MOOR INSIGHTS & STRATEGY

ZSCALER

A HOLISTIC ZERO TRUST PLATFORM

EXECUTIVE SUMMARY

Often misused in the cybersecurity industry, the term “zero trust” has been applied to products and solutions that do not provide the complete security the term suggests, creating market confusion and threatening to delay the adoption of zero trust in customer environments. While many companies claim to offer zero trust security, few deliver a holistic, end-to-end solution that extends beyond mere access controls.

How do enterprises evaluate numerous cybersecurity offerings to identify a solution that delivers a complete zero trust architecture? Is there a platform that can reduce the cost of integrating multiple point solutions while providing higher value and protection? This paper clarifies what true zero trust security should offer and evaluates the Zero Trust Exchange (ZTE) platform from Zscaler.

Let’s first examine what zero trust security means. A true zero trust platform must incorporate three levels of security:

- Never inherently trust any entity.
- Establish trust based on identity and policy, using contextual data derived from users, devices, applications, and content.
- Inspect all traffic, including Secure Socket Layer (SSL) and Transport Layer Security (TLS).

Traditional firewall and virtual private network (VPN) approaches authenticate users before granting access to the corporate network. However, users can move about unfettered once on the network, accessing resources and applications without additional authorization or verification. A genuine zero trust approach never places users on the network; instead, it directly connects users to specific resources and applications through a secure exchange providing the strictest level of protection.

A zero trust architecture also makes applications undiscoverable from the public internet, reducing the attack surface and making these applications invisible to potential attackers. For deep content inspection, it also terminates connections using a proxy architecture, not a passthrough firewall. An enterprise cannot implement a complete zero trust security posture with only firewalls and VPNs.

Enterprises demand a cloud-native security platform that is easy to deploy and manage but, most importantly, complete. For the latter, a zero trust platform must implement four key steps:

1. Terminate connections directly using a proxy-based architecture, not a passthrough firewall. This topology allows full inspection of the traffic exchanged, including all encrypted traffic, for a complete analysis of the content to identify potential threats. This also prevents data loss, blocks threats by holding data, and restricts the exchange of that data until it is validated against a defined policy.
2. Prevent unauthorized access by verifying policy through identity and the context of the connection. Contextual vectors should include user, device, application, and content.
3. Connect the user to the application, never the network, only after establishing proper verification based on defined business policies. This neutralizes lateral network movement that could compromise valued data and resources.
4. Hide applications and ensure they remain invisible to threat actors on the internet. Applications protected behind an intelligent switchboard or exchange are not visible and cannot be discovered, thus eliminating the attack surface.

Based on these criteria, Moor Insights & Strategy believes Zscaler delivers a complete zero trust solution built on a proxy-based architecture, policy verification that mitigates unauthorized access, lateral movement prevention, and managed threat-hunting capabilities. In addition to providing complete security, the ZTE platform improves the user experience by integrating advanced services such as digital experience monitoring, for unified, granular visibility into user, connection, and cloud app telemetry data.

THE SUPERPOWERS OF A PROXY-BASED ARCHITECTURE

A proxy-based architecture, like Zscaler's ZTE, serves as a safeguarding intermediary, facilitating the complete decryption and analysis of all traffic flows. In contrast, passthrough architectures employ firewalls and hold traffic for a verdict before delivery to a destination. By deploying this proxy architecture, Zscaler's ZTE and its two discrete services, Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA), can provide robust threat and data loss prevention.

ZPA is a cloud service that provides seamless, zero trust access to private applications running in public clouds, data centers, or the network edge. ZIA is a secure internet and web gateway delivered from the cloud and as a service, providing a comprehensive suite of security capabilities that spans all core enterprise security needs, including firewall, sandboxing, filtering, and browser isolation. ZIA's deep capabilities extend beyond the more classic proxy definition, such as a secure web gateway, which filters unwanted malware from user-initiated internet traffic and enforces a predefined policy.

Moor Insights & Strategy believes that Zscaler's proxy-based architecture enables the company to deliver a highly secure set of services that are easy to acquire and manage from a software-as-a-service (SaaS) perspective, while providing scale-out for future needs.

POLICY VERIFICATION THAT MITIGATES UNAUTHORIZED ACCESS

While the internet has caused digital enterprises to revolutionize business transactions and customer service, it has also enabled bad actors to launch sophisticated attacks that range from simple denial of service and phishing to ransomware. As a result, VPN solutions are highly vulnerable to compromise. The pandemic exposed the shortcomings of VPN as millions of knowledge workers transitioned to a work-from-home routine, and many will continue to do the same in the future. Moving forward, organizations of all sizes will require highly secure connectivity to support hybrid work that spans campus, branch, and the emerging micro-branch home office.

Moor Insights & Strategy believes that Zscaler can address these organizational needs based on its policy verification engine that employs its Zero Trust Network Access capabilities and removes the inherent risks associated with VPNs.

The Zscaler ZTE platform also aims to deliver direct, secure access to specific applications, based on access policies, rather than providing access to the corporate network – preventing the risk of lateral threat movement. The platform embraces the least privileged access for both the users who need access to business applications and application to application traffic through micro-segmentation. Some examples include:

- TT Electronics is a global provider of engineered electronics. The company struggled to restrict users to specific applications and gain visibility into public access as well as monitor resource utilization both internally and externally. ZPA now provides critical insights that enable tighter, granular control. This capability allows TT Electronics to configure tailored policies based on user geography and office and home environments.

- Takeda is a pharmaceutical company with over 70,000 employees in more than one hundred countries. Before deploying Zscaler, the company applied a single policy globally. Now, policy-based administrative controls deliver agility and a consistent user experience both on-premises and remotely.

- Sandvik Group is a global industrial engineering firm that manufactures tools, mining and construction equipment, and alloy materials. The company was struggling with a VPN solution that was not providing the support needed for remote productivity during the pandemic. To address the issue, the company deployed both ZPA and ZIA in less than a week. The result for Sandvik Group is an overall improvement in user application experience, network segmentation through policy-based tools that speed performance, and improved visibility and protection of applications.

Moor Insights & Strategy believes that Zscaler's ZTE platform provides a unique and compelling method to address dynamic policy verification that mitigates unauthorized access by bad actors.

Lateral Movement Prevention

Enterprises must rethink their approach to securing connectivity. The porous nature of corporate networks, combined with the proliferation of Internet of Things (IoT) sensors, bring your own device (BYOD), and other connected devices make corporate networks extremely vulnerable to attacks that can spread quickly. The Zscaler Zero Attack Surface mitigates lateral movement by hiding source identities and making applications invisible. By placing applications behind the Zscaler ZTE platform, enterprises are able to prevent inbound connections, thereby thwarting internet-based attacks. Additionally, this topology eliminates the possibility of a compromised VPN user inadvertently admitting an attacker to an internal network.

More importantly, Zscaler ZPA connects the correct user directly to authorized applications - not the network. This capability prevents users from pivoting from approved applications to other places on the network since users are never connected directly to the network. This approach is fundamentally different from legacy network security approaches requiring users to access the network to connect to an authorized application.

Moor Insights & Strategy believes that the Zscaler Zero Attack Surface capability is a potential game-changer relative to other cybersecurity platforms. If bad actors cannot discover internal applications or gain network access, they cannot find valuable applications and data to steal or encrypt for ransom.

Deception and Managed Detection and Response

Many, if not most, cybersecurity platforms are reactive. Today's enterprises require a proactive method to safeguard users, applications, and valuable company resources. To meet this need, Zscaler acquired Smokescreen Technologies in late May 2021 to enhance its ZTE platform through service integration. Smokescreen uses deception technology to provide tools that identify emerging adversary techniques, compromised users, and lateral movement attempts.

According to the company, the resulting detection and response capability is an industry first and, combined with the managed threat-hunting service, will deliver high fidelity signals of malicious activity. Additionally, Zscaler offers a complimentary white-glove managed detection and response service, which extends a customer's security team to help identify the highest priority threat activity in each environment, contextualize intelligence for quick containment action, and provide guidance for ongoing response and best practices to improve security posture continuously.

Moor Insights & Strategy believes that the additional capabilities of deception and managed detection and response extend Zscaler's strength in delivering an end-to-end zero trust architecture that is proactive versus reactive. It is a compelling feature that has the potential to mitigate ransomware and other lateral movement attacks.

Call to Action:

Zero trust has become a misused term in the cybersecurity industry, and enterprises need guidance in choosing a complete solution. Many platforms begin with the wrong architecture – inherently not zero trust – but use the popular terminology. Firewalls and VPNs fall short. Enterprises need solutions that deliver a complete zero trust architecture. Moor Insights & Strategy believes that Zscaler provides true zero trust security by:

- Eliminating the use of firewalls and VPNs with a proxy-based architecture.
- Verifying policy to mitigate unauthorized access.
- Connecting users to applications, versus a network, and,
- Hunting for threats proactively.

Zero trust is more than user access. True zero trust security maps users to application access, application to application access, and server to server access. This approach ensures that a zero trust platform can scale to meet future needs and offer additional capabilities.

Moor Insights & Strategy believes that Zscaler has effectively incorporated this design philosophy into its ZTE platform that has matured over the last fifteen years. The proof is in performance, and Zscaler now claims to be the largest cloud security vendor, processing over 180 billion transactions and blocking an astounding 150 million threats daily.

Important Information About This Paper

Contributor

Will Townsend, Vice President and Principal Analyst, Enterprise Networking, Carrier Services and Security Practices at Moor Insights & Strategy

Publisher

Patrick Moorhead, CEO, Founder and Chief Analyst at Moor Insights & Strategy

Inquiries

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

Citations

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

Licensing

Disclosures

This paper was commissioned by Zscaler. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.