Sekoia x zscaler

SOLUTION BRIEF

Zscaler and Sekoia Solution brief

Where the power of ZIA's secure internet access converges with Sekoia's cutting-edge intelligence-driven AI SOC platform.

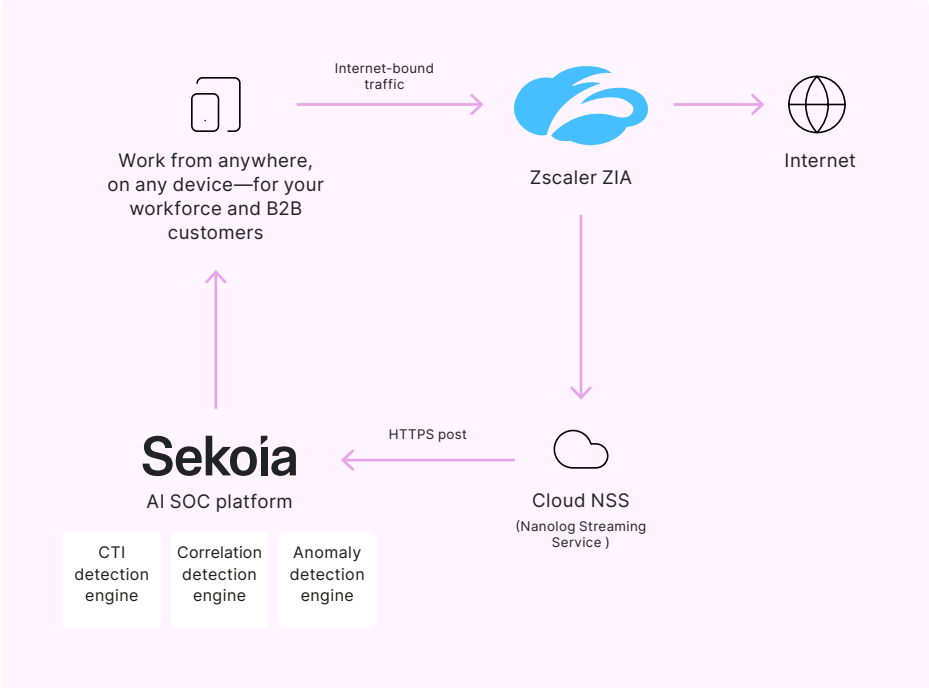
Stop fighting siloed tools. Integrating Zscaler Internet Access (ZIA) with Sekoia's AI SOC platform unifies your security operations. By feeding Zscaler traffic directly into Sekoia, your analysts get centralized visibility backed by native, automated Cyber Threat Intelligence (CTI) to eliminate visibility gaps across hybrid environments.

A seamless cloud-to-cloud integration

Stream Zscaler logs cloud-to-cloud without maintaining heavy logging infrastructure.

Zscaler Cloud NSS offers a simple, one-click integration with Sekoia's AI SOC platform using a secure HTTP push.

Configuration takes just a few clicks to begin instant streaming. As data arrives, Sekoia automatically normalizes the logs, allowing your analysts to immediately correlate Zscaler alerts with the rest of your security ecosystem.



ZSCALER AND SEKOIA IN ACTION

Detection improvement and orchestration

Use a single console

The integration of ZIA with Sekoia centralizes all security functions within a single platform, streamlining security operations. This eliminates the need to navigate between multiple security consoles, making your security operations more efficient and comprehensive.

Anomaly-based detection

Sekoia's anomaly detection capabilities help identify deviations from established baselines, enabling organizations to detect and respond to unusual and potentially harmful activities logged by Zscaler or other technologies.

Response capability

Sekoia excels in orchestration and incident response through its centralized AI SOC platform. Automated playbooks deliver swift, consistent responses to optimize incident management. This empowers your security team to orchestrate and control tools across your entire IT landscape.

Enrich Zscaler logs and alerts

This integration allows Sekoia to enrich ZIA logs with native Cyber Threat Intelligence (CTI). ZIA generates logs and security event data which are enhanced with real-time threat indicators, IoCs, and contextual information from Sekoia. This enrichment provides security teams with the necessary data to improve threat detection, incident response, and proactive security decisions, in addition to the base provided by Zscaler.

Correlation-based detection

Sekoia's Sigma Correlation engine enhances threat detection by correlating various security events and their behavior (from ZIA and other specific cybersecurity technologies) and creating a more accurate, comprehensive picture of potential threats.

CTI-based detection

Sekoia's CTI detection engine leverages a complete threat intelligence database (modelized in STIX 2.1) and compares it to the events integrated in the AI SOC platform. This ensures improved detection capabilities and associated threat context to help analysts correctly qualify and mitigate alerts.

Automated retrohunt

When a new IoC (Indicator of Compromise) is added to the Sekoia platform, it will search for this indicator in your logs, including historical data. This feature, combined with very strict IoC lifecycle management, ensures powerful automated retrohunt capabilities, with very few false positives. Necessary remediation actions can be taken retrospectively based on traffic logged by Zscaler that is considered malicious.

ABOUT SEKOIA

Sekoia is a European cybersecurity company delivering advanced defense against global threats. Our intelligence-led AI SOC platform unifies your security operations for real-time detection and response. Built on open standards, Sekoia integrates seamlessly with your existing tech stack to maximize your security investments.

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.

Learn more at zscaler.com or follow them on Twitter @zscaler.

Discover the full picture at sekoia.com

Ready to explore how Sekoia Intelligence can elevate your OpenCTI environment?

Activate a trial in your existing OpenCTI instance.

CONTACT US