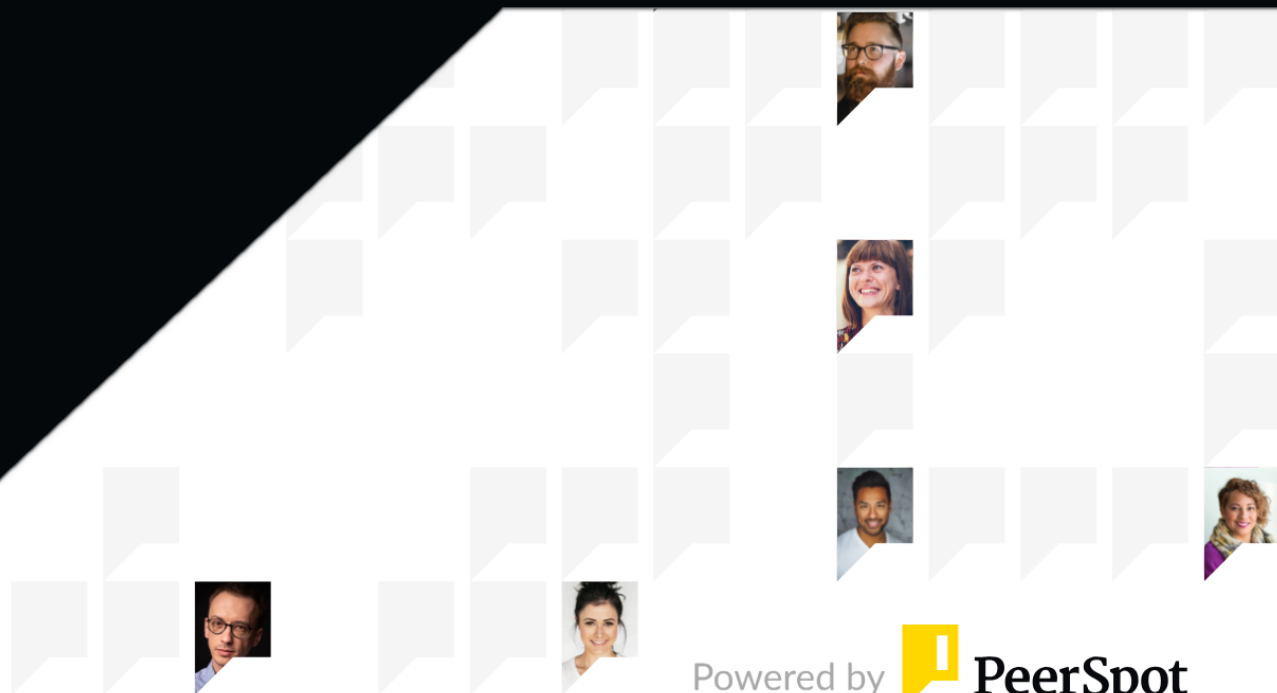


aws marketplace

Cisco Secure Access

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 14

Other Solutions Considered..... 15 - 18

ROI..... 19 - 22

Use Case..... 23 - 28

Setup..... 29 - 31

Customer Service and Support..... 32 - 34

Other Advice..... 35 - 39

Trends..... 40 - 41

About PeerSpot..... 42 - 43

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.”



Verified user

Network Operations Engineer at a media company with 1,001-5,000 employees



“Overall, Cisco Secure Access has been a valuable component of our security strategy.”



Vishnu Narahari

Manager at a computer software company with 201-500 employees



“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

- ✓ “If you have every solution with Cisco, you can see a very good ROI because you do not need to invest much on staffing for analyzing each and every console separately.”



GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

- ✓ “The return on investment in Cisco Secure Access is significant, providing substantial savings in time, data loss prevention, and management of protection, with time savings reaching up to 30% based on the processing time and retention policy of Cisco Secure Access, which is more than 30% better than others.”



Nassif Kaleny

IT Manager at Bavaria Egypt S.A.E.

- ✓ “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



“I can provide more advanced security features for my customers because Cisco Secure Access is built in the cloud, I don't have to worry about managing the security enforcement or the behind-the-scenes operational aspect, and it has resiliency in multiple data centers so I get increased availability with multiple redundant tunnels across different data centers.”



Abebe Gebrekirstos

Senior Design Specialist at TELUS Communications Inc.

What users had to say about valuable features:

“The advantages I see in Cisco Catalyst SD-WAN compared to their competitors is the seamless service scope, where I can have from Cisco the LAN, Wi-Fi environment, the SD-WAN environment, and the security environment, and as now announced from Cisco, all the management is combined in one orchestrator, which is the most beneficial aspect for me, not looking for the best of breed but more looking for the best fit.

“I have used the policy verification to help reduce policy misconfigurations.

“The multi-organization management capability of Cisco Secure Access in terms of usability and efficiency is quite good, as there is an RBAC system, allowing me to granularly define the access roles. I would rate this an eight..”

Eric Biederbeck

Enterprise Architect at a tech vendor with 10,001+ employees

[Read full review](#)

“The standout features of Cisco Secure Access are its Zero Trust Network Access, ZTNA, Secure Web Gateway, and multi-factor authentication, MFA, integration. I also appreciate its centralized policy management, which makes it easy to enforce consistent security rules across users and devices. The detailed visibility into user activity and security events helps with monitoring and troubleshooting. Additionally, its cloud-based architecture provides secure access for remote and hybrid users without relying on traditional VPNs, making it both scalable and easy to manage. Overall, these features significantly improve security while maintaining a smooth user experience.

“Compared with similar secure access solutions, Cisco Secure Access stands out because of its tight integration with the Cisco security ecosystem and its unified cloud-native platform. Instead of managing multiple separate tools, administrators can enforce consistent security policies from a single console. I also found the Zero Trust approach and detailed visibility into user activity to be stronger than many traditional VPN solutions. These features make it easier to secure remote users while simplifying management, making the platform a good fit for organizations with hybrid or distributed workforces..”

SehajVohra

Member at IEEE Signal Processing Society UPES

[Read full review](#) 

“Cisco Secure Access ZTNA feature helps in securing standard applications because it actually monitors every given interval as we configure. It checks for the security posture at every interval even after the device is connected. If a device gets connected and infected through some kind of malicious software or by using pen drives, it eventually gets isolated when Cisco Secure Access ZTNA finds that it does not fall under the given compliance. We have to give some security checks, and based on those checks, it will verify the security posture in ZTNA.

“Cisco Talos influences threat detection and response capabilities in the organization because Cisco Talos is a threat intelligence machine for the Cisco brand. They have integrations with Talos in all the solutions, whether it is EDR, Umbrella, or SecureX. Basically, they provide integrations with each and every engine, and the point I want to make is that Talos intelligence is inbuilt within Cisco Secure Access itself.

“SecureX incorporates all the other Cisco products. SecureX covers integration with all the Cisco solutions provided. For example, we can integrate SecureX with EDR, XDR, Cisco Secure Access, switches, routers, and Cisco firewalls, including email security solutions. In a Cisco environment, we can have full visibility, and this is what I see when protecting against threats such as phishing and ransomware—Cisco Secure Access is effective..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“The best feature that Cisco Secure Access offers is a single platform where DNS security, ZTNA, and everything are in one place, all managed through a single cloud dashboard.

“Having everything in a single platform and dashboard has made things easier for me and my clients because everything is available for checking or troubleshooting.

“Cisco Secure Access has positively impacted my organization because we are Cisco preferred partners. We deploy everything for our clients, so it is not just about deploying it in our organization. Since we are a preferred partner, many clients requiring Cisco Secure Access are routed to us from Cisco.

“After deploying Cisco Secure Access, I received specific positive outcomes and feedback from my clients. For the use case concerning DNS security over the last three months, their AD integration with Cisco Secure Access allows them to create user-based policies for DNS security based on identity and username. They also receive a dashboard to monitor reports on threats and everything online in the cloud. The customer is very happy that they are able to overview their organization, seeing the number of users utilizing maximum applications, the top talkers, and everything.

“Cisco Secure Access has greatly impacted protecting my organization and clients from threats such as phishing and ransomware. Because it has ZTNA and is cloud-based with VMs deployed inside the network, it creates best practice tunnels required for accessing applications from day one. Thus, we can deploy with peace of mind without juggling best practices or opening only specific ports..”

Verified user

[Read full review](#) 

PMN Design And Implementation Engineer at a computer software company with 201-500 employees

“I rely on continuous verification and application access the most in my day-to-day work. There are hundreds and thousands of applications running that need to be safe. We cannot just provide access to people since it's a very secured environment; a small mistake can cause bigger problems. Specifically, we operate at three levels on the same platform: Tier 1, responsible for basic monitoring; SROs who are more advanced engineers performing routine actions; and SREs with root privileges. Now, we can create three layers of access: Tier 1 gets access for monitoring only; SROs have privileges for a certain number of applications; and SREs have full access to do whatever is required, ensuring the people with the correct skill set and knowledge have the right access level. With most people working from home, it is crucial to protect our secure data from hackers and malicious attacks because they can exploit systems to bring the entire chain down quickly. It helps that there is a defined process with a series of sequences that need to be followed for logging in, and even post-login, there is a second layer of control ensuring privileges are used correctly without allowing mistakes that could cause platform blunders.

“There is a very common threat that happened three or four years back which was ransom. People were knocking into platforms using credentials and taking over servers. An incident happened at MediaKind where they had an attack from a ransom that froze the origin server. Origin server freezing means all data comes from there, and if hackers compromise that and stop streaming, it can collapse the entire media stream, resulting in huge losses for broadcasters and advertisers. MediaKind faced this for around 30–40 minutes because they used the normal VPN. We quickly realized that this wasn't going to work because VPN just uses credentials that anyone can exploit. Later, we moved to Cisco Secure Access, which goes through MFA. You log into a client, then enter Microsoft Entra ID, followed by MFA, and you authenticate through your phone and authenticator. There are policy engines and ZTNA, and only then you can log into applications and perform tasks.

“In my opinion, Cisco Secure Access offers excellent features, starting with application-level access, not network access, where each time a particular application needs to be accessed, there is a provision for that instead of giving entire network access. The verification feature is nice as it doesn't work as a one-time authenticator, but a continuous verification process occurs. It's more into a

zero-trust model, where if it identifies a deviation, it will not let you go in. Everything is centralized and very secure, considering it's on the cloud..”

AK sharma

Manager, Ott Platform at Synamedia

[Read full review](#) 

“I think Zero Trust Access for application is the feature I find most valuable in Cisco Secure Access.

“I only use Cisco Secure Access' AI Access feature for troubleshooting. It has a log feature, and there isn't really any AI element in that. The AI feature is more having an AI tool at the top where you can ask a question to get visibility. You can ask what a log means or ask a question that you want the AI to answer for you. There's an AI icon at the top of the bar, and then you can ask questions. That's basically where the AI feature is. There's no AI in terms of the telemetry unless you ask the AI feature to do it for you. If you want the AI element for that, there's another feature that Cisco has that you have to add as a feature add-on.

“Cisco Secure Access has a VPN as a service feature. You have that Zero Trust as well because it's almost a VPN but just for applications. You access the application encrypted, but you don't need a VPN tool to connect. You can just access the application, which is what Zero Trust basically is. If you want VPN as a service, Secure Access has it. If you want to allow remote access for a certain application, then you do the Zero Trust setup, which is also a VPN but you don't need a VPN client to make it work.

“Most of the time, I recommend my customers to use Cisco Secure Access' Experience Insights feature for Branch Access, which is basically when you want to tunnel all your traffic. You probably have a gateway in a branch and then you create a tunnel with Secure Access and then you send all clients through that tunnel to Secure Access. Everything including web traffic can be visible. You can also use it for VPN. You can use it to protect applications like I mentioned earlier about Zero Trust. You want to create an application that users can access remotely without using a VPN client, then you can do a Zero Trust setup. You can also do a proxy setup where you send all your internet traffic through Secure Access. These are the four features that I like about Secure Access.

“I use Cisco Secure Access' Hybrid Private Access feature for varying the enforcement location for ZTNA private traffic. ZTNA is Zero Trust Networking, the private one.

“The policy verification feature helps reduce policy misconfigurations in Cisco

Secure Access where you can check to make sure that all your policies are intact. That is something we definitely use, especially if you have a lot of rules going on. You want to make sure that your rules are intact and you don't have any conflicts going on anywhere. That is a feature I always recommend..”

Dennis Nnate

L4 Solutions Engineer at a financial services firm with 501-1,000 employees

[Read full review](#) 

Other Solutions Considered

“Before Cisco Secure Access, we were using VPNs, but we switched because it wasn't very secure; any exposed username and password posed a security threat..”

AK sharma

Manager, Ott Platform at Synamedia

[Read full review](#) 

“FortiGate cloud solution is what I usually recommend instead of Cisco Secure Access. They have something similar as well. If a customer says that Secure Access is too expensive for themselves, I recommend FortiGate because they're not too bad in pricing..”

Dennis Nnate

L4 Solutions Engineer at a financial services firm with 501-1,000 employees

[Read full review](#) 

“There was no single solution before. What we were doing before Cisco Secure Access was just a traditional on-premises VPN or other standalone remote access solutions, which was always, I think, a management headache. Multiple products were needed for different use cases. Moving to Cisco Secure Access really helped consolidate all that into one overarching end-user security platform..”

Chris Crotteau

Sr Sales Engineer at CrossConnect

[Read full review](#) 

“We previously relied heavily on traditional VPN connectivity for remote access, and Cisco Secure Access has played an important role in our transition toward the ZTNA model rather than providing broad network access through a VPN. ZTNA enables secure access to applications based on user identity, device posture, location, and security policies. The transition has significantly improved both security and user experience. With traditional VPNs, users often received access to a larger portion of the network than necessary, which increased risk and administrative complexity. Cisco Secure Access allows us to grant access only to the specific applications and resources required for the user's role, reducing the attack surface and supporting zero trust. From an operational perspective, the migration has simplified access management and reduced the number of VPN-related support issues. Users experience more seamless connectivity because they no longer need to establish a full VPN session for every task, and administrators can manage policies centrally through a unified platform. We still maintain limited VPN access for certain legacy systems and specialized use cases, but the majority of our remote access strategy now relies on ZTNA. Cisco Secure Access has made the transition from VPN to ZTNA smoother than expected by providing stronger security controls, better visibility into our user activity, simplified administration, and a more consistent experience for remote and hybrid workers..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

“We conducted a thorough evaluation of several secure access and zero trust solutions before selecting Cisco Secure Access. The products we considered included Zscaler Private Access, Alternate Network solutions, Netskope, Microsoft-based security, and remote access solutions that align with our existing cloud strategy. Our evaluation focused on several criteria, including zero trust capabilities, ease of deployment, visibility into applications and activity, integrations with existing security investments, scalability, reporting, and overall user experience. We also assessed each vendor's ability to support hybrid environments that include both cloud-hosted and on-premises applications. Ultimately, Cisco Secure Access stood out because of its strong combination of ZTNA functionality, unified policy management, cloud-delivered security services, AI-driven insights, Thousand Eyes integration for digital experience monitoring, and compatibility with broader security ecosystems. We also valued the ability to manage security policies consistently across remote users, branch locations, and private applications from a centralized platform. While the competing solutions offered strong features in specific areas, Cisco Secure Access provided the best overall security, visibility, operational simplicity, and long-term scalability for our requirements. The platform blended well with our zero trust strategy and offered a path for future required architectural changes..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

“While comparing Cisco Secure Access with competitors, Trend Micro would be an exact competitor. Trend Micro gives many solutions under a single console, such as Trend Vision One, and they have also incorporated AI security. However, when it comes to XDR solutions, there are several in the leader quadrant such as SentinelOne and CrowdStrike, but SecureX has not emerged as a leader in the XDR space. Cisco Secure Access itself is good, as we have not seen any attacks in Cisco environments, but as per compliance, we should not rely on a single vendor in our environment. Trend Micro is a leader quadrant product and has been a major provider for many enterprise banks, especially in large enterprises, making it one of the good competitors for Cisco Secure Access.

“For the CASB functionality with Cisco Secure Access, I have not worked that much on CASB for Cisco Secure Access. When it comes to CASB, we have solutions such as Forcepoint, CloudSEK, Netskope, or Zscaler. With these products, we have plenty of CASB use cases. I have not worked with Cisco Secure Access on CASB..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Quantifying the return on investment depends upon what the use case is and the automation we can build up. We just did some study where, with automation and all of that, we can get almost 30% ROI..”

Rajender Bhandari

Chief Technology Officer at Binary Global Limited

[Read full review](#) 

“For our customers, it has been a big time saver in terms of policy management. Because now, I do not have to maintain separate policies for my remote users versus my on-premises users or people in a hybrid environment. For our customers, there has been a pretty good ROI and pretty quickly too..”

Chris Crotteau

Sr Sales Engineer at CrossConnect

[Read full review](#) 

“We haven't broken down to the level of measuring ROI yet, but in terms of investment, it's been decent. We save effort, not just money, as it simplifies control and management. Previously, we managed numerous licenses for the same set of tasks, whereas with one license from Cisco Secure Access, we can multitask, providing application-level access and proper authenticators, making it a super tool overall..”

AK sharma

Manager, Ott Platform at Synamedia

[Read full review](#) 

“The return on investment in Cisco Secure Access is significant. With both wireless and security systems, it provides substantial savings in time, data loss prevention, and management of protection. If you are using other products and you are attacked with ransomware, you will pay a lot of money and have limited protection. Protection has a price and also has a benefit.

While ROI varies from customer to customer, regarding time saving, it can reach up to 30% savings. This is based on the processing time and retention policy of Cisco Secure Access, which is more than 30% better than others..”

Nassif Kaleny

IT Manager at Bavaria Egypt S.A.E.

[Read full review](#) 

“If you have a Cisco environment, it will give the best ROI. Everything must be of Cisco product family only, starting with EDR, XDR, mail security, switches, firewalls, and access through ZTNA. If you have every solution with Cisco, you can see a very good ROI because you do not need to invest much on staffing for analyzing each and every console separately. Everything will be monitored, and all those logs from various Cisco solutions will be coming under one console, which helps in clarifying what we have and any security loopholes in our environment that security teams need today.

“I cannot quantify ROI specifically, such as ten percent or twenty percent, as it varies based on the environment. For a fully Cisco environment, it could be around sixty percent to seventy percent ROI or more, but if it is not a fully Cisco environment, it would be much less due to various integrations with other third-party solutions, which are not at a very granular level. Therefore, the ROI is greater with more Cisco solutions and less with fewer solutions..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“We have seen a measurable return on investment from Cisco Secure Access, both from a security and operational perspective. One of the biggest benefits has been the reduction in administrative effort through centralized policy management and automated access controls. We estimate that tasks related to user provisioning, access modifications, and policy administration require approximately twenty-five to thirty percent less effort compared to our previous approach. We have also seen a noticeable reduction in access-related support tickets as users experience more reliable and streamlined connectivity through the zero trust model. This has allowed IT and security teams to spend less time troubleshooting remote access issues and more time focusing on strategic initiatives. Incident investigations and resolution times have improved as well due to better visibility into user activity, application access, and network performance. From a financial perspective, Cisco Secure Access has helped us consolidate several security and remote access functions into a single platform, reducing operational complexity and minimizing the need for additional infrastructure. The cloud-delivered architecture also lowers maintenance requirements compared to managing traditional remote access solutions. Overall, the combination of improved security, faster onboarding, and reduced administrative workload, fewer support issues, and better operational efficiency has delivered a strong return on investment. While the exact savings vary by organization, the productivity gains and the risk reduction have more than justified the investment for us..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

Use Case

“We use Cisco SD-WAN in our own company for our own needs, and we are also selling this to our customers while performing operations for customer networks. My personal customer scope is the large enterprise customer. We have integrated Cisco Identity Intelligence with Cisco Secure Access using Cisco ISE..”

Eric Biederbeck

Enterprise Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“I am dealing with Cisco Secure Access products. As a consultant and reseller, I am using it myself with Cisco Secure Access.

“You can have tenants with Cisco Secure Access. Tenancy is obviously part of it, so you can have multiple tenants on Secure Access. Especially if you're a managed service provider, you can have multiple tenants where you just have to flip the feature and specify which tenant you're working in. I've used that before to manage multiple infrastructures, and all you have to do is change the tenancy. That is quite useful. It used to be like that for Umbrella as well. Cisco basically just translated it back to Secure Access, so the same feature on Umbrella is on Secure Access as well. We have used it..”

Dennis Nnate

L4 Solutions Engineer at a financial services firm with 501-1,000 employees

[Read full review](#) 

“My main use case for Cisco Secure Access is providing secure remote access to internal applications while enforcing Zero Trust security policies. For example, in a lab environment, I used it to securely connect to internal web applications without exposing them directly to the internet. I also used its Secure Web Gateway to monitor and filter web traffic based on organizational policies. Day-to-day, it helps ensure that only authenticated and authorized users can access specific resources, improving security while maintaining a smooth user experience for remote users.

“One thing I appreciated about my main use case and the authentication process with Cisco Secure Access was how it centralizes access management and security policies in a single platform. Once authentication and access rules were configured, day-to-day administration became much simpler. It also provided good visibility into user access and security events, making it easier to identify and investigate potential issues. Overall, it improved security without creating unnecessary friction for end-users, which was one of the biggest advantages..”

SehajVohra

Member at IEEE Signal Processing Society UPES

[Read full review](#) 

“I have been working with Cisco Secure Access for the past five years. We have multiple use cases for Cisco Secure Access, with most of them associated with DNS filtering security. We use it as a replacement for secure internet, providing web filtering. Instead of giving a web filtering or proxy solution, we provide it as a DNS filtering solution where it helps us to stop the traffic even before reaching the malicious server. In normal traditional proxy solutions, end user traffic generated from the system and endpoints reaches the malicious or unauthorized servers, and then while getting a response back to the end-user machine, the proxy blocks that particular request or response sent from the server. In this case, what Cisco is providing is a DNS security advantage license and a security gateway. They have a higher role where they can control the traffic when the traffic is generated from the end-user endpoint machine itself. That itself is an advantage for controlling our traffic to the public IP of the malicious and unauthorized servers. That is one key advantage which we have for this use case.

“We also provide secure access for people who want to access the internal application from outside. We give AnyConnect, which checks whether they are connecting to the network from the proper device assigned to them. If not, we can block that particular device for a time interval if we see that the device is vulnerable. These are the kinds of use cases we are working with Cisco Secure Access..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“My main use case for Cisco Secure Access is for one client, where I deployed DNS security. Previously, Cisco DNS security was part of Umbrella; now, it has been moved to Cisco Secure Access. I implemented DNS security, which provided the client with cloud-based DNS security and intelligent proxy features, so they are protected from day-zero attacks with policy management in place. That was one use case for Cisco Secure Access, and for another client, I have recently deployed ZTNA using Cisco Duo MFA.

“For a specific example of how I used Cisco Secure Access for one of these clients, I will provide the example of one client where I deployed ZTNA through MFA. The client has around 1500 users working in a hybrid environment, so connecting every user on the VPN, whether hardware-hosted, VM-hosted, or anywhere else, causes unnecessary burden. SASE is the best use case of Cisco Secure Access in the hybrid environment, where if users want to access any of their private applications, they connect to Cisco Secure Cloud. From the cloud, the traffic is tunneled, providing zero-trust access and requiring MFA to access any internal application. This way, since it is cloud-based security, the routing and everything is taken care of in the cloud, avoiding dependency on hardware infrastructure or overusing the link in the data center itself..”

Verified user[Read full review](#) 

PMN Design And Implementation Engineer at a computer software company with 201-500 employees

“My main use case for Cisco Secure Access is especially for our security purposes as it provides secure access to only the permitted applications. We work on many applications where different teams come together. They are responsible for different clusters, different domains, different applications, and we are always in a requirement to have the selected level of access to a particular set of people. For that, Cisco Secure Access is a super tool to work with.

“Initially, VPNs were used, but the problem with VPNs was that it provides access all at once, and then we cannot continuously perform those verifications.

“In my day-to-day operations, we in Synamedia have three business units responsible for three different things: one is control plane, we are into the data plane, and there is a network team as well. Collectively, we are supporting a customer called Astro. There are different applications hosted on the same Kubernetes cluster. The thing is these are different BUs, so we are bound with the responsibilities and our action should be very much limited. To have a better solution where we can ensure that the right set of people have the right set of privileges and access, we have created Cisco Secure Access for different users accordingly. If anything needs to be done on the control plane side of things, that particular team can do it. If it requires only access to the data plane into the Kubernetes clusters, then the people in my team have those accesses, so they cannot touch on the control plane side, and the control plane team cannot touch on the data plane.

“The third team, which is on the network side, we don't want to expose our data plane and control plane to them and want to keep the network very much secure with them. So all of us are using the same platform, but we have limited or restricted access, and that's why we can collectively work better ensuring that we are not encroaching into different territories, and everything works very smoothly.

“Recently, we conducted the Olympics, where we had teams from Synamedia, Alibaba, and their affiliates, Mina Tech, involved. Since a lot of revenue is involved, it was an Olympic thing, and we cannot risk security. That's why we went with our Cisco Secure Access. Initially, Synamedia was itself Cisco, and then it moved out as a media domain out of Cisco. To ensure that there is a good level of security and proper access, the particular teams which are supposed to perform necessary

actions and need to put their scripts on the platform were taking care of that specific domain. The beauty of that is every time you enter into any platform, you have to go through a series of authentication that needs to be handled appropriately. If you fail, then that particular person cannot enter the platform, making it super secure. With events such as NBAs and Olympics, we want it to be very much secured as there are hackers looking for ways to access our system. In that scenario, it becomes very important that we keep all our clusters, platforms, and applications secured with a trusted solution, and that's why we have gone for Cisco Secure Access..”

AK sharma

Manager, Ott Platform at Synamedia

[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 installation procedure for Cisco Secure Access is case-to-case and depends on the customer workload, which allows for proper study based on customer instructions..”

SreejeshSoman

Technical Consultant at Vertex Techno Solutions (B) Pvt Ltd

[Read full review](#) 

“The initial setup of Cisco Secure Access was not straightforward. There were a lot of discussions, especially with our customer about what the benefits are, particularly regarding the cost and the cost-benefits ratio, with discussions being more governance-driven or management-driven rather than technical, which meant it took a lot of time..”

Eric Biederbeck

Enterprise Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“Regarding the deployment procedure of Cisco Secure Access, I cannot say it is straightforward, nor can I say it is complex. It depends on the design. However, overall, if you have someone at Cisco who knows the design procedures and the main objectives of Cisco Secure Access, it is straightforward and easy..”

Nassif Kaleny

[Read full review](#) 

IT Manager at Bavaria Egypt S.A.E.

“The authentication process for users in Cisco Secure Access was generally straightforward and easy to configure. Integrating it with an identity provider and enabling multi-factor authentication, MFA, was smooth, and the user onboarding experience was simple. The main challenge was configuring access policies correctly for different user groups during the initial setup, as it required careful planning and testing. Once those policies were in place, authentication became reliable and seamless. Overall, the setup was manageable, and the platform provided a secure, yet user-friendly login experience..”

SehajVohra

[Read full review](#) 

Member at IEEE Signal Processing Society UPES

“Overall, it has been a fairly good experience. Deploying Cisco Secure Access, because for a lot of customers they started with Umbrella, and it goes back to that same operational model, that same user interface, the same configuration model, has made it probably one of the easier SASE solutions to deploy compared to some of the other vendors out there..”

Chris Crotteau

Sr Sales Engineer at CrossConnect

[Read full review](#) 

“Our experience with Cisco Secure Access pricing and licensing has generally been positive. While the solution is not the lowest cost option in the market, we found that the value provided through security, scalable centralized management, and zero trust capabilities justifies the investment when evaluating the total cost of ownership. It helps reduce the need for multiple standalone security and remote access solutions, which simplified operations and improved overall efficiency. The initial setup and implementation costs were largely associated with planning, policy design, integration with identity providers, and migration from existing remote access technologies. Like most enterprise security platforms, deployment requires careful preparation and stakeholder involvement, but Cisco provided sufficient documentation and support resources to make the process manageable..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

Customer Service and Support

“The customer service is good and great because Cisco has a large team of engineers providing support. I would rate the customer service support from Cisco at eight or nine..”

Marghoob AhmadSalik

Se Presales at Redington Group

[Read full review](#) 

“I am happy with technical support from Cisco regarding Cisco Secure Access. They address all our questions and technical specifications. They provide answers and solutions effectively..”

Nassif Kaleny

IT Manager at Bavaria Egypt S.A.E.

[Read full review](#) 

“Regarding support, I do not know what happened to Cisco. I contact them, and the support has been a pain. The quality of support has dropped so drastically that it is not even funny..”

Vusa Ndlovu

Security Solution Architect at a tech services company with 501-1,000 employees

[Read full review](#) 

“Cisco customer service is average. It is neither good nor bad. I would rate Cisco customer service five out of ten points. For the support, I would say they could be faster. Two or three years ago, Cisco support was very good, rated around eight or nine, but now the support engineers seem unaware of what their product is capable of. I have seen issues where I needed to explain use cases multiple times and escalate them multiple times to get solutions, leading me to rate them five now..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“Technical support is perfect, and I find it fine. I would rate their support an eight out of ten.

“There is still room for improvement when it comes to response time, especially if you need some response from the US. If you need support from the US side, you can see the different countries, and sometimes it takes very long to get an approval from the US side, which is something that could be better..”

Eric Biederbeck

Enterprise Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“Our experience with Cisco Secure Access customer support has generally been positive. Cisco provides multiple support channels, including a support document knowledge base and access to specialists when needed. For standard issues and configuration questions, response times have been reasonable, and support engineers have demonstrated strong technical knowledge of both the platform and Cisco Secure Access. Another strength of the support has been their ability to assist with our complex deployment involving zero trust implementation, integrations with hybrid environments, and security policy management. During the implementation and ongoing operations, we have been able to leverage Cisco documentation and support resources to use new features more effectively. The critical issues escalation process has worked well, helping minimize our impact. We have also found community resources, including guides and best practice documentation, to be valuable supplements to direct support interactions. While it can vary depending on the specific issue and the support team involved, our overall experience has been positive with Cisco Secure Access support..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

Other Advice

“The AI element of Cisco Secure Access should have better guidance on the logs. To be honest, I can't think of anything else because it's quite a robust feature. My overall review rating for Cisco Secure Access is nine out of ten..”

Dennis Nnate

L4 Solutions Engineer at a financial services firm with 501-1,000 employees

[Read full review](#) 

“For those looking into using Cisco Secure Access, I would say it's a very good solution that fulfills your security needs. Cisco Secure Access is a good tool. I would give this product a rating of nine out of ten..”

AK sharma

Manager, Ott Platform at Synamedia

[Read full review](#) 

“I mentioned both the advantages and the use cases of Cisco Secure Access. Usually, what we do is block QUIC traffic because the QUIC traffic is based out of UDP on port 443. By initially blocking QUIC protocol traffic, if the customer specifically asks, we will enable QUIC traffic for particular applications alone. Since it is part of best practice, we usually block it. However, in some use cases, we have enabled the QUIC protocol and provided bypassing instructions for those UDP protocols. The basic reason we block QUIC protocols is that it is a safe encrypted protocol. We cannot inspect QUIC traffic using inspection engines in web proxy or SecureX, as established with HTTPS and HTTP. That is why we prefer to block QUIC protocols, but it does work well when enabled. I give this product an overall review rating of eight..”

GANESAN K

Senior Technical Engineer at Safezone Secure Solutions Private Limited

[Read full review](#) 

“For others looking into using Cisco Secure Access, my advice is that it is a good solution and they should experience it.

“I chose eight out of ten primarily due to only the PoP presence. I would rate the ease of managing Cisco Secure Access through its single cloud-managed console an eight.

“In my experience, it is easy to navigate and manage everything from the console, but compared to the FortiGate SASE platform, FortiGate has a unified platform for all their products, while Cisco has each platform operating differently.

“I use the Zero Trust Network Access (ZTNA) feature of Cisco Secure Access, and it is a great feature. We do not need to worry about the security of accessing applications from outside the environment. With ZTNA, each application access requires authentication, which is a truly great feature.

“This ZTNA approach has positively changed my client's security posture, and there are no significant challenges or surprises. I rate this product eight out of ten..”

Verified user

PMN Design And Implementation Engineer at a computer software company with 201-500 employees

[Read full review](#) 

“I would confidently recommend Cisco Secure Access to organizations looking to modernize secure remote access.

“Cisco Secure Access has a strong approach to AI governance and security. I appreciate that its AI-driven capabilities are supported by Zero Trust principles, identity-based access controls, and continuous monitoring. The platform provides good visibility into user activity and helps detect suspicious behavior while maintaining strict security policies. From a governance perspective, centralized policy management and detailed audit logs support compliance.

“I believe there is still room for improvement.

“I find the AI capabilities of Cisco Secure Access to be accurate and reliable for most security-related tasks. The platform consistently identifies potential threats, provides relevant security insights, and helps prioritize alerts, which reduces manual effort for administrators. In my experience, the recommendations are generally actionable and aligned with security best practices. While no AI system is perfect and some alerts may require manual verification, the overall accuracy is high enough to improve operational efficiency and support faster decision-making. I would consider its AI output trustworthy for day-to-day security operations. I gave this review a rating of 9..”

SehajVohra

Member at IEEE Signal Processing Society UPES

[Read full review](#) 

“My biggest piece of advice is to approach Cisco Secure Access as a strategic, zero trust initiative rather than simply a replacement for traditional VPN technology. Organizations get the most value when they take the time to understand application requirements and security objectives prior to deployment. Having a sound access strategy and well-crafted policy creation makes it much easier to maximize both security and user experience. I would recommend starting with a phased rollout, beginning with a simpler group of users and application policies, gathering feedback, and then expanding gradually. This approach facilitates smoother implementation and wider adoption. Another key takeaway is to take advantage of the platform's features, including digital experience monitoring through Thousand Eyes and centralized policy management.

“Overall, Cisco Secure Access has been a valuable component of our security strategy. The platform has modernized our approach to secure connections by supporting zero trust, improving user and application access, and reducing our dependence on traditional VPN-based remote access. We have benefited from centralized policy management, strong security controls, digital experience monitoring capabilities, and the ability to deliver a consistent experience for remote and third-party users. Continuous use of Cisco Secure Access has provided the flexibility and scalability needed to support changing business requirements without adding operational complexity. The overall benefits have far outweighed those challenges. If I were to summarize the platform in a few words, I would describe it as secure, highly reliable, and aligned with modern zero trust strategies. For organizations looking to strengthen security while managing a distributed workforce, Cisco Secure Access presents a strong option with both operational and security value. I would rate this solution a nine out of ten..”

Vishnu Narahari

Manager at a computer software company with 201-500 employees

[Read full review](#) 

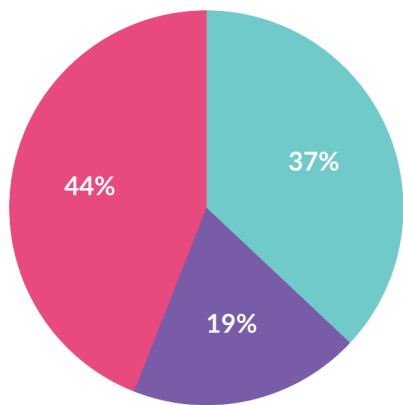
Top Industries

by visitors reading reviews

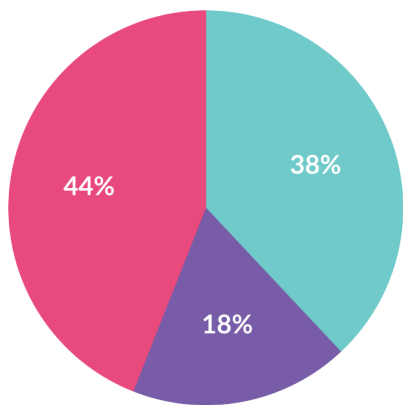


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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