ZSCALER — EMPOWERING DEFENDERS WITH ZERO TRUST AND AI

EXECUTIVE SUMMARY

Zero trust is unquestionably improving security postures and thwarting cyberattacks. Its foundational principle of least privilege access reduces attack surfaces and mitigates the risk of lateral movement. A growing number of governmental mandates and frameworks, such as those from NIST, are using zero trust deployment guidance to help companies of all sizes counter the onslaught of attacks. However, combatting increasingly sophisticated attacks like the Morris II worm, which accelerates the theft of sensitive data and enables significantly higher volumes of spam email distribution leading to massive malware propagation, requires more.

New applications of AI are starting to help defenders harden security through faster security analyst onboarding, the evaluation of large volumes of threat intelligence, situation report generation, and more. Various kinds of copilot applications aid security operations through generative AI.

Cyber protection is becoming increasingly complex with the use of these applications and the potential for data leakage. Further compounding matters is an ever-expanding threat surface brought about by hybrid infrastructure and operational technology network deployments. Consequently, securing the use of AI in the carpeted and uncarpeted areas of enterprises for productivity gains must be matched by using AI to deliver improved organizational security. If applied correctly, a reinvigorated approach to AIOps can play a pivotal role in securing multidomain environments and counteract the weaponization of AI by bad actors.

Given these challenges, how do organizations deploy zero trust and AI together to drive better security outcomes? A complete solution must consider protection of the data used in AI tools, the tools themselves, and the underlying algorithmic models. It must also drive improved security outcomes from prevailing security infrastructure vendors that broadly safeguard organizations.

AI is poised to supercharge zero trust architectures. Enterprises demand a complete security platform bringing AI and zero trust together that is easy to deploy and manage. Moor Insights & Strategy (MI&S) believes that Zscaler is well positioned to deliver a zero trust platform infused with AI that is predictive, broad and deep and complements the management and security of burgeoning GenAI applications.

FIGHTING AI WITH AI AND THE POWER OF ZERO TRUST

Any technology can be used for both harm and good, and AI is no exception. It is increasingly being leveraged to improve the sophistication of cyberattacks. AI's ability to learn, adapt, and automate a staggering number of processes allows it to do many things for bad actors. These include:

- Accelerated attack surface discovery
- Dramatically improved malware payload delivery through grammatically correct phishing attacks designed to steal credentials
- Faster mean time to lateral network movement
- Greater likelihood of data exfiltration given the large amount of data used for training and inference of AI models

AI and machine learning have been used for a while to improve IT and OT network operations. Today, AI is rapidly becoming platformed thanks to the introduction of GPU computing hardware, curated large language models, and new applications. The emergence of AI as a platform and the maturation of zero trust are separate but complementary technology trends.

Defenders can use AI securely to supercharge zero trust deployments to shrink and mask attack surfaces, enforce least privilege access, and create micro-perimeters that eliminate lateral movement and prevent data loss. This is a powerful combination—one that can mitigate security risk, prevent compromise, and limit the resulting blast radius damage.

With organizations facing daunting security challenges, including a shortage of fully trained cybersecurity professionals and the weaponization of AI, AI and zero trust together have great potential. The combination can tip the scale to defenders in fighting AI with AI—and can do so at a massive scale.

SECURING AI AT SCALE

Securing AI at scale involves both the secure use of AI and the application of AI to secure the enterprise. It is incumbent for defenders to secure the use of AI through the protection of large language models, applications, and data. The ramifications for not doing so are great and include the risk of exposing sensitive data through leakage and IP theft. The latter can immeasurably damage organizations from reputational and compliance perspectives, leading to customer, revenue, and profitability loss, as well as, ultimately, greater operational expense pressure. On the other hand, the application of AI to secure the enterprise delivers significant benefits, including improvements in threat visibility, phishing detection, segmentation, granular data discovery and control, and root cause analysis.

Several best practices can be employed to ensure the security of AI at scale. These include using secure web gateways and GenAI data protection to manage sanctioned AI applications and users, the application of risk assessment techniques when onboarding new AI applications, and prompt and response security management. Activation of data loss prevention across an organization's entire suite of AI applications and workloads can also mitigate—and ideally prevent—data exfiltration. Also, browser isolation can effectively combat ever-present poor security hygiene among users.

WHY ZSCALER?

Zscaler is a proven leader in delivering a holistic zero trust security platform, as evidenced by its operation of the largest zero trust security cloud. The company's platform depth includes a massive correlated data set that integrates a high volume of threat signals. This allows Zscaler to analyze a staggering 500-plus trillion signals and process 500-plus billion daily transactions while protecting over 50 million users. Through the training of large language models with complete logs and full URL and anonymized data, Zscaler can effectively combine AI and zero trust principles to offer potentially unmatched protection.

Zscaler also effectively utilizes this telemetry to offer organizations a mature security fabric that is fortified with new capabilities from its recent acquisition of Avalor. Zscaler's Data Fabric for Security reduces the complexity in analyzing the volume of data generated by modern security tools. It is designed to unify, normalize, and contextualize data from Zscaler and more than 150 third parties.

One of the challenges with existing data lakes is the volume of unstructured data, which makes it difficult to derive actionable insights and make informed security decisions for posture control. To address these challenges, Zscaler's Data Fabric for Security offers a robust data ingestion engine that can correlate insights, facilitate analysis, and make needed recommendations. This provides a consolidated view of risk, providing real-time visibility, fast remediation, and an enhanced ability to maintain compliance and data privacy, all at scale. Pristine security outcomes can only be achieved with pristine data, and Zscaler's Data Fabric for Security has the potential to deliver what is needed today.

MI&S believes that Zscaler is well positioned to deliver what organizations seek in securing AI at scale given its complete, battle-tested, and end-to-end zero trust architecture combined with its recent introduction of AI-powered tools.

AI — A Second Line of Defense

Cybersecurity is an evergreen endeavor requiring constant scrutiny and attention. Organizations continue to face an evolving threat landscape, and research efforts are instrumental in ensuring the most up-to-date security posture. Zscaler's ThreatLabz global research arm goes far in this regard. Its mission is to continually hunt for new cyber threats, conduct ongoing threat research, and perform behavioral analysis that feeds the company's future solution offerings.

A standout example of this is Zscaler's Breach Predictor. The company claims that it represents the first preemptive detection and response solution that identifies attacks in progress and anticipates potential ones utilizing advanced AI and ML techniques and Zscaler's vast telemetry. Breach Predictor's ability to prevent compromise is a possible game changer for security operations professionals, with the potential to dramatically simplify cyber defense.

ThreatLabz can point to some compelling statistical achievements. It provides outstanding visibility, as evidenced by a 600% increase in AI and ML transactions in the past year alone, with a significant number of anomalies successfully blocked, reducing noise and easing SOC operations. This surgical approach is significantly more efficient relative to other security solutions that either block or allow the totality of signals. Furthermore, ThreatLabz's annual security reports inform the broader cybersecurity industry on the company's most recent findings and suggestions for improving security posture.

Zscaler also effectively leverages AI and ML throughout its solution portfolio to fine-tune security efficacy and simplify operational deployment and management. Some examples include:

- **Enhanced data protection** in the form of AI-powered classification schemes that automatically categorize sensitive data and mitigate leakage and loss
- **Network segmentation** that leverages AI to automate processes and easily create zero trust access policies, bypassing traditional complexity
- **Smart isolation techniques** that use AI to identify and segment potentially malicious web content, complementing broader URL filtering that reduces risks from sanctioned sites

CALL TO ACTION

Bad actors are leveraging AI to improve the sophistication of attacks, making cyber defense a complex and ever-evolving challenge. However, the combination of zero trust and AI holds great promise for tipping the scales to defenders. Zero trust can reduce attack surfaces and mitigate the risk of lateral movement, and AI can supercharge these efforts through improvements in threat visibility, phishing detection, segmentation, granular data discovery and control, and root cause analysis.

MI&S believes that Zscaler is especially well positioned to deliver what organizations require in a modern security platform. The company’s leadership and solution depth in zero trust is anchored by the cybersecurity industry’s largest security cloud, a mature security data fabric, and practical research efforts through ThreatLabz. These are powerful capabilities that demonstrate what can be achieved in marrying zero trust and AI to combat a landscape of escalating threats.

Important Information About This Paper

Contributor

Will Townsend, Vice President & Principal Analyst, Networking & 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

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

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.