Enterprise Strategy Group™

BRIEF

JUNE 2025

Zscaler Showcases Innovation With Contextual Analysis and AI-driven Remediation at Zenith Live

Tyler Shields, Principal Analyst

Abstract: Organizations require comprehensive contextual prioritization and automated remediation of security vulnerabilities to scale their limited human cybersecurity resources effectively. At the Zscaler event, Zenith Live, the company showcased this vision, illustrating a platform that employs large-scale data collection, contextual AI data analysis, and intelligent automated security control implementation to mitigate risk and advance toward a self-healing system.

Key Highlights

- 47% of organizations believed that current tools aren't effective at detecting and investigating advanced threats.[1]
- Zscaler extends plans for modernization of security platform on the back of cybersecurity data fabric and agentic AI capabilities.
- By providing automated remediation and AI driven prioritization innovative platforms are pushing important new capabilities forward.

The Convergence of Threat and Exposure Management and Network Enforcement Capabilities

Cybersecurity programs have a clearly defined mission to reduce risk and limit threat exposure at a cost proportionate to the organization's risk tolerance. Traditional risk reduction methods concentrate on identifying vulnerabilities in large volumes and tracking remediation efforts to ensure the timely resolution of these security issues.

Until recently, cybersecurity teams had limited capability to scale their human-centric cybersecurity resources to meet the ever-increasing number of cyber assets needing security analysis. Software development is growing exponentially, and the infrastructure supporting modern software systems is expanding to match the services being provided. Endpoints and APIs are increasing rapidly, and vulnerabilities and exposures in the enterprise environment have reached an unsustainable level, necessitating a new approach to the challenge.

[1] Source: Enterprise Strategy Group Research Report, *The Future of SecOps in an AI-driven World*, April 2025. All Enterprise Strategy Group research references in this brief have been taken from this research report.

In the programmatic era we now operate in, the focus must shift to supporting automated risk discovery, contextual and holistic prioritization of issues, and programmatic remediation of exposures. This new approach is made possible by the rise of API-accessible technology stacks, cloud-based infrastructure, large-scale data analysis capabilities, and, most recently, agentic AI. The automated discovery of cyber assets and event states, a cybersecurity data fabric that stores and normalizes asset, exposure, and threat data, along with an AI-based prioritization engine and remediation capability, represent the next iteration of enterprise security platforms.

Market Insight

39% of security teams of current tools aren't integrated well—making threat detection and response more cumbersome than it should be.

Zscaler Launches Zero Trust, Data Security, and Agentic Initiatives

In the opening keynote of the Zenith 2025 event, Zscaler CEO Jay Chaudry positioned AI as a transformative wave comparable to the Industrial Revolution. Driving home this vision, he outlined three specific areas of innovation where Zscaler is actively creating new capabilities using AI: Zero Trust Everywhere, Data Security Everywhere, and Agentic Operations.

Zero Trust Everywhere: Zscaler is transcending its previous role as a network security company, evolving to safeguard all components of the technology stack, including endpoints, users, workloads, AI agents, large language models, and more. They are applying zero-trust principles at every layer of the communications stack as they adopt a comprehensive platform approach.

Data Security Everywhere: Zscaler is enhancing its data security capabilities by leveraging AI analysis to create a data protection solution that spans all environments. The same data loss prevention policies can be applied consistently across locations, whether in-line, on endpoints, in the cloud, or within AI applications, while utilizing AI features for rapid data classification and policy enforcement.

Agentic Operations: Zscaler acquired two companies, Avalor and Red Canary, to establish a security data foundation for processing both first-party and third-party security contexts. The Avalor solution integrates a platform approach with foundational cyber data collection and an AI-driven analysis framework, serving as an alternative to basic data lake capabilities. The cybersecurity data fabric enables Zscaler to take a more proactive stance, mitigating risks before attacks occur. The Red Canary acquisition was not discussed in detail during the Zenith presentations because it had not yet been finalized. However, it's believed that the managed detection and response vendor was acquired to fit directly into the automation and feedback loops essential for building agentic security capabilities, and to provide Zscaler with a better connection to customer security operations teams.

Analyst Insight

The key announcements at the Zenith event highlight Zscaler's future aspirations as it moves beyond its historical roots in network security. Zscaler is evolving past traditional network security controls while maintaining its historical lineage and DNA. The Data Security Everywhere initiative brings innovative AI capabilities to the forefront of the business, enabling the analysis of data both at rest and in transit as they transition their key offerings further up the stack. Later this year, Zscaler also plans to leverage its network security capabilities to enhance private access between organizations as it launches extended private access features. The connectivity between companies lays the foundation for agentic security technologies to facilitate inter-business communications, enabling a seamless flow of data between partners, vendors, and customers over time. This will be welcome news to Zscaler customers as they look to redesign their network connectivity capabilities.

> "Contextual prioritization and automated remediation are what the customer needs. Threat and exposure management vendors must lock in on these innovative features."
>
> **- Tyler Shields,** *Principal Analyst, Enterprise Strategy Group*

Moving beyond network innovations, emphasizing a data-driven contextual analysis approach that extends well beyond basic network traffic foundations is essential for pushing the boundaries of analysis and enabling richer insights. As they enhance the Avalor data security fabric capabilities with threat and exposure management, threat hunting, and security operations use cases, the new Zscaler platform will contextualize vulnerability data for more accurate risk prioritization. The ability to prioritize fixes not only on Common Vulnerability Scoring System, Common Vulnerabilities and Exposures, or Known Exploited Vulnerabilities scores, but also with a comprehensive understanding of the customer's environment, enabling Zscaler to devise innovative mitigation strategies, such as integrating infrastructure security controls as semi-permanent risk reductions until root cause issues can be resolved. Additionally, the acquisition of Red Canary, when completed, fills a natural gap around managed detection and response capabilities. Buyers of the Zscaler technology stack focus on outcomes that reduce risk and automate fixes. A top-tier managed detection and response (MDR) vendor provides human and technology-augmented scale to the platform. Zscaler plans to connect the MDR offering with increased agent-based AI and automation capabilities to drive value up and reduce the cost of goods sold, directly increasing their margins and bringing added value to their customers.

With these initiatives, Zscaler is well-positioned to lead in both the security of agentic AI and in utilizing agentic AI capabilities to enhance the security offerings it provides for its customers. Zscaler is working toward a vision of an agentic AI security operations center that automates the daily tasks of security analysts, freeing their time to address more complex issues that cannot currently be resolved through automation. The network security capabilities and zero-trust approach that Zscaler has developed since its inception create the foundation for secure agent-based communication, AI-based automated remediation, and an eventual self-healing system.

While Chaudhry avoids the term "platformization," the keynote and subsequent sessions describe the consolidation of tools and costs for its customers, explicitly stating that many current cybersecurity products and technologies will be unified into a single solution. As Zscaler moves forward, it will likely adopt a more direct and prescriptive approach to its platform offerings, as it begins to compete directly with vendors providing similar value to security operations and exposure management teams.

Conclusion

Zscaler is reinventing itself as a contextual data, AI-driven security operations and remediation platform. Its approach connects a cybersecurity data fabric foundation with AI analysis and prioritization capabilities. They plan to leverage their network security offerings to differentiate themselves while advancing toward a unified platform for customer adoption. The integration of multiple acquisitions with a strong AI-driven vision bodes well for the future of the Zscaler product lines.

These capabilities position Zscaler alongside other cybersecurity giants, creating solutions that reduce risk for customers faster than ever before. Enterprises today struggle to keep pace with the overwhelming number of security issues, remediations, exposures, and attacks, thereby increasing the demand for automation and preventive security solutions. The market recognizes this, as do the major vendors, including Zscaler.

Whether you are a Zscaler customer or not, cybersecurity teams should use this moment of innovation and change to evaluate a new approach to their risk reduction capabilities and consider new platforms that embrace AI and automation.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com