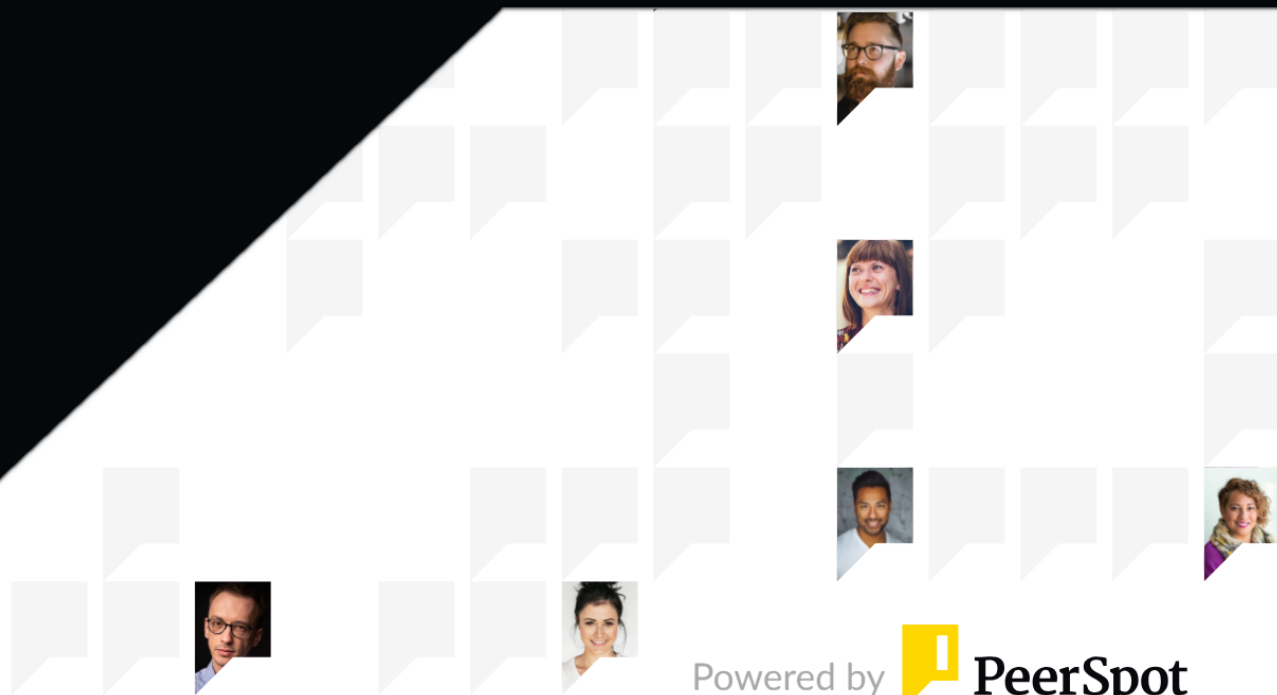




Cloud Security Connector for Zscaler

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 - 23

Setup..... 24 - 27

Customer Service and Support..... 28 - 30

Other Advice..... 31 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Cloud Security Connector for Zscaler

Cloud Security Connector for Zscaler

Recap

Cloud Security Connector for Zscaler is designed to enhance security by blocking malicious content and providing agentless integration with cloud workloads. It simplifies policy management and improves scalability, making it a critical tool for securing cloud environments.

Cloud Security Connector for Zscaler automates node detection, route selection, and offers centralized visibility, allowing businesses to focus on scaling without traditional firewall constraints. Its high availability routing, SIEM integration, and centralized log management streamline security operations. The solution reduces data leakage risk by enforcing consistent policies across infrastructures. However, areas such as remote user network resolution, configuration complexity, and enhanced routing require improvements for optimal performance.

What are the key features of Cloud Security Connector for Zscaler?

- **Automated Node Detection:** Enhances efficiency by reducing manual setup.
- **High Availability Routing:** Ensures seamless connectivity and service continuity.
- **Centralized Visibility:** Provides a unified view of security policies and incidents.
- **Policy Management:** Simplifies and unifies enforcement for consistent security.
- **SIEM Integration:** Enhances control with robust log management.
- **Agentless Support:** Facilitates easy integration with cloud environments.

What benefits should users expect when evaluating Cloud Security Connector for Zscaler?

- **Improved Scalability:** Eliminates reliance on traditional firewalls.
- **Risk Reduction:** Mitigates data leakage through enforcement of policies.
- **Operational Efficiency:** Streamlines management of security infrastructure.
- **Compliance:** Assists in monitoring and logging for regulatory adherence.

In industries like banking, Cloud Security Connector for Zscaler is vital for compliance support, as it monitors outbound traffic and enhances visibility over workload communication. Organizations benefit from zero-trust protection by inspecting all traffic for threats and accurately enforcing security policies, reducing configuration errors while supporting secure routing for cloud services like AWS.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Cloud Security Connector for Zscaler has had a very positive impact, especially in terms of security and operational efficiency.”



Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems



“Cloud Security Connector for Zscaler has had a positive impact by making the testing and validation process more efficient.”



Sini Maria Jose

Automation Engineer at Techmahindra



“Cloud Security Connector for Zscaler has positively impacted our organization by helping us in our cloud environment to connect our resources to Zscaler, ensuring that security policies are consistent with zero-trust access and increasing reliability by 28%.”



Jaspreet k

Head Of The Operations at Flash AI



“Cloud Security Connector for Zscaler has positively impacted my organization, because now whenever we log into our VDI, we can access our apps directly without connecting to a separate VPN, saving approximately five to ten minutes each time and significantly improving our productivity and screen time.”



Dhanesan Sridhar

Decision Scientist 3 at Mu Sigma Inc.



“Cloud Security Connector for Zscaler has positively impacted my organization by improving the ROI side, as it reduced tool and architecture complexity because it can replace or reduce dependence on VPN, virtual firewall, NAT, proxy tools, and other similar solutions.”



Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees



“Cloud Security Connector for Zscaler has positively impacted our organization in securing a lot.”



Mohamed Raiyan

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



“While we are operating Cloud Security Connector for Zscaler, we have noticed a radical drop in architectural complexity, along with a massive cloud infrastructure cost reduction and accelerated incident response times.”



Yousef Almomani

Systems Engineer at a consultancy with 51-200 employees

What users had to say about valuable features:

“The best features that Cloud Security Connector for Zscaler offers include a great login feature because I cannot log into Cloud Security Connector for Zscaler without my company's ID, and it requires Okta verification. It is pretty easy and safe as well. No other person can access Cloud Security Connector for Zscaler on their laptop because it has some separate code to log in and log out, which is provided by the administrator only. Security-wise, Cloud Security Connector for Zscaler is very helpful.

“Cloud Security Connector for Zscaler has positively impacted our organization in securing a lot. Previously, there were many security issues. Before using Cloud Security Connector for Zscaler, around five percent of security breaches happened without our notice. Thankfully, our client noticed these breaches and found them before they became problematic. We wanted to ensure it does not happen in the future, which is why we moved to Cloud Security Connector for Zscaler. Everything is good, and it has been working well. From a security perspective, everything is good in Cloud Security Connector for Zscaler, and our organization is mostly relying on Cloud Security Connector for Zscaler to safeguard everything..”

Mohamed Raiyan

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

[Read full review](#)

“The best features Cloud Security Connector for Zscaler offers include extended ZIA and ZPA to cloud workloads, secure internet inbound traffic from workloads with capabilities such as SSL inspection, IPS, firewall control, and DLP by ZIA. It enables app-to-app and app-to-private access connectivity using Zero Trust Exchange, including multi-cloud and hybrid cloud use cases. It supports AWS, Azure, and GCP deployment and includes centralized policy and visibility, automated orchestrated deployment support, Azure Resource Manager, and a highly scalable architecture.

“Out of those features, I find the strong zero-trust approach for cloud workloads to be the most valuable day-to-day because Cloud Security Connector for Zscaler is designed around zero-trust connectivity, not legacy network extension. It provides inside-out connections through Zscaler Zero Trust Exchange, which reduces exposure and avoids broad network-level access. For example, a workload in AWS can securely connect to a private application in Azure through Zscaler policy controls without building site-to-site VPNs or opening large network paths. This is a good replacement for legacy cloud networking components. Cloud Security Connector for Zscaler positions itself as a simple alternative to legacy cloud VPN, virtual firewall routers, proxy NATs, and other tools. This is a strong advantage for organizations trying to reduce architecture complexity..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“Cloud Security Connector for Zscaler offers the Cloud Firewall, IPS, DNS control, port visibility, and port protocol visibility, routing profiles, explicit profile configurations, and proxy configurations. These are the main features that we use in our infrastructure day-to-day.

“The majority of the time we rely on the Cloud Firewall, URL filtering, and Cloud App Control from Cloud Security Connector for Zscaler. These are the three main features which we mainly use because the Cloud App Control has really good features. It has all the applications, more or less all the applications that we want to block for our infrastructure and for the client as well. We find all of them in there itself at the first place, and if something is not there, we can always use the URL filtering and add URL categories or block those URLs or just monitor what our users are doing.

“The impact of Cloud Security Connector for Zscaler on our organization has been very positive as it is a very efficient application that we use for ninety percent of the clients. It has all the modules covered and the experience center built in there for ZIA, ZPA, ZDX, and we can do a lot from there itself. If we have to forward a profile, set up a tunnel, or anything else, it can be easily done via the ZCC agent itself..”

Verified user

[Read full review](#) 

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

“The best features of Cloud Security Connector for Zscaler are its seamless integration with the Zscaler cloud, secure traffic forwarding, and centralized policy enforcement. It provides consistent security controls without requiring complex on-premise infrastructure. I also appreciate its scalability, visibility into network traffic, and the ability to apply the same security policies across different environments.

The features that help my team the most are secure traffic forwarding, centralized policy enforcement, and visibility into traffic. In day-to-day work, these features make it much easier to validate whether traffic is reaching the Zscaler cloud correctly and whether the expected security policies are being applied. Instead of manually checking every scenario, I automate many of these validations using Selenium and Java, which saves time and improves test coverage. It also helps to quickly identify configuration issues or policy mismatches before they reach production, reducing troubleshooting effort and improving the overall quality of releases.

Cloud Security Connector for Zscaler has had a positive impact by making the testing and validation process more efficient. It helps ensure that traffic is securely forwarded to the Zscaler cloud and that security policies work as expected before changes are deployed. This has helped reduce manual testing effort, identify configuration issues more easily in the release cycle, and improve the overall quality and reliability of deployments. As a result, my team can deliver changes with greater confidence and reduce the likelihood of production issues..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

“The best features that Cloud Security Connector for Zscaler offers are not just about the security checkboxes; they are about the operational sanity for cloud engineers and system administrators.

“Managing cloud egress traffic using traditional methods such as virtual firewalls or complex NAT tables is famously tedious. Cloud Security Connector for Zscaler makes things easier for cloud engineers and system administrators compared to traditional methods, which highlights why it delivers operational sanity. The route management nightmare is gone, and we get automated next-hop selection. We only select the next hop, and the manual tunnel management is gone. We use Zscaler API automation.

“When we evaluate the governance and security for Cloud Security Connector for Zscaler, we find that it is highly advanced, particularly regarding how it tackles the shift from human users to autonomous, machine-speed AI workloads.

“When evaluating the accuracy and reliability of output for Zscaler AI capabilities, specifically how it handles the traffic following throughout Cloud Security Connector for Zscaler, we have to separate it into two distinct functions: AI-driven threat detection, which means analyzing the malicious traffic, and AI data classification, covering DLP and governance rules. Zscaler AI capabilities score incredibly high on reliability because they are built on a closed loop of data, but they face inherent limitations when dealing with the unpredictable nature of generative AI..”

Yousef Almomani

Systems Engineer at a consultancy with 51-200 employees

[Read full review](#) 

“The best features Cloud Security Connector for Zscaler offers are that even in our secure environment, we have a different region hosted, such as US and UK. Before that, we were using some private VPN, so we needed a US VPN separately and UK VPN separately. But now after using Cloud Security Connector for Zscaler, which becomes a centralized VPN, we are able to access the US-hosted app as well as UK-hosted app so that we can bypass using different VPNs for different regions. That is the main use case.

“Regarding ease of use, to connect to Cloud Security Connector for Zscaler, we need our org ID. Whenever we are authenticating using our org ID, it is easy to connect to Cloud Security Connector for Zscaler. It is pretty handy and user-friendly. Once it is connected, we can be able to access all the apps which are hosted inside our private environment.

“Cloud Security Connector for Zscaler has positively impacted my organization. Previously, as I mentioned, we needed to connect to VPN every time separately. But now whenever we log into our VDI, we can connect to the VPN by pre-default because Cloud Security Connector for Zscaler is already installed. Once it is already installed, we can access our apps directly without connecting to the VPN. Because of this, we are saving approximately 5 to 10 minutes of time, so that increases our productivity and screen time. If I want to access some information quickly, before it would take time because I would need to connect to VPN and open the app. But now because Cloud Security Connector for Zscaler is pre-defaultly connected, I do not need to connect to any private VPN separately, so it reduces my time.

“Previously, if a particular task was taking 10 minutes, now it is significantly reduced to two to three minutes only. We saved seven minutes of time in each and every task. It is actually an improvement..”

Dhanesan Sridhar

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

Other Solutions Considered

“Before choosing Cloud Security Connector for Zscaler, I have not evaluated any other option in terms of Cloud Connector, but I have worked on Netskope as well..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“We have evaluated a couple of them for Cloud Security Connector for Zscaler. The major ones were CrowdStrike, and we have gone for the Palo Alto SASE projects as well, but Zscaler was the best one we have ever used in those terms..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“It is not about using a different solution for me. I am a customer support executive, so I need to support different customers and solutions. Based on the customer requirement, I give them different solutions. Sometimes it is Zscaler and sometimes it is Netskope. It is not about switching one solution to another solution for me..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“We were not particularly using different solutions, but for that case, we had been using Trend AI, formerly known as Trend Micro. We were using the Trend Vision One XDR, but that was not capable enough, and on top of that, it was not giving us accurate results and there were a lot of things actually. It was not for network security, and we had to separately integrate the firewall..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“During the evaluation phase, I looked at other secure service edge solutions, including Netskope and Palo Alto Prisma Access. I ultimately chose Cloud Security Connector for Zscaler because of its strong integration with the Zscaler platform, cloud-native architecture, centralized policy management, scalability, and ease of deployment. It aligned better with my security and operational requirements..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

“Before using Cloud Security Connector for Zscaler, I had exposure to other cloud security solutions in enterprise environments, including Netskope and Cisco Umbrella. I moved to Cloud Security Connector for Zscaler because it offered better integration with the Zscaler platform, centralized policy management, easier scalability, and consistent security policy enforcement. It also simplified operations by providing a cloud-native approach, less infrastructure to manage, and better visibility into user traffic..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

ROI

Real user quotes about their ROI:

“From the security perspective, it has a layered approach for the connector. But with FortiGate, it's like simply connecting to the network, and it doesn't have that much security..”

Tejesh S

Technical Associate at IntimeSolutions

[Read full review](#) 

“I do not have much information about return on investment, but from a time saved perspective, previously when we wanted to access apps securely, we needed to connect to a VPN, which took around two minutes to connect. Now, with Cloud Security Connector for Zscaler, we do it in about thirty seconds, which shows significant time saved..”

Mohamed Raiyan

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

[Read full review](#) 

“We have definitely seen a return on investment with Cloud Security Connector for Zscaler, saving us money by at least 20 to 25%. In terms of time, we have saved at least 22 to 25% related to security and automation. The employees have become more productive and focused on the right direction..”

Jaspreet k

Head Of The Operations at Flash AI

[Read full review](#) 

“The return on investment from Cloud Security Connector for Zscaler is actually pretty nice because we have gained visibility over the employees and for the organizations as well. For example, if there is a team of ten members particularly for data analysis, we can get rid of three to four people out of them just because we got better visibility on one consolidated platform..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“Although I do not have the official return on investment figures, based on my experience, I estimate I have reduced the manual validation effort by around thirty-five to forty-five percent through automation. Regression testing is faster, and because configuration issues are identified before production, I have spent less time on post-deployment troubleshooting. Overall, this has improved team productivity, allowing the same team to handle more deployments without increasing headcount..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

“A return on investment has been observed, especially in terms of time savings, operational efficiency, and improved security visibility. For example, incident troubleshooting time reduced by 35 to 45 percent because Zscaler logs could be directly used instead of correlating multiple cloud and firewall logs. The need for managing additional firewall or proxy infrastructure in the cloud was also reduced, which helped lower operational overhead and reduce support burden on the team. From a security standpoint, around 25 to 30 percent improvement was seen in detecting and blocking suspicious outbound traffic, which reduced potential risk and manual investigation efforts. Overall, while it did not necessarily reduce headcount, it significantly improved team efficiency, allowing more workloads to be handled with the same team and enabling faster incident response..”

Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

Use Case

My main use case for Cloud Security Connector for Zscaler is to secure workload communication because we are operating in a hybrid multi-cloud environment. The connection is CSC, which connects our private resources seamlessly. Because it routes internal cross-cloud or cloud to data center traffic securely throughout Zscaler Private Access, it also hides our internal IP architecture from the public internet entirely. This ensures our backend resources are only reachable by authorized identities or authenticated workloads.

Yousef Almomani

Systems Engineer at a consultancy with 51-200 employees

[Read full review](#) 

“The main use case for Cloud Security Connector for Zscaler is monitoring the cloud traffic that we do, and we can connect cloud security applications with the AWS and GCP infrastructure so that we can get control over those infrastructures as well..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“Cloud Security Connector for Zscaler is mainly used to securely forward user and application traffic to the Zscaler clouds for inspection and policy enforcement. It enables organizations to apply consistent security policies, inspect internet-bound traffic, and protect users from threats regardless of where they are connecting from. It also provides visibility into network traffic, enforces compliance, and secures access to cloud applications and the internet.

In my role, Cloud Security Connector for Zscaler is mainly used to ensure traffic is securely redirected to the Zscaler cloud for inspection and policy enforcement. My focus is on validating that the connector works as expected after configuration changes or new releases. I create automated test scenarios to verify secure connectivity, policy enforcement, authentication, and traffic routing. This helps ensure that end users receive consistent security protection and that any issues are identified before deployment to production..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

“I am mostly using Cloud Security Connector for Zscaler as a VPN only. If I want to access any company-related web apps, I am using Cloud Security Connector for Zscaler for connection so that I do not want any third party to access my web apps. To explain how it works, consider that we are developing a web app which will hold financial-level information. On the organizational level, we do not want any of our competitor companies to access our web app even though they know the web app link. Because anyone can log into a particular web app using the username and password, which can be easily hacked, and they could be able to see our financial-related and recipe information because we are currently working for a CPG-related company. To restrict that, we are hosted in a very secure environment. To access our web app in that particular secure environment, we either need to connect to our office email or if I am accessing from home while working from home, I need some VPN to get connected. That is why instead of connecting to any third-party VPN, we have Cloud Security Connector for Zscaler, which enables us to connect. The main use case is to restrict any other third-party persons from accessing our recipe-level information or financial-level information. We are using Cloud Security Connector for Zscaler as a VPN so that we can be able to access the app securely..”

Dhanesan Sridhar

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“My main use case for Cloud Security Connector for Zscaler is to use it as a VPN. Instead of directly connecting to a separate VPN link, I connect to Cloud Security Connector for Zscaler, which acts as a VPN so that whenever I have a web app hosted in a firewall, I can access that particular web app via Cloud Security Connector for Zscaler only. I cannot access it using other networks.

“This setup has worked well for me because my company has a different environment called DNA. Whenever a web app or any other resources in Azure are hosted inside that DNA, I need to use or connect to Cloud Security Connector for Zscaler to access that particular resource. Cloud Security Connector for Zscaler acts as a VPN, so only users with a particular company ID can access that resource. No third party can access it. Even if I try to access the web app using my personal laptop or mobile phone, I cannot access it. I can only access those particular web apps and other resources like Key Vault inside Azure using Cloud Security Connector for Zscaler on my company's laptop only.

“I find Cloud Security Connector for Zscaler pretty useful for my main use case on a day-to-day basis because it really helps us as a security firewall. I do not want any other third-party companies or competitor companies to access my web app and see what I have developed. I need to keep it secure and do not want other companies to copy my web app or see the confidential information available in my web app. Cloud Security Connector for Zscaler is pretty useful while connecting..”

Mohamed Raiyan

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

[Read full review](#) 

“My main use case for Cloud Security Connector for Zscaler is that it provides security as a cloud connectivity security service that extends Zscaler Internet Access and Private Access to cloud-native workloads across AWS, Azure, and GCP. It is designed to secure workload-to-internet, workload-to-SaaS, and workload-to-private app communication without relying on traditional VPN, cloud firewall, or complex routing models.

“One specific example of how I use Cloud Security Connector for Zscaler in my environment is that it secures cloud workload traffic and gives zero-trust connectivity across AWS, Azure, GCP, and on-prem environments without depending on legacy VPN or firewall-heavy design. This is the main use case of Cloud Security Connector for Zscaler.

“The product has its own feature set, starting with extended ZIA and ZPA to cloud workloads, secure internet-bound traffic from workloads, enable app-to-app or app-to-private access connectivity using Zero Trust Exchange, and support AWS, Azure, and GCP deployment..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[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 for Cloud Security Connector for Zscaler is good because whoever is buying Zscaler purchases it from an ecosystem perspective, so I do not have any other choice in that regard..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“Security-wise, Cloud Security Connector for Zscaler is good. As I mentioned, I am mainly using Cloud Security Connector for Zscaler for security only. Governance-wise, it is also good and it is easy to set up. It is pretty easy..”

Dhanesan Sridhar

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“For the setup of Cloud Security Connector for Zscaler with GCP and AWS, what we usually do is we install the Cloud Connectors. We download the Cloud Connectors from the Zscaler portal, and then we usually go into our infrastructure machines, take their file into there and install it. Upon installing through SSO or maybe SAML request, we sign in there and we can apply our policies from there..”

Verified user

[Read full review](#) 

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

“My advice would be to spend time planning and deploying while understanding your organization's traffic flow and security requirements before implementation. Start with a pilot deployment, validate the policy thoroughly in a test environment, and gradually roll it out to production. It is also important to monitor logs regularly, keep the connector updated, and automate validation whenever possible. This helps identify issues early, reduce operational effort, and ensure smooth deployment. Overall, if it is implemented with proper planning and governance, Cloud Security Connector for Zscaler is a reliable, scalable solution for enterprise environments..”

Sini Maria Jose

[Read full review](#) 

Automation Engineer at Techmahindra

“The deployment of Cloud Security Connector for Zscaler in our environment is very straightforward with the option to pass configuration parameters via user data during initial setup. The connector integrates seamlessly with cloud-native services, in our case AWS, and it also works with load balancers, firewalls, and monitoring solutions, making the deployment straightforward and easy, with no challenges I remember in our organization.

The configuration process for Cloud Security Connector for Zscaler is excellent. We did not encounter any challenges, and it was very smooth. Even if it is complex, the team is always there to help, and customer service is excellent—always there to assist with deployment or configuration challenges..”

Jaspreet k

Head Of The Operations at Flash AI

[Read full review](#) 

“The primary factor regarding initial setup is deployment and routing complexity, especially in larger or multi-VPC environments where ensuring correct traffic flow and avoiding asymmetric routing can take considerable effort. Another aspect is policy tuning for cloud workloads. Since application servers may have specific dependencies, it requires careful fine-tuning of policies and SSL inspection to avoid impacting functionality during the initial rollout. Additionally, while the platform provides good visibility, having more cloud-native context and tighter integration with services such as AWS monitoring tools would further enhance troubleshooting and insights. These challenges are mainly around initial setup and optimization. Once implemented properly, the solution works effectively and delivers strong security and visibility..”

Vibin Thomas

[Read full review](#) 

Technical Team Lead - Content Security at Valuepoint Systems

Customer Service and Support

“The customer support for Cloud Security Connector for Zscaler is pretty good. Whenever I have issues and raise a concern, they resolve it within two or three hours..”

Mohamed Raiyan

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

[Read full review](#) 

“We reached out to customer support three weeks back due to an issue where Zscaler got stuck, and they identified and solved the problem within 45 minutes, which is exceptional. I give them a 10 out of 10 for customer support..”

Jaspreet k

Head Of The Operations at Flash AI

[Read full review](#) 

“We have not used much of the customer support because we have a lot of us here. We try to resolve any issues that come at our end first and majority of the time we do it. However, there was an incident where I had to reach out to the customer support for some turning blocking, and they were very amazing..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“We have used tech support to solve some kind of issues, network issues, or any product-level issues. We used to connect with the tech support of Zscaler.

Sometimes we used to get faster support. If it's an issue with the product level, then it will take some time. That's also fast only. The support is good from their end..”

Tejesh S

Technical Associate at IntimeSolutions

[Read full review](#) 

“The experience with Zscaler support has been generally positive. For most issues, especially those related to configuration or troubleshooting, timely responses and useful guidance were received. In more complex scenarios such as routing or policy tuning, support provided best practices and recommendations, which made the implementation smoother..”

Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

“Overall, I would rate Zscaler customer support eight out of ten. In my experience, the support team is knowledgeable and responsive, especially for standard issues. For more complex technical problems, they usually involve senior engineers or the appropriate product teams. Resolution time depends on the complexity of the issue, but they generally work with us until it is resolved. I believe they could improve by reducing the response time for high-priority cases and providing more proactive updates during long investigations.

The support engineers are technically knowledgeable and responsive, especially for standard issues. For more complex cases, they usually involve senior engineers or product teams to help resolve the issue. The reason I did not give it a perfect rating is that complex investigations can sometimes take longer than expected, and I would prefer faster resolution times and more proactive status updates during ongoing cases. Overall, the support experience has been positive..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

Other Advice

“My advice to others looking into using Cloud Security Connector for Zscaler is to definitely go with Cloud Security Connector for Zscaler. It is a good security connector. I would rate this product a 9 out of 10..”

Dhanesan Sridhar

Decision Scientist 3 at Mu Sigma Inc.

[Read full review](#) 

“Overall, I have had a positive experience with Cloud Security Connector for Zscaler. It is a reliable, scalable, and cloud-native solution that integrates well with the Zscaler platform. From my experience, it has helped improve my testing and validation process while ensuring secure traffic forwarding and consistent policy enforcement. Although there is room for improvement in areas such as troubleshooting and diagnostics, I believe it is a strong enterprise solution. I would definitely recommend it to organizations looking for a secure and scalable cloud security platform. I would rate this solution an eight out of ten..”

Sini Maria Jose

Automation Engineer at Techmahindra

[Read full review](#) 

“While I do not have a surprise, I think others should know that consistent security policy across cloud and user is one of the most top use cases along with multi-cloud and hybrid cloud flexibility.

“My advice to others looking into using Cloud Security Connector for Zscaler is that it is all about the Zscaler ecosystem. Whoever is using Zscaler knows Cloud Security Connector for Zscaler's importance, and they could use it from a centralized connectivity perspective. I have given this product a review rating of 10..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“The AI capabilities and governance that Cloud Security Connector for Zscaler offers are also amazing. We have been using the ZCC for monitoring the cloud responses, getting the prompt for the GPTs and Geminis, and blocking and downloading and uploading; everything is there. We usually do that on the main things that we block sensitive data which needs to be protected. Cloud Security Connector for Zscaler is able to do that, and it can help figure out what the solution is. They have almost every feature we would have a use case for in our day-to-day life.

“I would recommend others to have a look at Cloud Security Connector for Zscaler platform for sure because the amount of things we are selling for Zscaler itself is really, really reliable. I give this review a rating of seven..”

Verified user

Center Of Excellency For Sase And Ot And Io T Security at a outsourcing company with 51-200 employees

[Read full review](#) 

“I choose eight out of ten for Cloud Security Connector for Zscaler because it represents a tool that is highly successful and dominant in the specific category. However, it still has minor real-world operational friction points, keeping it from being absolutely flawless. In engineering terms, ten out of ten would mean a tool that introduces zero overhead, scales infinitely with zero configuration, and adapts perfectly to every single edge case out of the box. Cloud Security Connector for Zscaler does not quite hit that utopian standard, but it scores an eight out of ten, which is a very solid score on a clear balancing act.

“The best advice I would give to others who are considering using Cloud Security Connector for Zscaler is to view it as a fundamental architectural shift, rather than just a plug-in security tool, because it changes how you design cloud networking from the ground up. I assigned a rating of eight out of ten to this product..”

Yousef Almomani

Systems Engineer at a consultancy with 51-200 employees

[Read full review](#) 

“I rate Cloud Security Connector for Zscaler a nine out of ten. I reduce that one point because of the login feature only; otherwise, everything is good. From a security protection perspective, Cloud Security Connector for Zscaler plays a major role, so I am giving it a nine.

“I choose nine specifically because, as I mentioned, aside from the login feature, the rest is good. From a security perspective, Cloud Security Connector for Zscaler is very good.

“My advice for others looking into Cloud Security Connector for Zscaler is that it is the perfect cloud security system. If you have other options in mind, you should definitely give Cloud Security Connector for Zscaler a try because it is good. I have been using it for the past year. Even though I sometimes face downtime or other issues such as multiple login attempts, I still feel that from a security perspective, Cloud Security Connector for Zscaler is good, so proceed with it..”

Mohamed Raiyan

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

[Read full review](#) 

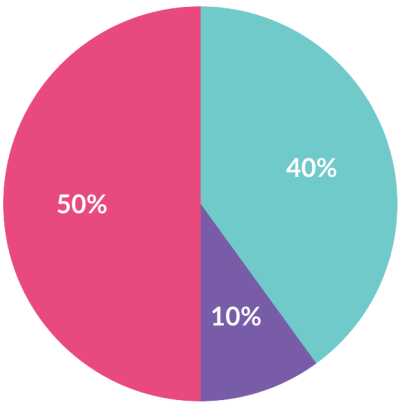
Top Industries

by visitors reading reviews

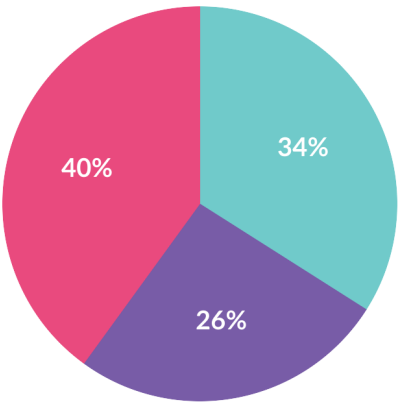


Company Size

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