

aws marketplace

Check Point WAF (formerly CloudGuard WAF)

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

- Product Recap..... 3 - 5
- Valuable Features..... 6 - 13
- Other Solutions Considered..... 14 - 16
- ROI..... 17 - 19
- Use Case..... 20 - 23
- Setup..... 24 - 26
- Customer Service and Support..... 27 - 29
- Other Advice..... 30 - 33
- Trends..... 34 - 35
- About PeerSpot..... 36 - 37

Product Recap



Check Point WAF (formerly CloudGuard WAF)

Check Point WAF (formerly CloudGuard WAF) Recap

Check Point WAF uses AI-driven threat prevention with seamless API integration, offering advanced DDoS protection. It auto-learns attack patterns, updates protection, and minimizes false positives. Its interface simplifies policy management for secure web applications across cloud environments.

Check Point WAF combines AI-driven threat detection with streamlined policy management to provide effective security for web applications and APIs. It offers zero-day protection, threat intelligence, and advanced DDoS protection. Users enjoy robust logging and compliance management across multi-cloud environments. Integration is smooth, with reduced reliance on signatures, facilitating multi-layer security. Despite its strengths, users note areas for improvement, such as latency and pricing, and call for enhancements in API security, real-time monitoring, and reporting. Challenges include integration complexity and limited technical support accessibility. Effective application security across dynamic environments is a key offering.

What are Check Point WAF's key features?

- **AI-Driven Threat Prevention:** Utilizes AI to identify and block threats, minimizing false positives.
- **Seamless API Integration:** Ensures integration into existing infrastructures without delays.
- **Advanced DDoS Protection:** Safeguards against large-scale attacks to maintain service availability.
- **Auto-Learning Capability:** Continuously adapts to new threat patterns for improved security.
- **User-Friendly Management:** Simplifies policy and compliance management tasks.

What benefits can users expect from Check Point WAF?

- **Extensive Logging:** Enables comprehensive analysis and auditing through detailed records.
- **Reduced Total Cost of Ownership:** Provides cost-effective security measures in cloud environments.
- **Zero-Day Protection:** Offers proactive defense against unidentified vulnerabilities.
- **Streamlined Deployment:** Reduces deployment times with easy integration processes.
- **Robust Multi-Layer Security:** Reinforces application security without heavy reliance on signatures.

Check Point WAF finds particular relevance in industries requiring robust cybersecurity measures such as finance, healthcare, and e-commerce. These sectors benefit from its advanced threat detection and adaptive security policy management, crucial for securing sensitive data across multi-cloud infrastructures. By managing API usage efficiently, it helps maintain regulatory compliance while ensuring optimal operation. Enhanced traffic logging and malware threat management add to its appeal for organizations focusing on securing transactions and sensitive information.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “In short, Check Point CloudGuard WAF is a powerful tool.”



KrishnakumarM
CISO at Pink Solutions

✓ “Check Point CloudGuard WAF has positively impacted our organization in security and operational efficiency, with a 30-40% drop in malicious traffic and a 15-20% reduction in manual intervention for our SOC team due to reduced false positives and automated protection.”



Verified user
Assistant Manager at a computer software company with 201-500 employees

✓ “The biggest benefit from Check Point CloudGuard WAF that I saw is that it comes with one solution that completely outperforms its competitors.”



Ricky Makkar
Senior Network Security Consultant at NTT DATA

- ✔ “Check Point CloudGuard WAF provides great visibility and flexibility to use multiple FQDNs in a single load balancer.”



Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

- ✔ “Check Point CloudGuard WAF has been especially helpful here, automatically learning and adjusting protection without requiring constant manual tuning.”



Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200 employees

- ✔ “Check Point CloudGuard WAF has really reduced the headache of IT engineers and has helped me in security through machine learning.”



Sachin-Yadav

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

- ✔ “Overall, it's a good solution, and it fulfills all our core purposes, providing complete visibility and security.”



Mantu Shaw

Project Manager at a outsourcing company with 1,001-5,000 employees

What users had to say about valuable features:

“Check Point CloudGuard WAF offers the best features through its dual ML engine with attack-based and context-based capabilities. The dual engine directly reduces the operational load and improves detection quality for my team on a day-to-day basis.

Additionally, it allows for less policy tuning. Check Point CloudGuard WAF has positively impacted my organization by reducing my manual effort. It reduces up to 2x my operational effects, leading to lower false positives..”

Nitin Yadav

Network & Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“The efficiency improvements provided by Check Point CloudGuard WAF are something I can describe. It was fairly easy to set up Check Point CloudGuard WAF if you are looking at the basic configuration. It was pretty acceptable with setting up rules, and so forth. If you were looking for advanced configurations, then you had to go for a different setup, and that made it a little bit complicated.

“In terms of efficiency, Check Point CloudGuard WAF is very straightforward to set up rules because you really do not need to do much customization, as it is the case with all Cloud WAFs.

“I have been familiar with Check Point CloudGuard WAF for about six months..”

Antonis Hassiotis

IT Security & Networks Administrator at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“The biggest benefit from Check Point CloudGuard WAF that I saw is that it comes with one solution that completely outperforms its competitors. While there are other vendors such as Azure or AWS that provide their own WAF solution, that is comparatively not good enough. Check Point CloudGuard WAF prevents everything, their applications, their APIs, protecting them completely from DDoS attacks. It also has an AI feature that learns automatically from patterns, implying remediation to mitigate regular attacks on the network.

Breach reduction occurs when there is a compliance issue or vulnerability within the organization. Since Check Point CloudGuard WAF has the capability to learn itself, as it understands the patterns of risks and attacks, it auto-generates remediation plans by itself, thus effectively reducing breaches on this platform..”

Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

“I have worked as a customer, partner, solutioner, and implementer. I have been with Check Point since Check Point NG's time. Check Point launched the new generation around 2000 if I understood correctly, and I have been with Check Point since then.

These kinds of Israeli products are strong, clever, and powerful tools. They are all strong, clever, and powerful tools compared with American products, to be honest and upfront. Palo Alto has beaten Check Point in the recent past by bringing these creamy layers of Israeli companies into their organization, if I understood correctly.

I am a CCSE by the way. Check Point Certified CCSE. I have been holding this certification for quite some time. In short, Check Point CloudGuard WAF is a powerful tool. In short, its look and feel is also not something everyone will like. People like me, a rare breed, will like Check Point CloudGuard WAF. Not everyone, to be honest.

There are some scoring companies I have worked with that focus on security scoring, risk scoring, and prioritization. These are all very good in Check Point CloudGuard WAF, I would say. Advanced threat detection is also fine. Check Point CloudGuard WAF also provides threat intelligence for us, which includes actionable information about current and emerging security threats. Check Point CloudGuard WAF produces all kinds of reports that involve collecting, analyzing, and sharing data about threat actors and their TTPs and IOCs. It is also strategic, tactical, technical, and operational. I like their threat intelligence products. It is strategic, tactical, technical, and operational..”

KrishnakumarM

CISO at Pink Solutions

[Read full review](#) 

“Check Point CloudGuard WAF offers various capabilities including AI-based threat prevention, API security, DDoS protection at multi-layer, L3 and L7 protection, bot protection, behavioral analysis, and fingerprinting.

AI-based threat prevention stands out for me because instead of relying on static signatures that have been added in the cloud, it uses behavioral baselines. For example, if I'm using an application with behavioral application capabilities, it provides me high security using AI-based threat prevention. Behavioral learning mode has been divided into various phases. The first phase is the learning mode where it automatically learns. Whenever I onboard any app, it observes the traffic for a short duration or builds a statistical model for that application, and no manual training is required. In phase two, enforcement mode, any new request is evaluated against known attack patterns via machine learning.

Real-time response is really helpful when onboarding any application with Check Point CloudGuard WAF. When we onboard any application, it creates a statistical model of that application, and according to that, it observes known attack patterns, then blocks them instantly, providing another layer of security.

Check Point CloudGuard WAF has really reduced the headache of IT engineers and has helped me in security through machine learning..”

Sachin-Yadav

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

[Read full review](#) 

“Check Point CloudGuard WAF provides great visibility and flexibility to use multiple FQDNs in a single load balancer. I am using multiple products with a similar solution, such as F5 and Check Point CloudGuard WAF. F5 operates with the discovery module and the API protection module only on a number of FQDN basis. This is a great, flexible option where I can implement multiple applications using a single load balancer.

“The total cost of ownership has definitely reduced for my application firewall because there is no limitation on the load balancer for implementing FQDNs. FQDN is a fully qualified domain name. For example, I have an application on the load balancer with a.novaktech.one, and similarly, b.novaktech.one is another application, while c.novaktech.in is a third application. I can implement multiple FQDNs in a single load balancer.

“Regarding the false positive rate, Check Point CloudGuard WAF has helped to reduce it as it gives more true positive cases rather than false positives. The technology leveraging Check Point's security provides threat intelligence where I can get DDoS and attack signatures and all AI/ML-based signatures. The false positive rate is very low. The approximately reduced false positive rate is about seventy percent. No product will give one hundred percent accuracy, but it detects seventy percent..”

Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

[Read full review](#) 

Other Solutions Considered

“I have experience with FortiWeb, although we just stopped using them. We used to have FortiWeb for the last few years, but now we have actually stopped using them..”

Antonis Hassiotis

IT Security & Networks Administrator at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“The price of Check Point CloudGuard WAF is not expensive, as it was the cheapest solution we found. There is good competition for Check Point CloudGuard WAF at the moment, with big players in the market..”

Antonis Hassiotis

IT Security & Networks Administrator at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“Before adopting Check Point CloudGuard WAF, we were using the AWS native WAF for some workloads and Imperva WAF in certain environments, which provided baseline protection but were found too limited in advanced threat protection..”

Verified user

Assistant Manager at a computer software company with 201-500 employees

[Read full review](#) 

“There are significant differences, as specifically for Check Point CloudGuard WAF, it outperforms competitors such as Cloudflare regarding accuracy and remediation. While Cloudflare is less expensive, it is not completely reliable. In contrast, Check Point CloudGuard WAF, despite being somewhat expensive, is completely reliable..”

Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

“We have had several protections from other WAF products that we have tested. Their implementations were longer, more complex, and sometimes, because of the speed we would implement it after it went live because of the times. The time to market was short, and we didn't have time to achieve the desired time window.

Today, with Check Point CloudGuard WAF, there is no way we'll go live without protection.

We used and evaluated Radware and Reblaze. They were very expensive and also dependent on third-party services. With Check Point CloudGuard WAF, everything was done easily in-house..”

Baruch Peretz

Ciso at a government with 1,001-5,000 employees

[Read full review](#) 

“We do not care about alternate solutions. We never care about the cost. There is something called pair-wise comparison. I am a CISO, by the way. When any of the clients are in a process of deploying a firewall or global firewall for their organization, they will come to me and request, "CISO Krishna, why can't you give me the top three or four firewalls in the market?" I normally say the first one is Palo Alto, FortiGate, and then Check Point Quantum. These are the three top firewalls I usually recommend. I have a readymade PowerPoint deck in comparison, a pair-wise comparison with these three. In that comparison, there is the cost of each one and everything.

Cost is normally something I do not worry about. I will explain to the client, and it is their responsibility. Finally, they will choose the cheap one. Many people are going with FortiGate. And some people come to Check Point CloudGuard WAF. Rare people go for Palo Alto, or someone is really worried about their security, like banking organizations or financial institutes, those people go for Palo Alto.

I will not give any total cost of ownership about the product. I will give the features for this cost. I will explain the advantages, disadvantages, pros, and cons of each product, and then I will present it to the customer. It is up to the customer who will select the product, and we will also recommend. Sometimes we recommend Palo Alto, sometimes we recommend Check Point CloudGuard WAF, sometimes FortiGate, and sometimes other firewalls. In many places, we will not recommend. We will give it as it is. That is called pair-wise comparison. We will compare it and give it to the client, and it is the client's responsibility to choose their own product..”

KrishnakumarM

CISO at Pink Solutions

[Read full review](#) 

ROI

Real user quotes about their ROI:

The return on investment is reflected in the improvement of the overall security posture. While it does not have a direct monetary impact, it enhances security with an improved NIST compliance score and better overall security scores for our organization.

Mantu Shaw

Project Manager at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“I observe a good return on investment from the product, as investing in securing clients proves worthy. If a serious breach happens, the cost to fix it could be in the millions, so preventing it is always beneficial for your investment..”

Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

“The ROI is that we are not attacked and are confidently protected. When we are attacked, we can understand how important the solution is. We have to get the blow to understand the importance of the solution..”

Verified user

[Read full review](#) 

Cyber security manager at a government with 1,001-5,000 employees

“The biggest ROI is that the time to market is good; I am not holding back the business. I do not look that much at attack prevention because that's something that every product usually does. The ROI is the time to assimilate and the short time to market. Those are its benefits..”

Baruch Peretz

[Read full review](#) 

Ciso at a government with 1,001-5,000 employees

“I have seen ROI. However, when I am not worrying about the cost, I am also not worrying about the ROI. Selling a product is not my job. I am a CISO for a service organization. If you want, I will create the solution. When someone is requesting a solution, if that someone is also requesting ROI information, then I will give all of those metrics. However, it is a rare case that they will request ROIs, because I am not going to worry about the cost of the product. I am worrying about the features and vulnerabilities. Reduction of vulnerabilities is important. I hope you understand..”

KrishnakumarM

[Read full review](#) 

CISO at Pink Solutions

“I have saved a significant amount of time and resources since implementing Check Point CloudGuard WAF. Before, our teams often spent several hours manually tuning rules and chasing false positives. The detection has now cut the workload by more than half, freeing up three or four hours less per week.

Check Point CloudGuard WAF has reduced our total cost of ownership by approximately 10%. I consider the time saved as a return on investment since using Check Point CloudGuard WAF. .”

Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200 employees

[Read full review](#) 

Use Case

“Check Point CloudGuard WAF's primary use is protecting web applications and APIs from application layer attacks in the cloud. I also use it to protect public-facing apps..”

Nitin Yadav

Network & Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“I am using not only Fortinet, but I am also dealing with other vendors as well, such as Check Point. I am working with email security by Check Point. I have a little bit of experience with Check Point CloudGuard WAF, as we ran a proof of concept here..”

Antonis Hassiotis

IT Security & Networks Administrator at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“The major use case is providing application security and API security solutions to the organization. For example, our client was HYG, and they wanted to ensure their applications and API security gets fully secured, which is why I proposed Check Point CloudGuard WAF to their solution..”

Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

“I use Check Point CloudGuard WAF for web application and API protection. I can provide a scenario where I used Check Point CloudGuard WAF to defend against an SQL injection attack on a web app. It detects query patterns via machine learning and then blocks requests instantly without needing any rule writing..”

Sachin-Yadav

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

[Read full review](#) 

“I can use Check Point CloudGuard WAF for multiple purposes, as I am using it as our cloud security posture management tool. I have started using it since cloud security posture management was sold to Wiz. Wiz is another product these days. I have started using Check Point CloudGuard WAF along with bot protection and API protection..”

Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

[Read full review](#) 


“I use Check Point CloudGuard WAF for CSPM and posture management. In some places, I use native app protection-related management, and in other places, I use it for runtime protection. These are all some of the use cases I have utilized it for. I also use it for CASB in some locations, compliance assessment, adaptive access control, UEBA, policy enforcement, and threat protection. I have performed all of these functions using firewalls.

Traditional WAF with Check Point CloudGuard WAF has some features that could be integrated inside the WAF that might be helpful. I normally use a separate tool for API security, and I used to perform OWASP top 10 or 20 assessments. Not everything falls under WAF.

However, if it is included, especially in today's market where AI-related features are all integrated, that would be tremendously helpful. AI and modern viruses such as token theft, tool poisoning, command injection, unauthorized access, and prompt injection are all concerns. If you have prompt injection detection in Check Point CloudGuard WAF, that would be the greatest help for the market. I would give you one more thing called a rug pull attack. Prompt injection is critical to address. Today everything is prompt-based and AI-based, and there will definitely be some bots. Those bots will definitely cross this WAF. There are some modern AI-based vulnerabilities such as token theft and tool poisoning. Tool poisoning means that some malicious command will be hidden inside, and then passwords will be saved insecurely. This happens everywhere, sometimes by mistake or unintentionally, but these mistakes are what allow hackers to penetrate. Token theft, tool poisoning, token passthrough, command injection, rug pull attack, unauthenticated access, and prompt injection are all seven major problems for people like me, CISOs..”

KrishnakumarM

CISO at Pink Solutions

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“Deployment of Check Point CloudGuard WAF is easy, as it comes with different modes depending on the agent that needs to be installed. Overall, it is simple and not very complex..”

Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

“I'm in charge of the regulations, the SECOPS team is the one involved in the deployment. I'm more of a policy guide, and from what I've noticed, the experience was good..”

Baruch Peretz

Ciso at a government with 1,001-5,000 employees

[Read full review](#) 

“The initial setup was very intuitive. I had minor issues, however, that was due to not reading the documentation properly. Overall, it was a very satisfying and straightforward experience..”

RicardoFernandes1

[Read full review](#) 

Team Leader, Cloudops & Cloud Architect at a consultancy with 501-1,000 employees

“The experience with pricing, setup cost, and licensing for Check Point CloudGuard WAF is straightforward, with the service being available as a fully managed service, and the pricing depending on traffic volume, number of protected applications, and cloud provider. I do not have a problem with this area..”


K.Q

[Read full review](#) 

IT Support at a security firm with 51-200 employees

“The setup was relatively easy; it's a product that is easy to deploy, and there were no big drawbacks. During the installation, we tested it on two apps first; we saw that it worked as it should, and then we moved on to the other apps. The process itself is not long at all. We have another WAF system that we use in other areas so we were aware of how to run these sorts of solutions..”

Verified user

[Read full review](#) 

Cyber security manager at a government with 1,001-5,000 employees

“Based on what the customer is requesting, if the customer wants some third-party integration, such as Wazuh, which is a SIEM tool, or they want to deploy with some open source product, then complexity comes in. However, if we are only installing Check Point CloudGuard WAF, the deployment is very nice and very cool. Check Point CloudGuard WAF has very nice videos, deployment documents, and deployment guides available. I have seen it, run it, and installed it in various operating systems and appliances, as well as virtual appliances in the cloud..”

KrishnakumarM

[Read full review](#) 

CISO at Pink Solutions

Customer Service and Support

“Customer support is usually needed during the implementation of the solution. After that, I have only opened a case two or three times, and the response time is very good..”

Charalampos Symeou

Information Technology - Infrastructure and Security at Cyprus
Development Bank

[Read full review](#) 

“Check Point CloudGuard WAF's customer support is very great and very fast.

I would give Check Point CloudGuard WAF a rating of 10 for customer support. .”

Ruben Ruiz

Sr. VP of Creative & Development at a non-tech company with 51-200
employees

[Read full review](#) 

“Check Point is known for providing really good service. If a ticket is opened, it is addressed and not neglected. The emphasis is on the Israeli team, which knows how to achieve escalations and provide a response. We were never left without an answer..”

Baruch Peretz

Ciso at a government with 1,001-5,000 employees

[Read full review](#) 

“I get the delivery I want from Check Point, I am a big enough customer to get the best delivery. I also received full technical support, especially during the implementation.

I would rate them a ten out of ten. They are always quick to respond to me..”

Verified user

[Read full review](#) 

Cyber security manager at a government with 1,001-5,000 employees

“Technical support is very nice. I have encountered a couple of issues related to the solution. They were not actual issues but things that needed clarification, and support was always there. They gave me the right reference to solve the issues that I faced. I do not have any complaints about the support and customer service aspects.

I would rate them an eight out of ten. They have very short working hours. Especially on the weekends, when you call them, the team is not working because they are a very small team. They need to increase the number of people for 24/7 support..”

Dialungana Malungo

[Read full review](#) 

Principal Cybersecurity Specialist at Unitel S.A.

“It has a user-friendly interface that makes monitoring and management easier with smooth integration with other Check Point and third-party security tools, and it provides a clear dashboard for visibility into attack and traffic patterns.

“I would rate customer support as eight out of ten.

“I chose this rating because sometimes the response will be delayed more than expected.

“Customer support is good, but sometimes it takes longer than expected..”

Verified user

Cyber Security Solution Engineer at a computer software company with 201-500 employees

[Read full review](#) 

Other Advice

“I want to strongly advise this product to other users. Not because of pricing—while the pricing is a little high, the level of security provided is much more critical. I would rate this product an 8..”

Sachin-Yadav

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

[Read full review](#) 

“I also use [Orca](#) and Palo Alto. With the four products — true positive, false positive, true negative, false negative — these are problems everywhere. That is the reason I recommend this tier-one firewall companies to the client. Out of ten, maybe one or two might be false positives..”

KrishnakumarM


CISO at Pink Solutions

[Read full review](#) 

“If we selected Check Point CloudGuard WAF, which we did not, it would certainly be much cheaper. I would recommend Check Point CloudGuard WAF to others at a rating of seven out of ten. I would recommend it if you have a simple setup, then it is cheaper and it does the job. My overall review rating for Check Point CloudGuard WAF is seven out of ten..”

Antonis Hassiotis

IT Security & Networks Administrator at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“Check Point CloudGuard WAF delivers clear efficiency gains over traditional WAFs in three main areas: operations, accuracy, and cost optimization. I do utilize Check Point CloudGuard WAF alongside other Check Point products. We use Check Point firewalls, security gateway, and load balancer, and they work together with Check Point CloudGuard WAF in our environment. My advice for others looking into using Check Point CloudGuard WAF is to first validate the use case and plan the deployment architecture. I would rate this product a nine on a scale of one to ten..”

Nitin Yadav

Network & Security Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“If I were to rate the support from zero to ten points, I would give them nine points.

“If I were to rate Check Point CloudGuard WAF on a scale from zero to ten points, I would give it nine points.

“Regarding the solution's ability for preemptive blocking of zero-day attacks and

detecting hidden anomalies, zero-day protection with Check Point products is very less compared to all other vendors. For example, I am using Fortinet and F5 as well. Every forty-five days, I have to forcefully update my firmware and other aspects, while I have never seen much zero-day vulnerability on Check Point CloudGuard WAF. Yearly, I only do the patch management and firmware upgrade. Compared to other service and security providers, the zero-day vulnerability on Check Point is very less. I know this because I am using all the products and understand the challenges. Check Point CloudGuard WAF has very low zero-day vulnerability, which is evident in security reports. My overall rating for this solution is nine out of ten points..”

Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

[Read full review](#) 

“I was working with Check Point CloudGuard WAF as a service provider, providing support to our clients from the Check Point CloudGuard WAF point.

When I assess the efficiency improvements provided by Check Point CloudGuard WAF compared to traditional WAF, I find that in traditional WAFs, we had to purchase a physical device or license from companies such as F5 or Cloudflare, which were really good in the market. However, since it has moved to the cloud, it completely goes virtual, meaning you don't have to buy or manage your own physical devices, making implementation really easy and very efficient with just a one-time purchase of the license from Check Point CloudGuard WAF.

Integration capability with existing systems was easy, as all vendors these days, such as Check Point, Fortinet, and Cisco, provide everything inbuilt. If you use the same vendor's firewall or EDR, it is easier to integrate their tool rather than purchasing from different vendors, which can become complex and challenging for engineers. When it is from the same vendor, managing different solutions is having only one platform to log in to.

Check Point CloudGuard WAF absolutely helps reduce the false positive rate, which is really very good, as the false positive rate is very low. The approximate false positive rate is one percent.

In assessing the solution for preemptively blocking zero-day attacks and detecting hidden anomalies, I find Check Point CloudGuard WAF amazing because it works on two engines: supervised and unsupervised. For zero-day attacks, it resolves issues immediately without waiting for another 24 hours or seven days.

I would rate the pricing at seven points, indicating it is expensive. I would rate this review overall as an 8 out of 10..”

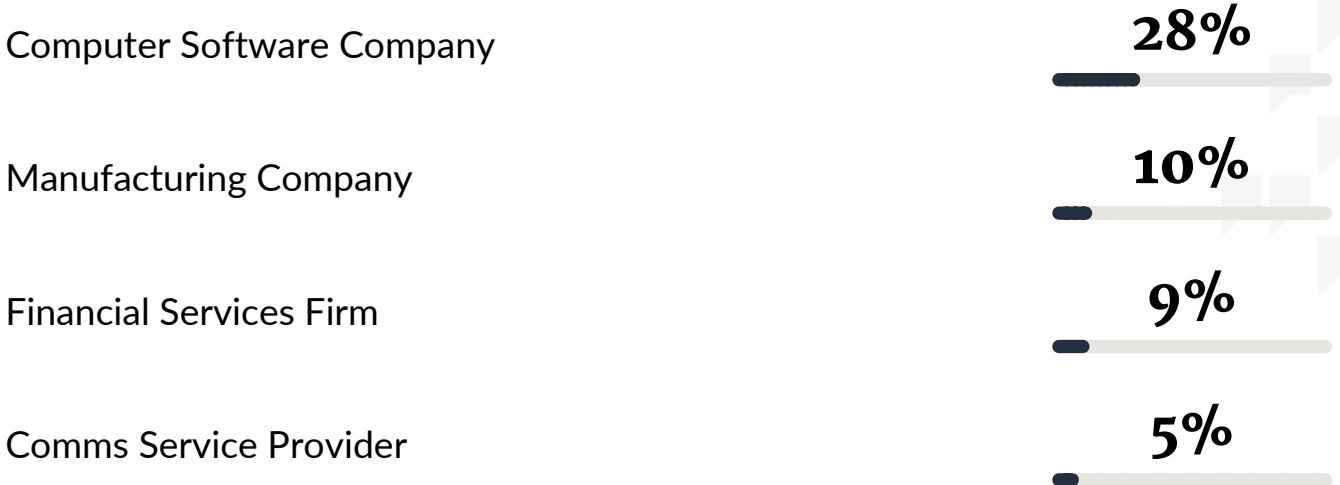
Ricky Makkar

Senior Network Security Consultant at NTT DATA

[Read full review](#) 

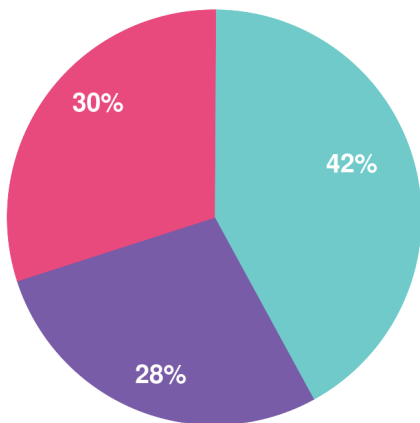
Top Industries

by visitors reading reviews

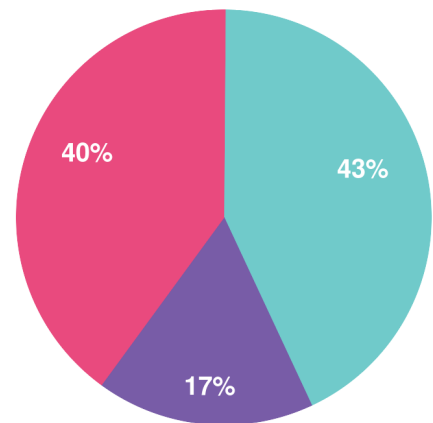


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944