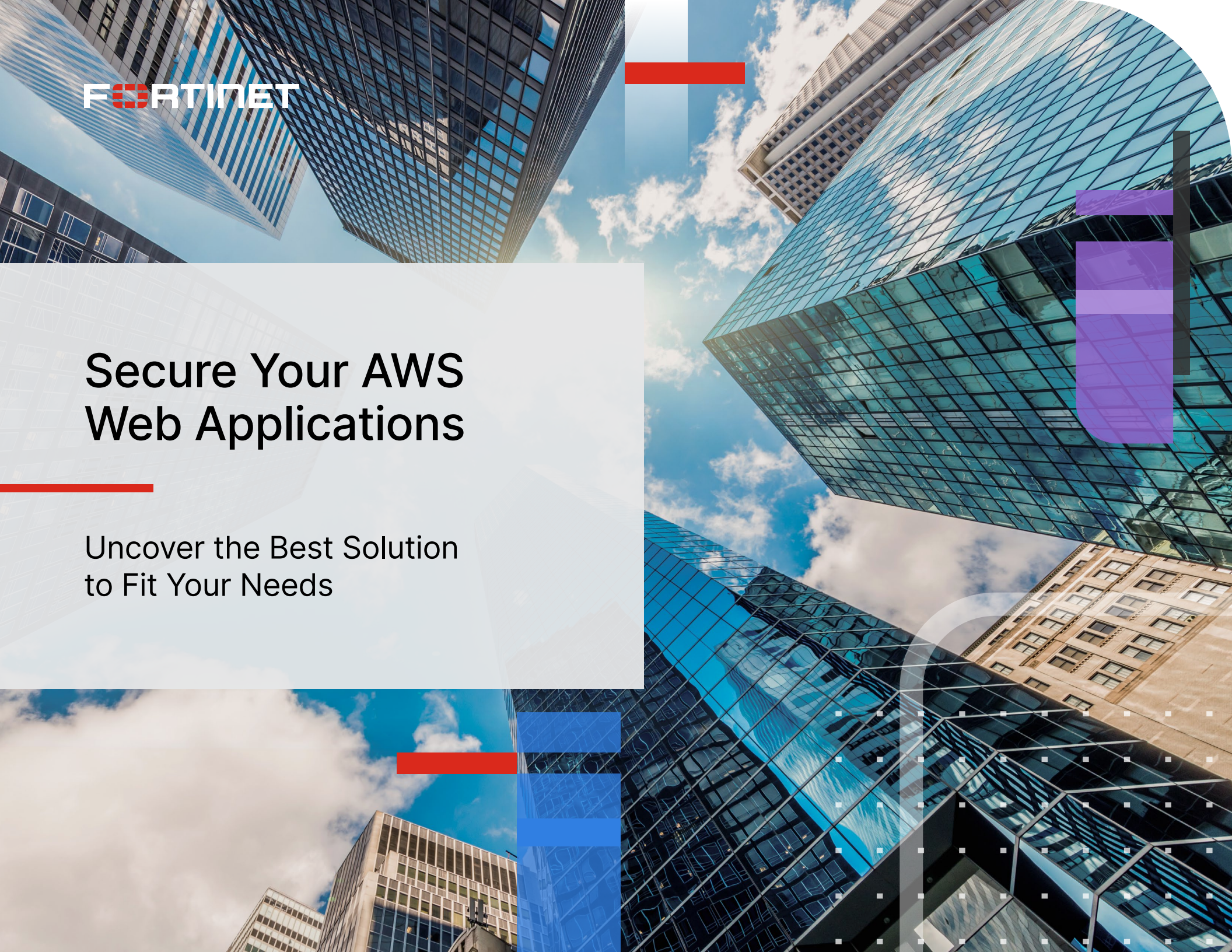


Secure Your AWS Web Applications

Uncover the Best Solution to Fit Your Needs

Table of Contents

I Built a Great Web App. How Do I Deliver It at Scale and Keep It Secure?

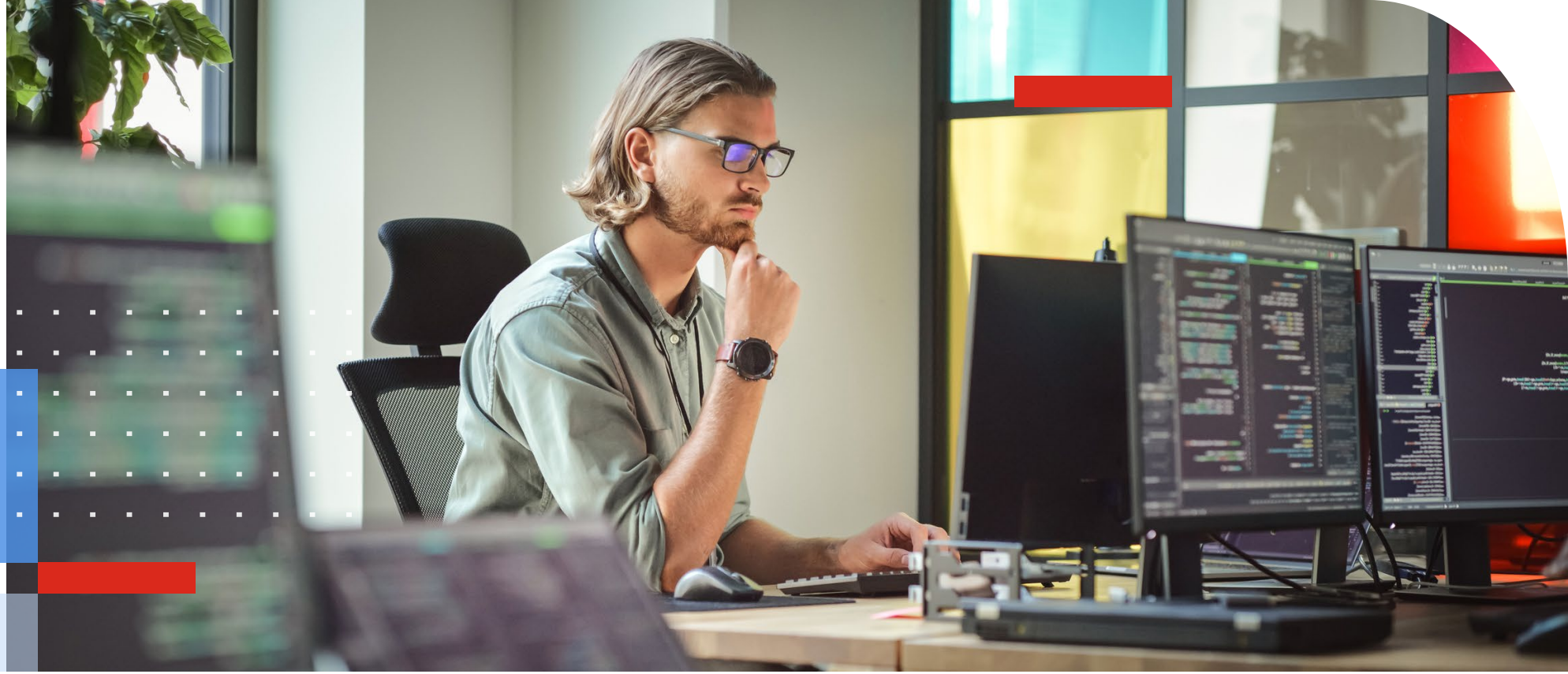
As companies accelerate digital transformation, web applications and web application programming interfaces (APIs) help drive the business forward. Often, these solutions support critical line-of-business functions, but areas such as e-commerce, human resources, and supply chain management touch sensitive assets are also attractive targets for threat actors.

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

The question is: How can companies deliver their web applications at scale and secure them as they evolve?

This ebook examines how Amazon Web Services (AWS) and Fortinet work together to deliver secure web applications at scale.

- **Amazon CloudFront** is a content delivery network (CDN) that allows developers to deliver applications globally. 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.
- **FortiAppSec Cloud** is a web application and API protection (WAAP)-as-a-Service that delivers machine-learning (ML)-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 using rules. These rules can block, allow, or monitor requests based on IP addresses, HTTP headers, or a combination. AWS WAF is highly customizable and has the flexibility to tune rules based on the specific needs of your application.

AWS WAF can 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 list 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 450+ edge locations where Amazon CloudFront operates.
- **Fast incident response:** In just under two minutes, you can deploy a rule on AWS WAF and then send it out globally into the CloudFront network.
- **Preconfigured 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 applications with APIs that deliver automated security.

Fortinet Managed Rules Automatically Updates with the Latest Threat Intelligence

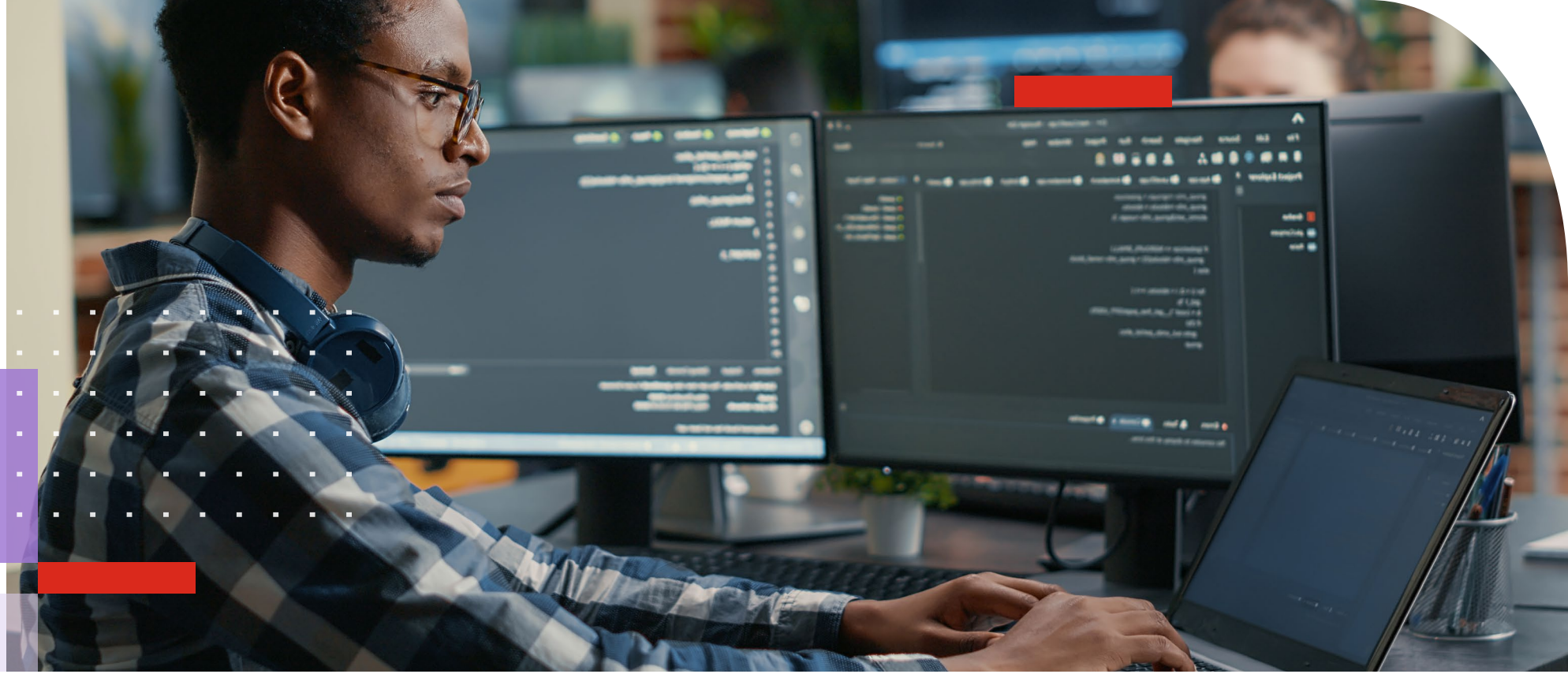
How can you make sure you have the right rules in place to block malicious traffic and stay ahead of changing threats?

FortiGuard Labs, Fortinet's elite cybersecurity research organization, develops and maintains rulesets to protect applications that face a constantly evolving threat landscape. FortiGuard Labs ingests trillions of security events, then automatically updates the managed rules to address the latest threats.

Fortinet Managed Rules for AWS WAF

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

- **The general and known exploits rule group** detects common and advanced Open Worldwide Application Security Project (OWASP) Top 10 threats. This group includes numerous injection attacks, URL redirects, HTTP response splitting, database disclosure vulnerabilities, and other common vulnerabilities and exposures.
- **The malicious bots rule group** analyzes requests and blocks known content scrapers, spiders looking for vulnerabilities, and other unwanted automated clients.
- **The SQLi/XSS rule group** protects the two primary web application attack types identified in the OWASP Top 10, SQLi and XSS.
- **The complete OWASP Top 10 rule group** combines other Fortinet AWS WAF rule groups into one comprehensive package, which includes the SQLi/XSS, general and known exploits, and the malicious bots rule groups.
- **The API gateway ruleset** defends against attacks that target the AWS API gateway and your organization's back-end applications.



FortiAppSec Cloud Deploys Customized Protection Tailored to Your Applications

Fortinet offers FortiAppSec Cloud for organizations with more robust security requirements so you can develop protections customized to the specific needs of your application. FortiAppSec Cloud is a cloud-native, SaaS-based WAAP that leverages ML to protect web applications and web APIs from OWASP Top 10 threats, zero-day attacks, and other application-layer attacks.

Key Benefits of FortiAppSec Cloud

- **Protection without compromise:** Unlike cloud-based web application firewalls (WAFs) that offer minimal, signature-based protection, FortiAppSec Cloud provides a fully featured WAAP powered by ML. It protects against zero-day attacks and other more sophisticated threats with near-zero false positives.
- **One for all or customized:** Whether you want to use the default security policies or to customize FortiAppSec Cloud to meet your requirements, FortiAppSec Cloud gives you the power to allow basic protections to be up and running in minutes while still allowing expert engineers full control and fine-tuning capabilities.
- **Exception management:** Easily tune and override policies to meet your needs or use a global configuration.
- **Multidimensional visibility:** View high-level traffic and attack trends or drill down to investigate specific violations.

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

FortiAppSec Cloud delivers the rules and the engine to keep your applications secure. With ML at its core, it delivers bot mitigation capabilities and API protection. You can customize the protection for your application while cutting down on manual fine-tuning to keep rules up to date.

ML and intelligence identify threats and reduces false positives

FortiAppSec Cloud uses ML to understand how users typically interact with your applications 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 instead of simply using a single rule generated from a lab organization, which might overlook user behavior

specific to your application. This level of intelligence reduces the number of false positives, minimizes manual tuning, and allows you to move faster because you don't have to spend as much time keeping WAF rules up to date as an application evolves.

Powerful bot mitigation capabilities help you differentiate between malicious and benign traffic

FortiAppSec Cloud includes sophisticated tools for monitoring bot traffic. For example, it watches what sequence links are clipped and can determine the percentage of the links on a page that are accessed from a particular IP address. Based on behavioral elements, FortiAppSec Cloud can determine what is a bot and understand how to interact with it. Not all automated traffic is malicious, and FortiAppSec Cloud provides the tools to automatically differentiate between malicious and good bots, so you can then control access where it makes sense.

API protection controls how applications interact with APIs

Mobile applications and devices often use APIs, but when misconfigured, APIs can provide unintended access to critical business assets. FortiAppSec Cloud protects your API endpoints using an automated positive security model that only allows access based on your API specification. Built-in FortiAppSec Cloud security policies also protect against the OWASP API Top 10 exploits.

How to Get Started

As your organization continues to reach more users through web applications and web APIs, you need to 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** brings in Fortinet threat intelligence to protect your web applications from advanced threats.
- **FortiAppSec Cloud** acts as a WAAP-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 FortiAppSec Cloud, visit **AWS Marketplace**.

www.fortinet.com

June 18, 2025 3:27 PM / MKTG-1584-0-0-EN