SOLUTION BRIEF

Zscaler Threat Hunting

Uncover advanced attacks to prevent breaches

Adversaries weaponize trusted traffic to evade controls

The modern threat landscape is defined by advanced persistent threats (APTs), living-off-trusted-sites (LOTS) tactics, and AI-accelerated attacks that blend into legitimate network traffic. Meanwhile, SOC teams face significant obstacles to uncovering those threats:

- **Limited staffing forces teams into reactive fire drills, leaving them buried in alert noise**
- **Limited threat hunting expertise makes it difficult to separate true threats from benign activity**
- **High SIEM ingestion costs restrict access to the zero trust telemetry essential for modern hunts**

SOCs must move beyond reactive triage to proactively uncover hidden adversaries, eliminate network blind spots, and disrupt attacks before business impact.

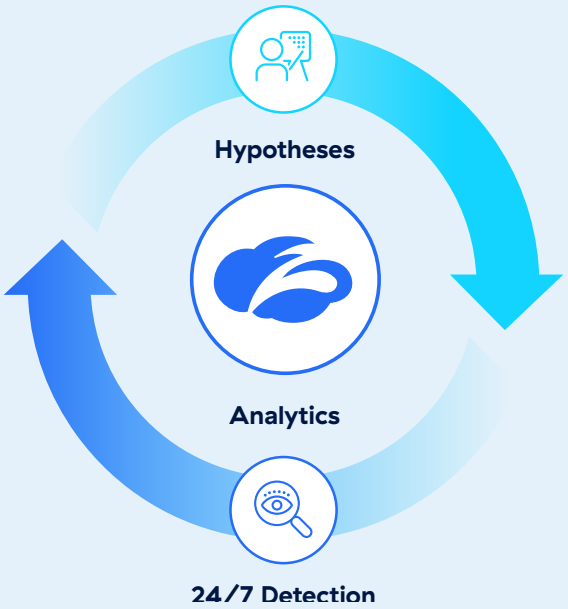
Proactive, expert-led threat hunting across global Zero Trust telemetry

Zscaler Threat Hunting delivers continuous, expert-led hunting across the world's largest security cloud to neutralize hidden threats early in the attack lifecycle.

Our elite threat hunters analyze data from **over 750 billion daily transactions across the Zscaler Zero Trust Exchange™**, using custom AI/ML detection models and proprietary ThreatLabz intelligence to expose evasive adversaries, LOTS tactics, and active Command and Control (C2) channels before they reach endpoints.

Rather than flooding teams with raw telemetry or unvetted alerts, Zscaler Threat Hunting distills complex traffic into high-fidelity, human-verified findings—enabling SOCs to execute closed-loop containment at machine speed without adding headcount or SIEM storage overhead.

ZSCALER THREAT HUNTING



Sample threats identified:

- **Nation-state footprint**
- **AI model impersonation**
- **APT impersonation of legit drivers**

©2026 Zscaler, Inc. All rights reserved.

24x7 Hunting for Hidden Threats

Raw Logs	Enrichment	AI and ML	Detection Engineering	Threat Hunting	Hunt Findings
Your ZIA telemetry	ThreatLabz intelligence and 40+ third-party threat intel fields	Continuously refined detection models	Expert-crafted hunting playbooks	In-house expertise	Evidence, IOCs, and recommended actions

UNCOVER ADVANCED ATTACKS

Our team finds hidden adversaries and sophisticated attacks lurking in allowed traffic before they cause damage.

- Gain hunting across ZIA telemetry using custom AI/ML models and ThreatLabz intelligence to detect APTs and nation-state actors.
- Get real-time visibility into unsanctioned GenAI tools, shadow IT, and hidden data exfiltration in encrypted traffic.

STOP THREATS EARLY

We disrupt attacks in internet and SaaS traffic before they reach endpoints or propagate across your environment.

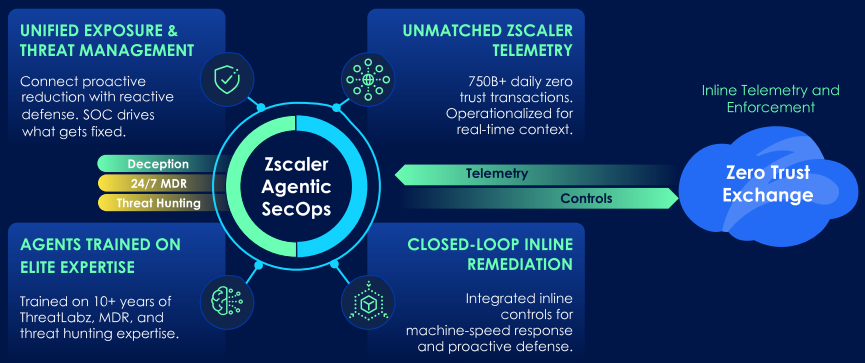
- Intercept threats during reconnaissance and initial access, often before endpoints are compromised.
- Expose Living off Trusted Sites (LOTS) tactics, evasive C2 channels, and insider threats that would otherwise go undetected.

MAXIMIZE ZSCALER VALUE WITHOUT ESCALATING SIEM COSTS

Add deep threat detection in your ZIA telemetry without the cost of SIEM data ingestion.

- Get native analysis of web and cloud traffic natively, eliminating log ingestion and storage costs.
- Turn existing ZIA log data into a zero-touch, proactive threat hunting operation that maximizes your security ROI while saving staff time.

INTRODUCING ZSCALER AGENTIC SECOPS A UNIFIED PLATFORM PURPOSE-BUILT FOR MODERN AI-DRIVEN SECURITY OPERATIONS



Learn more at zscaler.com/threathunting

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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com