End-to-End Visibility, Threat Detection, and Remediation Empowered by XDR

SentinelOne & Zscaler Joint Solution Brief

PARTNER BRIEF

Market Challenges

Today's enterprise technology stacks are complex — with distributed applications, users, and endpoints, an ever-expanding list of IoT devices, and new sanctioned and unsanctioned tools being deployed daily. As attack vectors multiply, from endpoints to networks to the cloud, security teams struggle to secure their valuable assets inside and outside the traditional network perimeter.

The more security controls that security operations teams deploy, the more alerts they get, but too often, the signal is buried in the noise. Security analysts are forced to pivot between tools that do not integrate and fail to connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect, leading to longer dwell times. This complexity has necessitated a new approach to securing access—one that provides frictionless security from endpoint to network to application.

Joint Solution

Together, SentinelOne and Zscaler unify to provide enterprise security across endpoint, network, and cloud, enabling enhanced end-to-end visibility, accelerated remediation, seamless sandboxing, and secure conditional access. The SentinelOne Singularity Platform, powered by Singularity Data Lake, continuously protects, detects, and responds to threats across endpoints, identities, and cloud workloads with unified analytics. The Zscaler Zero Trust Exchange provides secure access to internet, SaaS apps, and private apps for all users from any device or location, with inline AI-powered traffic inspection and advanced threat protection. With seamless integration between SentinelOne and Zscaler, security teams can minimize risk and block threats outright, while also accelerating investigations and remediating threats faster without pivoting between consoles. Security operation centers can triage, investigate, and remediate threats much more efficiently and with greater confidence.

INTEGRATION BENEFITS:

- Accelerate remediation with cross-platform response
- Minimize data silos within your environment
- Increase efficiency of incident triage and investigation

Joint Solution Highlights

- Zero Trust Security with Advanced Threat Protection and End-to-End Visibility
- Threat Enrichment with User Attributes, URL Lookups, and Sandbox Analysis
- Accelerated One-Click Remediation
- Zero Trust Conditional Access

Key Use Cases

COMPREHENSIVE VISIBILITY

SentinelOne and Zscaler integrate for expanded visibility to provide security teams with a holistic understanding of threat context and user attributes, allowing them to quickly triage and respond to attacks. While Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) offer secure internet, SaaS, and zero trust network access, the Singularity Data Lake continuously ingests Zscaler logs for deeper visibility and accelerated investigation with AI-assisted analytics. Once logs ingested into the Data Lake are normalized to the Open Cybersecurity Scheme Framework (OCSF) for faster correlation and analytics, security analysts can investigate threats in the SentinelOne console, without having to constantly switch between multiple dashboards.

EXPANDED ENRICHMENT

The SentinelOne and Zscaler integration provides further threat enrichment with correlated user details, related Zscaler threats, and URL look-ups. When a threat is detected by SentinelOne, Zscaler automatically correlates user attributes, such as if the user is an admin, their department, or if they are linked to any specific groups in the company. When applicable, URL lookup details are also shared and viewable within the XDR Feed of the SentinelOne console, such as Zscaler's categorization of the URL and other relevant information.

ACCELERATED REMEDIATION

With the integration, SentinelOne and Zscaler enable security analysts to accelerate response with policy driven actions that remediate threats automatically in Zscaler from the SentinelOne console. Analysts can trigger manual or automatic response actions to mitigate threats, moving users to a destination group where a specific policy can be applied. This includes limiting user access, quarantining a user, blocking access to one or a group of critical applications, or rendering applications in an isolated Zero Trust Browser session with restricted functionality to limit an attacker's ability to infiltrate and launch an attack.

SEAMLESS SANDBOXING

With the threat detection capabilities of the Singularity Platform in combination with Zscaler Sandbox, security teams benefit from a seamless sandbox analysis experience to further enrich threats. Based on the security team's configuration, when SentinelOne detects a threat, it can automatically send the threat file to Zscaler for sandbox analysis. Zscaler Sandbox provides AI-powered deep inspection and detonates the file in a virtual environment to detect any malicious behavior. The additional intelligence from the sandbox analysis is then directly observable in the SentinelOne console, such as threat classification, origin risk, risk summary, and detected malware.

ZERO TRUST CONDITIONAL ACCESS

The SentinelOne and Zscaler Zero Trust Exchange integration enables seamless conditional access, ensuring that the trusted identity on a trusted device can directly access authorized corporate applications without exposing the network. Zscaler and SentinelOne combine to provide best-in-class Zero Trust access control with unparalleled visibility, threat protection, AI-powered detection, and automated response across endpoints, applications, and cloud workloads. SentinelOne continuously checks policy and enforces compliance on the endpoint. At the time of access, Zscaler checks whether SentinelOne is

installed and running and considers this device posture as part of its dynamic risk analysis to grant or deny application access.

ACCELERATED THREAT HUNTING AND REDUCED RESPONSE WITH PURPLE AI AND ZSCALER

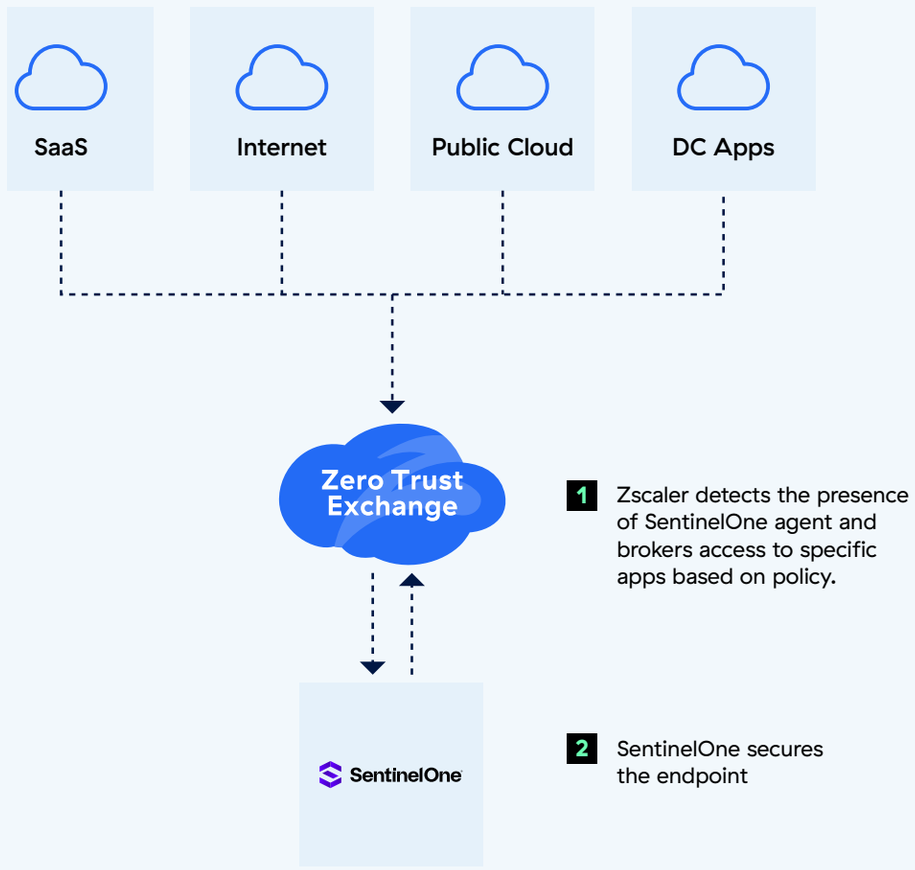
SentinelOne's Purple AI integrates with Zscaler's Zero Trust Exchange to automate and accelerate threat detection, investigation, and response using intuitive natural language interactions. Through a seamless, out-of-the-box integration, Zscaler ZIA and ZPA logs are ingested into the SentinelOne Singularity platform and normalized using the Open Cybersecurity Schema Framework (OCSF), enabling consistent correlation across endpoint, network, and cloud data. Security teams can ask simple, human-readable questions to PurpleAI that looks into the Zscaler logs to formulate a response, thus eliminating the need to write complex queries. Multilingual support broadens accessibility, empowering global SOC teams to conduct fast, context-rich investigations across their entire security stack. By unifying threat signals and reducing response times from hours to minutes, organizations gain comprehensive visibility, enhanced operational efficiency, and stronger enforcement of Zero Trust policies—all seamlessly managed within the Sentinel One console.

HYPERAUTOMATION THROUGH WORKFLOW ORCHESTRATION FOR STREAMLINED INCIDENT RESOLUTION

Together, SentinelOne and Zscaler empower security operations teams to achieve true hyperautomation by supporting both automated and manual creation and execution of playbooks within SentinelOne's Singularity Hyperautomation. Security analysts can design custom playbook workflows tailored to their organization's needs and manually initiate them directly from the SentinelOne console. This approach ensures human oversight for unique or complex incidents, allowing security analysts to respond effectively where it matters most. For example, when a suspicious user activity is detected in Zscaler logs, an analyst can manually trigger a playbook workflow that not only investigates the event but also orchestrates a series of actions—such as isolating the user, restricting access, and notifying relevant stakeholders. This approach appeals to personas seeking both control and efficiency, blending the speed of automation with the nuanced judgment of experienced analysts. The integration eliminates silos, reduces manual errors, and accelerates incident resolution, allowing SOC teams to focus on high-value analysis while ensuring consistent, policy-driven security outcomes across endpoints, networks, and cloud environments.

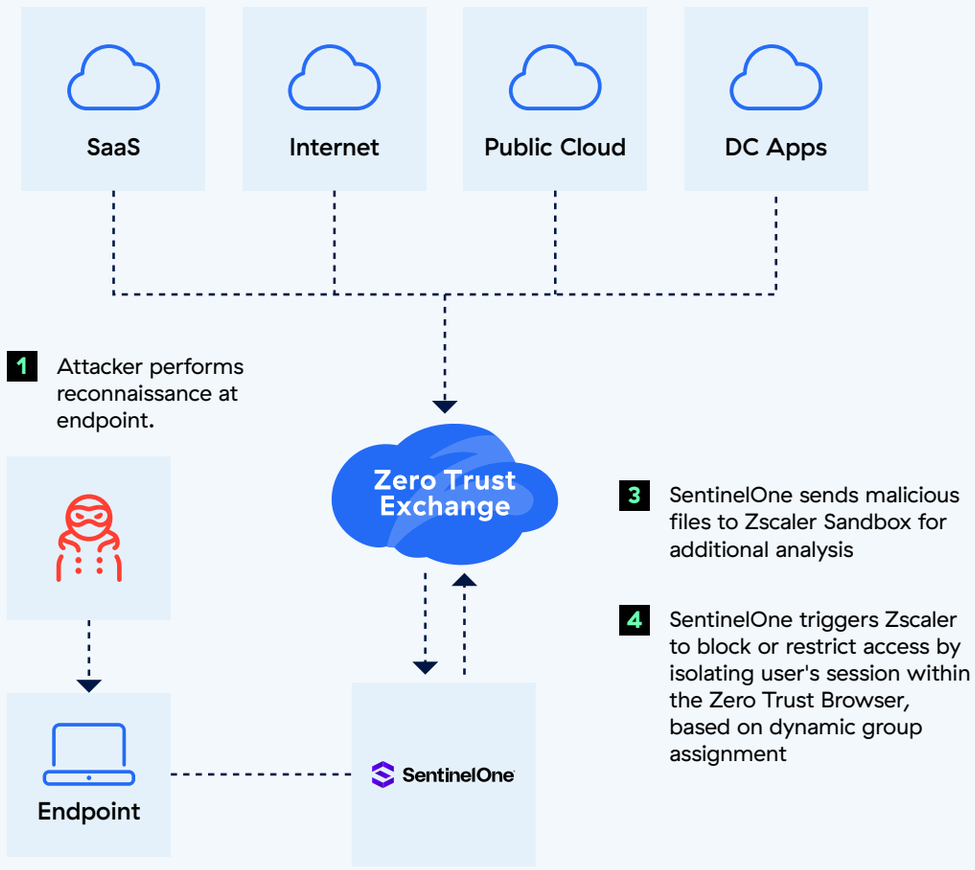
> Today's security challenges require defense in depth. SentinelOne and Zscaler are key components in our security stack that help us advance our overall security posture. Together, Singularity XDR and Zscaler automate the triage and investigation functions in the SOC, enabling a small team to respond against threats with speed and accuracy.
>
> **JOHN MCLEOD**
> CISO of NOV

Zero Turst Conditional Access



1. Zscaler detects the presence of SentinelOne agent and brokers access to specific apps based on policy.
2. SentinelOne secures the endpoint

Extended Visibility & Accelerated Remediation



1. Attacker performs reconnaissance at endpoint.
2. SentinelOne attack using behavroral analytics and additional context and logs/URL reputation from Zscaler security cloud.
3. SentinelOne sends malicious files to Zscaler Sandbox for additional analysis
4. SentinelOne triggers Zscaler to block or restrict access by isolating user's session within the Zero Trust Browser, based on dynamic group assignment

About SentinelOne

SentinelOne's cybersecurity solution encompasses AI-powered prevention, detection, response, and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous XDR platform. Learn more at sentinelone.com.

SentinelOne®

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