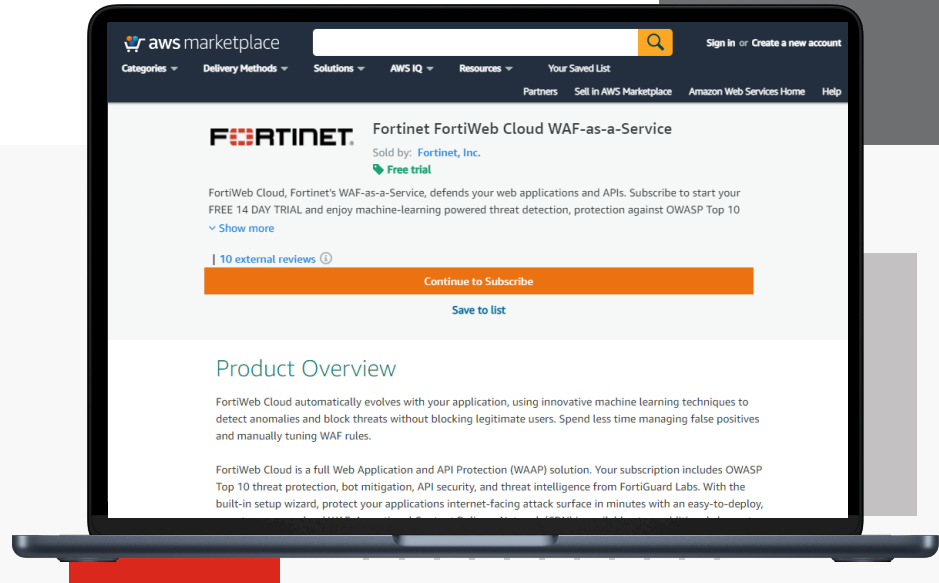# FORTINET®

FortiWeb™ Cloud WAF-as-a-Service for AWS

aws

Highlights

100% cloud-based WAF-as- a-Service

Pay as you go, based on traffic and the number of applications protected

Protection against OWASP Top 10, including cross-site scripting and SQL injection

Rapid deployment via AWS Marketplace

Advanced analytics and reporting

Fine tuning for exceptions

Secured by FortiGuard Labs

Delivered within the same AWS region as your application, providing improved performance, a simplified regulatory environment, and reduced bandwidth costs

A Cloud Native Solution Deployed in the Same AWS Region as Your Application

FortiWeb Cloud web application firewall (WAF) as a Service delivers web application security as a SaaS solution. Protect your hosted web applications without deploying and managing infrastructure — let Fortinet secure your applications while you focus on delivering business value with your web applications.

The solution requires minimal configuration and management and can be deployed in front of your applications by subscribing via the AWS Marketplace. The solution uses multiple protection techniques to quickly and accurately mitigate threats while allowing normal traffic to proceed.

Highlights

### A Full-featured WAF that's Easy to Deploy and Manage

With FortiWeb Cloud WAF-as-a-Service, enjoy the protection of a full-featured WAF as you rapidly roll out your applications in AWS without managing and maintaining your own infrastructure.

Your attack surface changes every time you deploy a new Internet-facing application, and with public cloud you can deploy those Internet-facing applications faster than ever. You need a solution that can protect any web-based application you deploy, including short-lived applications that may only run for a short time and long-lived applications that can evolve rapidly as you adopt a DevOps approach to deliver applications and services at high velocity.

Protecting your applications with a SaaS-delivered WAF solution also provides the ability to pay as you go, allowing you to provide the same protection for all of your AWS-hosted applications without standing up excess capacity that may be underutilized.

Web Application Threat Protection

FortiWeb Cloud WAF-as-a-Service uses the same comprehensive approach to security as other FortiWeb form factors, including IP reputation, DDoS protection, protocol validation, application attack signatures, and more to defend your application against a wide range of threats, including the OWASP Top 10.
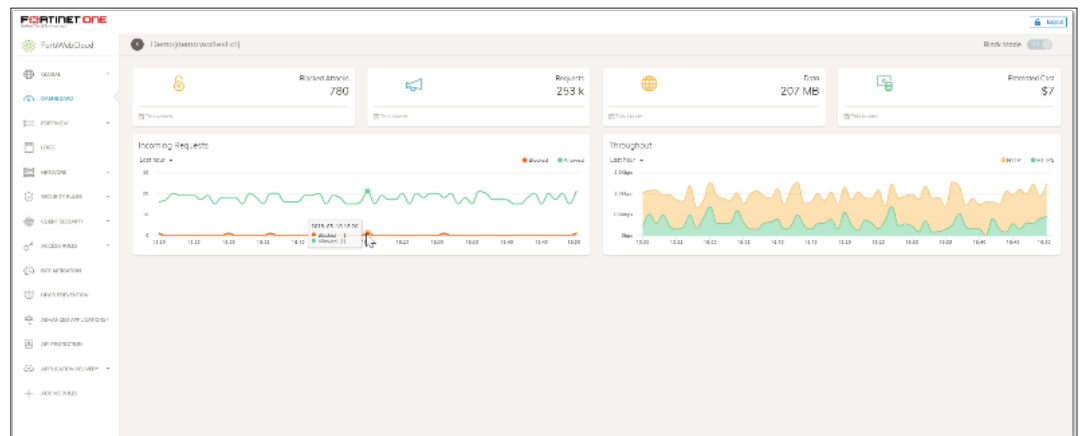
Highlights

Simplified Deployment

Simply purchase through the AWS Marketplace and follow the built-in setup wizard. With predefined policies, FortiWeb Cloud WAF-as-a-Service delivers the security you need 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. Deploy in minutes and you're protected from threats such as cross-site scripting, cross-site request forgery, denial-of-service, brute-force attacks, and SQL injection.

Deployed in the same AWS region as your Application

Because Fortinet delivers the service using a colony of WAF gateways in the same AWS region as your application, you enjoy the benefits of low latency, intra-region bandwidth rates for your traffic between your application and the WAF, and a simplified regulatory environment.
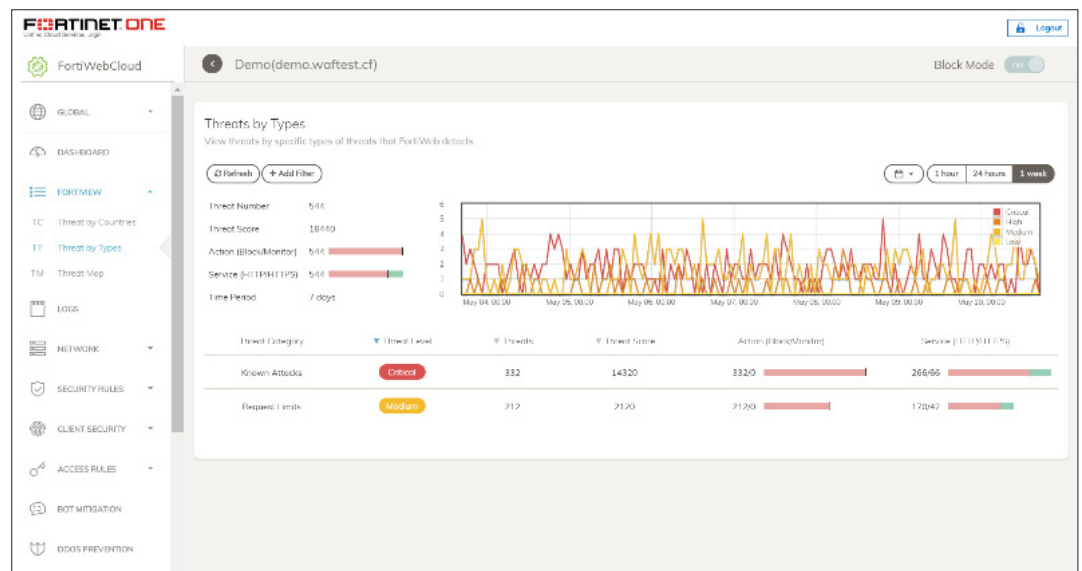
Secured by FortiGuard Labs

Fortinet's Award-winning FortiGuard Labs is the backbone for FortiWeb Cloud signatures and IP Reputation. As long as you're an active FortiWeb Cloud Subscriber you automatically have the latest protections and updates without having to do anything further.
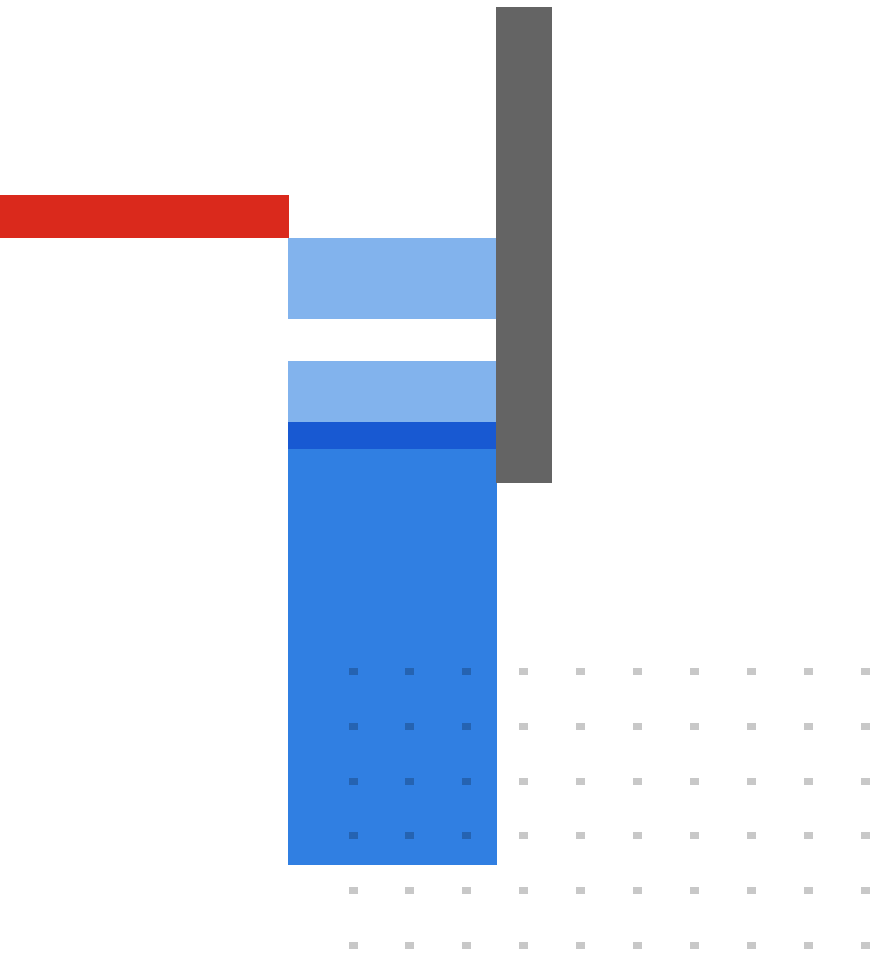
Ordering Information

Available through the Amazon Web Services Marketplace.

Units	Price
Total number of web applications protected by FortiWeb Cloud	$0.03 / unit
Total data transferred via FortiWeb Cloud (GB)	$0.40 / unit

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

FERTINET

January 27, 2023

FWEB-CL-AWS-DAT-R7-20230127