



SentinelOne & Zscaler™
End-to-End Visibility, Threat Detection
& Remediation Empowered by XDR



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 (SecOps) teams deploy, the more alerts they get, but the signals are often buried in the noise. Moreover, 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 time-to-resolution.

This complexity has necessitated a new approach to securing access—one that provides frictionless security from endpoint to network to application.

The Zscaler and SentinelOne joint solution

SentinelOne and Zscaler combine to simplify enterprise security across endpoint, network, and cloud, enabling enhanced end-to-end visibility, automated response, and conditional access.

With integration into SentinelOne's new Dataset offering, Zscaler logs are ingested into SentinelOne's Scalyr back end where they can then be queried and faceted, allowing security operations teams to quickly triage and respond to attacks.

This joint solution empowers Security Operations teams to accelerate response with policy-driven actions that remediate threats automatically in Zscaler before an endpoint compromise results in cloud data exfiltration or other damage.

Analysts can trigger automatic and manual response actions from SentinelOne into Zscaler such as revoking access or quarantining users or moving them into a more restrictive group. This automatically limits an attacker's ability to infiltrate and launch an attack.

Coordinated user access control via the Zscaler Zero Trust Exchange provides secure conditional access to private and SaaS applications based on zero trust principles. Additional zero trust integration points include device posture checks by the Zscaler Client Connector agent to enable conditional access policies based on whether the SentinelOne agent is installed and running. This thereby minimizes the enterprise attack surface with a zero trust policy for conditional access.

At a glance: Integration benefits

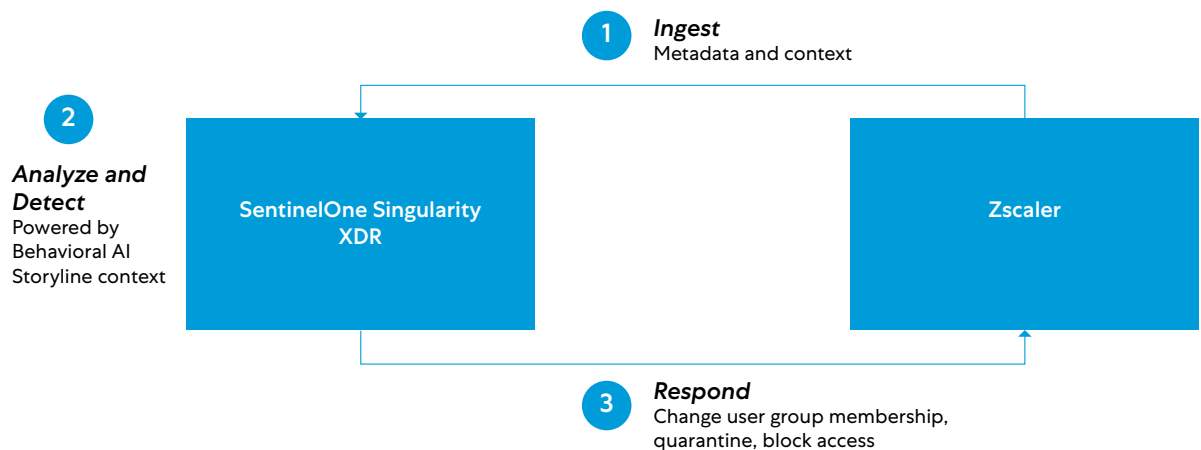
- ✓ **Enforce Conditional Access**
Endpoints enforce zero trust access policies
- ✓ **Zero trust Security with end-to-end visibility**
Minimize data silos and enhance detection
- ✓ **One-click remediation**
Trigger cross-platform response

With seamless integration, Zscaler and SentinelOne enable security teams to accelerate investigations and remediate threats without pivoting between consoles. Security Operation Centers can triage, investigate, and remediate threats much more efficiently and with greater confidence.

Key use cases

Extended visibility and accelerated remediation

This joint solution enables SentinelOne to consume Zscaler logs for expanded visibility and enables security analysts to configure flexible response policies right from the SentinelOne console. Analysts can quickly and automatically mitigate threats such as limiting user access, quarantining a user, blocking access to one or a group of critical applications, or restricting access to specific applications only with browser isolation.



The Zscaler and SentinelOne integration is deployed simply using the following steps:

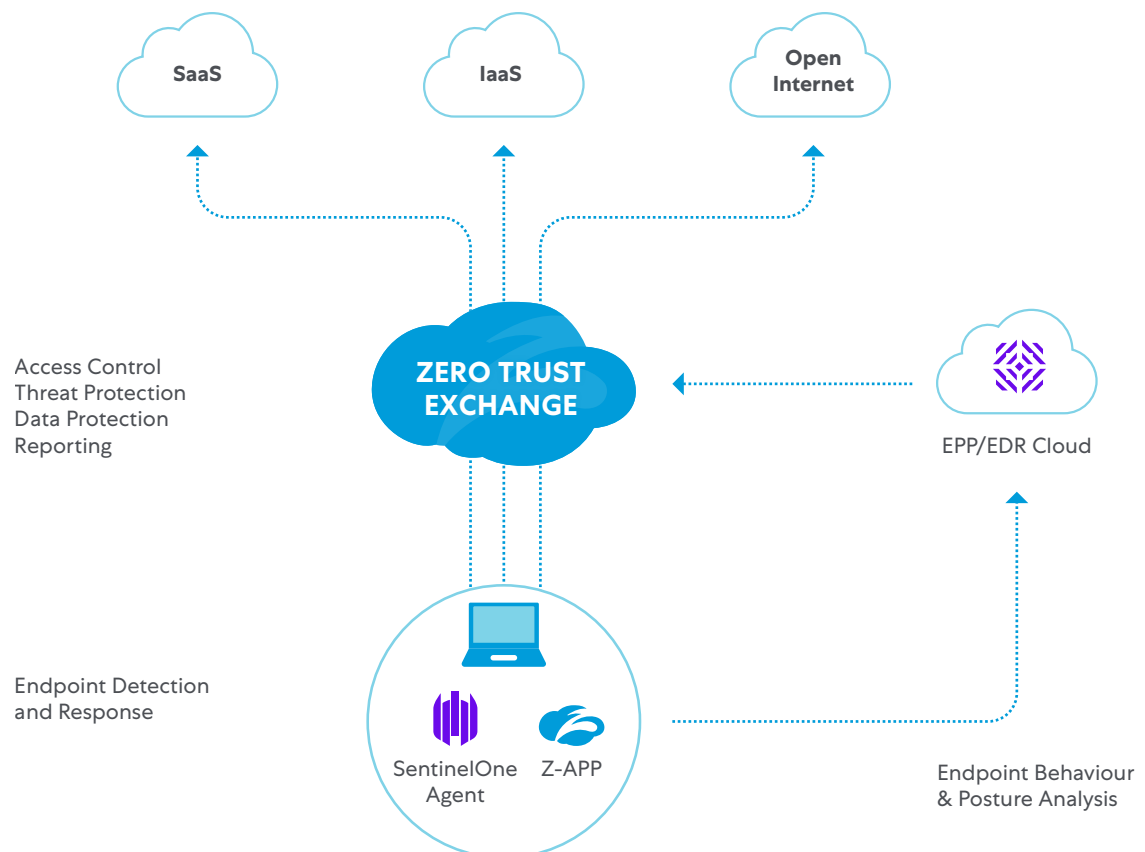
1. Install the free app from Singularity Marketplace and provide it with Zscaler API credentials.
2. Ingest the Zscaler logs into the SentinelOne Singularity XDR framework.
3. Use default or custom policies to trigger response actions by changing user group membership such as predefined restrictive or browser isolated groups. This ensure that users are granted access to enterprise applications and data based on the dynamic conditions of threats and user risk, with speed and consistency.

Zero trust conditional access

The SentinelOne and Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) integration enable seamless conditional access, ensuring that the trusted identity on a trusted device can directly access authorized corporate applications without exposing the network.

The guiding principles of zero trust are to assume that attackers are already in the network which means never implicitly trusting users or applications before verifying. Given the assumption that the environment is already compromised, nothing should be trusted until users, devices, and applications demonstrate their trustworthiness.

Zscaler and SentinelOne combine to provide best-in-class zero trust access control with exceptional visibility, 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, considers the endpoint's security posture and grants access to corporate applications. Here's how it works:



1. SentinelOne secures endpoints with enterprise-grade prevention, detection, response, and hunting.
2. Zscaler Client Connector verifies the presence of SentinelOne by using device posture as an additional authorization vector for access control. Zscaler ZIA and ZPA can be configured to allow only compliant endpoints—ones that pass the posture check—to access selected applications.
3. Zscaler admins can specify (for Windows and Mac workstations) that SentinelOne is installed and running for an endpoint to be granted access to critical business applications.

Conclusion

The integration of SentinelOne and Zscaler extends advanced threat detection and remediation across networks, endpoints, and cloud applications. The ability to configure automated policies across platforms provides flexible yet speedy responses to newly discovered threats. Seamless conditional access simplifies the adoption of zero trust, keeping users, devices, and applications secure. Together, SentinelOne and Zscaler provide joint customers with increased SOC efficiency, streamlined workflows, and enhanced threat protection across endpoint, cloud, and network.

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](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

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](https://www.sentinelone.com).