# Zscaler Agentic Security Operations

The rich context and agentic operations needed to assess and contain risks and threats in the AI era

## Human-scale security operations can no longer keep pace with agentic attacks

Frontier AI models are expanding the attack surface and compressing attack timelines from weeks to hours. Adversaries now automate initial access and execute complex multi-step attack chains — all while evading traditional endpoint controls. Running exposure management programs out of spreadsheets has never served teams well — with frontier AI models finding 1000s more vulnerabilities, exposure management teams need a new approach. Similarly, relying on EDR-centric detection and complex SIEM queries and correlation leaves SOC teams playing catch up.

Defense in the AI era requires more than incremental improvements. SecOps teams need an agentic foundation built on full-visibility telemetry, rich business context, unified exposure and threat management, and automated inline controls that contain threats the moment they occur.

## An agentic-powered solution for SecOps visibility, insight, and action

Zscaler Agentic SecOps applies unified threat and exposure management, unique zero trust telemetry, agentic workflows, and closed-loop enforcement to transform security operations. Built to activate the rich data flowing through the Zero Trust Exchange without SIEM ingestion fees, the platform correlates signals across network, identity, endpoint, cloud, and AI. It catches evasive threats that host agents miss, including risks from unmanaged devices, compromised identities, chained exposures, encrypted payloads, lateral movement, and data loss.

Zscaler Agentic SecOps delivers:

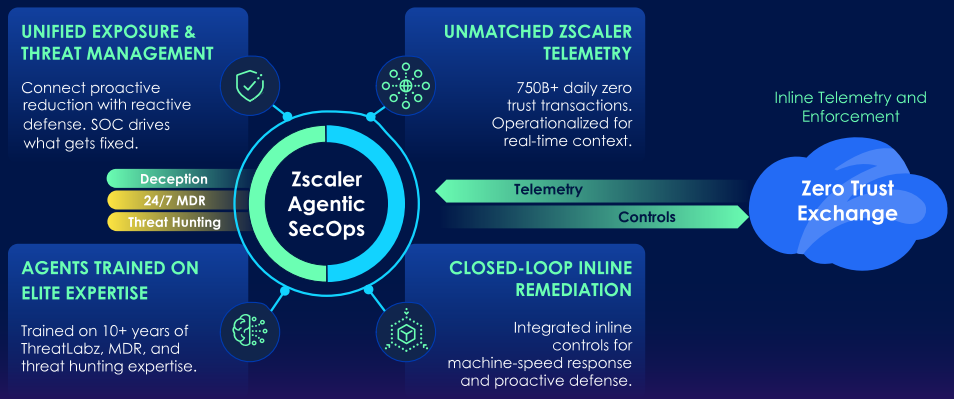
**Unique data for context and clarity:** Combines first-party inline telemetry from 750+ billion daily transactions with third-party signals to clarify risk and give SecOps full visibility without data ingestion penalties.

**Security graph for agentic insight:** The Data Fabric for Security correlates and enriches network, identity, asset, and cloud context so specialized AI agents can synthesize signals and prioritize high-risk threats and exposures.

**Adaptive responses for right-sized actions:** Turns insight into immediate defense with inline enforcement through Zscaler and third-party inline controls, automatically isolating users, restricting access, and shutting down attacks.

INTRODUCING ZSCALER AGENTIC SECOPS

A Unified Platform Purpose-Built For Modern AI-Driven Security Operations




©2026 Zscaler, Inc. All rights reserved.

# Defend Your Enterprise at Machine Speed in the AI Era

Manual vulnerability management and traditional alert processing can no longer keep pace with machine-speed adversaries. Zscaler Agentic SecOps shifts your security team from reactive analysis to proactive risk reduction and decisive containment.




## Exposure Management

**Know all your assets and identities. Fix your gaps. Reduce your risk.**

- Unify asset inventory, identity posture, and vulnerability findings from Zscaler telemetry and third-party security tools into a single, trusted view of organizational risk.
- Rank vulnerabilities and posture gaps based on business impact, dynamic identity risk scores, asset criticality, and active threat intelligence.
- Customize exposure prioritization applying your organization's risk model.
- Orchestrate AI-powered remediation workflows and bi-directional ticketing with ITSM and CMDB platforms to hit critical SLA targets and prevent repeat attacks.

## Agentic SOC

**Unify all your alerts. Prioritize what matters. Stop the greatest threats, fast.**

- Correlate raw signals across Zscaler inline telemetry and third-party security tools into unified, contextualized threat stories using the Data Fabric for Security.
- Leverage specialized AI agents trained on frontline ThreatLabz and MDR experience to deliver automated triage, visual MITRE attack path mapping, clear AI summaries, and transparent verdicts with explicit supporting and contradictory evidence.
- Enable machine-speed threat containment with right-sized response recommendations while eliminating high SIEM data ingestion costs for zero trust telemetry.

## Deception

**Deploy active, AI-driven defense. Catch hidden attackers. Protect your critical assets.**

- Deploy realistic decoys and lures across endpoints, identity systems, cloud apps, and GenAI environments to trap human adversaries and autonomous AI agents during reconnaissance.
- Trigger instant, high-confidence alerts with near-zero false positives the moment attackers interact with decoy sessions, credentials, bookmarks, or adaptive LLM decoys.
- Integrate directly with the Zero Trust Exchange to automatically isolate compromised users and shut down attack sources inline at machine speed.

## Expert Services

**Enlist expert threat hunters. Secure round-the-clock defense. Accelerate your incident response.**

- Get early warnings as our threat hunting team detects stealthy attacks like living-off-the-land tactics, weaponized RMM tools, ClickFix schemes, and stolen OAuth tokens, across your ZIA data with no SIEM ingestion fees.
- Our 24x7 Managed Detection & Response (MDR) operational expertise taps Zscaler inline telemetry to validate real threats, eliminate false positives, and identify complex multi-stage attacks.
- Enable rapid, guided containment using Zero Trust Exchange inline controls to isolate threats and protect business assets without scaling internal headcount.

**Learn more at 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**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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