Zscaler & SentinelOne — Unified Zero Trust & Endpoint Protection

AT-A-GLANCE

Key Benefits:

Enable Zero Trust access with real-time device posture validation.

Minimize data silos by unifying endpoint and cloud telemetry.

Accelerate remediation with cross-platform response.

Increase efficiency of triage and investigation with enriched context.

End-to-end visibility, AI-driven detection, and automated remediation across endpoints, networks, and cloud.

The Challenge

Enterprise technology stacks are increasingly complex—with distributed applications, remote users, IoT devices, and sanctioned and unsanctioned tools. As attack vectors multiply, security teams face:

- Siloed data analyzed without context.
- Alert fatigue and console pivots across disconnected tools.
- Longer dwell times from lack of correlation.

A new approach is required—one that delivers frictionless, end-to-end security from endpoint to application.

The Solution

Together, SentinelOne and Zscaler unify to provide enterprise security across endpoint, network, and cloud.

- The SentinelOne Singularity Platform, powered by Singularity Data Lake, protects, detects, and responds across endpoints, identities, and cloud workloads with unified analytics.
- The Zscaler Zero Trust Exchange™ secures internet, SaaS, and private apps for all users, devices, and locations with inline AI-powered inspection and threat protection.

With seamless integration, security teams can minimize risk, block threats outright, and accelerate investigation and remediation—without pivoting between consoles.

How It Works

- **Comprehensive Visibility** — ZIA and ZPA logs are ingested into the Singularity Data Lake, normalized via OCSF, and correlated with endpoint data for deeper investigation in a single console.
- **Expanded Enrichment** — Zscaler provides correlated user attributes, related threats, and URL categorization directly within SentinelOne's XDR feed.
- **Accelerated Remediation** — Policy-driven actions automatically enforce controls in Zscaler, from blocking to quarantining a user to isolating sessions in a Zero Trust Browser.
- **Seamless Sandboxing** — Threat files detected by SentinelOne can be sent to Zscaler Sandbox for AI-powered analysis, with enriched results returned to the console.

- **Zero Trust Conditional Access** — At access time, Zscaler checks device posture from SentinelOne and dynamically enforces secure, policy-based access.
- **Purple AI & Hyperautomation** — SentinelOne's Purple AI integrates with Zscaler telemetry to automate detection, hunting, and response using natural language queries. Combined with Singularity Hyperautomation playbooks, analysts can accelerate investigations, orchestrate cross-platform actions, and reduce response times from hours to minutes.

How We Do It: Our Joint Defense in Dept Integration Framework

Zero Trust

Device Posture-Based Zero Trust with Conditional Access
SentinelOne ensures endpoint compliance, while Zscaler dynamically analyzes device posture to grant or deny application access

Context Enrichment
Threat enrichment with correlated user details, related Zscaler threats, and URL lookups and sandbox

Threat Containment
Using SCIM based integrations to restrict access for risky users

AI-Driven Detection & Response

Comprehensive Visibility
Singularity Data Lake ingests and normalizes Zscaler logs streamlining threat investigation within the SentinelOne console without switching dashboards

Purple AI Support
Automate and accelerate threat detection, investigation, and response using intuitive natural language interactions

Hyperautomation & One-click Remediation
Accelerated incident resolution with customer playbook workflows with one-click remediation powered by detection from SentinelOne and response actions from Zscaler

Solution Highlights

- Zero Trust conditional access based on real-time endpoint posture.
- Threat enrichment with user attributes, URL lookups, and sandbox analysis.
- Accelerated one-click remediation from the SentinelOne console into Zscaler
- Zero Trust Security with advanced threat protection and end-to-end visibility.
- Purple AI integration and hyperautomation for streamlined SOC workflows.

Check out the demo video

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line 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**

zscaler™

Zero Trust Everywhere