Exaforce

zscaler

EXAFORCE AND ZSCALER

Continuous investigation and governed response across users, applications, and data

SOLUTION BRIEF

The Challenge

Zscaler gives security teams deep visibility and strong enforcement across internet access, private applications, and sensitive data. As security environments grow, that activity becomes part of a broader picture spanning identities, endpoints, email, SaaS, and cloud. The SOC must connect those signals quickly to determine whether activity is isolated, part of a wider attack, or evidence of data loss.

When context is distributed across multiple tools, investigations take time and high-priority threats can remain buried in the queue. Security teams need a faster way to connect Zscaler activity to the broader attack chain, reach a defensible verdict, and take the right action.

The Solution

Exaforce extends the value of Zscaler by turning its rich activity and policy context into investigation-ready security outcomes. It brings ZIA and ZPA logs and configuration, together with DLP activity (Endpoint and Inline), into a unified security view and correlates them with signals from across the security stack.

Zscaler remains the zero-trust control and enforcement layer. Exabots continuously triage activity, reconstruct the attack chain, and explain what happened, why it matters, and what should happen next. Analysts receive prioritized, evidence-backed incidents that are ready to review and act on, with governed response through approved Zscaler controls.

KEY HIGHLIGHTS

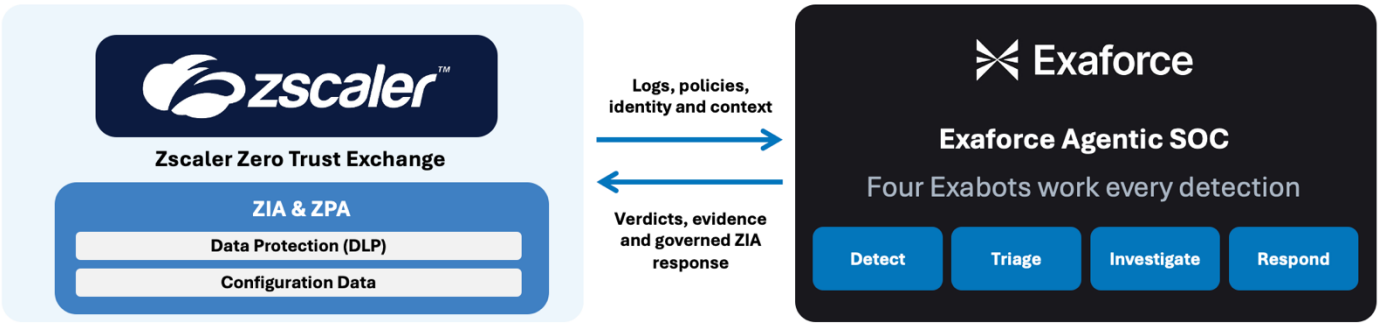
- **24/7 triage across ZIA, ZPA, DLP (Inline and Endpoint)**
- **One attack chain across user, device, application, policy, and data activity**
- **Natural-language investigation across Zscaler and connected security telemetry**
- **Configuration posture and threat detections from Zscaler data**
- **Governed ZIA response through URL policy and PAC controls**

Key Use Cases

USE CASE	SOLUTION	BENEFITS
Compromised user and session investigation	Correlate ZIA Web, Admin Audit, Firewall, and DNS activity with ZPA user, browser, and application events plus identity and endpoint evidence to reconstruct one session and attack chain.	Identify who acted, what they accessed, where activity originated, and whether it is isolated or part of a broader compromise.
Endpoint and Inline data-loss investigation	Ingest DLP sensitive-activity and incident logs, including file movement, printing, removable media, network shares, and personal cloud, then connect them to the user, device, session, and related ZIA and ZPA activity.	Prioritize high-risk exfiltration attempts and reduce manual pivots across DLP, endpoint, identity, and network tools.
Behavior-Driven Insider Risk Response	Continuously analyze employee file-access behavior for meaningful deviations to trigger Zscaler Remote Browser Isolation for designated high-value applications and data.	Limit insider-driven data exfiltration in real time while preserving complete session recordings for security, HR, and legal review.

How it Works

The Integration At-a-glance



Operational Outcomes

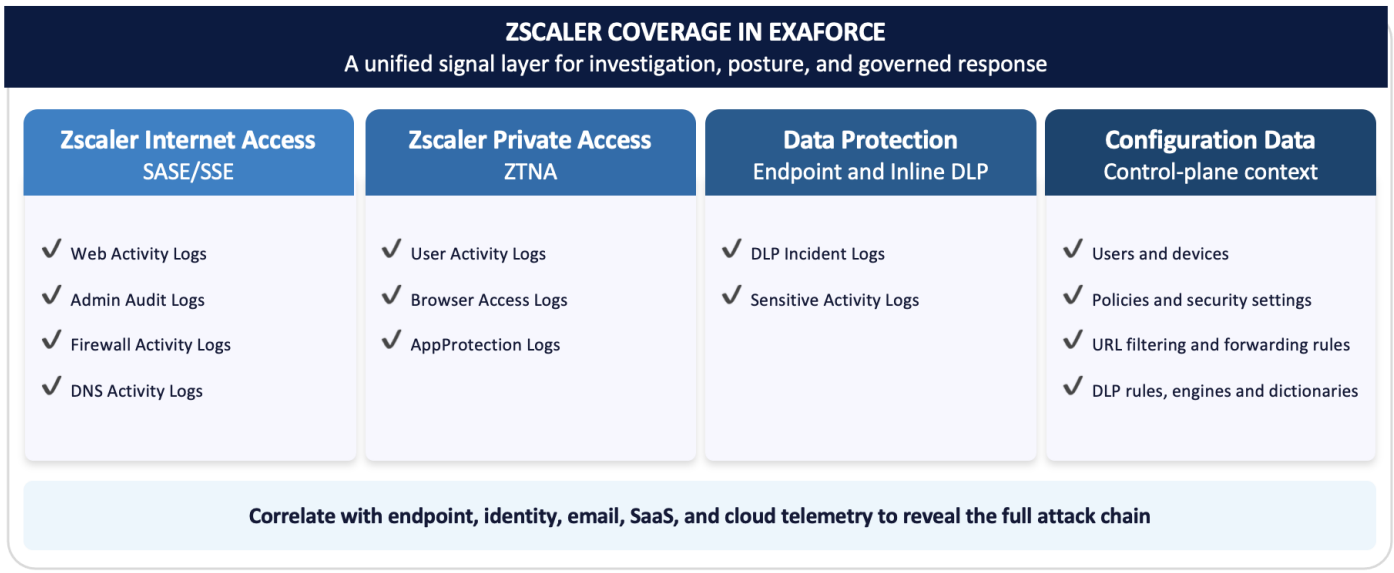
ZIA VISIBILITY
Web, Admin Audit, Firewall, DNS, and Endpoint DLP logs

ZPA VISIBILITY
User Activity, Browser Access, and AppProtection logs

CONFIG POSTURE
users, devices, policies, controls, and DLP settings

GOVERNED RESPONSE
approved ZIA URL policy and PAC actions

Exaforce connects to Zscaler APIs and customer-configured log streaming. ZIA and ZPA activity flows into Exaforce, while scheduled API collection adds the configuration, identity, policy, and posture context surrounding it. Exaforce maps those signals to the users, devices, sessions, applications, destinations, and controls involved, creating one investigation-ready view of the environment.



Zscaler activity and posture become one investigation-ready data layer in Exaforce.

Exaforce correlates Zscaler evidence with endpoint, identity, email, SaaS, and cloud sources to show the full attack chain and produce an evidence-backed verdict. Benign activity is closed with a clear rationale. Confirmed threats include timelines, root cause, blast radius, and recommended action. Under customer policy, Exaforce can block or allow a domain through ZIA URL policy, update a PAC profile to block a destination, or route consequential actions for human approval.

Integration in Action

When Endpoint DLP flags unusual movement of sensitive data, Exaforce immediately connects the event to the user, device, ZIA and ZPA sessions, and related activity. Analysts can ask follow-up questions in natural language at any point.

10:14:00

- Endpoint DLP records a high severity attempt to upload a sensitive finance file to a personal cloud account.
- Exaforce maps the event to the user and device, the triggered DLP rule, file hash, destination, and recent access history.
- ZPA shows finance-application access minutes earlier, while ZIA shows a new personal-cloud destination from the same session. Exaforce connects the sequence with endpoint and identity evidence.
- A true positive, high confidence: attempted data exfiltration using a compromised user session, with the affected data, user, device, destination, and root cause linked.
- Under policy, Exaforce blocks the destination through ZIA URL policy and surfaces the evidence for analyst review.
- The analyst asks, “What other sensitive files did this user access, and from which applications?” Exaforce returns an evidence-linked answer in seconds.

10:19:00

- With wider data-loss risk, Exaforce recommends an organization-level PAC block and routes it to the on-call analyst for approval.

From fragmented zero trust signals to one high-confidence decision, without the manual pivots.

About Exaforce

Exaforce delivers an agentic SOC platform that helps security teams detect, triage, investigate, hunt, and respond to threats with greater speed and consistency. Its task-specific Exabots operate on a shared reasoning foundation and a unified, real-time view of the environment, enabling transparent, evidence-linked decisions across the full SOC lifecycle. Exaforce is available as a SaaS platform. The platform is designed for strong tenant isolation and enterprise security requirements, with support for SOC 2, HITRUST, HIPAA, ISO 27001, PCI DSS, and GDPR compliance. Read our customer case studies, explore the platform, or learn more at exaforce.com

About Zscaler

Zscaler (NASDAQ: ZS) helps organizations securely connect users, devices, applications, and workloads through the cloud-native Zscaler Zero Trust Exchange. Built on zero trust principles, the platform protects against cyberthreats and data loss while enabling fast, secure access to internet, SaaS, and private applications. Learn more at zscaler.com.

See Exaforce + Zscaler in action

See how Exaforce turns Zscaler telemetry into continuous, evidence-linked investigation and governed response. Visit **exaforce.com** or scan the code to request a demo.

© 2026 Exaforce, Inc. Zscaler, ZIA, ZPA, and related marks are trademarks of Zscaler, Inc. Capabilities depend on customer licensing and configuration. The investigation example and timings are illustrative.

exaforce.com