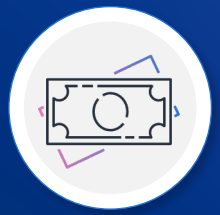
Reduce licensing costs by 10% with flexible pricing models



Save $2 million by consolidating steps and increasing visibility into procurement practices

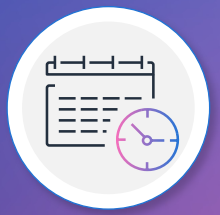
Halve time spent on invoicing processes

Reduce time spent researching and comparing vendors by 66%



Recapture 25% of at-risk committed spend with AWS and attain discounts

Reduce vendor onboarding processes by 75%, leading to time savings worth more than $62,000



Realize payback in less than six months

Amazon Web Services (AWS) Marketplace surveyed 500 IT decision-makers (ITDMs) and influencers across the US to understand software usage, purchasing, consumption models, and compared savings.

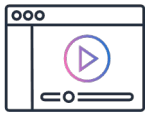
How to get started with WAF security solutions in AWS Marketplace

Barracuda

Product Overview | Video | Data Sheet

CEQUENCE SECURITY

Product Overview | Video | Data Sheet



How to improve your security posture with a web application firewall (WAF)

Webinar | 1-Minute Infographic | Whitepaper

Find, buy, deploy, and govern software solutions on AWS Marketplace

Get started with AWS WAF

AWS WAF helps you protect against common web exploits and bots that can affect availability, compromise security, or consume excessive resources

Visit AWS Marketplace

Learn more about AWS Security Partners and gain access to exclusive content on security solutions addressing security use cases on behalf of AWS customers

Find resources

Get connected with a solutions architect that can share best practices and help solve unique challenges

Get in touch with an AWS Expert