



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

SentinelOne & Zscaler Joint Solution Brief





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

SentinelOne & Zscaler Joint Solution 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

+ SentinelOne® 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.

“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

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 isolated containers with restricted functionality to limit an attacker's ability to infiltrate and launch an attack.

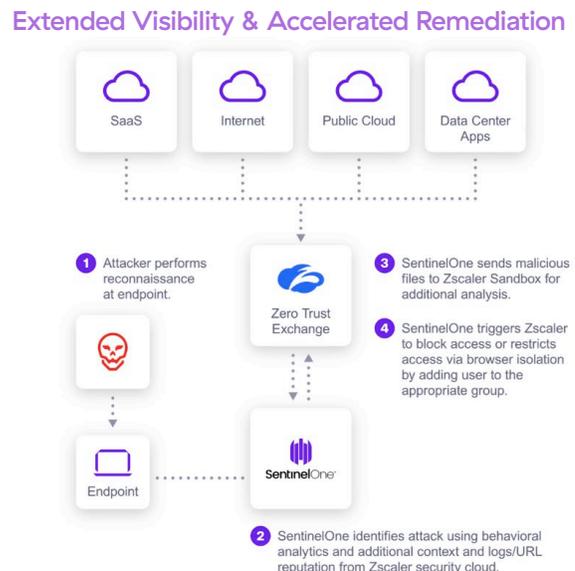
Seamless Sandboxing

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.



 | 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

©2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ 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.