SOLUTION BRIEF

# Secure your web applications and APIs at top speed with Fortinet and AWS

Today, businesses rely on cloud-based web applications for their most critical line-of-business applications. In the past, deploying in the cloud meant striking a balance between performance and security. While traditional web application firewalls (WAF) could help protect against some threats, many organizations find it difficult to absorb the administrative overhead needed to understand, prioritize, and respond to security alerts.

Together, Amazon and Fortinet deliver a combined solution that enables you to confidently deploy the web applications you need to support your business initiatives. Using Amazon CloudFront to deliver your application with low-latency and high availability, in combination with web application and API security from Fortinet, your development teams can access tools they need to optimize performance, security, and cost.

**Protect against a broad range of attacks**

- OWASP Top Ten
- DDoS attacks
- Malicious bots
- Zero-day attacks
- API abuse and attacks

## Choose the right security approach for your team

In addition to the improved application performance and availability, Amazon CloudFront offers built-in security capabilities including always on DDOS protection, field level encryption and HTTPS support. Integrating CloudFront with additional security services from AWS and Fortinet can provide enhanced threat detection, improved management, automated responses, and AI-based insights.

### Good CloudFront + AWS WAF

Seamlessly integrate CloudFront with AWS Web Application Firewall (AWS WAF) to protect against multiple types of attacks including network and application layer DDoS. AWS WAF helps enforce security rules you define, which block common attack patterns such as SQL Injection, Cross Site Scripting, and familiar Bad Bots.

### Better CloudFront + AWS WAF with Fortinet Managed Rules

Reduce the admin overhead of protecting your web applications using automatically updated WAF rules from Fortinet, written for AWS WAF and based on FortiGuard Labs threat intelligence. Fortinet's rulesets provide a comprehensive package for web application protection to help cover the entire list of OWASP Top 10 web application threats.

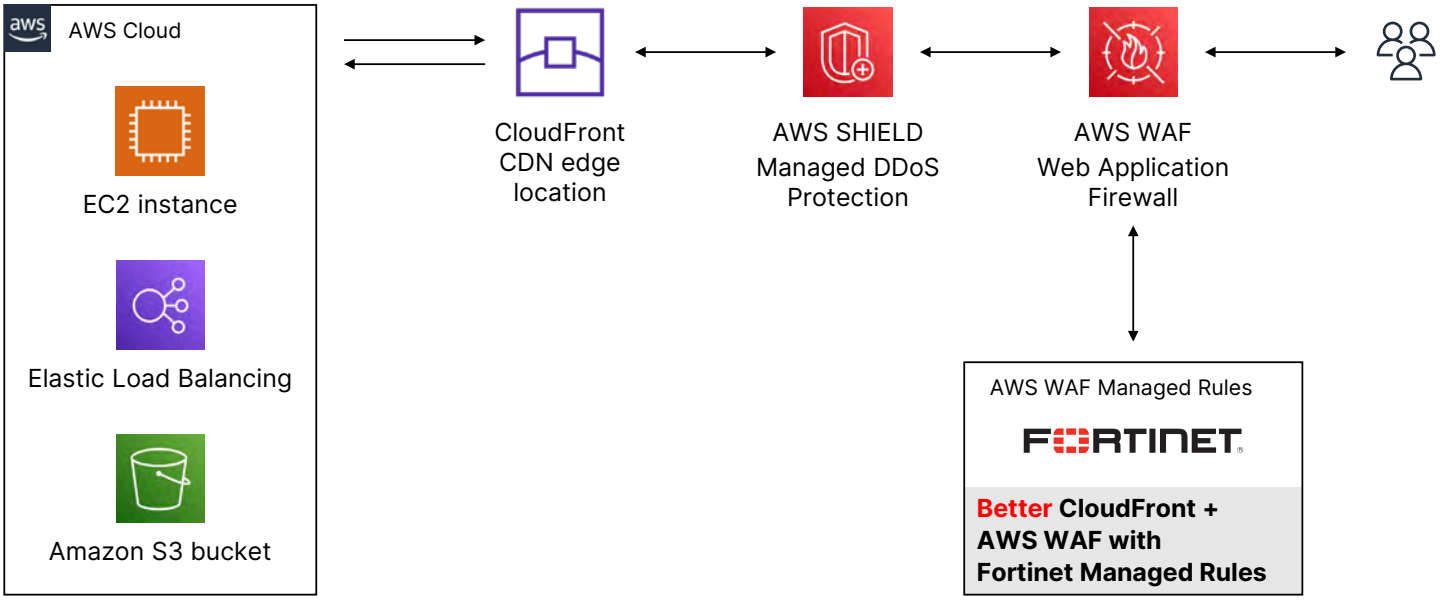
### Best CloudFront + FortiWeb Cloud

Simplify deployment and use machine learning to increase detection efficacy and lower the false positives that drive administrative overhead with FortiWeb Cloud WAF-as-a-service. FortiWeb Cloud also extends coverage for API security and bot mitigation, going beyond basic WAF use cases to deliver a full Web Application and API (WAAP) solution.

## Optimize within your AWS environment

**Good** AWS CloudFront and AWS WAF make it easy to protect your web applications against common web exploits and bots that affect availability and compromise your security. With AWS WAF, your security experts can write, customize, and deploy your security rules.

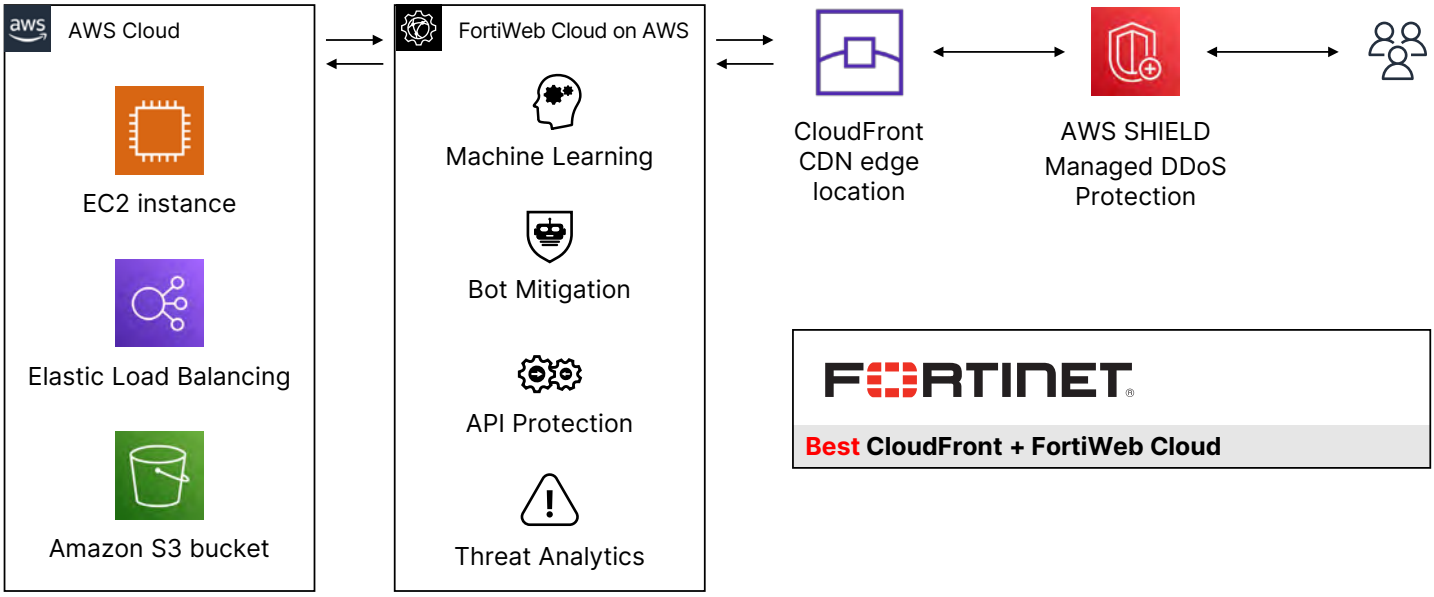
**Better** Enhance your AWS WAF using Fortinet Managed Rules for AWS WAF to automatically update rules using threat intel from FortiGuard Labs. By incorporating the latest insights from Fortinet's research, your team can focus on higher value tasks.




## Bring FortiWeb Cloud WAF into AWS

**Best** Stay on the cutting edge of security by running AWS CloudFront with FortiWeb Cloud WAF-as-a-Service. Fortinet's full web application and API Security solution uses machine learning to continuously update threat detection. FortiWeb Cloud also includes advanced bot mitigation, and API security capabilities to extend protection to the full attack surface of your CloudFront deployed web applications.

Complete with a built-in setup wizard and predefined policies, FortiWeb Cloud delivers essential security within minutes, removing the usual complexity required when setting up a WAF. More advanced users can easily enable additional security modules if needed, free of charge.




## AWS and Fortinet deliver comprehensive, consistent security

Fortinet's partnership with AWS is a better-together combination that ensures your workloads on AWS are protected by best-in-class security solutions powered by comprehensive threat intelligence and more than 20 years of cybersecurity experience.

Integrations with key AWS services simplify security management, ensure full visibility across environments, and provide broad protection across your workloads and applications.

### Better together

Working closely with AWS as an advanced Technology Partner to deliver a unified security experience since 2014

### Leading threat intelligence powered by FortiGuard Labs

Safeguarding your dynamic surfaces with security that innovates faster than attackers

### Demonstrated expertise

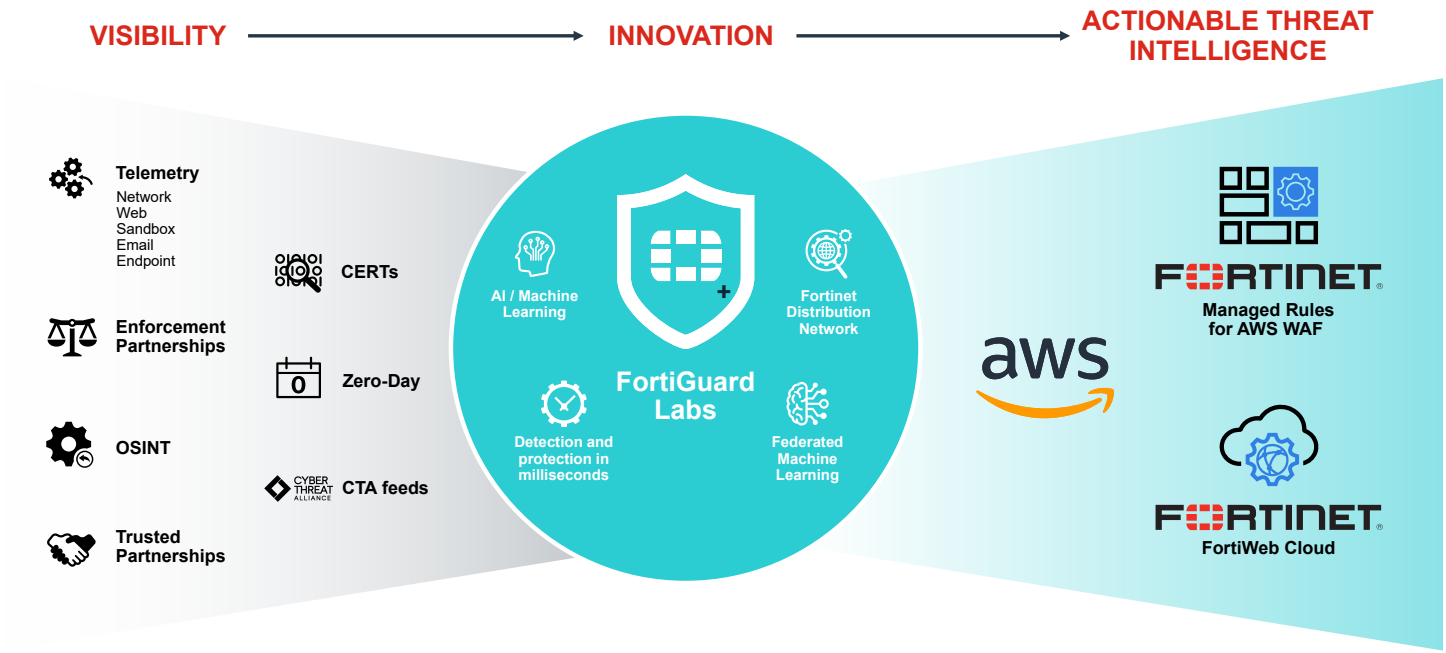
Bringing you security engineered for AWS, the market leading cloud, with more than 20 years experience

Whether you're expanding your AWS footprint, securing hybrid-cloud assets, or currently migrating to AWS, Fortinet Security Fabric delivers security-driven networking and adaptive cloud protection for the ultimate flexibility and control you need to build in the cloud.

## FortiGuard Labs delivers real-time threat defense

FortiGuard Labs is the threat intelligence and research organization at Fortinet. It is comprised of experienced threat hunters, researchers, analysts, engineers, and data scientists. Its mission is to provide customers with the industry's best threat intelligence to protect them from malicious cyberattacks.

Through artificial intelligence and machine learning, FortiGuard Labs can better understand, classify, and stop threats that aim to harm your workloads on AWS. The platform ingests over 100 billion security events and produces 1 billion security updates every day to enable a faster, more effective response to in-the-wild malware.




Start your free 14-day trial for FortiWeb Cloud WAF-as-a-Service.

Get the Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10.

FORTINET | aws

www.fortinet.com