FORTINET

Secure Your AWS Web Applications

Uncover The Best-Fit Solution For Your Needs

Table Of Contents

I Built A Great Web App, Now How Do I Deliver It At Scale And Keep It Secure?

As companies accelerate their digital transformations, web applications and web APIs are driving business forward. Oftentimes, these solutions support critical line-of-business functions. But because areas such as e-commerce, human resources, and supply chain management touch sensitive assets, they are attractive targets for threat actors.

In the past, applications were deployed on internal networks that were secured with traditional perimeter-based firewalls at the edge. But, today's web apps and APIs must be accessible to users outside the internal network to deliver their full promise. Users expect to access critical functions from any device on any network, using either a web browser or a mobile application. These new web-facing interfaces expand the attack surface for your organization and require new defenses.

Today, the question becomes: How can companies deliver their web applications at scale—and secure them as they evolve over time.

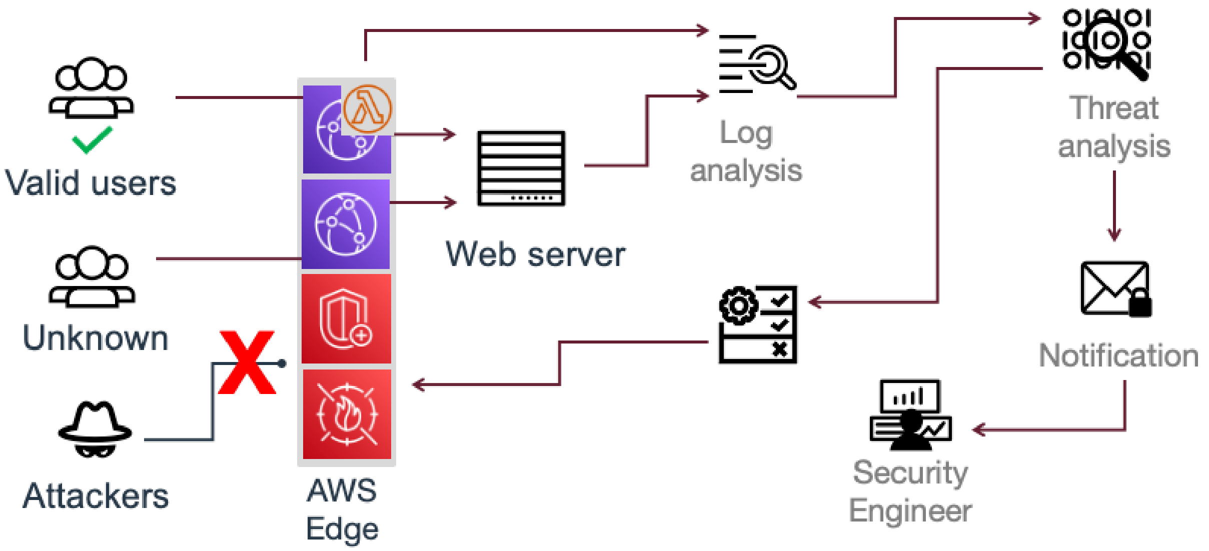
This ebook takes a look at how Amazon Web Services (AWS) and Fortinet work together so you can deliver secure web applications at scale.

- **Amazon CloudFront** is a content delivery network (CDN) that allows developers to deliver applications at a global scale. Built for high performance, it scales as application traffic grows.
- **AWS Shield** delivers automatic distributed denial of service (DDoS) protection.
- **AWS WAF** acts as a rules engine at the application layer.
- **Fortinet Managed Rules for AWS WAF** automatically updates AWS WAF with the latest threat intelligence from FortiGuard Labs.
- **FortiWeb Cloud** is a WAF-as-a-Service that delivers machine-learning enhanced threat detection, bot mitigation, and API security.

AWS WAF With Managed Rules Blocks Security Risks

With AWS WAF, you can keep your web applications secure via rules. These rules can block, allow, or monitor requests based on IP addresses, HTTP headers, or a combination of both. AWS WAF is highly customizable and offers the flexibility to tune rules based on the specific needs of your application.

Use it to recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS). You can also monitor and configure requests that are being blocked and allowed by the web access control lists rules.



Key Benefits Of AWS WAF

Global scale. Deploy on a global framework and eliminate threats before they come into your origin. AWS WAF is embedded into every one of the 300+ edge locations where Amazon CloudFront operates.

Fast incident response. In just under two minutes, you can deploy a rule on AWS WAF then send it out globally into the CloudFront network.

Pre-configured protections. AWS WAF allows you to create, deploy, and scale customized rules to protect against the latest threats.

APIs for automation. Minimize the manual resources you put into your security framework to protect your application with APIs that deliver automated security.

Fortinet Managed Rules Automatically Updates With The Latest Threat Intelligence

So how can you make sure you have the right rules in place to block malicious traffic and stay ahead of changing threats?

FortiGuard Labs, Fortinet's global threat research team, develops and maintains rulesets to protect applications that face a constantly evolving threat landscape. FortiGuard Labs ingests over 100 billion security events every day, then automatically updates the managed rules to address the latest threats.

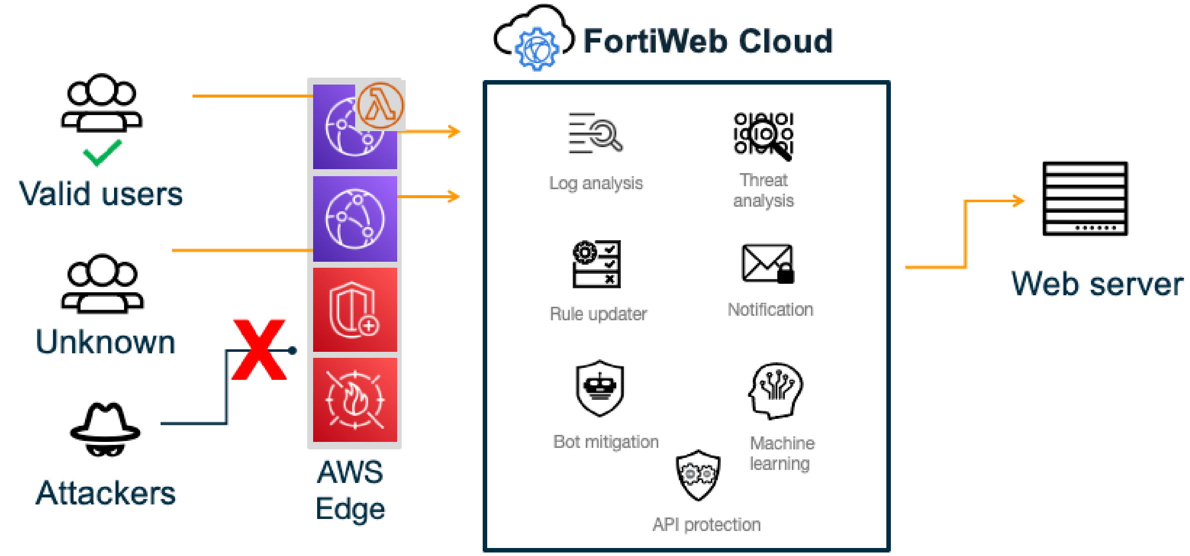
Fortinet Managed Rules For AWS WAF

For companies that subscribe to Fortinet Managed Rules for AWS WAF, rulesets are automatically provisioned. This way, they incorporate the latest threat intelligence from FortiGuard Labs.

- **General and known exploits rule group** detects common and advanced OWASP Top 10 threats. This includes numerous Injection attacks, URL redirects, HTTP response splitting, database disclosure vulnerabilities and other common vulnerabilities and exposures.
- **Malicious bots rule group** analyzes requests and blocks known content scrapers, spiders looking for vulnerabilities, and other unwanted automated clients.
- **SQLi/XSS rule group** provides protection from the two primary web application attack types identified in the OWASP Top 10, SQLi, and XSS.
- **Complete OWASP top 10 rule group** combines Fortinet's other AWS WAF RuleGroups into one comprehensive package. This includes the SQLi/XSS, general and known exploits, plus the malicious bots RuleGroups.
- **API Gateway ruleset** defends against attacks that target the AWS API Gateway and through that your backend applications.

Fortiweb Cloud Deploys Customized Protection Tailored To Your Application

For customers with more robust security requirements, Fortinet offers FortiWeb Cloud—a WAF-as-a-Service that allows you to develop protections that are customized to the specific needs of your application. FortiWeb Cloud is a cloud-native, SaaS-based WAF that leverages machine learning to protect web applications and web APIs from the OWASP Top 10 threats, zero-day attacks, and other application-layer attacks.



Key Benefits Of FortiWeb Cloud

Protection without compromise. Unlike other cloud WAFs that offer minimal, signature-based protection, FortiWeb Cloud provides a fully featured WAF powered by ML. It protects against zero-day attacks and other more sophisticated threats—all with near zero false positives.

One for all or customized. Whether you want to use the default security policies or customize per your own requirements, FortiWeb Cloud gives you the power to do so by allowing basic WAF users to be up and running in minutes while still allowing advanced and expert WAF engineers full control and fine tuning capabilities.

Exception management. Easily tune and override policies for your own needs or use a global configuration.

Multi-dimensional visibility. View high-level traffic and attack trends or drill down to investigate specific violations for the visibility you need.

Intelligent, Automatic Protection Keeps Your Web Apps Safe At Global Scale

FortiWeb Cloud delivers both the rules and the engine to keep your applications secure and reduce your operational lift. With ML at its core, it delivers bot mitigation capabilities and API protection. Customize the protection for your application, while cutting down on the manual fine tuning to keep rules up to date.

ML Intelligence Identifies Threats And Reduces False Positives

FortiWeb Cloud uses ML to understand how users typically interact with your application and detect anomalies in that behavior. Those anomalies undergo additional analysis, which helps identify zero-day threats. Examining application traffic from a broader view allows for an analysis of multiple interactions. This is instead of a single rule that's generated from a lab organization that overlooks user behavior specific to your application. This level of intelligence cuts down on the number of false positives, minimizing the amount of time you spend doing manual tuning. It also allows you to move faster. You don't have to spend as much time keeping WAF rules up to date with an evolving application.

Powerful Bot Mitigation Capabilities Help You Differentiate Between Malicious And Benign Traffic

FortiWeb Cloud includes sophisticated tools for monitoring bot traffic. For instance, it watches what sequence links are clipped. It also sees what percentage of the links on a page are actually accessed from a particular IP address. Based on behavioral elements, FortiWeb Cloud can determine what is a bot and understand how to interact with it. Because not all automated traffic is malicious, FortiWeb Cloud provides the tools to automatically differentiate between the malicious and good bots. Then you can control access where it makes sense.

API Protection Controls How Applications Interact With APIs

APIs provide a lot of power, especially for delivering user experiences on mobile applications and devices. However, when misconfigured, APIs can give unintended access to your critical business assets. FortiWeb Cloud protects your API endpoints. An automated positive security model only allows access based on your API specification. In addition, out-of-the-box security policies protect against the OWASP API Top 10 exploits.

How To Get Started

As your organization continues to reach more users with web applications and web APIs, ensure they're secure with services from AWS and Fortinet.

- AWS WAF is easy to deploy and delivers rules that block malicious traffic.
- Fortinet Managed Rules for AWS WAF bring in the threat intelligence to keep your web applications from advanced threats.
- FortiWeb Cloud acts as a WAF-as-a-Service that offers customized protection, while reducing time spent on manual tuning.

To learn more about these Fortinet services and start a free trial of FortiWeb Cloud, visit AWS Marketplace.

December 13, 2022