JOINT SOLUTION BRIEF

zscaler™ + EXTRAHOP

Unified Visibility Across Hybrid Environments, High-Fidelity Detections, and Stronger Zero Trust Powered by SSE + NDR

INTEGRATION HIGHLIGHTS

- Gain a complete picture of security events
- Pinpoint the root cause of performance issues
- End-to-end continuous monitoring and risk adaptation

The Challenge

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

The more controls that security operations teams deploy, the more alerts they get. Too often, the signal is buried in the noise. Analysts are forced to pivot between tools that do not integrate and fail to paint a complete picture of what is really happening.

Meanwhile, on the IT operations side, teams struggle to understand the root cause of application performance issues. Is it the user's device? The network? The cloud service? The application code?

Data is collected and analyzed in isolation, without any context or correlation, creating gaps in what both teams can see and analyze, leading to greater risks to the business. It's time for a new approach.

The Solution

Together, Zscaler and ExtraHop provide integrated enterprise security across endpoint, network, and cloud.

Zscaler Security Service Edge (SSE), powered by Zscaler Zero Trust Exchange™, helps security and IT leaders incorporate a cloud-delivered approach to enabling zero trust. Zscaler Private Access (ZPA) is a key component that provides secure, identity-based access to private applications for all users from any device or location, including third-party suppliers and contractors using unmanaged devices.

ExtraHop RevealX Network Detection and Response (NDR) uses machine learning and real-time behavioral analysis of network traffic to help organizations detect, investigate, and respond to cyber threats across hybrid and cloud environments. By deeply inspecting east-west traffic, ExtraHop excels at uncovering lateral movement, privilege escalation, C2 communication, and more.

With seamless integration between ZPA and ExtraHop, security and IT teams can accelerate investigations and simplify security operations with integrated workflows.

Together, Zscaler and ExtraHop provide end-to-end visibility into communication that traverses the Zscaler cloud and beyond. By correlating ZPA logs with network telemetry from ExtraHop, SOC teams get a complete view of events for faster response.

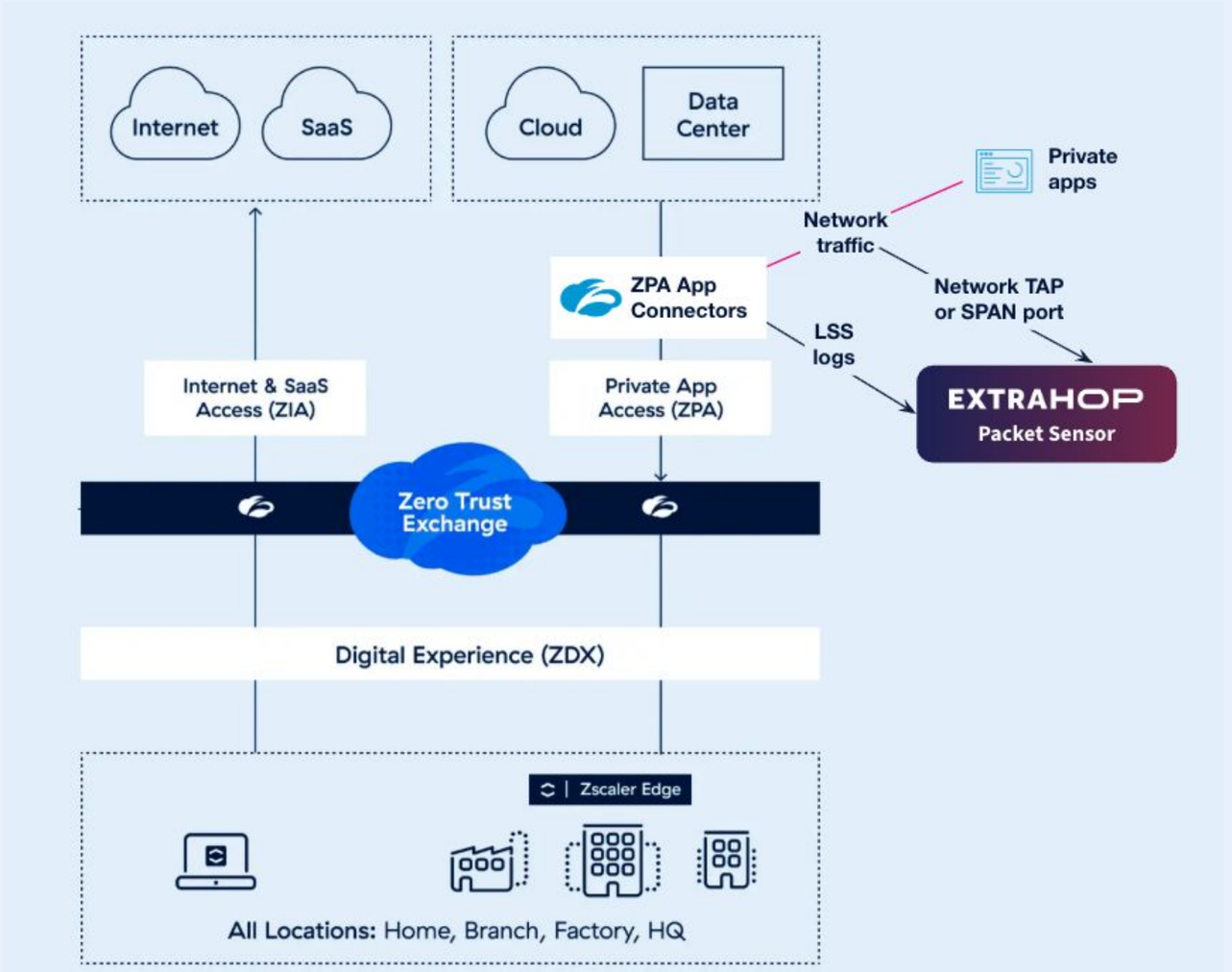
Solution Components Deep Dive

Zscaler Log Streaming Service (LSS) forwards ZPA user activity logs into ExtraHop RevealX packet sensors to provide comprehensive, end-to-end network visibility into east-west traffic including users, devices, and apps.

When a user connects to a private application, Zscaler creates user activity logs while securely giving the user access, or blocking the attempt.

When access is allowed, user packets route from ZPA App Connectors to the private app hosted in datacenters and the cloud. This traffic is already observed by ExtraHop through a TAP or SPAN, but metadata such as origin IP address and user name is obscured since all access looks like it comes from the ZPA server.

To solve for this, ExtraHop detections are automatically enriched with user activity logs from Zscaler, offering end-to-end L2-L7 visibility for all user-to-application communication. ExtraHop records are created and can be stored for analysis for up to 365 days.



KEY USE CASES

Comprehensive Visibility

Zscaler and ExtraHop 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 Private Access (ZPA) offers secure, zero trust network access, RevealX NDR continuously ingests Zscaler logs for deeper visibility and accelerated investigation.

Continuous Monitoring and Risk Adaptation

By analyzing traffic patterns and behavioral insights from RevealX, security teams can create more granular and effective Zscaler policies. RevealX can also help ensure that policies are working as intended or if there are misconfigurations or policy gaps.

Today's security challenges require modern approaches that unify visibility, continuously contextualize and prioritize alerts, and automate repetitive tasks. Together, Zscaler and ExtraHop are key components to help organizations modernize their defenses and strengthen zero trust.

Kanaiya Vasani
Chief Product Officer, ExtraHop

Zscaler + ExtraHop Benefits

ACTION	DESCRIPTION
Bridge the gaps	Gain visibility into communication that traverses the Zscaler cloud and beyond, with deep inspection of east-west traffic to identify behavioral anomalies, deliver high-fidelity detections, and speed investigations
Enrich detections for faster triage	Added context around origin IP and user identity helps security analysts prioritize and investigate detections more effectively
Detect lateral movement + enhance threat hunting	RevealX can identify initial access attempts and look for subsequent post-exploitation activity, such as lateral movement or privilege escalation. Hunt for threats across the entire kill chain.
Pinpoint the root cause of performance issues	RevealX uses Zscaler logs to enrich L2-L7 network packet visibility and understand network flows from origin to destination.

Conclusion

Minimize risk, reduce complexity, and better secure distributed environments with Zscaler and ExtraHop

Zscaler + ExtraHop deliver an end-to-end zero trust solution with unified visibility, real-time threat detection, and automated containment. The integrated solution helps security teams uncover lateral movement, stop modern threats, and strengthen their overall security posture. It also helps IT teams pinpoint performance issues to ensure availability and improve the customer experience.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | **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 in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.