SOLUTION BRIEF

Agentic Security Operations

Get smarter. Move faster.

Today's SOC is fighting a tougher battle than ever

The adoption of AI and the rise in new types of attacks are introducing risks that existing SecOps tooling and processes struggle to defend against. SecOps teams are overwhelmed by findings and alerts that lack the context needed to assess risk level. Teams spend hours in spreadsheets and querying log data to analyze information across separate systems in an effort to prioritize which exposures and threats to address first. Defending against these attacks requires the right data, broader context to accurately assess risks and threats, and agentic operations to enable machine-speed defenses.

Zscaler customers already have the foundation to address these challenges, including unique telemetry, rich business context, and inline controls that can dynamically mitigate risk. Zscaler brings these elements together to turn signals into prioritized insight and enable faster, risk-appropriate action.

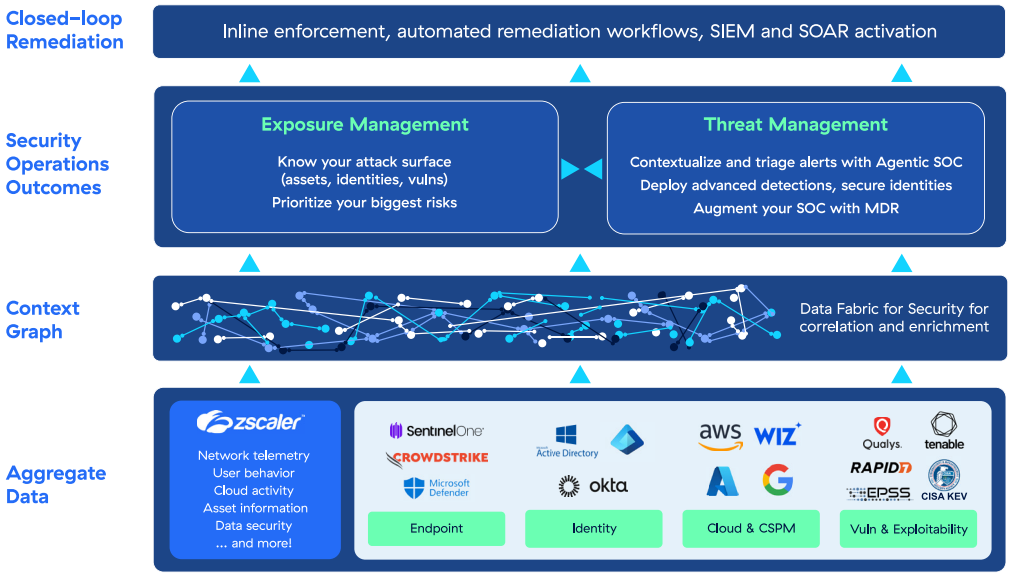
SOC under siege

- AI impact on attack surface
- New attack vectors
- Machine-speed adversaries
- Critcal network insight gaps

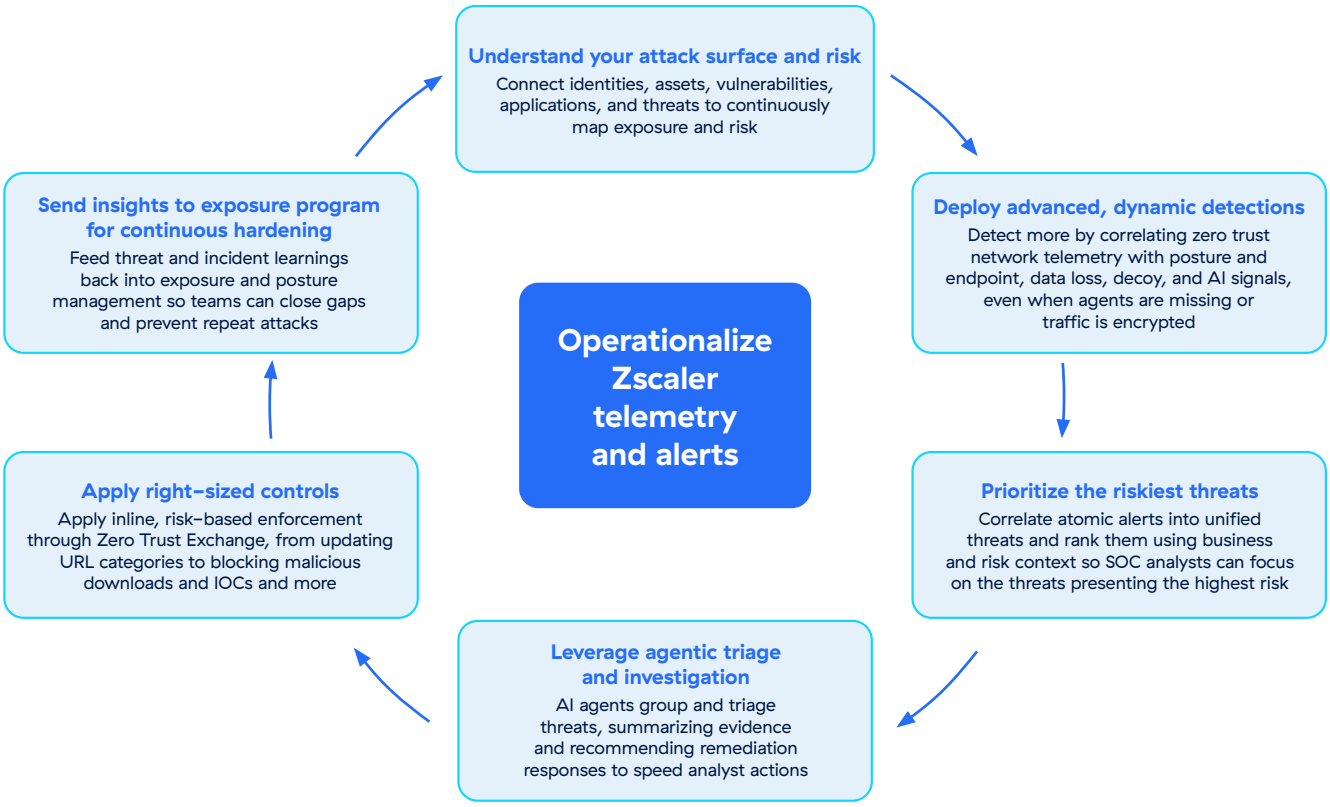
An agentic platform for SecOps visibility, insight, and action

The Zscaler Agentic SecOps platform brings unique network telemetry, business and risk context, agentic SOC workflows, and adaptive responses to proactive and reactive security operations. It combines zero trust with posture insights and alerts across endpoints, data, and AI to detect threats host agents can miss, especially from unmanaged devices, compromised identities, or attack payloads hidden in encrypted traffic. Network visibility also helps detect and stop lateral movement and data loss. The platform analyzes this telemetry natively, reducing the need to forward a high volume of network log data to a SIEM and the related need to build complex correlation rules.

Our Data Fabric for Security builds a context graph of entity relationships — across identities, assets, vulnerabilities, threats, applications, and other attributes — to map attack surface and posture and correlate alerts into unified, prioritized threats for unified action. We then put our AI agents to work on top of that clean, correlated, and enriched data — grouping, triaging, recommending remediation actions, and summarizing threats and exposures. Our agents have been continuously tuned using over a decade of real-world security operations expertise, improving consistency and speed for analysts. Inline enforcement ties response to risk.



Operationalize zero trust with agentic SOC workflows to contain breaches fast and shrink your attack surface



Achieve better security outcomes without added complexity (or added SIEM cost)

The platform centralizes SOC visibility, insight, and action across Zscaler products and key third-party sources like endpoint, identity, and cloud control planes. It augments your SIEM with native detections and richly correlated context, so teams can focus on prioritized threats instead of managing high-volume data and complex correlation rules. Customers can act directly on these outputs or feed these high-quality, contextual insights into their SIEM to drive existing workflows.

Augment your SOC with expert human assistance

We complement our SecOps solutions with managed services like detection and response (MDR) and threat hunting. Built on more than a decade of experience across thousands of customers, our MDR services augment your SOC team with 24x7 coverage and deep expertise to fill gaps, increase operational efficiency, and accelerate security outcomes. And our threat hunting experts leverage both your Zscaler and endpoint signals to uncover anomalies, sophisticated threats, and elusive threat actors who work to evade traditional security measures.

For more information or to schedule a demo: www.zscaler.com/security-operations

zscaler™ | Experience your world, secured.™

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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com