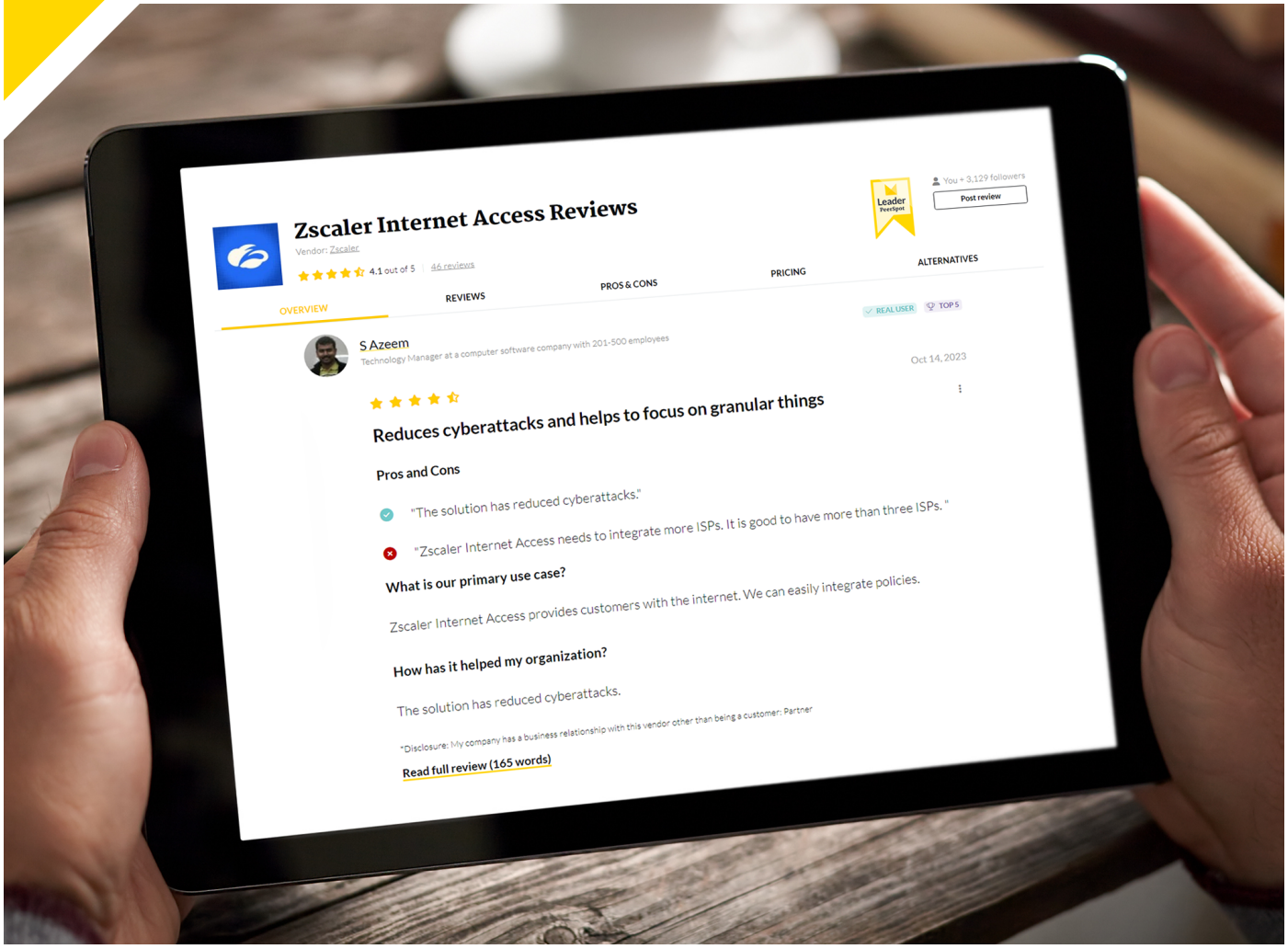
PeerPaper™ Report 2024

Based on Real User Experiences with Zscaler

The Layered Defense Capabilities of Zscaler: Real Users Speak



PeerSpot

Contents

Introduction

Despite significant investments in legacy security countermeasures like firewalls and virtual private networks (VPNs), today's organizations are finding that malicious actors can still make their way in and wreak havoc on systems and data. Firewalls have trouble inspecting encrypted traffic. A breached VPN provides a path into networks for attackers. Other legacy security controls operate out of band, meaning that traffic passes through them before it can be analyzed.

A layered defense strategy, based on a zero trust architecture and realized by Zscaler, offers a fundamentally different approach. At each stage of the attack chain—from "Reconnaissance" to "Initial Compromise" and "Lateral Movement" to "Data Exfiltration"—Zscaler reduces the attacker's ability to discover weak points in the attack surface, compromise systems, move laterally, and exfiltrate data. This paper, based on user experiences with Zscaler Zero Trust Exchange, Zscaler Internet Access, and Zscaler Private Access, discusses how this group of solutions delivers these results.

Overview of Legacy Security and Zero Trust

Legacy security solutions have had the unintended consequence of exposing a broad attack surface through public Internet Protocol (IP) addresses. For example, a cloud platform with a public IP becomes a magnet for attackers because it is visible to them. Figure 1 depicts this risk. VPNs serve as a bridge to the network, so if an attacker can breach a VPN, he or she can move around freely inside the network and perpetrate serious attacks. Zscaler deals with this risk by acting as a switchboard and connecting users directly to an application not to a network.

Firewalls, another mainstay of legacy security, typically cannot inspect enough encrypted SSL/TLS traffic, which accounts for 95% of traffic, because the process is extremely resource intensive. It would take 8X to 10X the computing power to inspect the SSL/TLS traffic, and there would still be performance degradation. As a result, many organizations do not fully inspect most of the traffic moving in and out of their firewall, which limits the security controls they can utilize and makes it easier for attackers to engage in malicious activities.

Security Architect
at a comms service provider
with 201-500 employees

"When you use a firewall, you have alerts and false positives, but Zscaler Internet Access pretty much decreases those errors and alerts."

Read review »

The zero trust model provides a solution. Zscaler, for example, places their Zero Trust Exchange in front of previously IP-exposed assets like VPNs, cloud platforms, branch offices, data centers, and applications. This approach renders these targets effectively invisible to attackers. It also prevents lateral movement and makes egress nearly impossible for attackers who might have found their way in.

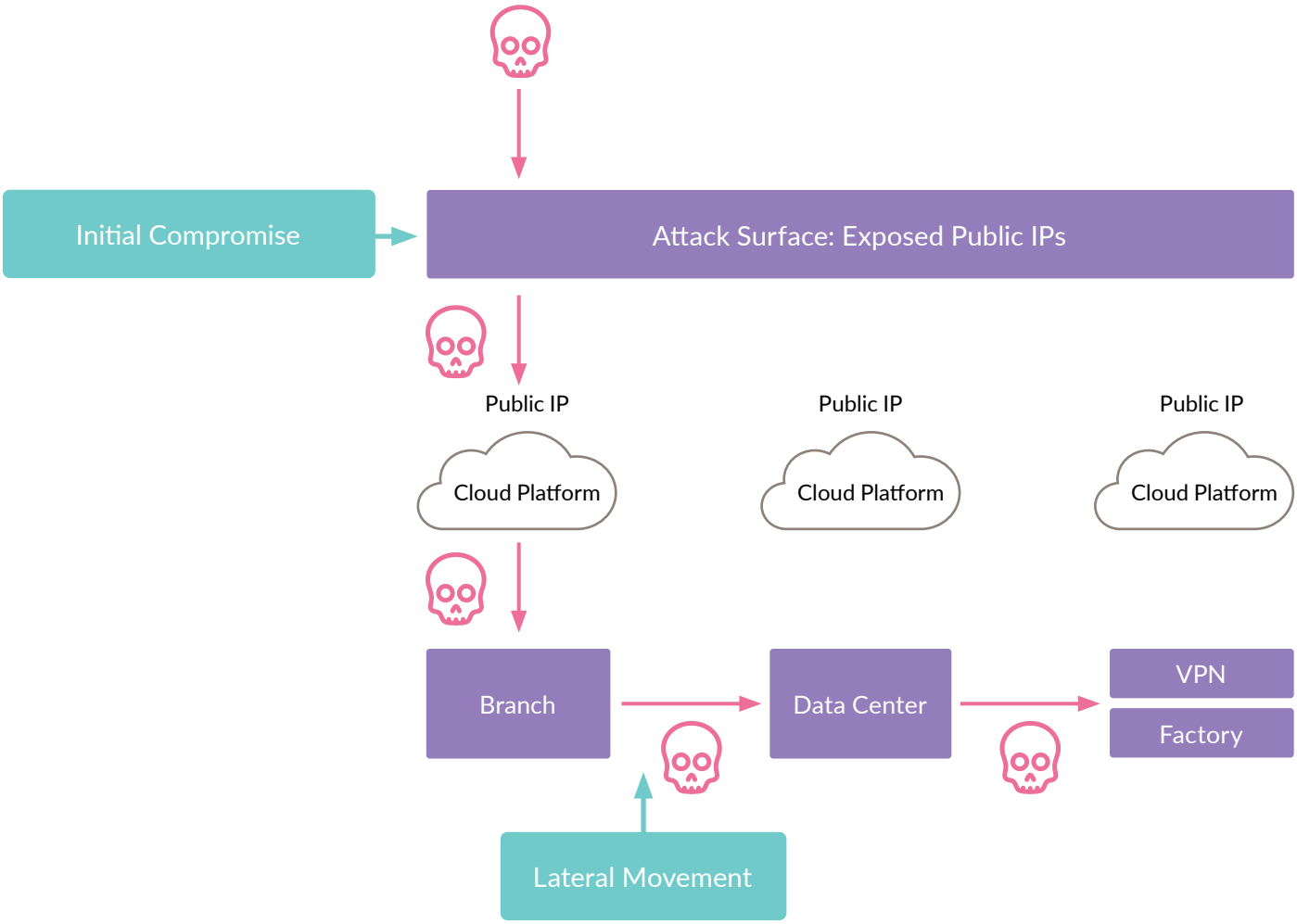


Figure 1 - Public IPs create an attack surface that can be exploited by attackers who can compromise the network and move laterally to data-rich targets.

The Zscaler Solution Compared to Alternatives

PeerSpot members who have embraced Zscaler for a layered defense explained why they selected the solution over alternatives. A Service Manager at a construction company with over 10,000 employees, for example, looked at Netskope, among other options. He found them similar in design, but preferred Zscaler because of its distinctive feature set. He shared, "Their scanning methodology is something like, 'Scan once, analyze many times.' That means there is a one-time scan of the traffic, but with multiple different threat engines, for antivirus and anti-malware, et cetera."

By performing this operation in cloud-hosted RAM memory, the process becomes "super-fast," in his terms. He added, "They can scan a lot of traffic in a very short amount of time. That part is something that a lot of other vendors are not doing. They're scanning in sequence, not in parallel." This capability represents a unique point of architectural differentiation for Zscaler. As a cloud-native platform running in 150 data centers globally, Zscaler analyzes traffic at the edge, close to the user. Zscaler's Single Scan Multi Action (SSMA) architecture also means that each packet gets scanned just once but is then analyzed by several different systems. Other solutions typically daisy chain their systems together. As a result, Zscaler is far faster.

Unmatched by Competitors

A Director at Aquila ICT Solutions, a Dutch system integrator, said Zscaler's services are "unmatched by competitors." He elaborated, saying, "Some may come with half the features that Zscaler can offer and be much cheaper. However, they do not have the global coverage that Zscaler has, and they will not provide the same low latencies and the same speeds that Zscaler can."

A tech services company with more than 500 employees had previously used Symantec. According to their Sr. Consultant, Cyber Security, "The main problem with Symantec was that they did not have a local data center here in UAE. That was one of the biggest requirements for our customers." Zscaler met this need.

Users also saw a range of security benefits from Zscaler. As the construction company's Service Manager put it, "Zscaler has helped to reduce the time we spend managing security policies." His organization relies on Zscaler Internet Access for its artificial intelligence-based "AI Instant Verdict". For example, his team can implement a sandboxing rule for how files of a certain type should be inspected. They can activate the AI decision making process to identify a PDF file's characteristics even if it's new to the sandboxing environment.

He went on, saying, "Based on that, the AI says that 'No, this file is not malicious,' even though it normally would have been quarantined and sandboxed and have gone through the whole analysis process. The AI helps out by minimizing the time to do that analysis. And that also helps in reducing the burden of someone actually having to do things manually."

Further comments about improvements in the security process included one from the construction company's Service Manager, who said, "Zscaler has helped us save costs by enabling us to decommission all of our legacy proxies. We had at least nine locations with appliances, and we had multiple appliances per location. It has helped us save money."

This user then said, "If you count everything that was involved in managing the appliances, the lifecycle management, and support contracts, in our old environment, we have reduced the number of FTEs [full-time employees] managing the environment from five or six to about two." On a related note, a Security Officer at a manufacturing company with more than 500 employees described how Zscaler made it possible for his team's engineer to spend time focusing on other business activities. He said, "The solution is saving 15 to 20 percent of our engineer's time, per day."

Service Manager
at a construction company
with 10,001+ employees

"Zscaler has helped us save costs by enabling us to decommission all of our legacy proxies."

Read review »

Zscaler's Layered Defense Across the Attack Chain

To mitigate the deficiencies of legacy security solutions, Zscaler provides a layered approach to defense based on zero trust. Each layer enables protective action across the various stages of the attack chain. At the reconnaissance stage, for example, Zscaler delivers secure access and reduces the attack surface. At the initial compromise stage of attack, Zscaler works to reduce threats and prevent compromise. Zscaler prevents lateral movement, while protecting data from exfiltration. Figure 2 shows this progression of attack and defense.

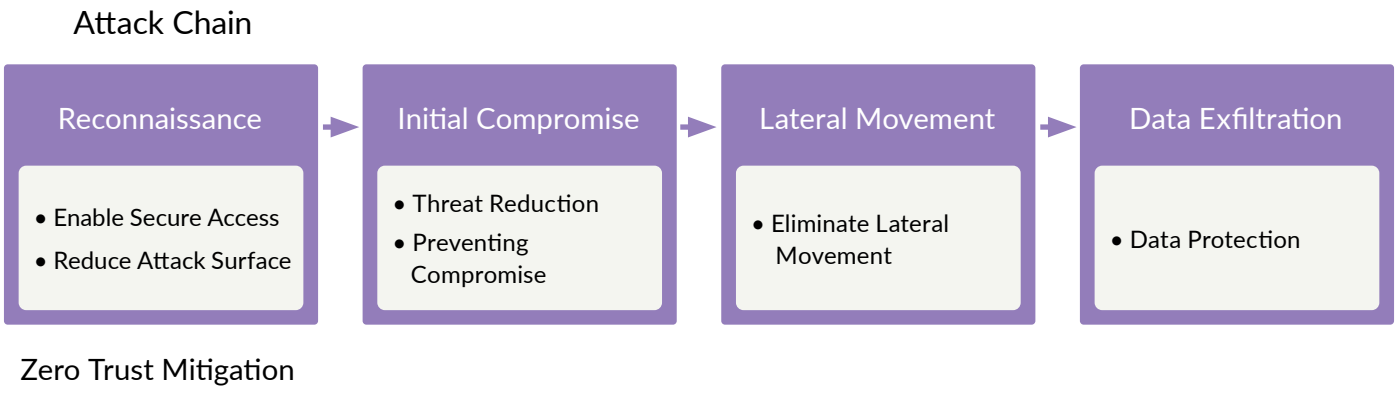


Figure 2 – Zscaler's layered defense zero trust architecture mitigates each stage of the attack chain.

Layered Defense

Blocking Reconnaissance With Secure Access and a Smaller Attack Surface

In the reconnaissance stage of an attack, malicious actors scan the Internet for vulnerable targets. The risk is that when applications are published on the internet, and discoverable, attackers can probe them for vulnerabilities. Once attackers have identified the IP address of a VPN, for example, they can then search for exploitable vulnerabilities that will help them initiate their attack. Zscaler offers countermeasures that block attempts at reconnaissance, e.g., secure access, wherein end users can access the Internet and applications without revealing their locations or IP addresses.

The Zscaler solution is to make applications invisible, as a Technical Consultant who uses ZPA at a tech vendor with 10,000 Employees explained. “We can protect the [VPN] application well. There’s no need to broadcast my network,” he said. “Only the application will be visible. Those kinds of things are very salient features.”

When it comes to reducing the attack surface, a key element of an anti-reconnaissance strategy, Zscaler Private Access makes it unnecessary for users to log into a VPN, among other countermeasures. A Senior Network Engineer who uses ZPA at Measat Broadcast Network System, a small manufacturing company, shared, "The most valuable feature of Zscaler Private Access is we do not have to connect to a VPN, it is seamless." This also resulted in convenience because they use just one agent to cover the internet and VPN access.

A Senior Technical Consultant at Meta Infotech Pvt. Ltd., an IT services provider, was pleased that Zscaler Private Access helped him replace what he called "flawed technologies" like VPNs and privileged access management (PAM) solutions. A Security Architect at a comms service provider with over 200 employees had a similar take, praising Zscaler "because they help me eliminate firewalls. I don't need to have firewalls, SIEMs, or an IPS/IDS."

Service Manager
at a construction company
with 10,001+ employees

"We have reduced the number of FTEs [full-time employees] managing the environment from five or six to about two."

Read review »

Phishing Protection

Preventing Initial Compromise and Reducing Threats

The next step in disrupting the attack chain involves preventing initial compromise. Achieving this goal takes several forms with Zscaler. For a Senior Consultant in cybersecurity, the solution provides phishing protection for web links. For the comms services provider's Security Architect, preventing compromise comes from the ability to inspect encrypted traffic and detect if threats are entering the network. As he said, "It intercepts incoming traffic and decrypts it, then reviews it."

This user felt he didn't need to use separate antivirus scanning or web filtering because Zscaler could now serve in that role. He added, "It protects me from man-in-the-middle attacks as well. When you use a firewall, you have alerts and false positives, but Zscaler Internet Access pretty much decreases those errors and alerts." Cloud browser isolation also stood out as a countermeasure for this user. He was pleased that Zscaler could deliver safe web browsing by creating a virtual air gap between users' devices and the web with fully isolated browser sessions.

Zscaler's secure web gateway (SWG) has an important role to play in preventing compromise, too. A Sr. Manager IT at a small non-profit put it like this: "When a user goes to the Internet to browse or download something, it is secured by this tool" that employs inline advanced threat protection that stops sophisticated attacks.

As the manufacturing company's Security Officer explained, "Zscaler has helped protect our employees wherever they are working, by delivering safe web access. We are doing the same things that we were always doing at our company, and in the same way, but now we are functioning safely outside of our premises. We were already able to work remotely using the Cisco agent, but the Zscaler agent is an improvement at the cybersecurity level."

"It allows the users quick access to the cloud, depending on where they are in the world," said an Architecture Senior Manager at an insurance company with over 10,000 employees. He added, "We have users all over the world who access cloud services in their native regions. Previously, we had to backhaul the traffic to our data centers somewhere in the world, then go back to that region. Now, we don't have to do that. A user and data stays within that region. There is no latency there."

Forrest W.
Sr. Manager IT at a non-profit with 51-200 employees

"It allows the users quick access to the cloud."

Read review »

Architecture Senior Manager
at a insurance company with
10,001+ employees

"It allows the users quick access to the cloud, depending on where they are in the world."

Read review »

A tech vendor with over 10,000 employees uses Zscaler Internet Access to block employees from accessing websites that are not connected by secure socket layer (SSL) to their Indian organization. Their Administrator said, "I use the solution primarily for security purposes. We are refusing authorization for users to access unauthorized sites. We are blocking through Zscaler. It's for web filtering."

For an Associate Consultant at HCL Technologies, a tech vendor with over 10,000 employees, the most valuable features in Zscaler Internet Access are the File Type Control and SSL bypass policies. He said, "We have multiple options, such as very flexible policies and modules in Zscaler. We will define them based on our requirements and the active Internet." He also uses the solution for geolocation challenges, saying, "For example, a user from Singapore moves to Dubai. When the user tries to access the Internet, Zscaler automatically detects the geolocation and drives our traffic to the other channel. There is no issue here."

The insurance company's Architecture Senior Manager had a similar insight into the product as an Internet proxy solution. He said, "We use it to manage our users' Internet access, making sure that they don't go to the wrong site." The construction company's Service Manager concurred, noting, "This architecture helps with cyber threats because we inspect most of the traffic and we can see that a lot of threats are stopped directly in the secure web gateway."

Zscaler's SSL/TLS inspection features further contributed to its ability to prevent compromise. The comms service provider's Security Architect remarked that if a threat were hiding, "you could do an inspection of your SSL traffic." He also pointed out that Zscaler Internet Access provides DNS security "that will help you route suspicious command-and-control attacks as well as detect threats when it does a full inspection."

Other notable comments about SSL/TLS inspection included:

- "[Zscaler] Internet Access enables the inspection of traffic, including SSLs. You want to make sure that nothing is coming in through your HTTPS traffic. For anything that is coming in that might be a threat, you want to ensure that you are using a good proxy for that." - Security Architect at a comms service provider with over 200 employees
- "The primary function for us is to do SSL inspection so that we can make use of the built-in anti-malware and antivirus—the advanced-threat features—within the platform. We do SSL inspection of some 80 percent of all the traffic and we can evaluate if it's malicious or not." - Service Manager at a construction company with over 10,000 employees
- "I like the granularity of the control of all the traffic, including SSL inspection." - Director at Aquila ICT Solutions

Carlos S.
Director at Aquila ICT Solutions

"I like the granularity of the control of all the traffic, including SSL inspection."

Read review »

Architecture Senior Manager
at a insurance company with
10,001+ employees

"The data loss prevention feature is the most valuable… It stops our users from inadvertently leaking our customers' data to the Internet or anywhere else it shouldn't go."

Read review »

Threat reduction is a further benefit of compromise prevention. After all, the fewer the threats, the lower the odds of compromise. A Sr. Manager IT at a small non-profit shared that Zscaler helped his team reduce the number of infected devices in the organization by "proactively preventing attacks" that they were at risk of experiencing because, as he said, "some users were unaware of some malware sites."

"It has also definitely helped reduce the number of infected devices in our organization by proactively preventing attacks," said the construction company's Service Manager. Elaborating, he added, "Since we scan almost all of the traffic, we now see how much of the traffic is 'malicious.' In our environment, we block about 1.6 million threats every quarter…. there are real threats that are being blocked, like botnet callbacks, cross-site scripting, and browser exploits. On average, per month, we are blocking about 500,000 threats per month." The comms service provider's Security Architect simply stated, "The fact that none of my end users are experiencing any threats, zero-day, bots, or malware says a lot about the solution."

Eliminating Lateral Movement

An attacker that can move laterally across a network can compromise multiple applications and databases. The potential for damage is extreme if this movement cannot be stopped. To mitigate risks at this stage of the attack chain, Zscaler Private Access offers a secure point-to-site or point-to-point connectivity to a dedicated service, which a Cloud Architect Azure at Thales, a tech vendor with over 10,000 employees, found helpful.

An SME-Support Manager of Architecture at Cognizant, a consultancy with over 10,000 employees, explained how it works: "Zscaler Private Access can help users sitting in our organization domain and trying to access their own internal company sources. The traffic is forwarded to us through the Zscaler Private Access node, which we can have in our own infrastructure, or it can be hosted on the Zscaler private cloud."

This approach restricts lateral movement by limiting the range of access allowed to the user. In this context, a Chief Digital Officer at a small consultancy shared that Zscaler Private Access "empowers organizations to grant access to internal applications and services while maintaining the utmost security for their networks."

Restricts Lateral Movement

Data Loss Prevention

Protecting Data to Prevent Exfiltration

The final disruption of the attack chain is about stopping the attacker from exfiltrating, or stealing, the target's data. Zscaler meets this requirement through a robust suite of data protection capabilities that rely on AI-powered data classification and full SSL/TLS inspection of outgoing traffic. "The data loss prevention feature is the most valuable," said the insurance company's Architecture Senior Manager. He added, "It stops our users from inadvertently leaking our customers' data to the Internet or anywhere else it shouldn't go."

Or, according to the comms service provider's Security Architect, "Zscaler Internet Access protects using data loss prevention." This user also pointed out that Zscaler offers data detection with exact data match, which, in his words, "improves the data coming into your cloud so you are protecting it." Exact data match enables customers to prevent data loss by identifying a record from a structured data source like a database that matches the customer's predefined criteria. For example, Zscaler's exact data match could identify credit card numbers and prevent them from leaving the database.

Conclusion

Zscaler succeeds in mitigating the risks of system compromise and data exfiltration by deploying a layered defense through a zero trust architecture. At each stage of the attack chain, Zscaler's solutions reduce the potential for attackers to engage in reconnaissance, achieve an initial compromise, move laterally, and exfiltrate data. The vendor's key capabilities reduce attack surface and prevent initial compromise with browser isolation and SSL/TLS filtering. Zscaler also prevents lateral movement with point-to-point connectivity while preventing data loss. This layered defense works, enabling Zscaler users to move past the deficiencies of legacy security solutions and establish a more robust overall security posture.

About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.