DATA SHEET

Zscaler Threat Hunting

Hunt. Detect. Defend.

Uncover and defend against covert, sophisticated attacks to prevent potential breaches.

The Security Challenge

Constantly evolving threats and alert fatigue: Adversaries—particularly advanced persistent threats (APTs)—evolve on a daily basis. The MITRE ATT&CK framework has more than 190 techniques and 385 sub-techniques. Because of the high volume of breaches globally and the ever-changing threat landscape, your organization constantly faces evolving attacker techniques. The high volume of alerts often exhausts defenders and leads to indicators of compromise being overlooked.

Threat intelligence overload: With an endless amount of threat intelligence available from countless sources, defenders are often unable to distill it into actionable insights to detect sophisticated attacks.

Talent shortage: Amid the ongoing global security talent crunch, defenders are overwhelmed and overworked, even though they are armed with more tools and telemetry than ever before.

Lagging threat identification: It takes an average of 212 days for organizations to identify a security incident, during which untold damages can occur. Even dedicated threat hunting teams typically focus only on endpoint data, guaranteeing that they will only discover internet-borne threats after they've already gained access to your infrastructure.

Not every threat is equal and not every attack vector is relevant, so what should your defenders focus on? How do you keep your defense proactive when you have personnel constraints? And how do you ensure everyone, from your junior analysts to your purple team, is working in lockstep on threat defense initiatives that have the highest impact?

Zscaler Threat Hunting Service

Discover the power of Zscaler Threat Hunting™: round-the-clock expert-led hunting for anomalies, sophisticated threats, and elusive threat actors who work to evade traditional security measures. Using data from the Zscaler Zero Trust Exchange™, the world's largest security cloud, the Zscaler Threat Hunting team leverages its diverse expertise and custom machine learning models to proactively seek out, analyze, and neutralize threats. With our cloud native platform monitoring more than 400 billion daily transactions and our in-house ThreatLabz research team equipped with top-tier private threat intelligence on more than 200 threat groups, Zscaler Threat Hunting works every hour of every day to help your SOC achieve its security goals.

Key Benefits:

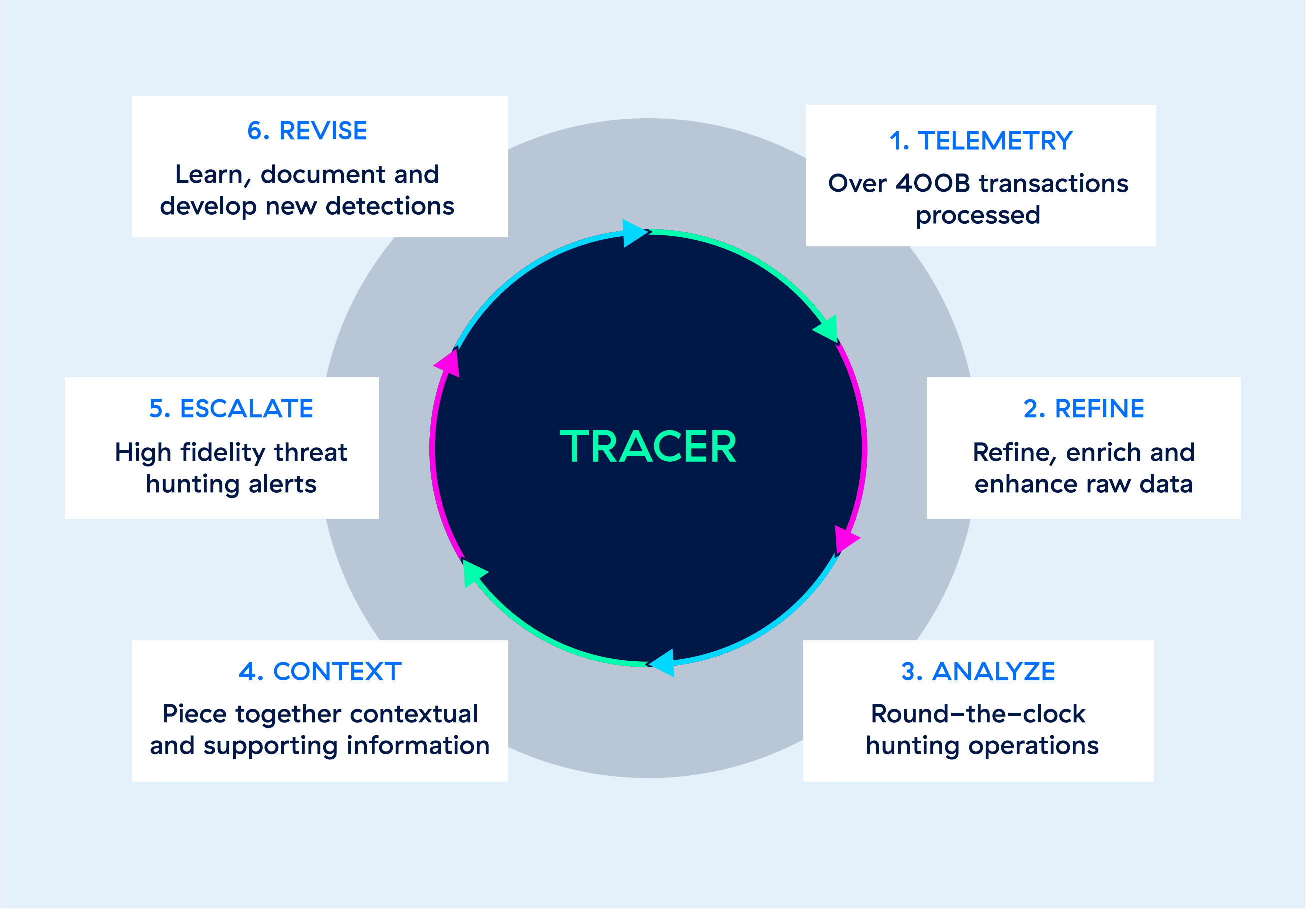
- **Hunt and detect advanced threats**
  Zscaler Threat Hunting combats threats with precision, accuracy, and speed like never before. Our mission is to disrupt advanced threats by harnessing the diverse expertise of our human-driven hunt team, all powered by the unparalleled Zscaler platform. Reduce both dwell time and impact through proactive hunting.
- **Augment your SOC and IR team—our experts are your experts**
  Significantly reduce alert fatigue as our proprietary tooling and 24/7 hunting team distill billions of raw transactions into context-rich alerts, extracting the most actionable insights for SecOps.
- **Stop threats early in the attack chain**
  By analyzing internet and SaaS traffic rather than endpoint data, Zscaler Threat Hunting can detect and disrupt attacks sooner, often before they've gained access to your endpoints and caused damage.
- **Get an enterprise-level experience, designed for you**
  Upgrade to the Zscaler Threat Hunting Advanced service for tailored threat hunting solutions that adapt to your unique business challenges. Designed for industry leaders in need of customized hunting strategies, Zscaler Threat Hunting Advanced offers personalized onboarding, strategic briefings, tactical reports, and ongoing threat hunting support. Elevate your security with a trusted partner focused on your organization's success.

Zscaler Threat Hunting Methodology

The best signal powers the best response. The Zero Trust Exchange platform brokers all connections between users, resources, and destinations, giving Zscaler unrivaled visibility. Zscaler Threat Hunters collect, correlate, and hunt across the entire global Zscaler install base, providing the cloud-scale telemetry needed to identify and defend against emerging threats, exploits, and attack tactics.

The Zscaler Threat Hunting framework merges zero trust principles, threat intelligence focus, hypothesis testing, and playbooks for effective threat hunting. Honed by years of hands-on experience and tuned for the latest threats, our framework equips organizations to combat evolving threats with precision and speed. Our approach is both flexible and scalable, offering battle-tested processes to identify and defend against cyberthreats efficiently. Through a blend of human expertise and cutting-edge AI, our hunting methodology ensures thorough threat detection. With a focus on adaptability and efficiency, our hunting framework is designed to tackle the dynamic threat landscape head-on.

TRACER: The Zscaler Threat Hunting Methodology
TRACER, an acronym for “Telemetry, Refine, Analyze, Context, Escalate, and Revise.


6. REVISE
Learn, document and develop new detections
1. TELEMETRY
Over 400B transactions processed
5. ESCALATE
High fidelity threat hunting alerts
TRACER
2. REFINE
Refine, enrich and enhance raw data
4. CONTEXT
Piece together contextual and supporting information
3. ANALYZE
Round-the-clock hunting operations

- **Telemetry:** Zscaler Threat Hunters gain unparalleled real-time visibility from the best-in-class Zscaler Secure Web Gateway (SWG), which processes more than 400 billion daily transactions
- **Refine:** With the help of AI, Zscaler Threat Hunters refine, enrich, and enhance the billions of transactions with threat intelligence, leveraging custom tools and threat hunting playbooks to detect threat actors attempting to blend in with legitimate network traffic
- **Analyze:** Zscaler Threat Hunters zoom in and out of different enriched data views, conducting round-the-clock structured, unstructured, and situational hunting operations
- **Context:** To transfer knowledge to your SOC/IR team, Zscaler Threat Hunters piece together contextual information and supporting information
- **Escalate:** Once all relevant information and intelligence has been stitched together, a Zscaler Threat Hunter escalates actionable alerts to your SOC/IR team
- **Revise:** Hunters learn, document, and develop new playbooks that enhance Zscaler products and our threat hunting efficiency

Zscaler Threat Hunting Advanced

Take your security to new heights with Zscaler Threat Hunting Advanced, where personalized threat hunting meets expert advisory, and where your peace of mind is our highest priority.

This elevated service assigns a designated threat hunter to craft a defense strategy specifically and exclusively for your organization. Your designated threat hunter is your strategic partner, customizing playbooks and actively identifying digital threats on your behalf.

Zscaler Threat Hunting Advanced Features

- **Designated threat hunter:** Your personal liaison with the Zscaler Threat Hunting service ensures an enhanced experience.
- **Tailored recommendations and contextual information:** Tailored guidance and contextual information enhance your understanding of how to hunt for threats targeting your organization.
- **Actionable emerging threat reports:** Stay ahead of the game by learning how to proactively hunt for the next emerging threat.
- **Laser-focused tailored threat hunting:** Optimize the effectiveness of the Zscaler Threat Hunting service with a customized approach to hunting operations.
- **Comprehensive tactical reporting:** Gain in-depth insights into hunting operations, specifically designed for SOC analysts, hunters, and incident responders.
- **Strategic hunting reviews:** Get quarterly executive presentations and monthly technical reports summarizing Zscaler Threat Hunting operations. Align security priorities and gain industry-specific threat hunting insights.
- **Verification hunts:** Verify your security posture and gain peace of mind with hunting reassurance from your designated threat hunter.
- **Enhanced environment understanding:** Leverage your threat hunter's profound understanding of your environment to identify and neutralize threats quickly.
- **Early access to hunting patterns and features:** Collaborate with your threat hunter to gain early access to new hunt patterns and feature releases for advanced threat detection.

Zscaler Advanced delivers the next level of tailored, strategic, consultative threat hunting

	Zscaler Threat Hunting Essentials	Zscaler Threat Hunting Advanced	Zscaler Threat Hunting Advanced Dedicated
24/7/365 Threat Hunting Operations	Global Hunt Team	Global Hunt Team + Advanced Hunt Team	Global Hunt Team + Advanced Hunt Team + Dedicated Hunter
Tailored Threat Hunting	–	✓	✓
Technical Threat Hunting Reports	–	Monthly	Weekly
Executive Hunting Presentation	–	Quarterly	Quarterly (in person)
Rich Hunting Insights from the Front Line	–	✓	✓
Emerging Threats	Continuous Hunting	Proactive Email	Proactive Phone Call
Hunting Playbooks	Essentials	Advanced	Custom
Early Access to New Behavioral Analytics and Hunt Patterns	–	✓	✓
Access to Early Release Features	–	✓	✓

Get Started

Talk to your Zscaler representative today or email zth-sales@zscaler.com to learn more about Zscaler Threat Hunting and schedule a complimentary proof-of-value.

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**.