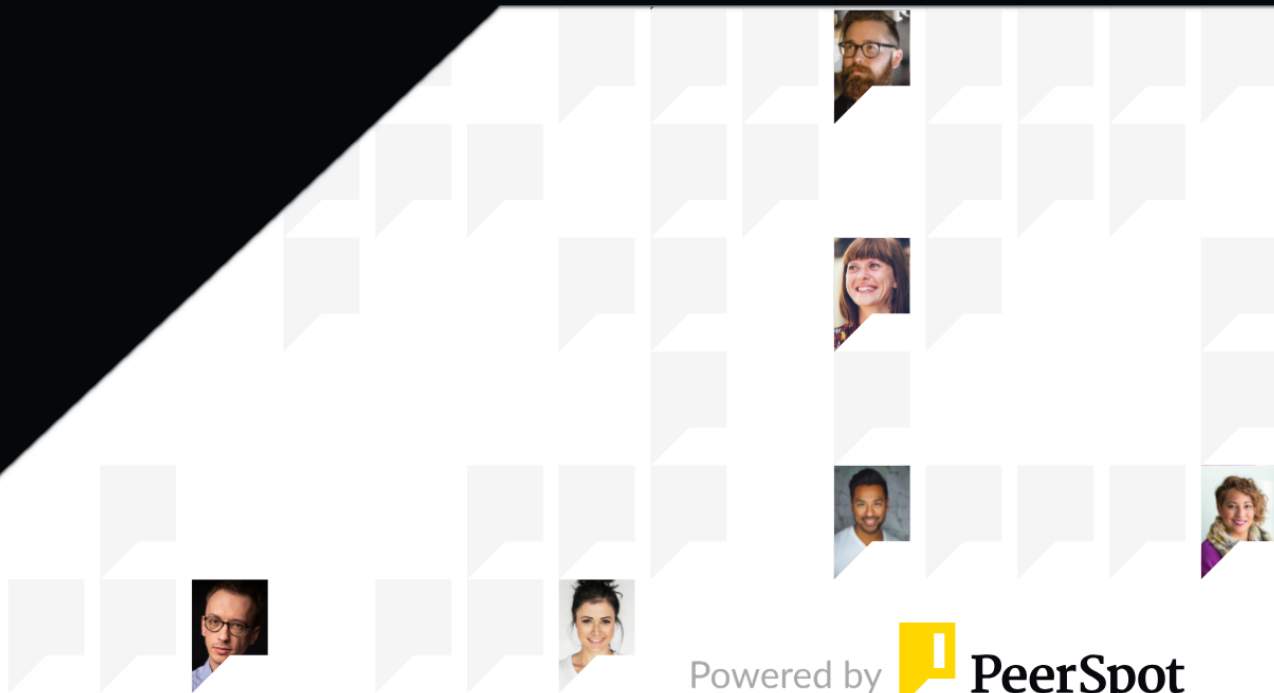




Cisco Secure Firewall

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 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Cisco Secure Firewall

Cisco Secure Firewall Recap

Cisco Secure Firewall provides comprehensive network security with advanced features such as application visibility, URL filtering, and malware protection. It combines a user-friendly interface with robust VPN capabilities, making it a reliable choice for varying network environments and industry applications.

Cisco Secure Firewall offers exceptional protection with its integration into Cisco's broader ecosystem, ensuring enhanced threat detection and policy unification. Despite its complexity in command-line interfaces and management, Cisco Secure Firewall remains a potent tool for safeguarding data. It is widely adopted for edge security, VPN services, perimeter defense, and traffic segmentation, especially in hybrid settings. Essential sectors like banking and telecom benefit from its stable connectivity and centralized security management. Though there are challenges with costs and support for third-party APIs, the firewall's scalability and high availability provide comprehensive support for protecting network assets.

What are the key features of Cisco Secure Firewall?

- **Application Visibility:** Offers in-depth visibility of application traffic to monitor and protect against threats.
- **Advanced Malware Protection:** Protects against known and emerging malware threats with powerful detection capabilities.
- **URL Filtering:** Manages and restricts access to websites, enhancing organizational data security.
- **VPN Capabilities:** Ensures secure remote access and encrypted communication through strong VPN features.
- **Integration with Cisco Ecosystem:** Enhances security measures with seamless integration with Cisco's suite of security tools.

What benefits and ROI should be expected from Cisco Secure Firewall?

- **Comprehensive Protection:** Offers multi-layered security for diverse network environments, increasing overall data protection.
- **Performance Efficiency:** High availability and scalability lead to improved network performance and resource management.
- **Management Simplification:** Centralized security management streamlines policy deployment across networks.
- **Enhanced Threat Detection:** Integration capabilities improve threat detection and mitigation for better security posture.

Cisco Secure Firewall is widely implemented across sectors like banking, education, ISPs, and telecoms. It fortifies data centers and network edge security, delivering strong protection for client access, hybrid environments, and intrusion prevention. In these industries, firewall

solutions ensure secure connectivity and manage RTU traffic effectively, leveraging centralized management and integration with Cisco's security tools.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“I find the integration with Cisco products in Cisco Secure Firewall most valuable because the majority of the features are equivalent to other OEMs, and the ecosystem integration with Cisco is what I prefer.”



RajeshKumar

Network Consultant at a outsourcing company with 1,001-5,000 employees



“Cisco has definitely done an excellent job in the last two to three years.”



Tejas Jain

Principle Cloud Architect at a tech services company with 11-50 employees



“Using Cisco Secure Firewall is financially beneficial as it provides clear settings for all members managing the solution, making it easy to teach the engineering team how it works and how to configure it, ultimately reducing the time needed to apply policies or make changes in the infrastructure.”



MarcosCaballero

Global Tech Security Architect at AVOLTA AG.



“There is a lot to appreciate about Cisco Secure Firewall and its next-generation features, as one firewall can, if it's a mid-scale project, serve as a perimeter firewall that is more than enough to protect you from all of the outsourced bad actors, which includes the web filtering, URL filtering, and also the VPN, which includes the antivirus, IPS, and IDS.”



Muhammad Awais Afzal

Sr Ict Engineer at ICAD-KSA



“I assess the stability and reliability of this firewall as both very good.”



Sébastien Peeters

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



“Cisco Secure Firewall impacts my organization positively since we are using Cisco AnyConnect, and most users who work from home rely on it, facilitating content filtering, traffic filtering, and Layer 4 security for users in both remote and office settings.”



ChandanKumar

Network and security lead at Hughes systique pvt ltd



“Whenever the traffic comes to the server farm and whenever a user accesses the application, we have one hundred twenty-five applications behind Cisco Secure Firewall, and it is almost all the bank which is using Cisco Secure Firewall.”



AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

What users had to say about valuable features:

“My organization benefits from utilizing Cisco Secure Firewall. I do not know the details of everything, but I hope my colleagues do a great job and Cisco Systems could help us to identify any of these constraints that could exist..”

Bruno da Silva

Senior Manager at Timestamp, SA

[Read full review](#)

“Cisco Secure Firewall has very good IDS and IPS capabilities, as well as excellent threat intelligence features, which are some of the best aspects of the product that I appreciate.

It actually helps with integration by allowing me to integrate different solutions within one platform..”

Vijai-Cyriac

Director at Movate

[Read full review](#) 

“What makes Cisco Secure Firewall appealing to customers is that all the features are the same across all firewalls, but customers appreciate that it is a stable solution and more secure. There are not as many security breaches as with Fortinet, and that is the reason why they often choose Cisco firewalls because of the stability of enterprise-level cybersecurity protection and overall position in the market.

“I have used new features recently in Cisco Secure Firewall, including AI support and AI central management, which is the latest feature from Cisco central management that allows me to manage all those appliances and firewalls centrally, also with some AI agents and chats and some additional regression features.

“The integration of the SecureX feature has helped my productivity and response time, but I need to ask colleagues about this since they are more involved in this.

“I assess the product's ability to unify and consolidate policies across my environment as quite straightforward and easy to do with this central management console..”

MartinsZipp

Consultant at SKYE AS

[Read full review](#) 

“Cisco Secure Firewall offers very good threat engines as its best features.

“Those threat engines, specifically Cisco Talos, help identify threats that can be exploited on zero-day vulnerabilities, and we used to see updates from Cisco Talos on a very regular basis, which is helpful for us.

“Additionally, the Layer 4 security is phenomenal and very easy to use, even for network or security engineers, and it is easy to deploy as well as to make policies such as Layer 4 and Layer 7 policies.

“Cisco Secure Firewall impacts my organization positively since we are using Cisco AnyConnect, and most users who work from home rely on it, facilitating content filtering, traffic filtering, and Layer 4 security for users in both remote and office settings.

“This has led to easier management and minimum false positives, along with the reliability of the operating system, as we do not have to upgrade very frequently, alleviating the burden for security engineers regarding constant upgrades..”

ChandanKumar

Network and security lead at Hughes systique pvt ltd

[Read full review](#) 

“One of the biggest strengths of Cisco Secure Firewall is the integration of multiple next-generation security capabilities into a single platform. For mid-sized deployments, a single firewall appliance can provide comprehensive perimeter security without requiring multiple standalone security solutions.

Key features include next-generation firewall capabilities, IPS/IDS, application control, URL and web filtering, VPN, malware and threat protection, and SD-WAN capabilities. Having these functions integrated into one platform provides centralized policy enforcement and better visibility into network traffic.

I particularly value the combination of firewall and threat-prevention capabilities because it allows organizations to inspect and control traffic at multiple levels rather than relying only on traditional stateful firewall policies. IPS and threat intelligence help identify and block malicious activity, while URL and web filtering provide additional protection against malicious or inappropriate destinations.

Another advantage is the scalability of the platform. Depending on the project requirements, Cisco Secure Firewall can be deployed for Internet and WAN security, perimeter protection, data center segmentation, or other security zones.

Overall, I would say its strongest feature is the ability to combine firewalling, threat prevention, traffic inspection, and secure connectivity into a unified security platform. This can simplify the architecture and operations while providing the security controls required for many enterprise environments..”

Muhammad Awais Afzal

Sr Ict Engineer at ICAD-KSA

[Read full review](#) 

“Cisco Secure Firewall, especially the next generation FTD firewalls, offers application visibility, the intrusion prevention system, advanced malware protection, Snort rules, and threat intelligence feed from Cisco's Talos cloud, which I find very useful.

“Cisco Secure Firewall has provided us the ability to go a long way towards zero-trust architecture, which is useful in implementing because zero-trust architecture has many more features such as multi-factor authentication, encryption, and segmentation. We have integrated Cisco's ACI, the Application Centric Infrastructure, the software-defined networks with Cisco Secure Firewall to achieve micro-segmentation and a good, fair bit of zero-trust architecture.

“We are using Cisco's XDR platform, which was previously labeled as Cisco SecureX. We have been using the Cisco XDR, Extended Detection and Response platform for the last two years, integrating Cisco Secure Firewall, Cisco Stealthwatch, Cisco Umbrella service for secure DNS, as well as Cisco endpoints with the XDR platform. We have onboarded Cisco's MDR service, Managed Detection and Response service onto the XDR platform.

“It has a very useful impact on productivity because when we integrate our ecosystem with the XDR platform, it operates on the AI algorithm, correlating and analyzing incidents for severity level by the AI algorithm, which gives the severity of the incident as well as eliminates false positives and provides it to the SOC level two analyst to contain or remediate the incident. This is a good feature and has automated somewhat the first level of incident response..”

AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

[Read full review](#) 

Other Solutions Considered

“I included Palo Alto and Fortinet firewalls in our RFP process before opting for Cisco, but I believe for data center firewalling, Cisco is best suited amongst its competitors..”

AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

[Read full review](#) 

“What stood out to me during the evaluation process was that choosing Cisco made sense primarily because we are already a Cisco shop and are familiar with their sales representatives, products, and dashboards..”

Verified user

Network Engineer at a comms service provider with 11-50 employees

[Read full review](#) 

“I have used Fortinet and Palo Alto as alternatives to Cisco Secure Firewall.

“It is hard to say, but right now I have been working with Palo Alto. That is currently my best option and I learned a lot from this vendor compared to Cisco Secure Firewall..”

Julian Paez

Technical Account Manager at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“Prior to adopting Cisco Secure Firewall, I have always had Cisco firewalls in the environment across my entire tenure. It has never been a complete rip and replace. We did have a point in time where at the edge we had Check Point firewalls. They worked well, but when it came time for replacement, we put Check Point against Cisco and Cisco won out, which I was happy about because I prefer Cisco..”

Verified user

[Read full review](#) 

IT Security Administrator at a government with 10,001+ employees

“Cisco Secure Firewall helps with a Zero Trust security model, and I am implementing a ZTNA access model. I have already implemented Zero Trust. Other vendors besides Cisco also provide ZTNA solutions. Fortinet and Palo Alto are all working with ZTNA and have moved into the ZTNA platform..”

Vijai-Cyriac

[Read full review](#) 

Director at Movate

“I have not tried or used the solution within the last twelve months period because I use Apache but I'm not using it now.

“I have used it for a long time, three or four years, but now I am not using it. Since, I think, three years, four years approximately..”

Bruno da Silva

Senior Manager at Timestamp, SA

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen ROI mainly because our firewall runs our internal infrastructure, and we offer some services behind it, so overall, I would say the ROI is positive..”

Verified user

[Read full review](#) 

Network Engineer at a comms service provider with 11-50 employees

“I have seen a return on investment since installing Cisco Secure Firewall, as we have observed very minimal false positives regarding threats, and using the same firewall for Cisco AnyConnect has saved us a lot of costs compared to our previous solution for remote VPN..”

ChandanKumar

[Read full review](#) 

Network and security lead at Hughes systique pvt ltd

“I have seen a return on investment with Cisco Secure Firewall. Generally, where it sits in my network, there are other vendors as well, but Cisco Secure Firewall is a better product and easier to manage than those alternatives. It does more of the features that I want it to do to be more secure, and I will move the other vendors into Cisco Secure Firewall..”

Verified user

[Read full review](#) 

Network Security Engineer at a manufacturing company with 5,001-10,000 employees

“Of course, what we are getting from Cisco Secure Firewall is worth it. There is always a return on investment because you find you invest heavily, but your environment is secure and then you are at rest; you do not need to panic. Even if attackers are coming, you know you will be rest assured that you are covered. Although other firewalls are okay, they cannot be compared to Cisco Secure Firewall..”

FataiAkinwande

[Read full review](#) 

Chief IT Consultant at d3astech

“I see some ROI through savings, including time and money savings. When evaluating Cisco over a longer period, I save money because the service renewal costs are substantial compared to alternatives. If I consider FortiGate, each module costs money and each renewal costs money. When comparing Cisco with other vendors, I believe Cisco's licensing is better..”

Nassif Kaleny

IT Manager at Bavaria Egypt S.A.E.

[Read full review](#) 

“From a return on investment perspective, I think Cisco Secure Firewalls keep our organization safe and protect the organization's image from a governance standpoint. With cybersecurity being a big issue in the world, Cisco Secure Firewalls protect data, the environment, organization, and keep things safe. It is always reassuring for customers to know that the organization I work for invests in products like Cisco Secure Firewall to protect ourselves..”

Verified user

Senior Network Engineer at a insurance company with 5,001-10,000 employees

[Read full review](#) 

Use Case

“As a bank, I serve as the Chief Technology Officer at one of the largest banks in Pakistan, UBL, United Bank Limited, and we have Cisco Secure Firewall deployed at the bank in the data center. We apply unified policies across the environment because we have two data center core firewalls running at the production as well as DR site..”

AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

[Read full review](#) 

“I have been working with Cisco Secure Firewall for almost nine years, and I want to share my experience with this solution.

I have been working with both the on-premises and cloud versions of Cisco Secure Firewall.

The choice between deployment models depends on the use cases. For on-premises use cases, I deploy an on-premises firewall, but for workloads that are based on the cloud, I use the cloud-based firewall..”

Vijai-Cyriac

Director at Movate

[Read full review](#) 

“My main use case for Cisco Secure Firewall is generic, focusing on normal L3, L4, and Layer 7 securities.

“A specific example of how I use Cisco Secure Firewall in my environment is that we have production firewalls positioned between our separate zones, which allow us to segregate our LAN infrastructure and server infrastructure with the firewalls.

“My main use case includes using Cisco AnyConnect for VPN connections, which is one of the biggest use cases, along with using it as a normal next-generation firewall for content filtering and Layer 4 security..”

ChandanKumar

Network and security lead at Hughes systique pvt ltd

[Read full review](#) 

“My main use case for Cisco Secure Firewall is as a security program, and I am using it to establish VPN connections. We are logging into this system to protect all information.

“For a quick specific example of how I use Cisco Secure Firewall in my daily work, we log into this program every day using a specific network. I use my company email and a password to access this program, allowing us to use all the systems and programs in the credit and collections area.

“Cisco Secure Firewall serves as the main security tool I use nowadays, primarily to protect information, the systems, and all the facts about the company..”

Verified user

Credit analyst at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“Regarding the implementation of Cisco Secure Firewall, I imagine that my colleagues from the security department and networking have a lot of complex configurations based on the requirements that we need.

“ We have an EVID ecosystem, and this implies very different kinds of configurations and rules.

“There are general rules, and then there are some specific rules based, for example, on users that are in different geographies, accessing different applications, and with different needs and requirements in terms of security.

“There are the back-end applications that must communicate between them and with external partners. There is also another integration complexity that my colleagues must face.

“Currently, I am working with some multivendors, for example, with Salesforce, Microsoft Dynamics, EVM DataPower, OpenAI, and Anthropic. I think I could miss other providers, but basically, these are the ones..”

Bruno da Silva

Senior Manager at Timestamp, SA

[Read full review](#) 

“I have been working with firewalls for more than eight years throughout my career, with extensive experience in network architecture and security design.

In my current role as a network architect, I evaluate firewall solutions based on the project RFP, client requirements, technical specifications, and consultant recommendations. My responsibility is to select and size the appropriate solution based on the specific requirements and use case of each project.

We use Cisco Secure Firewall in various network environments to secure WAN and perimeter traffic and to provide next-generation firewall capabilities, including IPS, IDS, URL and web filtering, application control, and SD-WAN for environments with multiple WAN links and high-availability requirements. Depending on the RFP and security architecture, Cisco Secure Firewall can also be deployed as a data center firewall to secure and control data center traffic.

For larger or more complex environments, we may implement a segmented firewall architecture, using dedicated firewalls for different security zones—for example, a WAN firewall, Internet/perimeter firewall, and DMZ firewall. The design depends on the traffic flows, security requirements, performance requirements, and overall architecture of the project.

Although Cisco is one of the firewall platforms we frequently deploy, we also work with other vendors depending on the project requirements. For example, some projects use Cisco for the perimeter firewall and Fortinet, Palo Alto Networks, or Sophos for the data center, while other projects may use Cisco for the data center and another vendor for the perimeter.

Ultimately, the firewall selection is driven by the customer's requirements, RFP specifications, technical use cases, performance and security needs, and the consultant's design. Using different firewall vendors across different security zones is sometimes a deliberate customer requirement or architectural decision..”

Muhammad Awais Afzal

Sr Ict Engineer at ICAD-KSA

[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.

“My experience with pricing, setup cost, and licensing indicates that the licensing part is still pending, but it is very minimal and not very hard for our organization to move forward..”

ChandanKumar

Network and security lead at Hughes systique pvt ltd

[Read full review](#) 

“The deployment was very seamless because we have our own team in the bank for deployment, and we also took professional services when we deployed Cisco Secure Firewall. I do not think that we faced any challenges or hiccups during the deployment..”

AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

[Read full review](#) 

“I would describe my experience with deploying Cisco Secure Firewall as positive because there is extensive documentation and support available, making the deployment very straightforward..”

Jeff Nagel

Network Engineer at Navitus

[Read full review](#) 

“The deployment for the product was not quite simple, but it was acceptable. I received support from Cisco during the process, so the overall experience was good.

I would rate the technical support from Cisco at an eight out of ten, with ten being the best..”

Vijai-Cyriac

Director at Movate

[Read full review](#) 

“The implementation of Cisco Secure Firewall is more or less straightforward. I have not encountered any problems lately or at all.

“It takes a couple of days, I would estimate, usually to deploy the product. However, this depends on the configuration..”

MartinsZipp

Consultant at SKYE AS

[Read full review](#) 

“My experience with pricing, setup, and cost licensing is that cost is always an issue for everyone. I think it has gotten easier, especially when it comes to larger customers with enterprise agreements. For example, my organization, while we have 5,000 users and around 18,000 endpoints, there was a time when we were considered not big enough to take advantage of an enterprise agreement. Considering the amount of product that we buy, that was a bit disheartening. But now, with more flexible options for purchasing and enterprise agreements, it has made it easier for us to not only purchase product but also have a clear idea of what we are allowed for growth and have something that is predictable for the cost of that management piece. Cisco has done a really good job with that..”

Verified user

IT Security Administrator at a government with 10,001+ employees

[Read full review](#) 

Customer Service and Support

“Customer support for Cisco Secure Firewall is very good; we can reach them on the spot, and they are quite helpful, leading to my overall satisfaction with their support..”

ChandanKumar

Network and security lead at Hughes systique pvt ltd

[Read full review](#) 

“Regarding Cisco technical support, I have communicated with them, and they are helpful and responsive. I rate them eight out of ten. It is a standard procedure, and I do not have any problems with it..”

MartinsZipp

Consultant at SKYE AS

[Read full review](#) 

“I have not needed to reach out for help regarding Cisco Secure Firewall. I believe the issues are more about the network or internet connections than Cisco Secure Firewall itself..”

Verified user

Credit analyst at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“I evaluate customer service and technical support as quite good. The documentation could use some improvement overall, as there are some errors in it. However, when we interact with support personnel and the AI agent, the experience is usually very good..”

Verified user

[Read full review](#) 

Network Engineer at a comms service provider with 11-50 employees

“I evaluate customer support and tech support as excellent, and I would rate it as a very high number on a scale of one to ten. There were a few years, especially following COVID, where it was very challenging even for severity three incidents that we had open where it would take up to a month to have some initial contact, which was very disheartening. However, now with that same level of severity, you are getting a callback within 30 minutes. My most recent case that I had to engage on, the engineer went way above and beyond what I had asked for, and I was very happy with the support that they have given us..”

Verified user

[Read full review](#) 

IT Security Administrator at a government with 10,001+ employees

“I would rate Cisco TAC support **9 out of 10** based on my experience.

I regularly work with Cisco TAC, particularly when upgrading Cisco Secure Firewall to a latest stable release. For example, during our airport operations and maintenance projects, we open a TAC case before the upgrade and work with a Cisco engineer throughout the process. After the upgrade, we validate the firewall policies, rules, and overall functionality before closing the case.

Overall, Cisco TAC engineers are knowledgeable and effective, especially when dealing with complex issues. However, my experience over the last two to three years has been that the quality and speed of support can vary depending on the engineer assigned to the case. Sometimes the initial engineer requires multiple rounds of log collection and escalation before the issue reaches a senior engineer who can resolve it quickly.

For this reason, I would give Cisco TAC **9/10**. The technical capability is strong, but faster access to experienced engineers and more consistent support quality would make the service even better..”

Muhammad Awais Afzal

Sr Ict Engineer at ICAD-KSA

[Read full review](#) 

Other Advice

“The deployment was very seamless because we have our own team in the bank for deployment, and we also took professional services when we deployed Cisco Secure Firewall. I do not think that we faced any challenges or hiccups during the deployment.

“Whenever the traffic comes to the server farm and whenever a user accesses the application, we have one hundred twenty-five applications behind Cisco Secure Firewall, and it is almost all the bank which is using Cisco Secure Firewall. If I can give an exact number, probably we have thirty-one thousand employees in the bank, and all their applications are hosted behind Cisco Secure Firewall. I rate this product nine out of ten..”

AwaisEjaz

Chief Technology Officer at a financial services firm with 51-200 employees

[Read full review](#) 

“I believe I am not familiar with the product Secure Cloud Protection for Salesforce. I don't know because I am working with the integration and also with the Salesforce component integrations between Salesforce and billing and invoicing platforms.

“In terms of security, I must comply with the guidance of the corporation that I am in.

“In terms of security, it is another area. We need to only comply and be compliant with the guidance and requirements that they demand.

“I would rate this review an eight out of ten..”

Bruno da Silva

Senior Manager at Timestamp, SA

[Read full review](#) 

“My advice for others looking into using Cisco Secure Firewall is to compare the feature sets, pricing, and the support Cisco provides, including the security modules like Cisco Talos and their threat feeds, as proper evaluation will likely lead to choosing this firewall.

“As of now, we are not using a Zero Trust security model, but we have done proofs of concept that were very good, and we are planning to move towards Zero Trust.

“I do not think I have used any new features or functionalities recently in Cisco Secure Firewall.

“I have provided this review with an overall rating of 9..”

ChandanKumar

Network and security lead at Hughes systique pvt ltd

[Read full review](#) 

“I would rate Cisco Secure Firewall 10 out of 10 overall. I have hands-on experience sizing and configuring Cisco Secure Firewall through CCW based on customer requirements, and I also compare it with solutions from other vendors.

Cisco Secure Firewall is a stable and reliable platform with strong build quality and good hardware support. With the appropriate Smart Net service, hardware replacement can also be very fast when required.

From a sizing perspective, Cisco provides a good range of throughput and interface options, although comparable firewalls from other vendors may offer more interfaces at a similar price point..

My advice to organizations is to consider Cisco Secure Firewall when reliability, enterprise integration, security capabilities, and long-term support are priorities. However, customers should carefully evaluate sizing, licensing, interface requirements, and total cost against competing solutions before making the final decision..”

Muhammad Awais Afzal

Sr Ict Engineer at ICAD-KSA

[Read full review](#) 

“I think the end-to-end visibility from Cisco optimizes the experience in a hybrid setup.

“I face specific challenges with hybrid and distributed enterprise networks, particularly feeling a little insecure when working from home. Cisco Secure Firewall is a great option because it provides a quick and secure program, allowing me to confidently access the company's systems.

“My advice for others looking into using Cisco Secure Firewall is that it is a quick security program, helping you connect from various places, such as the office, coffee shops, or home. You could try other methods to access the security system, like voice approval or other specific options.

“I would rate this product a 9 out of 10..”

Verified user

Credit analyst at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“I am using Cisco SecureX with Cisco Secure Firewall in some cases.

“My evaluation of Cisco Secure Firewall in helping my organization implement a Zero Trust security model is that it functions more or less as a marketing abbreviation, but Cisco has all the features and configuration possibilities to implement Zero Trust out of the box. We have seen some cases when we combine it with [Cisco Duo](#) to achieve the highest level of Zero Trust access to devices and also to firewalls.

“In terms of price, Cisco Secure Firewall is appealing for many in the enterprise segment, though for many customers it is too expensive. However, for customers in enterprises or at large corporations, the price is acceptable, depending on whether the customer is a small-medium business or enterprise. It is positioned more for enterprise customers.

“I rate this product eight out of ten overall..”

MartinsZipp

Consultant at SKYE AS

[Read full review](#) 

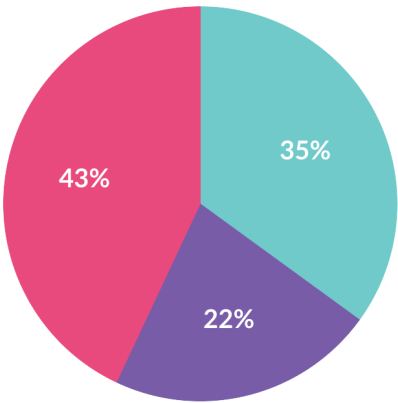
Top Industries

by visitors reading reviews

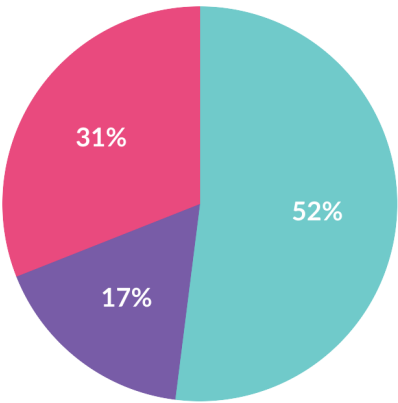


Company Size

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