SOLUTION BRIEF

Zscaler Agentic SOC

Consolidate alerts into incidents. Prioritize and stop the greatest threats, fast.

Human-speed SOCs can't keep up with machine-speed attacks.

AI-powered attacks, expanding attack surfaces, and rising volumes of fragmented alerts are putting tremendous pressure on SOC teams to detect, investigate, and respond before threats escalate. Adversaries increasingly rely on identity, browser, cloud, and AI attacks to move faster and evade traditional controls, breaking the conventional SOC model as:

- **Disparate tools flood analysts with alerts and findings that lack the context needed to assess real risk**
- **Manual investigation across dashboards, spreadsheets, and log data slows triage and leaves high-impact threats unchecked**
- **Reactive workflows can't keep pace with machine-speed attacks or deliver fast, risk-appropriate response**

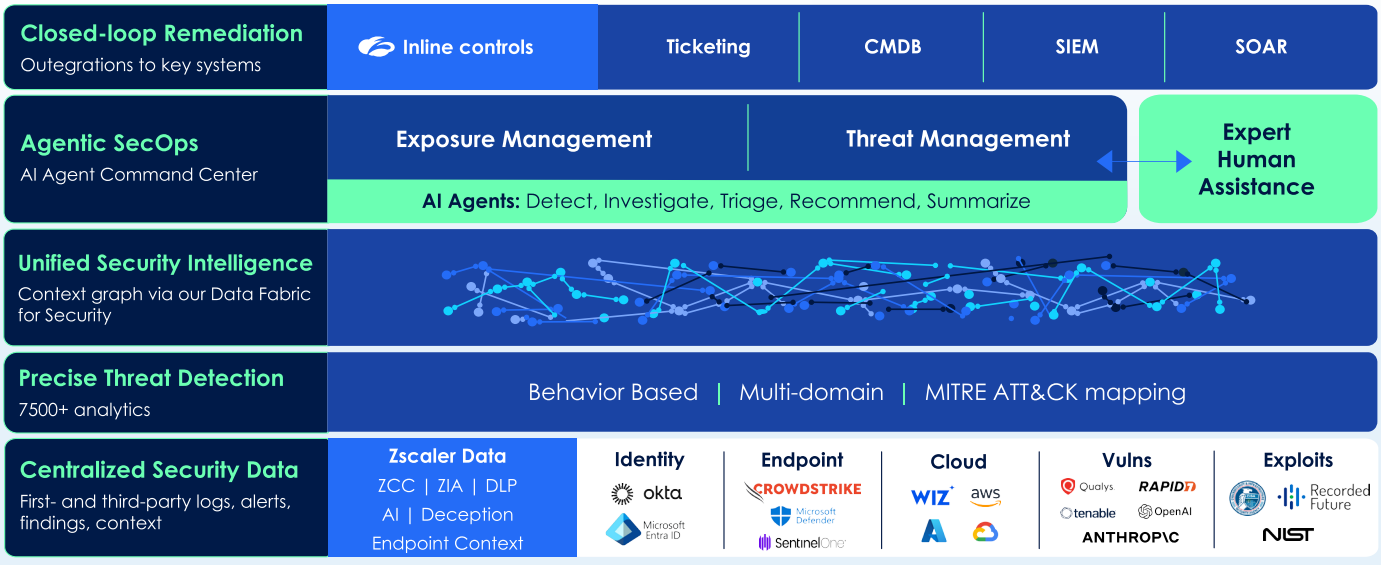
Security operations must move beyond manual alert triage and correlation and leverage automation to turn fragmented signals into prioritized threats and enable faster, right-sized action.

Cut through alert noise, find the biggest threats, and respond with precision.

Zscaler Agentic SOC transforms fragmented alerts into actionable, prioritized threat stories. It brings together signals from across your security stack and then enriches each incident with the business context analysts need to assess what matters, including asset criticality, user identity, exposure conditions, and remediation status. AI agents drive triage, investigation, verdicts, and remediation playbooks, freeing SOC teams to quickly validate the results and enable machine-speed response.

Tied to Zscaler and third-party inline controls, Zscaler Agentic SOC enables faster, accurate, and appropriate containment.

The result is a more efficient SOC that contains threats sooner, minimizes business disruption, and strengthens security posture as attacks grow faster and more complex.



©2026 Zscaler, Inc. All rights reserved.

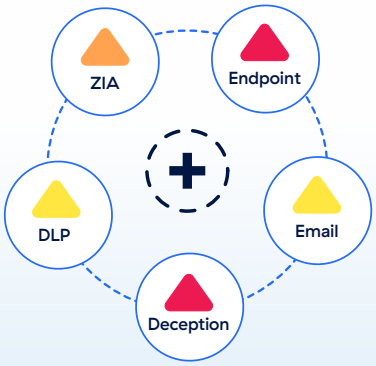
Shift your SOC from endless alert processing to decisive action

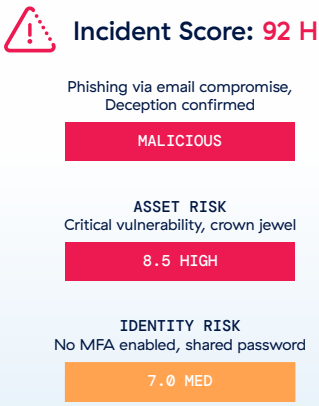
Correlate isolated alerts into unified incidents → Add context (asset, identity, network, business) → Investigate threats and provide holistic verdicts → Prioritize most critical threats to focus on first → Surface ideal actions (highest impact, least disruption → Initiate optimal playbook (human led or automatic) → Determine root cause and elevate priority of fix

Unify alerts to reveal the whole story

Turn the mountain of disparate alerts into a manageable set of unified incidents, by aggregating alerts and adding critical context

- Correlate alerts across Zscaler and third-party tools to show how activity connects across users, devices, apps, network, and data
- Group fragmented alerts into unified threats with AI-powered context so analysts can quickly understand scope, relationships, and attacker intent





Focus on the most important threats

Prioritize the threats with the highest potential impact using AI-driven insights, industry best practices, and your unique business logic

- Leverage network traffic, connections, and behavioral context to factor in attacker activity and movement
- Rank threats by business impact using context such as asset criticality, identity risk, exposure conditions, and remediation status for faster, more consistent triage

Take faster, right-sized action

Leverage agentic recommendations to reveal the most appropriate action with the least potential business impact, often via inline zero trust controls

- Accelerate decision making with agentic triage, AI-generated summaries, and recommended next steps tailored to threat severity and context
- Contain threats with inline zero trust controls and coordinated response workflows to reduce risk quickly while minimizing business disruption



Learn more at zscaler.com/AgenticSOC

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