

aws marketplace

Cisco Secure Access

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

Product Recap.....	3 - 4
Valuable Features.....	5 - 12
Other Solutions Considered.....	13 - 15
ROI.....	16 - 18
Use Case.....	19 - 24
Setup.....	25 - 28
Customer Service and Support.....	29 - 32
Other Advice.....	33 - 36
Trends.....	37 - 38
About PeerSpot.....	39 - 40

Product Recap



Cisco Secure Access

Cisco Secure Access Recap

Cisco Secure Access is a comprehensive Security Service Edge (SSE) solution (a key component of a SASE solution) that addresses the complexities of securing a hybrid enterprise. Cloud-delivered and grounded in zero trust, it delivers a unique blend of user simplicity and IT efficiency for frictionless, secure access to *all* applications—SaaS (with gen AI), private apps, and the internet—regardless of user location or device. Secure Access protects users, data, and devices against relentless, sophisticated, and constantly evolving threats including AI-driven attacks and identity breaches.

Provides all core SSE components (ZTNA, SWG, CASB, and FWaaS) plus extended capabilities.

- Includes VPN-as-a-Service (VPNaaS), data loss prevention (DLP), AI Assistant, visibility/control/guardrails for generative AI use, digital experience monitoring (DEM), reserved IP, remote browser isolation (RBI), DNS-layer security, flexible security enforcement (in cloud or on-premises), policy verification, and more.
- Protects users as they seamlessly access resources and apps with no extra steps needed, regardless of protocol, port, or level of customization
- Simplifies IT operations through a single client, single dashboard, single license, and unified policies.
- Lowers risk with least privilege, granular controls backed with unmatched threat intelligence of Cisco Talos.
- Eases interoperability with other products from Cisco and third-party vendors with common administrative controls, data structures, and policy management.

Robust integrations

- Integrates with Cisco Identity Intelligence to protect against the startling increase in identity-based attacks.
- Integrates with many SAML Identity Providers (IDPs) such as AD, Azure AD, Okta, Ping, etc.
- Integrates with Cisco offerings including SD-WAN, Splunk, XDR, Thousand Eyes, third party technologies such as Menlo RBI, Chrome Enterprise Browser, and AppOmni for SSPM.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “From my experience, Cisco Secure Access is very stable and has not crashed.”



Kartik Amin

Network Operations Engineer at Redex IT Limited

- ✓ “It has not only been a better solution overall, but also been cost saving, which is unusual—too good to be true at one point, but it has delivered.”



Junaid Ali

Head Of IT at a non-profit with 501-1,000 employees

- ✓ “Cisco Secure Access has definitely helped our organization, cutting incident response time at least in half and giving us analytics that let us quickly identify devices and users so everything from headquarters contacting the base to the on-site tech removing a rogue device from the classroom network is much quicker.”



Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

- ✓ “The biggest return on investment from Cisco Secure Access, from my perspective, is the end usability from a client perspective.”



Andy Thomas

Cyber Security Manager at a non-profit with 501-1,000 employees

- ✓ “The features of Cisco Secure Access that I most prefer are easy management or manageability, and overall security.”



Vasil Blagov

Manager, Network at Duracell International, Inc.

- ✓ “The product is giving whatever you need from a customer point of view.”



Bharath_Kumar

Solution Architect at Velocis Systems

- ✓ “The most valuable feature of Cisco Secure Access is the VPN, which I find very easy to use.”



Misbah Syed Khaja

Senior Manager at a retailer with 10,001+ employees

What users had to say about valuable features:

One of the advantages of Cisco Secure Access is the price, and we are able to get a unified dashboard, providing a single pane for everything.

After implementing Cisco Secure Access, I observed complete automation, a complete Zero Trust architecture, and complete automation of security.

“It has worked well for protecting our organization from threats including ransomware, phishing, and spamming. .”

Mahesh Bhadoriya

Technical Manager at Allianz Cloud Private Limited

[Read full review](#) 

“What I like the most about Cisco Secure Access is that it has continuous updates for signatures for advanced ransomware; for example, Cisco Umbrella also does this. We can implement controls to prevent access to newly observed domains, with Cisco providing signatures and this information as quickly as possible compared to other vendors. This means if a new website can be malicious and contain ransomware, Cisco ensures that we have immediate information about it. It is fast to gather more information about ransomware and malware, including newly observed domains. Thus, we can say that Cisco provides updated signatures rapidly..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

I describe the performance and security levels provided by the Hybrid Private Access feature as solid; we are using a cloud firewall for security. The cloud firewall includes application filtering, DNS filtering, and everything is managed in the cloud, so we apply these conditions to ensure access to either public or private cloud.

Our customers use VPN as a Service (VPNaaS) in Cisco Secure Access, as we are providing POC and offering that solution to some customers. It is new for them, particularly in India, where they are launching and promoting it now. We are trying to explain and educate customers on the differences between traditional VPN and Secure Access, and what the advantages are. We are doing all these initiatives while completing the POC as well. .”

PSaravanakumar

Network Engineer at vatanix

[Read full review](#) 

“In my experience so far, I haven't noticed any best features that stand out with Cisco Secure Access. One feature that does sound useful to me is Zero Touch.

The Zero Trust feature in Cisco Secure Access works very well, but I have no idea about its specifics. Some common positive impacts I mention include faster troubleshooting, which I have noticed since using Cisco Secure Access.

Cisco Secure Access has helped with faster troubleshooting because when we were troubleshooting a loop in a network of our customers, with just a few clicks, I found where it came from and where it was going, so I closed this interface and everything is good.

I am using the AI Assistant feature in Cisco Secure Access, and it has helped in improving my security administrative tasks by summarizing pages or outputs of troubleshooting, which is helping so much. The most helpful thing the AI assistant has done for me is making recommendations for solutions during troubleshooting, which helps me focus on what to think about..”

Verified user

Network Technician at a tech services company with 501-1,000 employees

[Read full review](#) 

“Cisco Secure Access offers seamless access and replacement for VPN; VPN can be quite clunky when you need to access cloud solutions. With Secure Access, you create tunnels to everything basically in the solution, simplifying things while improving security for our customers. I particularly appreciate the ZTNA story and accessing SaaS, on-premises, and cloud resources all at once.

Usability is one of the key factors in selling the product; it has to be easy to use. I think Cisco has done a good job there with Secure Client, and since many of our customers and a lot of the market are familiar with AnyConnect, showing them Secure Client, which is basically the same thing but with a new coat of paint, and telling them that it improves security while not being more difficult to handle is great.

Customers spend much less time troubleshooting VPNs because ZTNA works more stably, and therefore it has become a pretty good point of sales for us as a reseller to increase our revenue at the customer level, because it's an extra layer of security that you can add to an already existing networking solution. On the customer side, it increases performance and helps ease of use, and from the reseller side, it's a great product to add on to existing network solutions.

The customer's experience has gone from "Our VPN doesn't work and we need to troubleshoot it all the time" to "Our ZTNA does work and we don't need to troubleshoot it all the time." Cisco Secure Access has been very stable.

Cisco Secure Access's scalability is great; from a technical point of view, it's quite simple. However, from a licensing and cost point of view, there could be improvements in ease of licensing and better pricing.

The multi-organization management capability of Cisco Secure Access is excellent; it's a great feature that you can do with the multi-tenancy mode, and I think it's great that you can roll it out to separate organizations..”

Erik Jonasson

Network Presale at Advania Sverige

[Read full review](#) 

“The actual technology itself is valuable. Cisco Secure Access functions as a cloud firewall where there is no real need for on-premises firewalls for many client devices. This feature is excellent because I no longer need million-dollar Palo Alto firewalls sitting at a data center where I would be forced to route all traffic through an MPLS circuit to those firewalls for filtering before getting to the internet.

Cisco Secure Access takes on the responsibility of filtering traffic, and I do not have to deal with hardware anymore. When hosting my own firewalls, I had to worry about upgrades, maintenance, and license costs for physical Palos. With Cisco Secure Access, I do have license costs, but they are very streamlined with their new smart licensing features.

From a network perspective, it makes management easier for my network operations team. Previously, I had complicated, complex, high availability meshed firewalls. Now I can have a single pane of glass solution where I can still get all URL filtering and content filtering done through web access. I no longer have to worry about hardware and setting up high availability pairs for physical firewalls. I am just focused on putting a client on the user's machine. Even if I do not want to put a client on a machine from an operational perspective, I can pair Cisco Secure Access with other Cisco products like SD-WAN. Even without the Cisco Secure Access client on actual laptops for the organization, I can still filter that traffic from the router level by telling my Cisco router that its next hop is the Cisco Secure Access cloud for filtering.

Coming from an environment primarily using Ruckus and Brocade at the Department of Defense, then switching to Cisco Secure Access to meet the zero trust requirements set forth by the Pentagon has been tremendous. It checks most of the boxes. I would say it is probably a little weak in the area of IPv6 still. I have actually gotten the chance to talk with the actual developers developing Cisco Secure Access at Cisco. There is still a lot to be desired in the IPv6 realm, but from what the developers are telling me, it is coming in the near future.

As I left the organization, we were getting into using more of the policy verification feature to help us since we have our hands in a lot of different areas at the

Department of Defense. Policy verification definitely helps a lot because sometimes there are too many people making policies.

Cisco Secure Access provides great visibility with a single pane of glass. The data is actually useful, and I can make decisions based on it rather than just receiving raw data. For multi-organizational sites, it is absolutely a great tool.

The artificial intelligence assistance is tremendous. If I do not know something, I can use the Cisco AI to ask how to do something or how to get something working, and it will step-by-step tell me or point me in the right direction on what I need to do. On-premises solutions do not really have large language models or AI built into them, so I would be left needing to know what I need to do. This feature helps a ton..”

Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

[Read full review](#) 

Other Solutions Considered

“Before adopting Cisco Secure Access, I used Zscaler, which is along the same line, but I am not a fan. I am happy because I find with Cisco it ties well with the rest of the ecosystem, unlike Zscaler, which does not. We did look at Zscaler..”

Robert Ley

[Read full review](#) 

Manager, Infrastructure Services at a energy/utilities company with 1,001-5,000 employees

“Since I am working for the Cisco competence center, I did not consider another solution before choosing Cisco Secure Access. We just sell Cisco, so no Palo Alto, no FortiGate, no Zscaler..”

Verified user

[Read full review](#) 

Junior Information Technology Consultant Security at a tech services company with 10,001+ employees

Before choosing Cisco, I considered FortiGate as an alternative.

I chose Cisco instead of Fortinet because, while FortiGate has everything, Cisco is a leader in networking and is more mature compared to Fortinet. .”

Mahesh Bhadoriya

[Read full review](#) 

Technical Manager at Allianz Cloud Private Limited

“The main factors that led me to choose Cisco Secure Access after Check Point included cost; Cisco was substantially cheaper, and we also had a poor experience with Check Point, which we found unreliable. We faced constant tickets and multiple versions of the same client causing inconsistent user experiences, leading to difficulties in product cohesion. Ultimately, cost was the most persuasive factor..”

Andy Thomas

Cyber Security Manager at a non-profit with 501-1,000 employees

[Read full review](#) 

“A single pane of glass solution was important to me. Cisco Secure Access was just cheaper than putting a Palo Alto firewall solution at every school or using Prisma, their secure solution. It just worked out to be better. The integration into products like ICE, DNAC, and SD-WAN was a lot better on the Cisco side because Cisco to Cisco integration is better than Cisco to Palo Alto. Product integration among the other Cisco products we had was just better overall..”

Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

[Read full review](#) 

“I didn't think about another solution before choosing this one since we're moving into many services more and more, and we're basing the managed services on Cisco solutions; I would prefer to use as much of Cisco ecosystem in our managed services, as it's easier for us as a service provider to handle the customer needs if we can have everything in one ecosystem.

“We have partnered with other vendors like Check Point and Fortinet, but I would prefer Cisco if possible..”

Torbjörn Zars

Special Sales Business Development at Tele2

[Read full review](#) 

ROI

Real user quotes about their ROI:

My major concern is to justify not only the ROI but also the complete security model of our organization, ensuring there are no security gaps from edge to core to cloud.

Mahesh Bhadoriya

Technical Manager at Allianz Cloud Private Limited

[Read full review](#) 

“Since using Cisco Secure Access, I haven't seen a return on investment and I do not have this information regarding saved time, money, or fewer employees..”

Verified user

Network Technician at a tech services company with 501-1,000 employees

[Read full review](#) 

“I can definitely say I have seen a return on investment from having Cisco Secure Access, as it has cut down our admin cost. I have eliminated three sets of firewalls that I did not need to have. I would say we probably save about 30% in hardware and about 20% in administration right now..”

Robert Ley

Manager, Infrastructure Services at a energy/utilities company with 1,001-5,000 employees

[Read full review](#) 

“I do not have concrete numbers that I can share because I do not currently have them, but the customer's experience is that they are spending pretty much no time troubleshooting ZTNA, down from spending a lot of time troubleshooting VPNs. I would estimate it is probably in the 60 to 70% range of time saved when it comes to VPN troubleshooting..”

Erik Jonasson

Network Presale at Advania Sverige

[Read full review](#) 

“I believe it is too soon to say that I have seen a return on investment from having Cisco Secure Access. The good thing with it is that you can also place other products, such as Cisco Duo for example. Today, I saw Neil present something at the convention, and now you can combine Cisco Duo directory with Cisco Secure Access. So, there will be a return on investment, but it is too soon..”

Verified user

[Read full review](#) 

Junior Information Technology Consultant Security at a tech services company with 10,001+ employees

“The price to value from Cisco Secure Access is justified. Money has been saved by moving to one vendor, and that has been a material cash saving that was able to be handed back to the business. It has not only been a better solution overall, but also been cost saving, which is unusual—too good to be true at one point, but it has delivered. Approximately half a million pounds a year is the amount that has been saved..”

Junaid Ali

[Read full review](#) 

Head Of IT at a non-profit with 501-1,000 employees

Use Case

“My main use case for Cisco Secure Access is to secure our network. A specific example of how I'm using Cisco Secure Access to secure my network is that we use it for our customers as an internet service provider to ensure everything is safe..”

Verified user

[Read full review](#) 

Network Technician at a tech services company with 501-1,000 employees

“Cisco Secure Access serves as a replacement for customers' old VPN solutions while increasing security through Zero Trust Network Access (ZTNA). We had a chicken production client that identified their current VPN as the lowest hanging fruit for increasing security. Since the customer already had Secure Client or AnyConnect previously, introducing the ZTNA module into Cisco Secure Client felt quite straightforward. We implemented it step-by-step, side-by-side, and rolled it out for that customer, which improved secure access for both on-premises and cloud solutions and turned out to be very effective..”

Erik Jonasson

[Read full review](#) 

Network Presale at Advania Sverige

“In my previous role, we managed the IT infrastructure for U.S. military base schools worldwide. We implemented Cisco Secure Access primarily as a cloud-based firewall replacement. Previously, we utilized a centralized architecture with Palo Alto firewalls in a U.S. data center, which meant all of our global traffic had to be backhauled to the U.S. before going out to the internet. We rearchitected the network to enable local internet breakouts at every individual base. Instead of deploying expensive physical firewalls at each local site, we deployed Cisco Secure Access as our cloud firewall solution. Now, local traffic routes directly up to Cisco's cloud for filtering before reaching the internet, ensuring our users are secured regardless of their geographical location. I still closely support customers utilizing this architecture..”

Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

[Read full review](#) 

I evaluate Cisco Secure Access's AI Access feature for providing deep visibility and control over AI applications as something we have just started using, with not much experience yet. The Canva features are in beta mode at the moment, so we are in the early stages.

Our customers use VPN as a Service (VPNasS) in Cisco Secure Access, as we are providing POC and offering that solution to some customers. It is new for them, particularly in India, where they are launching and promoting it now. We are trying to explain and educate customers on the differences between traditional VPN and Secure Access, and what the advantages are. We are doing all these initiatives while completing the POC as well.

“The features mostly used in Cisco Secure Access by our customers include roaming clients, which is the major aspect because the clients are roaming around and accessing from anywhere. They need secure access to their private applications as well as public applications. Some applications are hosted in their own on-premises data center, others in their private cloud, and some in the public cloud. Therefore, they need to access all parts of their portfolio securely, and this is the main use case we propose. .”

PSaravanakumar

Network Engineer at vatanix

[Read full review](#) 

Cisco Secure Access is a major part of our organization, focusing on networking, audio, and video, though we are not implementing it with proper security measures.

I use Cisco Secure Access as an on-premises solution.

“For security, we use Cisco Secure Access for email security, endpoint security, networking, and gateway-level firewall, and we are also using Cisco Meraki.

“Cisco Umbrella helps us with securing applications, and we are using Cisco Umbrella.

“Cisco Umbrella is helping us significantly with securing standard applications, but not in a complete manner, as there are some gaps in the product which the product team needs to focus on.

“My perception of Cisco Secure Access's ability to provide secure security via protocols such as HTTP, HTTP/2, and QUIC is that the overall impact is significant.
.”

Mahesh Bhadoriya

Technical Manager at Allianz Cloud Private Limited

[Read full review](#) 

“Cisco Secure Access has many features, and I want to clarify whether the discussion pertains to Cisco ISE or the Cisco client, as the new product name created some confusion with other Cisco products. The solution allows users to connect with our organization's assets from anywhere in a secure manner by providing controls, including firewalls and URL filtering, to deliver comprehensive security for our users and protect them from advanced malware and harmful websites. Overall, its purpose is to safeguard our users during access to our infrastructure on the cloud.

The no-cost migration tools from Umbrella have assisted in streamlining our security policy migration. We also have the cloud to manage all of these products, which works very well for us. We have comprehensive rules from Umbrella, acting as our main firewall. We also implement controls on application control, URL filtering, allow lists, and destination lists to permit or block specific access, including our domain. Therefore, this is very helpful to streamline the implementation for Cisco Secure Access.

Regarding the AI Access feature, I used to use OpenAI, but I will try Cisco's AI tools next time to search for logs. I have tried one, and I think it is very good at allocating logs and knows exactly where the product is and where the issue is. I find it very helpful for us.

I have not yet used the Experience Insight feature, powered by ThousandEyes, but I will do so next time.

I have used the AI assistant feature in Cisco Secure Access. I find it very helpful for viewing logs, analyzing logs, and assisting with issue resolution whenever I am searching for issues. The replies I receive are very quick, professional, and helpful for us.

I am using the Hybrid Private Access feature for varying the enforcement location for ZTNA private traffic. We provide access for our users while enforcing security using these features. It is very good technology overall, and Cisco simplifies it for us and for their customers.

I have tried integrating Cisco Secure Access with Identity Intelligence; we have a trial license for it, and we have gained insights from this license. It is very good and helps us to identify and protect our digital assets. We are considering a decision to purchase this after trying it for the first time.

I have used the policy verification feature to help reduce policy misconfigurations. It acts as a health check for policy configurations and is a powerful tool that recommends settings and configurations for policies.

The effectiveness of AI supply chain risk management is currently under testing. One of my team members is configuring this or working on it, but it is still under evaluation. .”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[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.

Cisco Secure Access's initial setup is straightforward; it is a GUI-based cloud-managed deployment. If everything is configured correctly, we can complete the deployment within an hour, having all IPs and other elements ready.

PSaravanakumar

Network Engineer at vatanix

[Read full review](#) 

“The initial setup was pretty straightforward. If there were any complexities, Cisco was right there with their support to help us. I would say it was pretty simple..”

Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

[Read full review](#) 

“The deployment process of Cisco Secure Access is very easy because there is a wizard with seven steps that allows you to configure it, and it works without complications..”

YordanYordanov

Network Security Engineer at IT-Services der Sozialversicherung GmbH

[Read full review](#) 

“My experience deploying Cisco Secure Access is that it is very intuitive for a technical team, though the challenge lies in understanding the underlying processes; once that knowledge is acquired, deploying Cisco Secure Access becomes much easier, and if the team does not understand how the underlay routes work, that presents complexity..”

Lado Ninikashvili

CTO at GT Group

[Read full review](#) 

“Cisco Secure Access is deployed in my organization on-premises. I'm not sure if we use VPNaaS in Cisco Secure Access. I haven't used the Experience Insights feature powered by ThousandEyes yet; I know about ThousandEyes, but we do not use it yet.

I'm not sure if I have integrated Cisco Identity Intelligence with Cisco Secure Access. I haven't used policy verification in Cisco Secure Access as I am still new and do not configure any policies. I help mostly with troubleshooting something that's already running, just looking for anything wrong here and there..”

Verified user

[Read full review](#) 

Network Technician at a tech services company with 501-1,000 employees

“My experience with deploying Cisco Secure Access involves starting a proof of concept when the customer is almost ready to buy. I have a flyer that I set up to explain how it is going to work. Before starting the proof of concept, I create a questionnaire, asking how many private apps they have and how many remote workers they have, and I gather all the information. We usually conduct a proof of concept with the customers, meeting their requirements in a short amount of time. As soon as the customer is satisfied, they can test in real time how it is going to function. You also have to educate the customer on what is new, explaining how the traffic apps work, including blocking pages, warnings, and all features. It is fundamental during the proof of concept, as the customer has many questions about why certain things are done a particular way. That is pretty much how the deployment works. We do the proof of concept, present the software, take the formula to meet the requirements, put them in place, and as soon as it is ready to go, we make the switch and it runs..”

Verified user

[Read full review](#) 

Junior Information Technology Consultant Security at a tech services company with 10,001+ employees

Customer Service and Support

“Customer support is decent; it is slowly getting better now with the new NIS2 and cybersecurity laws that are being implemented. I would give customer support a rating of five..”

Erik Jonasson

Network Presale at Advania Sverige

[Read full review](#) 

“I have worked with many technical engineers for Cisco Secure Access, and I think they are very professional and provide a good experience.

I would rate them a 10 out of 10..”

YordanYordanov

Network Security Engineer at IT-Services der Sozialversicherung GmbH

[Read full review](#) 

I rate the technical support based on the individuals who connect; some provide correct solutions while others may take a lot of time.

On average, I would rate the technical service around seven, or perhaps seven point five out of ten.

“There is indeed room for improvement regarding first-level support; they need to ensure that knowledgeable people are available. .”

PSaravanakumar

Network Engineer at vatanix

[Read full review](#) 

“The experience with Cisco Secure Access customer support is good. They have always been reachable, and fortnightly cadences have been established now that things have settled down. Meetings with the actual product engineers working on the solution have also been arranged. When there are more complex issues, they work with the team to pull that data directly from systems and take that back to improve on it and work on it. This has been a very collaborative experience.

“Cisco support is rated an 8 overall. From feedback received from the team, it is between an 8 and a 9..”

Junaid Ali

Head Of IT at a non-profit with 501-1,000 employees

[Read full review](#) 

I have worked with the support team, and they are really good; I am actually about to meet one of the guys now to have a chat and catch up, so we have had some good exposure to the support teams.

The support team assigned to us is very good, so I would rate them an eight or a nine, but if you are raising a TAC case, it can be hit or miss regarding the knowledge of the TAC engineer that picks it up; on the whole, it is quite good, probably a six or a seven. However, there have been times when it has been lower due to the confusion between Cisco Secure Access and Secure Connect, especially when integrating Meraki support cases. Many of the Meraki engineers did not recognize Cisco Secure Access and only knew about Secure Connect, leading to some communication problems between Meraki and Cisco. .”

James Grimwood

Network Security Manager at Gamma Telecom Infrastructure


[Read full review](#) 

“My experience with Cisco support has been brilliant. We had a couple of issues recently, but I think the team has been very helpful. We had some planned upgrades in Cisco's data center, and after that, we had some posture issues. We escalated to Cisco, and once the issue was identified, we received really good support. I am pleased with the support we have from Cisco.

“I would rate Cisco support an eight out of ten. I would have given them a ten if we did not have those issues last week. Based on that, I would probably say eight. The recovery was alright, but I think there is quite a bit of work to do around making us aware of the works taking place and what we need to be aware of. Other than that, I think it is brilliant support from Cisco. I quite appreciate your experts; specifically Luke Abditch has been a brilliant resource. He helped us set up the entire platform..”

Misbah Syed Khaja

Senior Manager at a retailer with 10,001+ employees

[Read full review](#) 

Other Advice

“Cisco Secure Access always requires monitoring for updates and signatures, similar to a health check, but not intensive maintenance. It is very good and very stable. I provide this product with an overall rating of ten out of ten..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“Since I started using Cisco Secure Access, I have noticed positive impacts on my organization. My advice for others looking into using Cisco Secure Access would be to try it; it is very nice to have in a good environment, such as service providers. I would give this product a rating of 8 out of 10..”

Verified user

Network Technician at a tech services company with 501-1,000 employees

[Read full review](#) 

“I would urge any customer to look up their numbers and see what works best for them. It is not always going to be the Cisco product that works best. Sometimes the Cisco product is the nicest product out there, but that does not necessarily mean it is going to be the best. Look at what works for your organization and go with whatever your staff feels most comfortable with because at the end of the day, your staff is going to have to support that solution. No one wants to support something that they do not really want in the first place. My overall rating for Cisco Secure Access is 9.5 out of 10..”

Brandon McPherson

Sr. Service Delivery Engineer at Colossal, LLC

[Read full review](#) 

I do use the [Zero Trust Network Access](#) feature of Cisco Secure Access.

Before choosing Cisco, I considered FortiGate as an alternative.

“I chose Cisco instead of Fortinet because, while FortiGate has everything, Cisco is a leader in networking and is more mature compared to Fortinet.

“The decision was more about Cisco's brand and complete branding.

“The price of Cisco Secure Access is quite cheaper than [VMware NSX](#).

“I would rate this review as nine out of ten. .”

Mahesh Bhadoriya

Technical Manager at Allianz Cloud Private Limited

[Read full review](#) 

“ The AI access feature of Cisco Secure Access is really interesting. I do not think it is really there yet; the product has to mature a bit more for us to give it an honest

evaluation. However, from what I have seen in the upcoming feature releases, I think it is a really interesting way to go for the AI agents in the solution.

We do not use VPNaaS in Cisco Secure Access.

I do not know how it has impacted incident resolution time because we have only used the Experience Insights feature in a proof of concept stage, and I have not yet done it in a full rollout.

The AI assistant feature in Cisco Secure Access has helped with the documentation and with administrative duties.

We have not integrated Cisco Identity Intelligence with Secure Access.

Everybody has a need for a VPN; VPN is not as secure as it once was because the market is moving fast. Cisco Secure Access and ZTNA is the way forward to ensure easy access and secure access to your preferred on-premises or cloud instances. I would suggest to customers that they allow us to help them by choosing ZTNA rather than VPN. I rate Cisco Secure Access an eight because an easier license structure, easier pricing structure, and better pricing structure would bring it to a ten..”

Erik Jonasson

Network Presale at Advania Sverige

[Read full review](#) 

I am using Cisco Secure Access's Hybrid Private Access feature for varying the enforcement location for [ZTNA](#) private traffic.

I have integrated Cisco Identity Intelligence with Cisco Secure Access, where the IDP-related functionalities play a role. ISE is for centralized policy management, and within that context, it is not a major component; however, [IDP](#) integration is a significant part of Secure Access specifically for roaming clients.

“The policy verification in Cisco Secure Access is very effective; since Secure Access is a cloud platform, we configure policies based on requirements and deploy them accordingly.

“I would like to add that while the integration into one platform is important, security-wise, Cisco Secure Access is a good product. The complexity I see primarily relates to management, and they are gradually integrating towards a single platform, which is the only concern I have.

“I believe Cisco Secure Access is the best option on the market at the moment; it is the right and recommended choice. I would rate this solution an eight out of ten overall. .”

PSaravanakumar

Network Engineer at vatanix

[Read full review](#) 

Top Industries

by visitors reading reviews

Manufacturing Company

11%

Financial Services Firm

8%

Computer Software Company

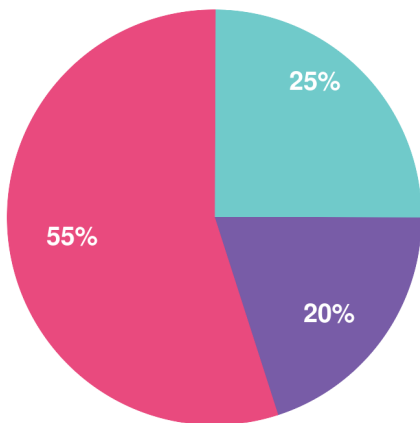
8%

Comms Service Provider

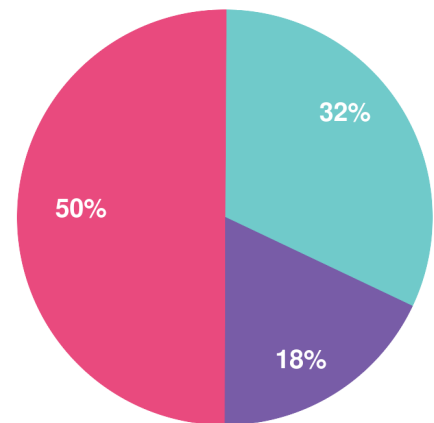
7%

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