aws marketplace

Cloud Security Connector for Zscaler

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Cloud Security Connector for Zscaler

Cloud Security Connector for Zscaler Recap

After launching the CSC Mux 4 or 8 from the AWS Marketplace using the CloudFormation template provided, the CSC Mux 4 or 8 will automatically select the best ZEN nodes, do the GRE tunnels and create the Location on your Zscaler console.Simple to install and not further management is required.All Zscaler ZIA functionalities are available, providing complete visibility of all Internet traffic.In addition to this, the CSC provides high availability changing the default route to Zscaler when configured as High Availability pair, and an easy way to manage direct bypasses to trusted sites using your public IP.When deployed as HA Pair, you can duplicate your Web Traffic to 8 or 16 Gbps to Zscaler (ZIA).

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

Team Lead, Technical Content Security at Valuepoint Systems

"Cloud Security Connector for Zscaler has positively impacted my organization significantly, as we have consistent, enforced policies on all cloud traffic, reduced risk of data leakage, easier audits, and from an operational standpoint we have saved time not having to manage individual workload agents, which is a win both in security and efficiency."

Ron Machan

Cloud Engineer at HCLTech

"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 Development at Flash.co

"The solution is secure."

Deepak Nagar

Manager, Strategic Alliances at Softcell Technologies Limited

"It is very useful .....visibility on the end-user,"

Tejesh S

Technical Associate at IntimeSolutions

What users had to say about valuable features:

"It is very beneficial in preventing the end-user system from being compromised. It can give visibility on the end user's internet access. If the user is accessing any malicious content, suspicious things, or phishing attacks, those things can be mitigated by using Zscaler. Those kinds of traffic will be blocked. That is one of the advantages.."

Tejesh S

Technical Associate at IntimeSolutions

Read full review

"Cloud Security Connector for Zscaler offers multiple features, but the major feature I love specifically is automated Zscaler node detection, which helps detect any kind of problem first. Additionally, it is available all the time, providing high availability routing for seamless failover, which is one of my favorite features. It also provides Layer 4 routed bypass for TCP, UDP, and ICMP traffic, enabling granular traffic control that streamlines our services working with Zscaler. It has provided complete visibility of internal IPs on the Zscaler console, allowing us to monitor and troubleshoot whenever there is a problem, making things transparent and easy for us to monitor. The integration with SIEM or syslog enhances centralized log management for our organization.."

Jaspreet k
Head of Development at Flash.co

Read full review

"The most valuable features of Cloud Security Connector for Zscaler include centralized visibility and control. It allows routing of all cloud workload traffic through Zscaler, which means full visibility into what applications and servers access externally. This is very critical in banking environments where audit and monitoring are mandatory. The second key feature is unified policy management. Instead of managing separate security controls for users and cloud workloads, the same Zscaler policies such as URL filtering, SSL inspection, and threat protection can be applied across both. This simplifies operations and ensures a consistent security posture. Another important aspect is the ease of integration with cloud security environments such as AWS and Azure, without needing traditional firewall appliances, which reduces complexity and improves scalability.

"These features make a significant impact on day-to-day operations, especially in terms of visibility, troubleshooting, and policy management. With centralized visibility, instead of checking multiple tools or cloud logs, all cloud workload traffic can be directly viewed in Zscaler logs. This makes troubleshooting much faster when users or applications report issues because it is possible to quickly identify whether traffic is being blocked, allowed, or flagged as suspicious. Unified policy management also simplifies operations since the same policies apply across users and cloud workloads. There is no need to maintain separate rule sets, which reduces configuration errors and makes policy changes much faster and more consistent across the environment. From an operational standpoint, it reduces the dependency on traditional firewalls or proxies in cloud environments, which means less infrastructure to manage, fewer points of failure, and easier scalability. Overall, Cloud Security Connector for Zscaler helps the team be more efficient by reducing troubleshooting time, simplifying policy management, and giving better control and visibility from a single platform.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"One of the best features Cloud Security Connector for Zscaler offers is its agentless design for cloud workloads. There is no need to install endpoint agents. It also automates routing and policy enforcement for all outbound traffic, so we get consistent zero-trust policies across our cloud infrastructure.

"The agentless design of Cloud Security Connector for Zscaler has been a game-changer. We do not have to install or maintain agents on every workload, which reduces operational overhead. It also made deployment faster since we just integrated at the VPC level, allowing us to focus on policy rather than per-machine management.

"Another feature of Cloud Security Connector for Zscaler is its centralized policy control being a major plus. Being able to push consistent security rules across all cloud environments from one place has made operations more efficient.

"Cloud Security Connector for Zscaler has been central to my organization's cloud security strategy overall. Instead of relying on traditional network boundaries, we now enforce security at every cloud workload's traffic flow. This shifted our strategy from perimeter-based to workload-centric, improving both security consistency and cloud agility.

"Cloud Security Connector for Zscaler has positively impacted my organization significantly. We have consistent, enforced policies on all cloud traffic. It has reduced risk of data leakage and made audits easier. From an operational standpoint, we have saved time not having to manage individual workload agents, which is a win both in security and efficiency.."

Ron Machan
Cloud Engineer at HCLTech

Read full review

Other Solutions Considered

"We also evaluated Forcepoint. We did a POC and demo of the solutions. We evaluated the products based on the use cases and their performance. Then, we chose Zscaler.."

Deepak Nagar
Manager, Strategic Alliances at Softcell Technologies Limited

Read full review

"Previously, we relied on a combination of cloud provider native security groups and manual firewall rules before choosing Cloud Security Connector for Zscaler. We switched because we needed unified, consistent policy enforcement across multi-cloud environments, which became hard to manage manually at scale.."

Ron Machan
Cloud Engineer at HCLTech

Read full review

"Before choosing Cloud Security Connector for Zscaler, we evaluated options such as native cloud provider security hubs, AWS Transit Gateway with firewall add-ons, and other third-party cloud firewalls. Cloud Security Connector for Zscaler stood out for its centralized policy enforcement and seamless multi-cloud support.."

Ron Machan
Cloud Engineer at HCLTech

Read full review

"We used to use FortiSASE from Fortinet. It follows the same zero-trust security access concept. It is also in the same picture. But if you compare it to Zscaler, Zscaler is better compared to FortiGate.

Zscaler is very secure, and it has more features, like application segmentation, where only trusted users can access limited resources within the private environment.."

Tejesh S
Technical Associate at IntimeSolutions

Read full review

"Before adopting Cloud Security Connector for Zscaler, the primary approach involved traditional cloud security methods, mainly NAT gateway combined with firewall-based controls for managing outbound traffic from cloud workloads. While this setup worked, it had limitations. Visibility on the outbound traffic was limited and policy enforcement was not centralized. Troubleshooting also required checking multiple tools such as cloud logs and firewall logs, which made operations more complex. Cloud Security Connector for Zscaler was adopted to achieve centralized visibility and consistent policy enforcement through Zscaler. This allowed the same security controls such as URL filtering, SSL inspection, and threat protection to be applied to both users and cloud workloads. The switch was primarily driven by the need for a zero-trust approach, better visibility, and reduced dependency on traditional firewall infrastructure in the cloud.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"We did not use a different solution, but we have evaluated some alternatives, including Fortinet SASE, Cisco Umbrella, Netskope Security Cloud, and Palo Alto Networks Prisma Access.

Before choosing Cloud Security Connector for Zscaler, we definitely evaluated other options and looked at several solutions. We chose Cloud Security Connector for Zscaler because it is a scalable solution. Increasing the number of seats or users did not show any signs of crashing or lagging.."

Jaspreet k
Head of Development at Flash.co

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

"The solution provides security. The users can access the application securely. The user experience is also good. The solution improves the latency and connectivity. When we connect through our legacy solution or VPN, we face delays. Zscaler is a fast solution.."

Deepak Nagar
Manager, Strategic Alliances at Softcell Technologies Limited

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 Development at Flash.co

Read full review

"We have seen a return on investment with Cloud Security Connector for Zscaler. We saved about twenty percent in time by reducing manual agent deployment tasks and fewer incidents tied to unsecured outbound traffic. We did not need additional staff for cloud traffic security, and audit prep became faster, which helped optimize overall cost.."

Ron Machan
Cloud Engineer at HCLTech

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
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Use Case

“This solution is for hybrid users who work from anywhere. It's like an end-user firewall. We can have restrictions on the end-user. If they come to the office, we have the infrastructure set up, and we can restrict access.

But if they are connecting to the office from a personal network, like when working from home, we don't have any visibility. That is where Zscaler will help us get control over the end user. Wherever they are, on any network, the organization policy will be pushed to the end-user..”

Tejesh S
Technical Associate at IntimeSolutions

Read full review

"Our main use case for Cloud Security Connector for Zscaler is securing outbound traffic from our cloud workloads. We deploy Cloud Connector in our VPCs to ensure that all workload traffic destined for the internet or SaaS apps is routed securely through Zscaler, ensuring policy enforcement and zero-trust protection.

"One specific example of how I use Cloud Security Connector for Zscaler in my environment is during a project when we migrated a set of microservices to AWS. We deployed Cloud Connector in each VPC. As these services needed to reach external APIs, Cloud Connector ensured all traffic was inspected by Zscaler, enforcing our security policies, preventing data exfiltration, and improving compliance.

"My main use case for Cloud Security Connector for Zscaler has been invaluable in hybrid environments. We use Cloud Connector to securely route traffic between on-prem workloads and cloud services, ensuring consistent security policies no matter where the workload sits. It simplified security across the board.."

Ron Machan
Cloud Engineer at HCLTech

Read full review

"In our current organization, we have been using Cloud Security Connector for Zscaler by Maiden Edge, Maidenhead Bridge for almost two and a half years. They are providing us specialized virtual appliances to simplify and secure connectivity between cloud environments. For our case, this involves AWS and Zscaler Internet Access, with a focus on zero trust and high availability, and it also helps with performance enhancement.

Our main use case for Cloud Security Connector for Zscaler is that we have been using it as a pre-configured virtual machine that we deploy on our AWS system with minimal networking requirements. This connector helps us automate Zscaler node detection and route selection, which reduces the manual configuration and operational burden for our organization's administrators. Management is quite straightforward through it being available with SSH and AWS System Manager. The appliance also includes built-in utilities for traffic monitoring and troubleshooting and log export to syslog. Our day-to-day use case is primarily that it helps us automate Zscaler node detection and route selection.

Automating node detection and route selection has helped us reduce the number of errors we were getting and made Zscaler more reliable and less dependent on Zscaler directly. Before using this solution with Zscaler, the Zscaler used to malfunction frequently, impacting our productivity. After implementing Cloud Security Connector for Zscaler along with Zscaler, we have seen positive effects, saving time as well as resources, which has left a very good impression on us.."

Jaspreet k
Head of Development at Flash.co

Read full review

"Cloud Security Connector for Zscaler securely routes traffic from cloud workloads, such as applications running in AWS or Azure, through the Zscaler cloud for inspection and policy enforcement. In a traditional setup, Zscaler is primarily used for user traffic, but with Cloud Security Connector for Zscaler, the same security controls extend to server-side or workload traffic inside the cloud environment. For example, if application servers in an AWS VPC require internet access, instead of allowing direct outbound access, that traffic routes through Cloud Security Connector for Zscaler into Zscaler. This ensures that all traffic is inspected for threats, URL filtering policies are applied, and data protection controls are enforced. Another important use case is for east-west and server-to-internet communication, where visibility and control over workload behavior is desired, especially for compliance in industries such as banking or finance. Cloud Security Connector for Zscaler also helps maintain a consistent security posture across users and workloads since both are governed by Zscaler policies. Overall, Cloud Security Connector for Zscaler enables a zero-trust approach for cloud workloads by eliminating direct internet exposure and ensuring all traffic is inspected through Zscaler.

"A specific example from a banking client involved application servers hosted in AWS that required outbound internet access for updates and API communication. Initially, these servers had direct internet access through the NAT gateway, which created a visibility and security gap since the traffic was not being inspected or controlled centrally. To address this, Cloud Security Connector for Zscaler was implemented in the AWS environment. Routing was configured so that all outbound traffic from the application subnet was redirected through Cloud Security Connector for Zscaler into the Zscaler cloud. Once integrated, Zscaler policies such as URL filtering, SSL inspection, and threat protection were applied to the workload traffic. This ensured that even server-to-internet communication was fully inspected, similar to user traffic. As a result, centralized visibility and control were achieved, the risk of malicious outbound connections was reduced, and the environment was aligned with compliance requirements such as PCI DSS. Additionally, the architecture was simplified by removing the need for additional proxy or firewall appliances in the cloud.

"Apart from outbound workload protection, Cloud Security Connector for Zscaler

adds value in controlling traffic in microservices architecture, where applications often communicate with external APIs or third-party services. Using Cloud Security Connector for Zscaler, this traffic is routed through Zscaler for inspection, which helps detect any malicious behavior or potential data exfiltration attempts. Another important use case is enforcing consistent security policies across both users and workloads. Instead of having separate security controls for endpoints and cloud servers, Cloud Security Connector for Zscaler allows unified policies to be applied through Zscaler, which improves visibility and simplifies management. Cloud Security Connector for Zscaler also plays a key role in compliance-driven environments, especially in banking and finance, where monitoring and logging all outbound traffic is mandatory for audit purposes. Overall, Cloud Security Connector for Zscaler extends zero-trust principles beyond users to cloud workloads, ensuring that no traffic is trusted by default and everything is verified and inspected..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

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.

"For others looking into using Cloud Security Connector for Zscaler, I recommend starting with a clear map of your cloud network and traffic flows. The smoother your architecture understanding, the easier the deployment. Additionally, engaging with Zscaler support early can help tailor policies to your exact environment.."

Ron Machan

Cloud Engineer at HCLTech

Read full review

"The deployment time depends on the environment and how many users are there. For example, for a hundred users, we can complete the deployment within two weeks.

It can integrate with multiple third-party solutions like Microsoft for authentication purposes, and Splunk, QRadar, and any antivirus solutions if they have them. It is feasible to integrate with third parties so that we can get access together to protect the end-users and the environment.."

Tejesh S

Technical Associate at IntimeSolutions

Read full review

"The tool is easy to deploy. We have to deploy the agent on the user's machine. The agent takes 20 minutes to be installed. The tool is deployed in the data center. If the prerequisites are set up already, the product can be deployed in two or three hours.

It is a cloud-based solution. We need two support engineers and one senior resource with more than seven years of experience in networking to deploy and maintain the tool. We need one product manager for coordination.."

Deepak Nagar

Read full review

Manager, Strategic Alliances at Softcell Technologies Limited

"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

Read full review

Head of Development at Flash.co

"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

Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Customer Service and Support

"We contact the support team two or three times a year if we need to change some configuration. The technical team is good. The team works on our requests according to the priority levels assigned. The team calls us quickly if we raise a P1 request.."

Deepak Nagar
Manager, Strategic Alliances at Softcell Technologies Limited

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 Development at Flash.co

Read full review

"Customer support for Cloud Security Connector for Zscaler was strong. They were responsive whenever we had deployment or policy questions, and they helped ensure best practices. Overall, we felt supported throughout.."

Ron Machan
Cloud Engineer at HCLTech

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
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Other Advice

"I would rate it a nine out of ten. It is recommended for hybrid users, where the work-from-anywhere concept is followed. It is very useful for them to get complete visibility on the end-user and to secure their environment by bridging from outside.."

Tejesh S
Technical Associate at IntimeSolutions

Read full review

"Once the sales activity and upgrades were complete, we requested some licenses and started utilizing them. I will recommend the solution to others. Organizations must remove the bottlenecks and latency issues before converting from the legacy VPN connectivity to Zscaler. Otherwise, we will face some connectivity issues. Overall, I rate the tool a nine out of ten.."

Deepak Nagar
Manager, Strategic Alliances at Softcell Technologies Limited

Read full review

"Organizations should plan the deployment carefully, especially around routing and network design. Understanding the traffic flow and dependencies upfront helps avoid issues later. It is important to start with a phased rollout and proper policy tuning rather than enabling stricter policies immediately. This ensures minimal impact on applications while maintaining security. This review has been given an overall rating of 8.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"Cloud Security Connector for Zscaler is a solid fit for organizations moving to a zero-trust model in the cloud. If you plan well, it can simplify and strengthen your cloud security posture. I give Cloud Security Connector for Zscaler a rating of eight because it delivers on its core promises: agentless deployment, strong security, and simplified operations. I did not rate it higher simply because there is room for even more seamless cloud-native integration and a few user experience refinements.."

Ron Machan
Cloud Engineer at HCLTech

Read full review

"One more thing I want to mention is the built-in tools for testing and troubleshooting, which include traffic logs, TCP dump, speed test, and MTR.

Everything else is good. The user interface is very attractive and does not require any change.

If you are looking into using Cloud Security Connector for Zscaler, I recommend it highly if you are committed to Zscaler and want a very simple automated GRE and IP routing from Azure, AWS, or GCP, without having to manage tunnels or custom NVA designs yourself.

Cloud Security Connector for Zscaler is a good solution that can help your Zscaler work better and secure your environment more effectively. It can also integrate with multiple cloud platforms like Azure, AWS, and GCP, making it a must-have solution for organizations based on my observation. I provide this review with an overall rating of 4 out of 5.."

Jaspreet k
Head of Development at Flash.co

Read full review

Top Industries

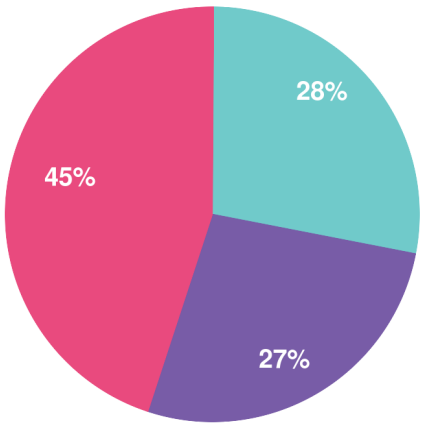
by visitors reading reviews

Construction Company	23%
Manufacturing Company	13%
Insurance Company	12%
Financial Services Firm	11%

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 software running on AWS and other platforms. 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