JOINT SOLUTION BRIEF

zscaler + Exaforce

Complete correlated context across network, identity, endpoint, email, cloud, and SaaS to deliver true XDR.

INTEGRATION HIGHLIGHTS

- ✓ Correlates Zscaler network telemetry with identity, endpoint, email, cloud, and SaaS signals for true XDR.
- ✓ Enriches Zscaler detections with complete user and device context to reveal full attack stories.
- ✓ Accelerates investigations with unified visibility and AI-driven triage across all data sources.

The Market Challenge

Modern enterprises generate massive volumes of network, identity, endpoint, email, cloud, and SaaS signals, but these insights are often spread across disconnected tools. Security teams struggle to connect related events, determine user intent, and distinguish real threats from normal activity. A spike in downloads, a phishing attempt, an unusual login, or a blocked URL often lacks the identity, device, and behavioral context needed to understand what actually happened. Without correlated telemetry, investigations slow down, attack visibility remains fragmented, and critical risks can be missed.

Organizations need AI-powered security operations that unify all signals and automatically correlate network activity with identity and cross-platform behavior. By turning raw telemetry into clear, actionable intelligence, teams can accelerate investigations, gain complete visibility, and respond to threats with greater speed and confidence.

The Solution

Zscaler and Exaforce combine network, identity, endpoint, email, cloud, and SaaS visibility into a single correlated view. Zscaler provides rich real-time network telemetry, while Exaforce ingests and enriches this data with user identity, device posture, behavioral patterns, and cross-platform detections. All relevant signals are automatically merged into one coherent investigation so analysts see the entire story without searching across tools or stitching together isolated alerts.

AI-driven correlation transforms raw telemetry into complete and actionable threat narratives. In a phishing scenario, analysts can instantly see whether the user clicked the link, how many others engaged with it, whether any related endpoint detections occurred, and what critical SaaS applications the user accessed and what they did inside them. Each alert presents the full set of associated activity in one place, enabling faster understanding, fewer missed connections, and more confident response.

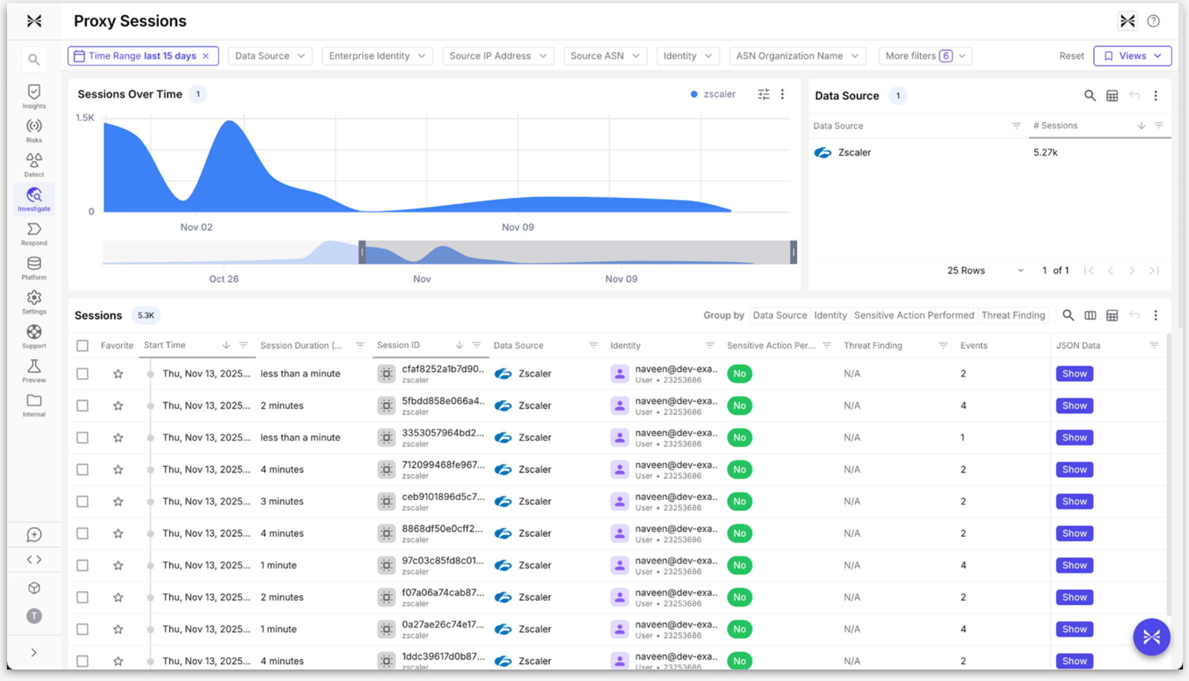
Together, Zscaler and Exaforce deliver a comprehensive XDR solution that provides fast and secure access to the internet, SaaS, and private applications while ensuring complete visibility, intelligent threat detection, and automated response.

Solution Components Deep Dive

Exaforce adds an AI-driven security operations layer to Zscaler, enabling security teams to automatically triage, investigate, and respond to threats across ZIA, endpoints, and email without manual correlation or context-switching.

Exaforce continuously ingests Zscaler telemetry (URL requests, policy actions, SSL inspections, and admin audit logs), normalizes it into a universal schema, and enriches events with identity, device, and behavioral context. The platform's agentic AI consolidates related ZIA events into single investigations and surfaces high-fidelity threats that demand attention.

For example, when ZIA blocks a suspicious URL, Exaforce automatically correlates the event with endpoint detections and phishing emails targeting the same user, building a complete attack narrative in seconds. By consolidating all relevant signals into a single investigation, Exaforce ensures analysts have immediate clarity without searching across platforms or piecing together isolated events.



Data Source	# Sessions
Zscaler	5.27k

Favorite	Start Time	Session Duration (...	Session ID	Data Source	Identity	Sensitive Action Per...	Threat Finding	Events	JSON Data
☆	Thu, Nov 13, 2025...	less than a minute	cfaf8252a1b7d90.. zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show
☆	Thu, Nov 13, 2025...	2 minutes	5fbdd858e066a4.. zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	4	Show
☆	Thu, Nov 13, 2025...	less than a minute	3353057964bd2... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	1	Show
☆	Thu, Nov 13, 2025...	4 minutes	712099468fe967... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show
☆	Thu, Nov 13, 2025...	3 minutes	ceb9101896d5c7... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show
☆	Thu, Nov 13, 2025...	4 minutes	8868df50e0cff2... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show
☆	Thu, Nov 13, 2025...	1 minute	97c03c85fd8c01... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	4	Show
☆	Thu, Nov 13, 2025...	2 minutes	f07a06a74cab87... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show
☆	Thu, Nov 13, 2025...	1 minute	0a27ae26c74e17... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	4	Show
☆	Thu, Nov 13, 2025...	4 minutes	1ddc39617d0b87... zscaler	Zscaler	naveen@dev-exa.. User • 23253686	No	N/A	2	Show

KEY USE CASES

Accelerated Triage, Investigation, and Response

Security teams can rapidly understand the full scope of an alert by combining Zscaler network telemetry with identity, endpoint, email, and SaaS activity in a single correlated view. Analysts immediately see who triggered the event, what actions occurred before and after, and whether related signals point to escalation or lateral movement. AI-based correlation removes manual searching and reduces false positives, enabling teams to validate severity, determine impact, and take decisive response actions in significantly less time.

Insider Threat Detection and Data Loss Prevention

By fusing network signals with identity attributes, device posture, and SaaS activity, analysts can quickly identify patterns indicative of insider threats or high-risk data handling. Correlated insights reveal anomalous file access, suspicious SaaS downloads, privilege misuse, or attempts to exfiltrate sensitive data across sanctioned and unsanctioned channels. With complete cross-platform context, teams can distinguish legitimate user behavior from potential data theft and respond with targeted controls before material loss occurs.

> **By combining Zscaler's rich network telemetry with Exaforce's cross-platform context, we give security teams a complete and correlated view of every event and incident. This partnership dramatically accelerates how analysts investigate and respond to threats.**
>
> **Ariful Huq**
>
> Co-Founder and Head of Product, Exaforce

Zscaler + Exaforce Benefits

ACTION	DESCRIPTION
Integrate Zscaler Telemetry	Automatically ingest and normalize Zscaler network activity, policy actions, and threat signals to form the foundation of a complete, correlated investigation.
Enrich with Cross-Platform Context	Combine network data with identity, endpoint, email, cloud, and SaaS signals to deliver full user and device context that clarifies intent and reveals the true scope of any incident.
Accelerate Investigation and Response	Use AI-driven correlation and guidance to surface high-fidelity threats, reduce manual analysis, and enable analysts to make confident decisions in significantly less time.
Hunt external and insider threats using natural language	Search months of Zscaler and related data using plain English queries like "show risky file-movement patterns for this user" to speed threat investigations without complex filters or engineering support.

Conclusion

Zscaler and Exaforce together deliver a true XDR solution that unifies network, identity, endpoint, email, cloud, and SaaS signals into a single correlated view. By automatically enriching Zscaler telemetry with deep cross-platform context, the joint offering removes blind spots, accelerates investigations, and helps analysts understand the full impact of an incident without searching across tools. AI-driven correlation, complete context, and unified threat stories enable security teams to make faster, more confident decisions and strengthen their overall security posture.

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.