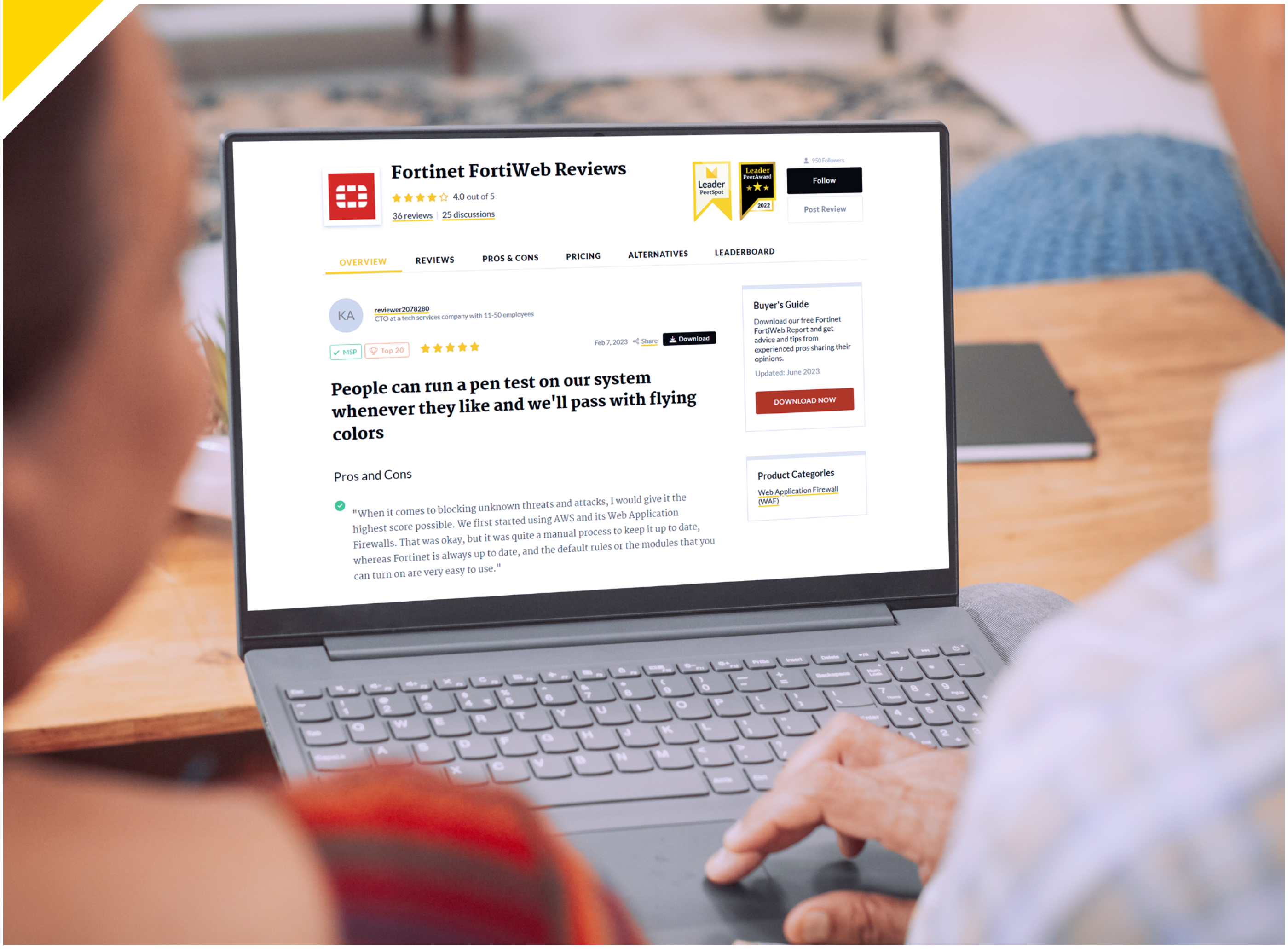
PeerPaper™ Report 2023

Discover how your peers are leveraging FortiWeb Cloud

How to Defend Your Web Apps and APIs from the Known and Unknown



Fortinet FortiWeb Reviews

★★★★☆ 4.0 out of 5

36 reviews | 25 discussions

reviewer2078280
CTO at a tech services company with 11-50 employees

Feb 7, 2023

People can run a pen test on our system whenever they like and we'll pass with flying colors

Pros and Cons

"When it comes to blocking unknown threats and attacks, I would give it the highest score possible. We first started using AWS and its Web Application Firewalls. That was okay, but it was quite a manual process to keep it up to date, whereas Fortinet is always up to date, and the default rules or the modules that you can turn on are very easy to use."

Buyer's Guide

Download our free Fortinet FortiWeb Report and get advice and tips from experienced pros sharing their opinions.

Updated: June 2023

Product Categories

Web Application Firewall (WAF)

PeerSpot

Contents

Introduction

As web applications grow in importance and touch more business-critical workflows, their security becomes an ever-higher priority. As a result, security professionals need a Web Application Firewall (WAF) that can protect the entire web application and API attack surface. This capability cannot create complexity and overtax resources, however. PeerSpot members have found that Fortinet's FortiWeb Cloud WAF-as-a-Service (WAFaaS) enables them to succeed in this mission. As discussed in this paper, the key factors that drove their selection of FortiWeb Cloud included the ability to save time, money, and resources. They also highlighted the importance of identifying unknown threats and reducing false positives through machine learning.

A Brief Overview of Web Application Firewalls

A WAF is a specialized form of firewall that is designed to defend web applications. As WAFs have evolved and extended themselves into protecting APIs, Gartner now refers to them as Web Application and API protection (WAAP) solutions. Labels aside, WAFs filter, monitor, and block HTTP traffic that is going into and out of a web service.

By performing these inspections on HTTP traffic, a WAF can prevent attacks that exploit vulnerabilities in the app, e.g., SQL injection and cross-site scripting (XSS). FortiWeb Cloud protects against the Open Worldwide Application Security Project® (OWASP) Top 10 and includes more robust features, such as anomaly detection, API discovery and protection, and bot mitigation. FortiWeb also provides multi-dimensional reporting as well as advanced threat analytics.

Web Application Firewalls

Why PeerSpot Members Chose FortiWeb Cloud Over Competitors

PeerSpot members revealed why they selected FortiWeb Cloud over alternatives on the market. For example, a Director of IT at a small tech services company found Microsoft Azure's WAF solution to be "a little bit expensive for a startup project." She also said, "The Azure firewall has limited configuration options that aren't helpful in our use case. FortiWeb is easier to configure and has pay-as-you-go pricing based on traffic, which is ideal for a startup company."

For a Security Specialist at Hitachi Energy, a manufacturing company with over 10,000 employees, what mattered was ease of configuration. He explained, "We also checked other WAF solutions such as Akamai and CloudFlare but didn't do a PoC [Proof of Concept] with them. We did a PoC with OCI WAF, Microsoft Azure WAF, Google Cloud Armor, and Fortinet FortiWeb." However, for OCI WAF, Microsoft Azure WAF, and Google Cloud Armor, as he put it, "their configuration isn't very easy."

Blair Griffith-Barwell
Principal Network Architect
at Global Processing

★★★★½

> "Implementing FortiWeb was extremely fast and easy, which was a significant advantage. It comes with several preconfigured rule sets and templates."

Read review »

CTO
at a tech services company
with 11-50 employees

★★★★★

> “With the machine learning and getting the benefit of traffic that is going to many different sites, Fortinet is able to know which traffic is legit and which isn’t. As a result, we get fewer false positives.”
>
> **Read review »**

In contrast, he said, “It’s pretty simple in FortiWeb, and we can enable or configure whatever we want.” In the end, they went with FortiWeb because his team “wanted a single solution that can be implemented anywhere.” In other words, going with Azure WAF makes it a challenge for those with multi-cloud environments.

“There are many security constraints that cannot be fulfilled by native cloud firewalls such as Azure and AWS,” said a Cloud Architect/Solution Architect at a tech services company with over 10,000 employees. “For example, AWS has a limitation of 8GB with regard to request values.”

Manual processes drove competitive selection for the CTO of Probax, a small tech services company. He said, “We first started using AWS and its Web Application Firewalls. That was okay, but it was quite a manual process to keep it up to date, whereas Fortinet is always up to date, and the default rules or the modules that you can turn on are very easy to use. We saw value from it immediately.”

This user also shared that he was uncertain about how the AWS WAFs were protecting his web applications. He said, “We weren’t that confident, because we couldn’t really see what was happening. Management was kind of uneasy as a result. As soon as we had this [FortiWeb Cloud] implemented, we could see the stats and a few graphs. Immediately, that peace of mind was had by all.”

Key Selection Factors

What makes for an effective WAF solution? What came through in PeerSpot reviews was a desire to deploy a WAF that strikes an optimal balance between protection capabilities and the administrative overhead required to run the WAF itself. Users wanted ease of use, streamlined tasks, and reductions in false positives, which create alert fatigue. At the same time, they wanted to use machine learning to block unknown threats.

Ease of Use

A WAF needs to be easy to use, and unfortunately, WAFs have historically been complex to set up and put to work. Security teams are already dealing with enough complexity, so a WAF that can simplify life is a boon. As a Senior Manager at CLOUDSUFI, a software company with more than 200 employees, put it, “FortiWeb Cloud is straightforward to use; with a basic overview of how to apply policies, create NAT [Network Address Translation] rules, etc., it’s easy. The console is user-friendly enough that anyone can create and apply policies.”

Easy to Use

Hitachi Energy's Security Specialist concurred, saying, "It's easy to use. I don't have to do any changes in my environment. For example, if I use Azure WAF, I have to use a traffic gateway, load balancer, or something similar, whereas, with FortiWeb, I don't have to change any architecture. I just have to change my DNS entry. That's it. If I'm able to change my DNS entry, FortiWeb works. Every team has different requirements, but if you need an easy solution that can be deployed in a very short time, FortiWeb is the right one."

This user also commented that adding new applications to FortiWeb was "quite easy." He said, "You just add the application and change the DNS settings, and you are good to go. Whether you want to block or unblock, or you want the learning mode or protection mode, you can enable or disable it with just one click, and you are good to go. The configuration part is easy. The configuration and implementation process is streamlined. We don't have to change anything. We don't have to follow 10 processes. It's a single process with which everybody is familiar."

“FortiWeb’s ease of deployment is what we liked the most about it,” said a Principal Network Architect at Global Processing, a financial services firm with more than 200 employees. He added, “Implementing FortiWeb was extremely fast and easy, which was a significant advantage. It comes with several preconfigured rule sets and templates.”

He further shared, “FortiWeb is effortless to use and manage. The documentation is excellent, which is another huge advantage. The layout is logical and intuitive. You can create templates and reapply them to new applications, so we don’t need to do a fresh configuration for each application. We have a template that represents our security benchmark. There are a few exceptions that we need to add for each application, but we can redeploy the security benchmark template for each new application that we create.”

Blair Griffith-Barwell
Principal Network Architect
at Global Processing

★★★★½

“FortiWeb is effortless to use and manage. The documentation is excellent, which is another huge advantage. The layout is logical and intuitive. You can create templates and reapply them to new applications.”

Read review »

CTO
at a tech services company
with 11-50 employees

★★★★★

> “That’s the whole advantage of using a cloud-based platform. You get the benefits of another site seeing an attack and Fortinet works out if traffic should be filtered or not. It’s great all around.”
>
> Read review »

Block Unknown Threats

Ability to Block Unknown Threats

Unknown threats keep security teams up at night. Machine learning within a WAF can help solve this. FortiWeb leverages machine learning to model each application, identifying malicious anomalies to block unknown, or zero day, threats.

While machine learning “could be a little bit of a buzzword” for Probax’s CTO, he explained, “That’s the whole advantage of using a cloud-based platform. You get the benefits of another site seeing an attack and Fortinet works out if traffic should be filtered or not. It’s great all around.”

In his case, he is “quite particular about what I allow into our network.” He added, “With the machine learning and getting the benefit of traffic that is going to many different sites, Fortinet is able to know which traffic is legit and which isn’t. As a result, we get fewer false positives.”

A Security Engineer at a small tech consulting company attributed the protection against unknown attacks to FortiWeb’s effective machine learning. He said, “It operates on the probability of attacks. The most valuable feature is the attack signature and machine learning.”

The CTO of Probax added context, saying, "Being a data protection company, we have to meet a lot of specific requirements for customers. When people would say, 'Our standard practice is to do a pen test against your outward-facing servers,' there was always a little bit of worry in the back of my mind: 'Oh, man, is there something that I've forgotten about?'"

This user no longer has this concern. He said, "I know that people can run a pen test whenever they like and we'll pass with flying colors. When it comes to blocking unknown threats and attacks, I would give it [FortiWeb] the highest score possible."

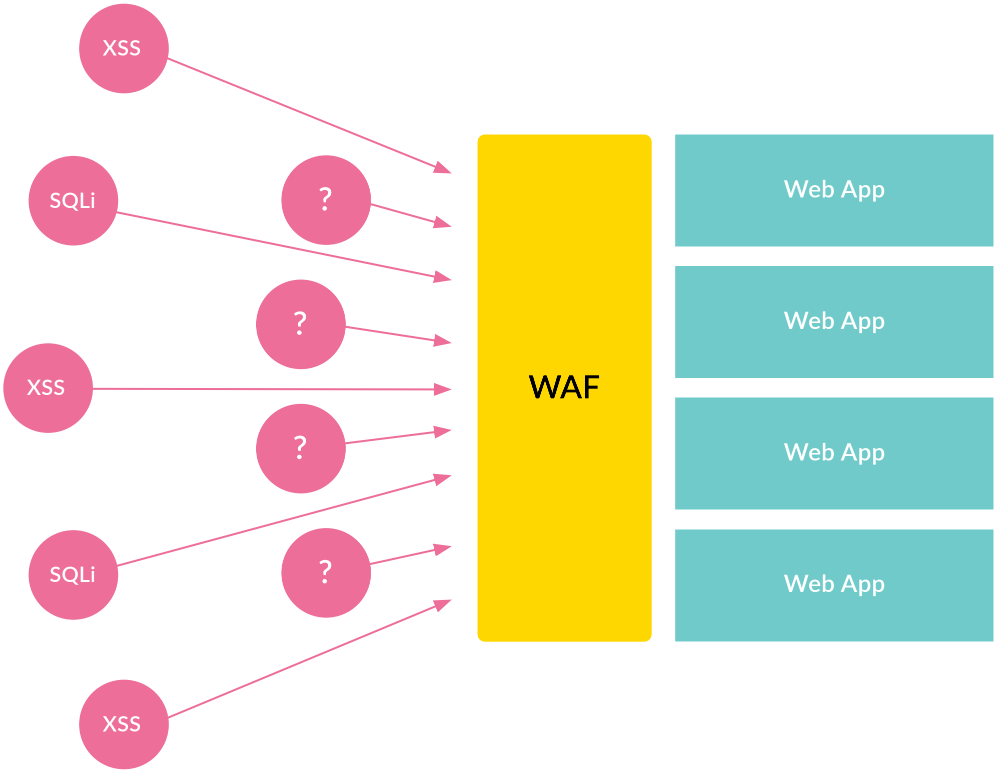


Figure 1 - A WAF needs to be able to block both known and unknown attacks.

Pawan K.
Senior Manager at a
computer software company
with 201-500 employees

> "The product is great for blocking unknown threats and attacks. We've had excellent results over the past two years, and the way it detects and filters traffic is outstanding."
>
> **Read review** »

"FortiWeb effectively addressed unknown threats," said Global Processing's Principal Network Architect. "We get regular reports that we check. So far, we've had no issues at all. Around 99 percent of our public-facing infrastructure is restricted by source IP to our partners' networks, so our attack surface is restricted. WAF picked up and blocked any attacks before they can impact us." Figure 1 depicts this capability.

Detection analytics and the filtering capabilities are what stood out to a Director of IT at Dynamic Access Systems, a small consultancy. FortiWeb shows what threats have been detected and mitigated, along with where they are coming from. He said, "That has allowed us to do some additional filtering because by looking at threats, we can apply additional filters and try to minimize some of them."

Other notable comments about blocking unknown threats included:

- "Fortinet FortiWeb seems to have worked well for blocking unknown threats and attacks." - Director of IT at Dynamic Access Systems
- "The product is great for blocking unknown threats and attacks. We've had excellent results over the past two years, and the way it detects and filters traffic is outstanding." - Senior Manager at CLOUDSUFI
- "FortiWeb is good for blocking unknown threats and attacks. I've done a PoC with Azure WAF and OCI WAF, and in comparison, FortiWeb is quite good." - Security Specialist at Hitachi Energy

Relief from Alert Fatigue

False positives and alerts consume security analysts' time. With analysts already overburdened, and alert fatigue a common challenge, the fewer false positives, the better. Global Processing's Principal Network Architect spoke to this need when he said, "We already had a low false positive rate, but FortiWeb has lowered it further. Detections in our report tend to be accurate. We still get occasional false positives, but some of that probably relates to our custom-built applications. FortiWeb decreased our false positives by around 30 percent." Figure 2 shows a WAF keeping false positives away from security admins.

Less Alert Fatigue

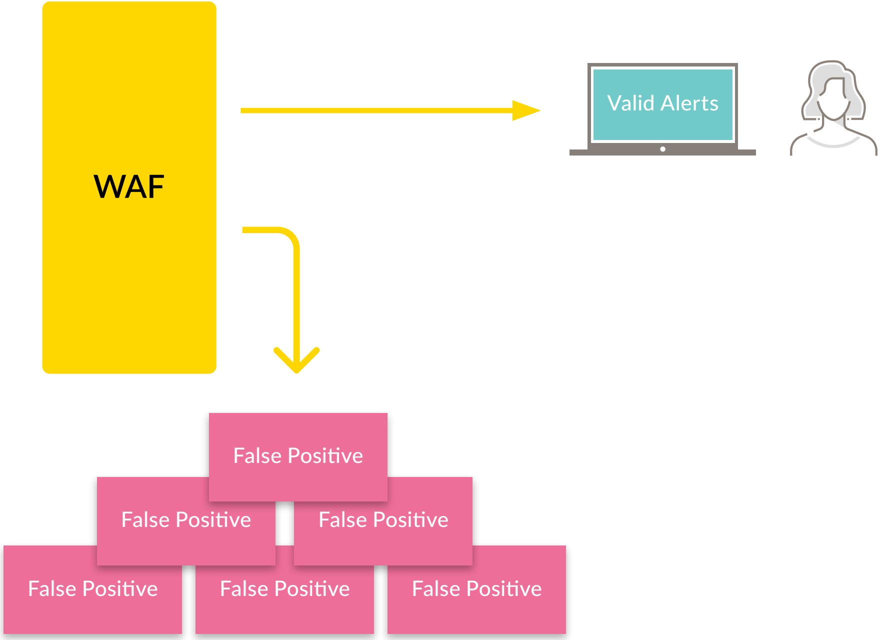


Figure 2 - A WAF needs to reduce the rate of false positives, ideally only showing valid alerts to security analysts.

Pawan K.
Senior Manager at a
computer software company
with 201-500 employees

> “Our organization receives fewer alerts thanks to the solution, and we don’t have to think about the security of the URLs for applications.”
>
> **Read review »**

The solution also reduced Global Processing’s alerts by between 70 and 80 percent. This user added, “The alerts coming from FortiWeb are helpful. They inform us of things that require action. We previously got many alerts from our public-facing services. We didn’t have an efficient means of getting alerts. The same threat provided multiple alerts. That would keep going and could be overwhelming at times.”

Other PeerSpot members were also able to quantify their reductions in false positive and alerts after adopting FortiWeb. CLOUDSUFI’s Senior Manager said FortiWeb helped reduce false positives by 20-25%. He observed, “Our organization receives fewer alerts thanks to the solution, and we don’t have to think about the security of the URLs for applications. We put the whole domain behind the WAF, and if it’s configured correctly from the beginning, we spend minimal time making changes and get the precise results we need. Our alerts have been reduced by approximately 5%.”

“It has reduced false positives,” said Hitachi Energy’s Security Specialist. He went on to say, “As compared to my old solution, there is at least a 17% to 18% reduction. It has reduced the number of alerts that our organization receives. There is a 50% to 60% reduction in alerts.”

Efficiencies to Alleviate Security Skills Shortage

According to recent research, there is currently a global cybersecurity workforce shortage of 3.4 million people. A WAF solution should ideally make it possible for security and network teams to work more efficiently by streamlining tasks to save time and free up staff. As Dynamic Access Systems' Director of IT noted, "It [FortiWeb] has minimized the number of technical resources and the amount of time that we've had to dedicate to setting up and managing the front-end firewall capability. From that standpoint, it has saved us time."

According to Hitachi Energy's Security Specialist. "We were spending around three to four days setting up our old solution, whereas now, we are spending a maximum of four hours."

Free Up Staff

CTO
at a tech services company
with 11-50 employees

★★★★★

> **“FortiWeb has saved us hundreds of hours.”**
>
> **Read review »**

FortiWeb Cloud streamlines tasks for Global Processing’s Principal Network Architect because, as he remarked, “We’ve eliminated other functions like load balancing.” He offered an example of what he called “the excellent API,” which allowed someone on his team to create an application that integrates with the API to quickly add new IP addresses without changing the templates. He said, “We’ve found it’s helped us streamline some of our usual BAU [business as usual] tasks.”

FortiWeb Cloud has enabled Probax to free infrastructure team for other work, because they no longer have to look after the AWS Web Application Firewalls, according to their CTO. With AWS WAFs, he said, “The process would be to look at our web servers and see if there was any suspicious-looking traffic that had gotten to those web servers through the AWS firewalls, and then we would adjust the AWS firewalls accordingly to filter that out. We might even have had to write new code to stop things at the server level. FortiWeb has saved us hundreds of hours.”

Conclusion

WAFs play a critical role in defending web applications and APIs. They must also be efficient, easy to use, and able to prevent alert fatigue. These qualities, along with machine learning to block unknown threats and the ability to save time, were what drove PeerSpot members to select Fortinet's FortiWeb Cloud WAF-as-a-Service. With FortiWeb Cloud, security teams can defend their web applications and APIs that help support business critical workflows and enable innovation.

You can get a 14-day free trial through your cloud marketplace of choice at: fortiweb-cloud.com

About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

About Fortinet

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking consistently as a leader in firewalls, more than 650,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone.