

Zscaler Threat Hunting

Uncover and defend against advanced attacks to prevent breaches



AT-A-GLANCE

Today's Security Challenges

The modern security landscape is characterized by relentlessly evolving threats from advanced persistent threats (APTs), leading to an overwhelming volume of alerts and lagging or unvetted threat intelligence that cripples security teams with severe alert fatigue. Compounded by a global talent shortage, this environment results in overworked personnel and a significant delay in incident identification, averaging over 200 days. This prolonged detection gap significantly increases both the dwell time and the overall impact of a breach on the organization.

Zscaler Threat Hunting as a Service

Discover the power of Zscaler Threat Hunting: continuous, 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, our threat hunting team leverages its diverse expertise, proprietary tooling, and custom machine learning and AI models to proactively seek out, analyze, and neutralize threats. By analyzing internet and SaaS traffic, Zscaler Threat Hunting identifies and disrupts attacks early in the kill chain, often before they have gained access to your endpoints.

With our cloud-native platform monitoring more than 500 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 continuously works to help your SOC achieve its security goals.

Key Benefits

- **Hunt and detect advanced threats**
Disrupt advanced threats using our expert-led hunt team and the Zscaler platform
- **Augment your SOC and IR teams**
Reduce alert fatigue as our global team distills billions of transactions into context-rich alerts
- **Stop threats early in the attack chain**
Detect and disrupt attacks in internet and SaaS traffic before they reach your endpoints

What's Included

- Point-in-time hunts for threats related to current events and emerging threats
- Continuous monitoring and threat detection coverage from Zscaler Threat Hunting-developed detections

Learn More

Contact your Zscaler representative today or email zth-sales@zscaler.com.