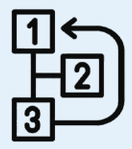
Agentic SecOps Core

Tap Zscaler data and agentic operations to transform your SOC

DATASHEET

Zscaler Agentic SecOps Core shifts your SOC from endless alert processing to decisive action. It leverages AI to unify alerts across your stack, enrich every threat with business context, prioritize risk based on impact, and guide right-sized containment tapping your Zscaler inline controls to stop the incidents that pose the greatest risk to your business.

Unlock critical zero trust insights
Uncover attacks before they can reach the endpoint by incorporating Zscaler telemetry and context into threat analysis and investigations



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

Unify alerts to reveal the whole story
Turn the mountain of disparate alerts into a manageable subset of unified threats by aggregating and grouping alerts with critical context

Take faster, right-sized action
Leverage agentic triage recommendations to reveal the most appropriate action with the least potential business impact, often via inline zero trust controls

Today's painful reality: Human-speed SOCs can't keep up with machine-speed attacks

SOC teams are already drowning in alerts from dozens of sources, and the challenges are only increasing as bad actors increasingly tap AI to propagate attacks. As the speed of attacks ratchets up, having analysts sift through isolated signals with no context leaves organizations vulnerable. Slow investigations, missed high-impact incidents, and costly disruptions come at too high a price. Inefficiency and alert overload keep security teams reactive instead of resilient. It is time for a new approach.

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

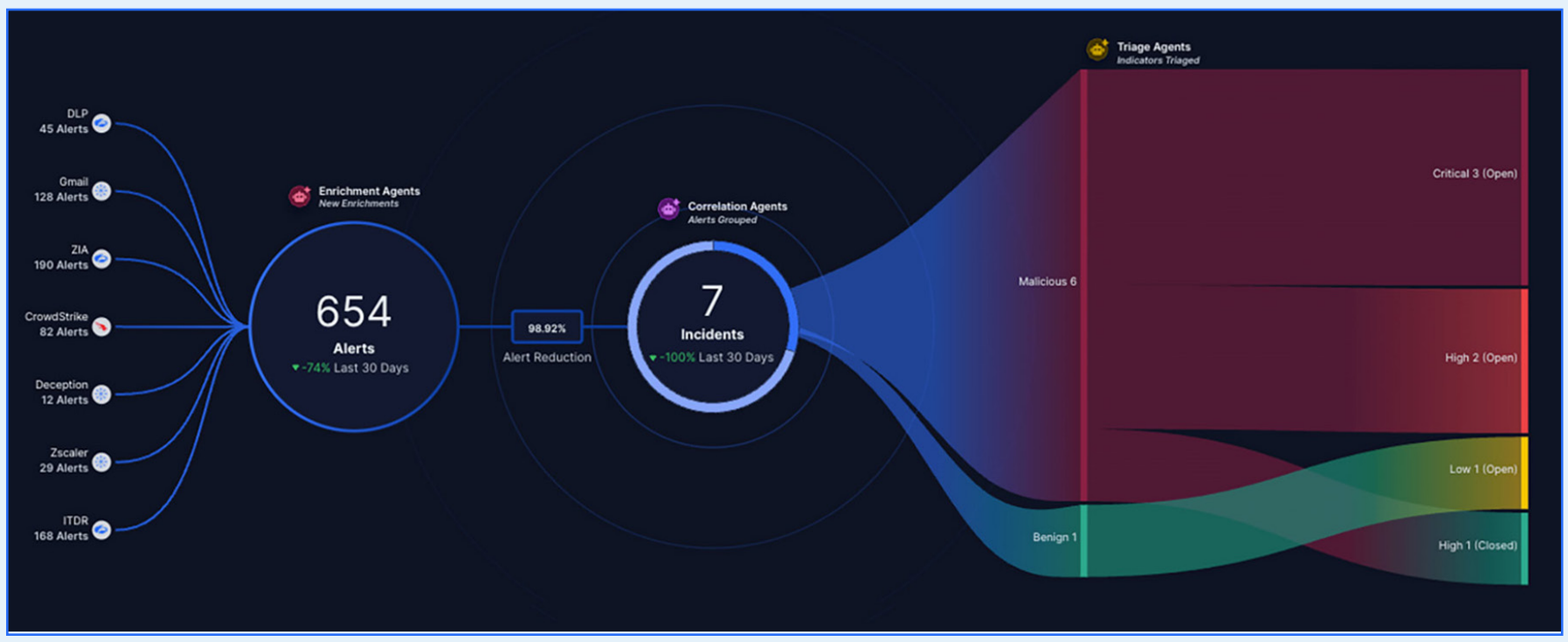
Agentic SecOps Core unifies alerts across your security stack into actionable, prioritized threat stories. Each incident is automatically enriched with business-relevant context such as asset criticality, user identity, and exposure so analysts can quickly separate signal from noise. With agentic guidance, orchestrated workflows, and inline containment actions, SOC teams can investigate, contain, and remediate incidents in one place, improving efficiency while strengthening security posture.

Leverage untapped zero trust signals. Most attacks do not start on a managed endpoint. They begin with compromised identities, unmanaged devices, risky cloud activity, or payloads concealed in encrypted traffic. Agentic SecOps Core surfaces these early indicators by grounding detection and investigation in the zero trust telemetry your Zscaler deployment already produces. Instead of relying solely on endpoint agents and downstream logs, your SOC can use real traffic behavior, policy decisions, user and app activity, and enforcement outcomes to understand what is truly happening across the environment.

By combining Zscaler telemetry with posture insights and alerts across endpoints, data, and AI, the Agentic SecOps platform improves coverage for scenarios where traditional tools struggle. Network-level visibility adds the context needed to detect lateral movement attempts and data loss behaviors, even when signals are fragmented across tools. Because Zscaler analyzes this telemetry natively, you can skip forwarding high-volume network logs to a SIEM just to reconstruct the story. You get higher-fidelity evidence earlier, better certainty, and faster identification of threats that matter before they become incidents that impact your business.

Unify isolated alerts to reveal the whole story. Alert fatigue is not just a volume problem. It is a context problem. When alerts aren't stitched together to reveal the complete picture, analysts waste time manually analyzing fragments of evidence. Agentic SecOps Core unifies alerts across your security stack, including Zscaler and third-party tools, and turns them into cohesive threat stories. Your SOC can see how signals connect across users, devices, apps, and data without pivoting between systems.

Zscaler aggregates data through robust connectors and entity mapping, then creates a security context graph to relate alerts to the assets, identities, and exposures behind them. AI-powered groupings surface relationships that are easy to miss in manual investigations. Customizable grouping rules let you align correlation to your operating model and risk perspective, so teams get consistency without a one-size-fits-all approach. As alerts roll up into unified threats, investigations start with clarity. Analysts can quickly validate scope, understand attacker intent, and focus on what is actionable. If you continue to respond to alerts via your SIEM, you can forward distilled, enriched threat insights to reduce cost and complexity while improving outcomes.



Protect your organization from an expanding attack surface and AI-driven threats with Zscaler Agentic SecOps Core

Focus on the most important threats. When everything is urgent, nothing is. SOC teams need a reliable way to separate high-impact threats from low-value noise as environments and adversaries evolve. Agentic SecOps Core prioritizes what matters by combining AI-driven insights, industry best practices, and your own business logic. Threats are evaluated in context, not isolation, so teams focus effort where it matters most.

Each unified threat is enriched with business-relevant details such as asset criticality, identity context, exposure conditions, and remediation status. This enrichment shows analysts what is at stake, not just what detection fired. The platform can elevate activity tied to crown-jewel assets, privileged users, and mission-critical applications, while incorporating device, user, and app posture to clarify urgency. Prioritization is dynamic. As new evidence appears or behavior changes, scores adjust dynamically, so teams do not miss threats that are escalating. You can also tailor scoring to match compliance requirements, operational priorities, and risk appetite. The outcome is faster triage, more consistent decisions across shifts, and better risk reduction per analyst hour.

Take faster, right-sized action. Speed matters, but precision matters more. Containing a threat too slowly increases risk, yet overreacting can disrupt the business. Agentic SecOps Core enables faster, right-sized response by pairing agentic triage with impact-based recommendations and execution paths that fit your environment. Analysts get clear guidance on next steps, supporting evidence, and the potential business impact of different actions.

The platform accelerates investigations with AI-generated summaries and a unified view of related alerts and entities, so teams start from understanding rather than starting from scratch. Agentic workflows can recommend investigative pivots, propose containment actions aligned to severity, and standardize response quality across experience levels. When it is time to act, the platform connects insight to enforcement through inline, risk-based controls in the Zero Trust Exchange, including stepped-up authentication, reduced access, user isolation, and more. Where third-party tools are required, orchestrated playbooks and SOAR or ITSM integrations help keep response coordinated. The result is quicker containment with minimal disruption, plus feedback loops that help harden posture and prevent repeat attacks.

Leverage your zero trust foundation to meet the moment

Today's expanding attack surface and AI-driven threats demand a SOC built for speed, context, and precision. Agentic SecOps Core unlocks the zero trust telemetry and business context you need to focus on the most important threats, then stop them quickly with closed-loop, risk-based containment through the Zero Trust Exchange. By unifying proactive and reactive security operations in one platform, your team can reduce noise, minimize disruption, and strengthen resilience across endpoints, identities, cloud apps, and data.

See how Agentic SecOps Core helps your SOC unify alerts, prioritize the threats that matter, and take right-sized action. Schedule a demo today.

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

zscaler™

Experience your world, secured.™