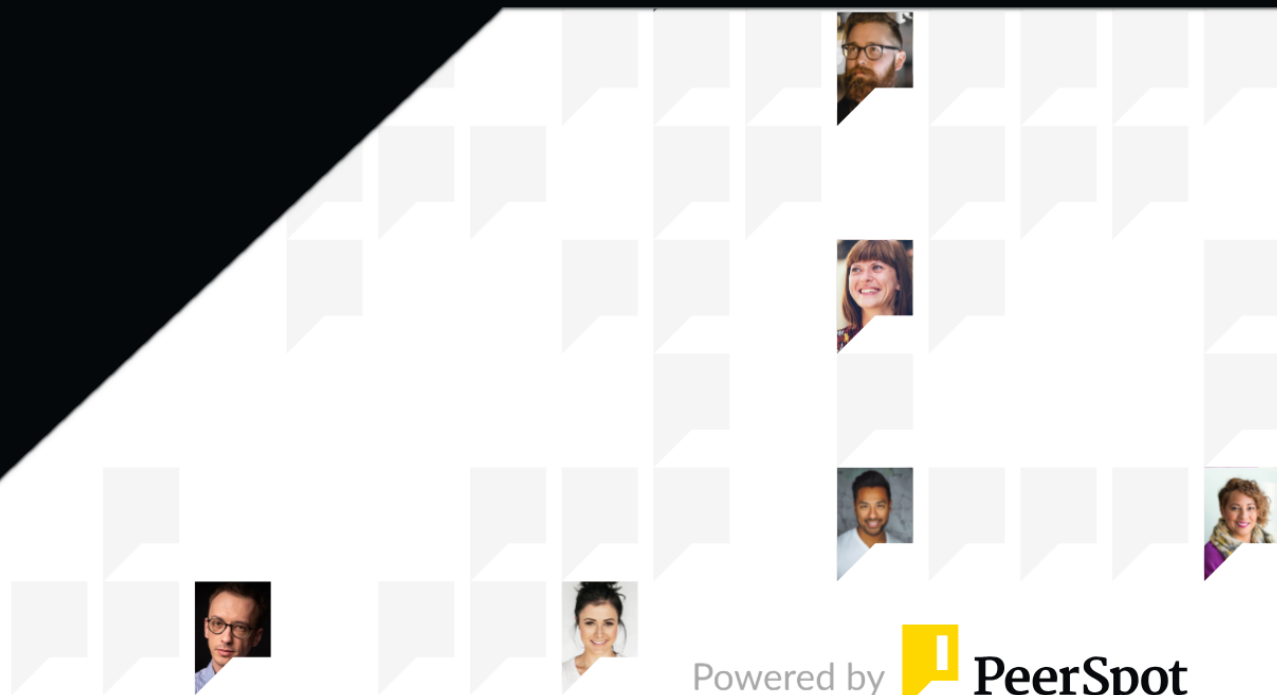




**Check Point Cloud Firewall (formerly
CloudGuard Network Security)**

**Reviews, tips, and
advice from real users**



Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 28

Customer Service and Support..... 29 - 31

Other Advice..... 32 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

Product Recap



Check Point Cloud Firewall (formerly CloudGuard
Network Security)

Check Point Cloud Firewall (formerly CloudGuard Network Security) Recap

Check Point Cloud Firewall, previously known as CloudGuard Network Security, provides advanced threat prevention, centralized management, and VPN capabilities, enabling robust cloud security across various platforms including Azure and AWS.

Check Point Cloud Firewall delivers seamless cloud integration with advanced automated threat prevention and centralized management to enhance security posture. It offers auto-scaling for dynamic environments and a comprehensive policy enforcement framework in hybrid settings. The unified interface streamlines administration across cloud infrastructures, ensuring consistent protection and reducing risk.

What important features does it offer?

- **Advanced Threat Prevention:** Safeguards against sophisticated threats.
- **Centralized Management:** Simplifies control for cloud infrastructures.
- **Auto-scaling:** Adapts to changing workloads seamlessly.
- **VPN Capabilities:** Enables secure connections across environments.
- **Integration with Azure and AWS:** Ensures compatibility with leading cloud services.
- **Visibility Tools:** Enhanced monitoring and management for security enforcement.

What benefits can users expect?

- **Enhanced Security:** Comprehensive threat management reduces risk.
- **Operational Efficiency:** Automation capabilities streamline processes.
- **Cost Management:** Efficient resource usage with auto-scaling reduces expenses.
- **Integration Flexibility:** Adapts easily into existing cloud platforms.
- **Simplified Administration:** Unified management reduces complexity.

In manufacturing and conglomerate sectors, Check Point Cloud Firewall is utilized for protecting cloud environments and implementing network segmentation. It supports secure cloud migration on AWS, Azure, and GCP, ensuring compliance, perimeter defense, and traffic inspection, facilitating sophisticated threat prevention strategies.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “With Check Point Cloud Firewall (formerly CloudGuard Network Security) and centralized management, changes propagate simultaneously to absolutely all gateways—that is, all the firewalls that are distributed geographically across several cities from a single console, which drastically reduces time, eliminates errors of inconsistency between devices, and maintains a single, consistent rule and object base for everyone.”



Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

- ✓ “The main benefit and main advantage of using Check Point Cloud Firewall (formerly CloudGuard Network Security) is that we use unified security approaches both on on-premises segments and in the cloud.”



Verified user

Network Engineer at a outsourcing company with 10,001+ employees

- ✓ “Check Point Cloud Firewall (formerly CloudGuard Network Security) saves a lot of time, effort, and cost, and having the centralized deployment across all accounts really makes our life easier by potentially improving visibility, reducing cost, reducing effort, reducing time, and certainly increasing the time to market or improving the customer experience.”



Prasanth Penuboina

Architect at Cognizant Technologies

- ✓ “Check Point Cloud Firewall (formerly CloudGuard Network Security) has significantly reduced our organizational risk.”



Viral Shaa

IT Security Analyst at Eos Energy Enterprises, Inc.

- ✓ “Check Point Cloud Firewall (formerly CloudGuard Network Security) is easy to implement, easy to use, easy to install, and easy to configure, especially compared to other competitors such as Palo Alto, Fortinet, Sophos, and SonicWall.”



Rahul Kamble

Sales Manager For Network at One Network Infosol Pvt. Ltd.



“If you are looking at the value and security and you do not want to compromise, then Check Point CloudGuard Network Security is one of the best solutions you could have in your organization.”



Devraj Kc

network and security engineer at Max international



“Since deploying Check Point CloudGuard Network Security, I have seen about a 40% drop in cloud network alerts, which has cut down noise and false positives, helping my team save roughly 25% of time previously spent on manual investigation and threat cleanup.”



Pedro Leão

Networking and System Consultant at Orbcom,Lda.

What users had to say about valuable features:

“The most valuable aspects of Check Point Cloud Firewall (formerly CloudGuard Network Security) are the VPN secure site-to-site and remote access connections along with threat prevention. Malicious traffic can be detected using security features such as IPS, anti-bot, antivirus, and URL filtering.

“Check Point Cloud Firewall (formerly CloudGuard Network Security) has positively impacted confidence in secure cloud deployment and migration. The migration was completed successfully and proved to be very feasible..”

Yabaluru Deepthi Naga Ramya Sravani

Admin at Infosys

[Read full review](#) 

“The most useful element of Check Point CloudGuard CNAPP is its advanced threat prevention capabilities. This functionality is vital because it proactively addresses security issues before they affect cloud applications and notifies a real-time incident, ensuring the integrity and availability of critical services.

Furthermore, the platform's full visibility and control across many cloud environments allows us to effectively monitor the security posture, uncover vulnerabilities, and consistently enforce security standards..”

Ajenthana Aiyathurai

Manager - IT at NVCL Group

[Read full review](#) 

“Check Point is the leader in gateways, and this is supported by Gartner, Forrester, and other review platforms. My customers with real cases also speak about this.

“The major reason for choosing Check Point is that we have qualified engineers for this product, which influences my decision towards this solution. If you speak about small and medium-sized businesses, middle market, and the enterprise level, we provide appropriate solutions for these customers, and we use this vendor's solution. For smaller businesses, we also use other solutions, which are quieter.

“All Check Point products are integrated with each other. We use Harmony, we use solutions from gateways, Harmony, Quantum Group solutions, web application firewall, and SmartCM, which is a tool for log analysis and visibility. We use more than fifty percent of the portfolio..”

Ігор Кузьменко

Key Executive at ITBiz Solutions

[Read full review](#) 

“From our personal usage, the most valuable feature I would say is the centralized policy management. We have organization accounts or root accounts in AWS through Landing Zones. In the case of Check Point Cloud Firewall (formerly CloudGuard Network Security) as well, we have centralized policy management. As I highlighted, we have closely 500 AWS accounts. If we have to configure them independently or individually, that becomes a complex, mammoth, and very tedious task, even to update something. With centralized policy management, we can apply consistent firewall and threat prevention rules across AWS environments without managing security for each VPC. I would say you configure something there, and it is applicable for all our AWS environments. The single view of all policies across all AWS accounts, I would consider it as the most beneficial feature. We have other options as well, such as integration with other AWS network services. Apart from that, the centralized monitoring and logging is very valuable. If we want to see which customers are having some issues or check the DDoS attacks, it will be easy for us to keep an eye on the monitoring and then evaluate the logs. There might be genuine cases of failures as well, which we are supposed to address. We have both the monitoring and logging capabilities..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

“I use it in multitenant environments with an MDS architecture, the Multi-Domain Management, to manage security policies in a centralized manner for different organizations at the same time.

“As I mentioned in the previous section, what I think are the best features it has is centralized management from SmartConsole with MDS. I think that is the strongest point it has, because you can have threat prevention with the blades, as I mentioned, IPS, Anti-Bot, and Anti-Virus, which are very well integrated. The ClusterXL function for high availability works very well. As I said, it is very reliable, very intuitive, and I think it is a very good tool.

“What seems very good to me, as I mentioned, is the integration it has for threat prevention with the IPS, Anti-Bot, and Anti-Virus blades. That seems to be its best integration. It is very intuitive—significantly, even if you come from other firewalls, this is very intuitive; you can manage it without any problem. You do not have to learn absolutely everything from scratch. I think this part is very well integrated..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

“Check Point Cloud Firewall (formerly CloudGuard Network Security) has centralized policy management, and the logging and monitoring is the extensive solution that we have really appreciated, as it supports multiple SIEM solutions to have logging and monitoring in place from a security perspective.

“The product has native integration support, and all of them are integrated with each other. It has been quite simple for us as we have the entire Check Point suite. It has been quite helpful, and it has been easy to integrate with each other.

“We have been utilizing the overall Check Point suites, including the email collaborations, Harmony, and Check Point Cloud Firewall (formerly CloudGuard Network Security). This includes the Cloud Network Security, AppSec, the WAF firewalls, and Cloud Native Security..”

Harshal Pachpande

Security Operation Consultant at SecurView

[Read full review](#) 

Other Solutions Considered

“I have worked with other firewalls, specifically on Check Point Cloud Firewall (formerly CloudGuard Network Security), and I can say that as compared to FortiGate and Palo Alto, I found Check Point Cloud Firewall (formerly CloudGuard Network Security) as a market leader in the security, as their IPS signature and the firewall provide enhancements with the IPS signature and the traffic..”

Chetan Thakur

Aws Infra Technical Specialist at Galaxy Office Automation Pvt. Ltd.

[Read full review](#) 

“There is something like a SmartConsole. We do not have the full permissions on the SmartConsole interface, but we got to know that there is a SmartConsole interface that provides very good visibility and simplifies the ongoing security management. We have two to three people that have access to that SmartConsole, and we can see whatever ongoing security changes are made in terms of good visibility onto where could be our next focus areas..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

“We always looked at several options. We evaluated Palo Alto with Panorama first. The second option was FortiManager from Fortinet, and we also looked at Cisco Firewalls with its manager, which is the FMC. In the end, we put everything on the scale—what best covered our needs based on the complexity and growth of users and the geographic distribution of offices—and ultimately we opted for Check Point Cloud Firewall (formerly CloudGuard Network Security)..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

“We previously relied on the standard AWS cloud-native services such as WAF, NACL, and security groups.

“The licensing and pricing are beyond my responsibilities, as the cybersecurity team handles configuration at the top layer. They take care of the licensing, and pricing is purely from an organization decision. I do not have a say on that..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

“By default, most companies do not use separate firewalling solutions in the cloud at all. They use basic functions such as security groups, NACLs, target evaluation, and similar tools. This is sufficient for them. However, all these solutions do not allow the network to be protected from more advanced attacks above standard firewalling. Check Point Cloud Firewall (formerly CloudGuard Network Security) or any NGFW solution makes it possible to protect against a large number of attacks at the IPS, antivirus, and anti-bot level. If there is a sandbox—SandBlast—then the solution can also inspect what is inside the packets themselves to maximally protect the corporate network. By default, cloud-native solutions do not provide this capability..”

Verified user

[Read full review](#) 

Network Engineer at a outsourcing company with 10,001+ employees

“Before we used, for example, solutions from Cisco ASA and, in other cases, Fortinet, as they did not offer a multitenant management model as mature as Check Point Cloud Firewall (formerly CloudGuard Network Security) MDS. So when the number of customers and devices grew significantly, it became evident that we needed a platform or tool that would allow us to manage all these completely isolated domains from a single console without compromising the separation between customers. That is when we made this migration.

“I have used other manufacturers. For example, I have a lot of experience with Palo Alto, and you could say that the main difference is the user experience when using Panorama as the centralized management console, which is like an MDS. It has a more modern and intuitive interface than SmartConsole, which, I repeat, I think should be web and should have a facelift. I have been using SmartConsole since 2018 or 2019, and it looks very similar now that we are in 2026; many years have passed. Another point is the visibility of applications with App-ID; it is very well integrated into the security policy from the beginning, while in Check Point Cloud Firewall (formerly CloudGuard Network Security) it requires more configuration to reach a similar level. For example, in multitenant environments with MDS, I feel that Check Point Cloud Firewall (formerly CloudGuard Network Security) is much better than Panorama for managing many customers in an isolated manner. We also use Fortinet, whose equivalent would be FortiManager, but it also has many complexities. I think Check Point Cloud Firewall (formerly CloudGuard Network Security) surpasses Fortinet in threat prevention and the inspection engine; I think Check Point Cloud Firewall (formerly CloudGuard Network Security) is much better than Fortinet. With Cisco Firewalls, with the FMC, Cisco has many shortcomings; I do not like Cisco much. I do not think the firewalls and the FMC are Cisco's strength. You need a very high learning curve to manage an FMC or Cisco Firepower Firewalls because within Firepower there are several layers of firewall—FTD and other derivatives of that—so Check Point Cloud Firewall (formerly CloudGuard Network Security) is very intuitive compared to Cisco. In conclusion, we could say that Check Point Cloud Firewall (formerly CloudGuard Network Security) is not easy to use, nor is it economical, but it is very robust and very mature in complex enterprise environments..”

ROI

Real user quotes about their ROI:

“Despite the price being on the higher side, the value for investments is substantial. It meets the requirements of suppliers or other business parts for security and protection against cyber risks, functioning like insurance..”

Ігор Кузьменко

Key Executive at ITBiz Solutions

[Read full review](#) 

“Check Point Cloud Firewall (formerly CloudGuard Network Security) is definitely a cost-effective solution. When customers buy it and when they expand on this technology, it definitely gives them ROI, return on investment..”

Rahul Kamble

Sales Manager For Network at One Network Infosol Pvt. Ltd.

[Read full review](#) 

“It is very difficult to determine any return on investment with Check Point Cloud Firewall (formerly CloudGuard Network Security) within a very short span of time. It has only been a year, so I may be able to assess this after another year or so..”

Wealie Antar

[Read full review](#) 

Manager, Systems, Information Technology at a educational organization
with 1,001-5,000 employees

“The main investment effect and everything I can say is that for all the time of my personal work at companies, our services have never been hacked with Check Point Cloud Firewall (formerly CloudGuard Network Security). There were many attempts, they were all logged, but there were no successful hacks. This is the main benefit we gained from working with this product..”

Verified user

[Read full review](#) 

Network Engineer at a outsourcing company with 10,001+ employees

“The return on investment is certainly positive. The time to market is very fast compared to the standard process that we used to do. The fewer employees needed category shows that we technically are now focusing only on the customer-specific rules rather than on the standard rules. Whenever you build an account, those configurations come in-built from the Landing Zone configurations. We are pretty much sure that our environment is secured from day one.

“I cannot quantify it, but I would say the centralized system has really helped us achieve things a bit faster..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

“Based on the complexity and growth of users and the geographic distribution of offices—and ultimately we opted for Check Point Cloud Firewall (formerly CloudGuard Network Security). I think there is a long-term return that would be very beneficial for a company. I also think they should take into account the issue of updates. If they are already going with Check Point Cloud Firewall (formerly CloudGuard Network Security), they must be very careful when testing Jumbo Hotfixes and upgrades by doing it first in a preproduction environment, thoroughly reading the notes for each version, and verifying that the bugs that exist between one version and another are fixed in the new update. If necessary, consult directly with TAC of Check Point Cloud Firewall (formerly CloudGuard Network Security); they have helped me a lot when I have had doubts about version upgrades. TAC is very friendly and answers all these questions without problems, and I think that is a very good option. As for licenses, hardware, and training, you have to do a prior analysis so that the engineers who are going to be in charge of the licenses and the solution to be acquired fully understand what is needed and what is going to be deployed..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

Use Case

“We use both on-premises and cloud solutions and work with both. Regarding the use cases for Check Point Cloud Firewall (formerly CloudGuard Network Security), customers want to protect their infrastructure, and it was particularly valuable when part of the infrastructure is on-premises and another part is on the cloud. Government requirements sometimes mandate only on-premises infrastructure when these requirements are not present, necessitating this solution. Government customers often prefer the on-premises solution, as cloud options are not always suitable..”

Ігор Кузьменко

Key Executive at ITBiz Solutions

[Read full review](#) 

“Securing our hybrid cloud environment and safeguarding vital operational and manufacturing workloads is our main use case for Check Point Cloud Firewall.

We use the platform to examine and secure East West traffic (between virtual networks and cloud workloads) as well as North-South traffic (between our on-premises network/factories and the cloud). In order to secure our production data and systems from cyber attacks and maintain continuous operational uptime, it offers advanced threat prevention, such as IPS, anti-bot, and zero-day protection. It also allows us to administer security policies centrally throughout our multi-cloud system..”

Ajenthana Aiyathurai

Manager - IT at NVCL Group

[Read full review](#) 

“What I appreciate is that centralized management is obtained from SmartConsole with MDS, which seems very positive to me, as that is the strongest point. With that, you can have threat prevention with the blades, IPS, Anti-Bot, and Anti-Virus. I think it is very well integrated, and also for ClusterXL for high availability, it works very well; it is very reliable.

“The primary impact we have had is the ability to manage security policies in a centralized manner for multiple customers from a single platform, because this significantly reduces operational time when performing, for example, rule changes or policy updates. What is more important is the availability from ClusterXL, which allows you to have production environments without service interruptions—that is, business continuity. Additionally, the threat prevention capabilities, and what I like most is that they have added a robust protection layer without the need for third-party solutions; everything is very well contained there. I estimate a reduction of between 30% and 40% in management time compared to solutions without multi-domain centralized management..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

“Check Point Cloud Firewall (formerly CloudGuard Network Security) is used for access control to allow or block traffic based upon the source and destination. Network segmentations and logging and monitoring are implemented to monitor connections, block traffic, and manage security policies through creating and managing firewall rules via Check Point's management platform.

“Check Point Cloud Firewall (formerly CloudGuard Network Security) can send events to SIEM platforms such as Splunk for centralized monitoring and incident investigation. Threat intelligence is utilized to identify malicious IPs as a criterion for the platform. Additionally, Check Point Cloud Firewall (formerly CloudGuard Network Security) provides security solutions for cloud environments such as AWS and Azure, which deliver firewalling and threat prevention for cloud workloads..”

Yabaluru Deepthi Naga Ramya Sravani

Admin at Infosys

[Read full review](#) 

“Check Point Cloud Firewall (formerly CloudGuard Network Security) has been acting as a perimeter device for our architecture, and it has been helping us to secure and have centralized management and visibility of the cloud network security. As a security analyst, we have been forwarding those logs with the SIEM solutions where we are monitoring network traffic flows for any abnormalities, applications and services, and for potential security breaches.

“We have been forwarding those logs over to the SIEM, and we have deployed this firewall in our environment to secure the perimeter by introducing policies. We have utilized the features to have the policies in place for communication with the destinations, to identify the source and destination ports and protocols, and the allowed and blocked connections to the firewalls. These were our basic use cases.

“We also use it for network traffic inspections, firewall policy enforcement, application and service controls, and the centralized policy management tool..”

Harshal Pachpande

Security Operation Consultant at SecurView

[Read full review](#) 

“I have been using Check Point Cloud Firewall (formerly CloudGuard Network Security) for the past one and a half years.

“My focus is on cloud-related aspects like AWS cloud and Azure cloud. The primary purpose that we use Check Point Cloud Firewall (formerly CloudGuard Network Security) is for the AWS account environment, securing our AWS accounts and environments.

“We manage approximately 500-plus AWS accounts, handling all of our internal customers' AWS accounts. Most of the customers expose their applications using the internet-facing load balancers and expose some APIs to external web vendors or something similar. Our AWS environment is primarily made of EKS clusters, load balancers, transit gateways, and we have direct connect associations with our on-premises infrastructure. We have a lot of ECS and EC2 services. To manage all of them, when you build applications, you primarily expose them to the outside world or internet users across the globe. To protect all of this infrastructure, our applications, and our data running behind a VPC, we deployed Check Point Cloud Firewall (formerly CloudGuard Network Security) to monitor all our inbound traffic, ingress and egress traffic, and to potentially have some kind of threat intelligence in place.

“We use it only for cloud, so I can recommend it only for cloud. I am not aware of the on-premises capabilities, but the name says CloudGuard Network Security, so I have focused my discussion on AWS..”

Prasanth Penuboina

Architect at Cognizant Technologies

[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.

“The configuration was easy, time-saving, and cost-saving, resulting in customer satisfaction, time to market improvements, and we have confidence in the solution. We pretty much focus on the custom requirements rather than standard requirements of all the accounts..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

“The initial setup was quite easy. We have the support team with us to have support, and they have all these SOPs and help documents and the steps on how to perform the tasks. How to perform the onboarding of these firewalls was all in one portal, which was documented with the SOPs. This helped us in a very positive manner..”

Harshal Pachpande

Security Operation Consultant at SecurView

[Read full review](#) 

“The initial setup was somewhat challenging. Check Point Cloud Firewall (formerly CloudGuard Network Security) offers versatility and elasticity for expansion. In case of major workloads, I can vertically stack and grow by adding new hardware. The old and new hardware work in harmony together..”

Wealie Antar

[Read full review](#) 

Manager, Systems, Information Technology at a educational organization with 1,001-5,000 employees

“I do participate in the initial setup of Check Point Cloud Firewall (formerly CloudGuard Network Security).

There is no complexity in the implementation for Check Point Cloud Firewall (formerly CloudGuard Network Security); it is easy to configure.

I have not faced many challenges during the initial setup; it has always been straightforward and simple..”

RahulKamble

[Read full review](#) 

Sales Manager For Network at One Network Infosol Pvt. Ltd.

“We have had all possible options for deploying Check Point Cloud Firewall (formerly CloudGuard Network Security). Approximately sixty percent are solutions represented as Quantum (CloudGuard) in configurations like VSX and standalone. We had solutions integrated with VMware NSX, but we have already abandoned them because VMware no longer supports such architectures. Forty percent of our current firewalls are firewalls deployed in public clouds—Azure and AWS..”

Verified user

[Read full review](#) 

Network Engineer at a outsourcing company with 10,001+ employees

“This could be when migrations are carried out.

“For several customers, but I will mention one: when a migration to a centralized architecture with MDS was performed. The customer asked us to unify the management of multiple gateways distributed geographically, because before, each policy change required manual intervention on each individual device; instead, with Check Point Cloud Firewall (formerly CloudGuard Network Security) and centralized management, changes propagate simultaneously to absolutely all gateways—that is, all the firewalls that are distributed geographically across several cities from a single console. This drastically reduces time; we went from using hours to minutes, and we also eliminated errors of inconsistency between devices. It is one thing to create several rules and then have to replicate them on multiple firewalls, or create objects and have to replicate them, but now with this, what you do is create a single rule, a single object, a single network and propagate it to the rest of the firewalls. This way you maintain, you could say, a single object, a single rule that is the same for everyone. This eliminates human errors such as a missing IP, a different rule name, misconfigured IP ranges, or ports, those things..”

Oscar Nunez

[Read full review](#) 

Ingeniero en redes y Telecomunicaciones at K-IT

Customer Service and Support

“I am very happy with the customer service from Check Point. We have a private engineer who is closely connected to the vendor and engaged in ongoing learning programs and accreditation. For support, I would rate it around seven to eight..”

Igor Кузьменко

Key Executive at ITBiz Solutions

[Read full review](#) 

“Technical support is excellent, and we have a country SE who provides support. The TAC support is also strong. The support from TAC has been consistently good, and there is nothing negative to comment on regarding that aspect..”

Arshad Fazly

Technical Engineer at a tech services company with 51-200 employees

[Read full review](#) 

“I do not often communicate with the technical support of Check Point Cloud Firewall (formerly CloudGuard Network Security) because we have our expert team that implements those solutions themselves..”

Rahul Kamble

Sales Manager For Network at One Network Infosol Pvt. Ltd.

[Read full review](#) 

“The customer support for Check Point Cloud Firewall (formerly CloudGuard Network Security) is pretty good.

I would rate the customer support a 10 out of 10 because it provides a lot of information and it quickly helps in resolving the issue..”

Karsh Trivedi

Security Engineer at Payatu

[Read full review](#) 

“The work of Check Point's customer support for Check Point Cloud Firewall (formerly CloudGuard Network Security) varies. We had a large number of cases with Check Point. There were cases that were solved fairly quickly. There were very long ones. There are still cases that we have not closed, but we are no longer actively dealing with them—we have found workarounds to temporarily close certain problems..”

Verified user

Network Engineer at a outsourcing company with 10,001+ employees

[Read full review](#) 

“I think the most critical point is the initial response time. For cases of medium severity, which are the most frequent in day-to-day operations, response times are usually very slow, sometimes many hours. You open a case one day and the next day you still do not have a response. However, once the technicians take the ticket, I think they are very professional. We have done updates, troubleshooting sessions, log reviews, rule changes and networking changes, many things. I think TAC of Check Point Cloud Firewall (formerly CloudGuard Network Security) is very competent; they really know what they are doing. But in terms of agility in the response, I think the problem is in the first line of support: the person who initially manages the incidents. I think that is where the problem is and where they could improve so that tickets are immediately redirected to engineers and then a quick solution can be provided. I think the bottleneck is in the first-line support, and that could be improved, because once a specialist engineer takes the ticket, they are very professional and resolve it. They are engineers who are there every day consulting, asking questions, working with you, and they do not leave you alone with the incident or the case you opened..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

Other Advice

“For new users, we would recommend starting with a clear understanding of the cloud network architecture first: how the traffic flows, how the security policies should be made before major configuration changes, and to start monitoring with logging first and understanding how the policy behaves. These are the primary checks that we would advise new users. Our overall score is eight out of ten..”

Harshal Pachpande

Security Operation Consultant at SecurView

[Read full review](#) 

“Many companies are opting for Check Point Cloud Firewall (formerly CloudGuard Network Security) as it is cost-effective and integrated with the cloud at affordable prices according to each company's environment. The licenses and overall offerings are favorable, making it a preferable choice.

“Check Point Cloud Firewall (formerly CloudGuard Network Security) is definitely recommended because it includes threat detection, the latest technologies integrated with the cloud, and is affordable according to most companies' requirements. The number of users using Check Point Cloud Firewall (formerly CloudGuard Network Security) is approximately ten thousand users. The overall review rating for this product is eight on a scale of one to ten..”

Yabaluru Deepthi Naga Ramya Sravani

Admin at Infosys

[Read full review](#) 

“I think if they are considering investing in Check Point Cloud Firewall (formerly CloudGuard Network Security), they should first look at the initial design of the architecture they are going to use or that they are going to need. Based on that, they should go directly with Check Point Cloud Firewall (formerly CloudGuard Network Security), because I think it is a product where initial architectural decisions have a very large impact on long-term operability. If you build a solid foundation with the architecture you need, I think Check Point Cloud Firewall (formerly CloudGuard Network Security) is a very good solution and, in the long term, will be a better ally than other manufacturers. However, this is achieved by working hand in hand with Check Point Cloud Firewall (formerly CloudGuard Network Security) engineers, and if it is implemented very well from the beginning, the investment is very good. I think there is a long-term return that would be very beneficial for a company. I would rate this review a 9 out of 10..”

Oscar Nunez

Ingeniero en redes y Telecomunicaciones at K-IT

[Read full review](#) 

“I am not using other products such as Harmony or CloudGuard, only Check Point Cloud Firewall (formerly CloudGuard Network Security) with management and gateway.

“I cannot say why I chose Check Point Cloud Firewall (formerly CloudGuard Network Security) because I am working as a professional engineer, and that OEM partnership and engagement decision is taken by the management only. The engineers deploy and work on Check Point Cloud Firewall (formerly CloudGuard Network Security).

“Currently, I do not have any examples where Check Point Cloud Firewall (formerly CloudGuard Network Security) helps to reduce organizational risk, but it does help to reduce the risk.

“I give a final rating for Check Point Cloud Firewall (formerly CloudGuard Network Security) a nine..”

Chetan Thakur

Aws Infra Technical Specialist at Galaxy Office Automation Pvt. Ltd.

[Read full review](#) 

“I know Trend Micro and Palo Alto products, but I am not too focused on them, and I think approximately ten to fifteen percent resemble Check Point, for example. That is why I cannot be so objective about this.

“We are a partner with Check Point, and we have status, although unfortunately I cannot remember what kind of partnership we have.

“Check Point Cloud Firewall (formerly CloudGuard Network Security) deployment model is primarily cloud-based. We use different cloud providers, primarily private clouds and seldom AWS or Azure.

“I am absolutely happy with how secure my cloud deployments are, as the government requirements are being met. It requires qualified engineers for selling at a high level and some competitive engineering expertise.

“My general rating of the product is around eight to nine..”

Ігор Кузьменко

Key Executive at ITBiz Solutions

[Read full review](#) 

“Since I am not the one who configured it end-to-end, and since my expertise is not in cybersecurity, I would rate the solution a seven.

“Check Point Cloud Firewall (formerly CloudGuard Network Security) saves a lot of time, effort, and cost. Rather than managing each individual account, having the centralized deployment across all accounts really makes our life easier. If you are currently handling 500 accounts or something similar, you cannot have a single entity that manages everything, which we did not have initially. But with Check Point Cloud Firewall (formerly CloudGuard Network Security), we have that option in place. It potentially improves visibility, reduces cost, reduces effort, reduces time, and certainly increases the time to market or improves the customer experience.

“My deployment is in AWS.

“It is not a direct use of the AI features from Check Point Cloud Firewall (formerly CloudGuard Network Security). But from my experience, I would rate it a seven, considering the feedback I have received from my cybersecurity team.

“We are using cloud-native products like [AWS WAF](#). We have NACLs, security groups, and [AWS WAF](#) is there. All of them are internal services. If you want to rely on that, you end up configuring all such rules or configurations across all the accounts. But when you compare this with Check Point Cloud Firewall (formerly CloudGuard Network Security), it provides a significantly much better centralized policy management, good visibility onto the policies, and advanced threat prevention capabilities. From an administrative perspective, that would be beyond my expertise, but closely working with the cybersecurity architects, we are convinced that Check Point Cloud Firewall has brought in a lot of value-add, rather than purely relying on the cloud-native AWS services for our day-to-day policy management.

“My overall rating for this solution is seven out of ten..”

Prasanth Penuboina

Architect at Cognizant Technologies

[Read full review](#) 

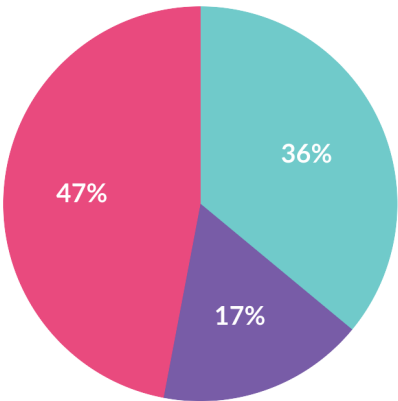
Top Industries

by visitors reading reviews

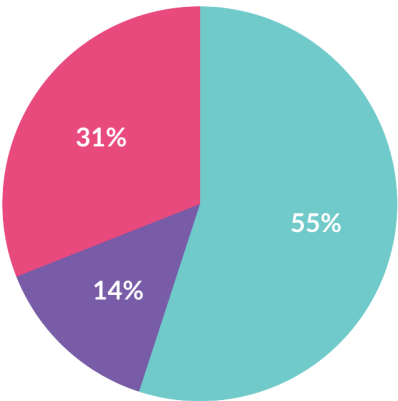


Company Size

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