EXTRAHOP | zscaler

Raising SOC Efficacy with SSE and NDR for Greater Contextual Evidence

SSE + NDR for Unified Visibility and Stronger Zero Trust Across Hybrid Environments

SOLUTION BRIEF

Unified Intelligence for Modern Security

Today's distributed enterprise creates a "visibility paradox:" while Security Service Edge (SSE) provides essential cloud-delivered protection, proxied traffic often obscures critical user and device metadata. Operating network detection and response (NDR) and SSE in isolation leads to dangerous blind spots where lateral movement goes undetected and forensic investigations stall. Security teams struggle to correlate external web activity with internal network footprints, resulting in siloed data analysis and delayed response times.

The integration of ExtraHop RevealX™ and Zscaler's Zero Trust Exchange bridges this gap, providing 360-degree visibility across hybrid environments. By correlating Zscaler user activity logs with ExtraHop's deep packet-level analysis, SOC teams gain a unified source of truth from origin to destination. This combined solution addresses the challenges of obscured metadata and siloed telemetry, enabling primary use cases, including detecting lateral movement, rapid incident forensics, and automated threat containment. Prospective customers benefit from accelerated triage, continuous risk adaptation, and the ability to pinpoint performance root causes. By unifying these world-class platforms, organizations ensure a robust Zero Trust posture that secures every user, device, and workload while reducing the time between detection and defense.

Gain a complete picture of security events

Pinpoint the root cause of performance issues

End-to-end continuous monitoring and risk adaptation

Together, Zscaler and ExtraHop provide end-to-end visibility into communications that traverse the Zscaler cloud and beyond. By correlating ZPA and ZIA data with ExtraHop's network telemetry, SOC teams get a complete view of events to drive faster detection and response.

ExtraHop RevealX + Zscaler Private Access (ZPA) Integration

THE CHALLENGE

When organizations implement Zero Trust Network Access (ZTNA) solutions like Zscaler Private Access (ZPA) independently, they often encounter a significant "visibility paradox." ZPA provides secure, application-specific access by tunneling private traffic through App Connectors, but this process inherently obscures critical network-level metadata.

Because the connections appear to originate from the ZPA proxy or connector rather than the actual user device, the original source IP addresses and authenticated usernames are stripped from the packet telemetry. This metadata gap creates dangerous blind spots for security operations teams. Without the context of the originating device or identity, analysts cannot effectively track internal communications or identify lateral movement between sensitive workloads.

This lack of transparency forces security teams to manually pivot between disparate tools during investigations, significantly increasing the time required to detect and remediate threats. Consequently, attackers who compromise a legitimate user session can expand their footprint across the data center while remaining hidden.

THE SOLUTION

The integrated solution combines ExtraHop RevealX Network Detection and Response (NDR) with Zscaler Private Access (ZPA) to restore complete visibility across the hybrid enterprise. By leveraging Zscaler's Log Streaming Service (LSS), real-time user activity logs are forwarded directly into ExtraHop sensors, where they are automatically correlated with observed network telemetry.

This synergy enriches high-fidelity NDR detections with essential identity metadata, such as authenticated usernames and device posture details. The result is the ability to enrich end-to-end Layer 2 through Layer 7 visibility for all user-to-application communications, even when traffic is tunneled or proxied. Security analysts no longer need to perform tedious manual lookups to identify the true origin of a network flow. Instead, they receive a unified, forensic-ready view that maps malicious behavioral patterns directly to specific users and devices.

This integration strengthens a Zero Trust architecture by providing the continuous monitoring and deep packet-level insights required to validate access policies and respond to sophisticated internal threats instantly.

Key Use Cases

Detecting Lateral Movement	Identify adversaries attempting to scan internal resources or access sensitive databases by unmasking the true origin of east-west traffic. By correlating network flows with identity metadata, RevealX uncovers attackers who try to expand their footprint while hidden within ZPA-proxied traffic streams.
Rapid Incident Forensics	Accelerate investigations by viewing authenticated usernames and device IDs directly alongside network-level behavioral detections. Analysts can see past the App Connector to identify exactly which user account initiated a suspicious transaction, reducing forensic lookup times from hours to seconds.
Zero Trust Policy Validation	Verify that ZPA access policies are correctly segmenting the network and identify unauthorized communications that bypass intended controls. RevealX provides the behavioral insights needed to create more granular policies and identify misconfigurations that leave private applications exposed.

RevealX + Zscaler Internet Access (ZIA) Integration

THE CHALLENGE

Protecting internet-bound and SaaS traffic with Zscaler Internet Access (ZIA) is essential for modern workforces, yet using it as a standalone silo creates significant operational hurdles for Security Operations Centers (SOC). One major challenge is the disconnect between external web activity and internal network behavior. When ZIA operates independently, there is no automated way to correlate a user's internet-bound actions with their east-west communications inside the data center.

This fragmentation leads to siloed data analysis, where security teams fail to see the complete progression of a multi-stage attack. Furthermore, the lack of real-time integration with internal network sensors prevents organizations from responding quickly to high-risk detections. For instance, if an internal device is identified as compromised by an NDR platform, the process for blocking its outbound web access at the cloud edge typically remains a slow, manual task.

This delay provides attackers with a window of opportunity to connect with command-and-control servers or exfiltrate sensitive data.

THE SOLUTION

The integration of ExtraHop RevealX with Zscaler Internet Access (ZIA) establishes an automated defensive loop, connecting internal network intelligence with cloud-delivered security. RevealX uses Zscaler's Nanolog Streaming Service (NSS) to ingest traffic data, correlating anomalous internal behaviors (like data staging) with suspicious external activities (such as uploads or downloads).

This unified intelligence helps security teams identify threats across the entire kill chain, from initial web access to internal lateral movement. Crucially, the integration enables automated response orchestration via Zscaler's Cloud Firewall APIs. When RevealX detects a high-severity threat, including ransomware or data exfiltration, it instantly triggers ZIA policies to isolate the compromised device at the cloud edge. This automated containment prevents malicious communications in seconds, even outside business hours, removing the need for manual analyst intervention.

Centralizing these controls allows organizations to reduce operational complexity and maintain a resilient, proactive security posture globally.

Key Use Cases

Exfiltration and Shadow IT Discovery	Correlate anomalous internal data staging detected by RevealX with unauthorized SaaS uploads logged by ZIA. This unified view helps security teams detect "low and slow" data exfiltration and identifies risky usage of unsanctioned cloud applications before a major breach occurs.
Performance Root-Cause Analysis	Pinpoint whether application latency originates at the endpoint, the local network, the Zscaler cloud, or the SaaS provider itself. By correlating RevealX round-trip time metrics with ZIA performance logs, IT teams can resolve distributed application issues with unprecedented precision.

Solution Component Deep Dive

The unified architecture establishes an end-to-end telemetry loop between the endpoint, the Zscaler Zero Trust Exchange, and ExtraHop sensors. When a user initiates a connection via the Zscaler Client Connector, traffic is routed to ZIA Public Service Edges for internet access or ZPA App Connectors for private applications.

Simultaneously, Zscaler's Log Streaming Service (LSS) pushes identity-rich metadata to ExtraHop sensors. RevealX correlates this with raw network packets to provide high-fidelity behavioral analysis. Upon detecting a threat, RevealX uses its REST API to communicate with the Zscaler Cloud Firewall API, dynamically updating policies to contain the offending device at the edge. This closed-loop system ensures that visibility directly informs control, automating the path from detection to defense.

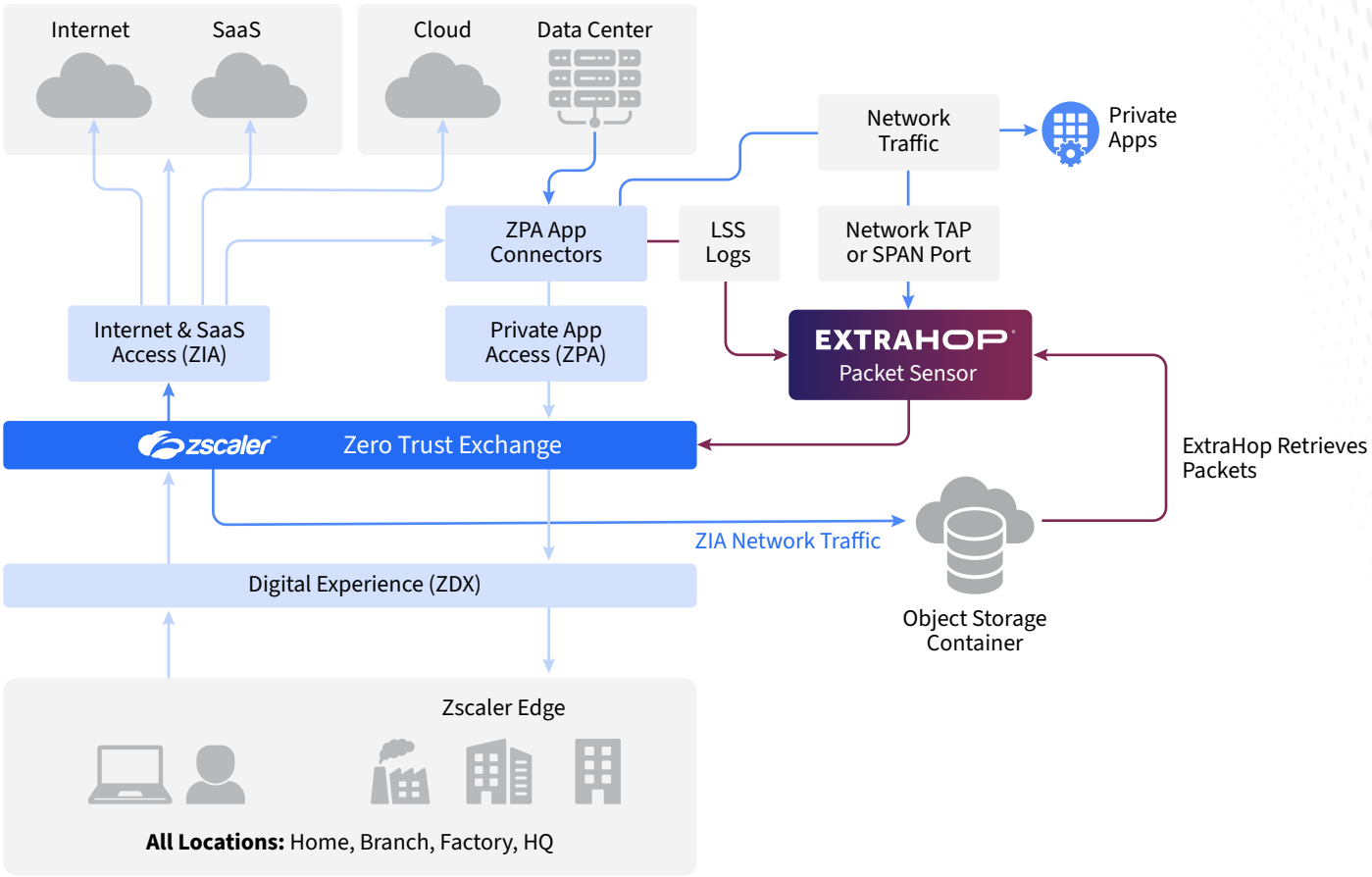

Figure 1: Reference architecture for integrating Zscaler's ZIA and ZPA with ExtraHop RevealX sensors

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 and resolve performance issues to ensure availability and performance, and improve the overall user experience.

> "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 defense and strengthen zero trust."

KANAIYA VASANI
Chief Product Officer
ExtraHop

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com