SOLUTION BRIEF

Zscaler™ Insight

zscaler™

The industry's only managed detection and response service powered by cutting-edge active defense technology and threat intelligence from the world's largest security cloud.

The challenge

As sophisticated attacks continue to escalate in scope, volume, and impact, defenders are at a significant disadvantage. Despite more investment in cybersecurity than ever before, the proliferation of alerts generated by disjointed point products–compounded by a lack of skilled experts–has become a barrier to effective operations, making it impossible to separate the signal from the noise to identify attacks before they can impact business operations. The outcomes are clear: alert fatigue, missed threats, and blind spots, resulting in successful cyberattacks ranging from ransomware and large-scale data theft to software supply chain compromises.

Introducing Zscaler Insight

To defeat modern adversaries and holistically reduce business risk, a different approach is needed. Zscaler Insight rebalances the attack equation in favor of defenders by bringing white-glove level expert threat hunting, investigation, response, and best practices review services to every aspect of the Zscaler Zero Trust Exchange. Leveraging your Zscaler estate, our ThreatLabz experts deliver:

- Tailored cyberthreat awareness and risk briefings: stay ahead of emerging campaigns and tactics with continuous updates on your local threat environment and attacks targeting your industry peers.
- In-depth posture assessment and hardening guidance: constantly improve your risk posture with guidance on Zscaler policy best practices based on your personal threat environment, insight from the world's largest security cloud, and proactive hunting from ThreatLabz.
- Turn your enterprise into a hostile environment for attackers with integrated active defense: immediately detect active attacks with dissolvable decoys that deliver high-fidelity alerts, rich telemetry collection, and false attack paths.
- Continuous security monitoring and proactive hunting with full adversary context: continuous structured and unstructured hunting across your Zscaler environment identifies the most impactful threats with the intelligence needed to drive effective response.
- Expert-led response guidance: in the event of a security incident, get expert guidance on next steps to contain the attack and mitigate potential damage.

Benefits

- **Find and stop the most advanced, stealthy attacks:** get peace of mind with white-glove, proactive threat hunting from world-renowned Zscaler ThreatLabz experts to detect and prioritize the most advanced hidden attacks.
- **Reveal and contain active adversaries:** rapidly identify lateral movement with tightly integrated active defense technology to contain and respond to attacks in progress.
- **Rapidly adapt to prevent future threats:** reduce risk with tailored threat reports and best practices recommendations to improve your security posture and prevent future attacks.

Built on the world's largest security cloud

The best signal powers the best response. As the Zero Trust Exchange brokers all connections between users, resources, and destinations, our expert threat hunters have unrivaled visibility extending across more than 300 trillion signals and 150M+ unique threat events per day. All telemetry is collected, correlated, and made accessible to ThreatLabz experts across the entire global Zscaler install base, providing the cloud-scale telemetry foundation needed to identify and defend against emerging vulnerabilities, exploits, and attack tactics.

Powered by the world's premier cloud threat research team

Zscaler Insight is powered by ThreatLabz, which is composed of more than 100 global experts in threat research, adversary operations, malware reverse engineering, cyber espionage, and crimeware from diverse backgrounds in both public and private sectors. The team has access to proprietary tooling and ML-models to hunt for the telltale tactics, tools, and procedures of the most advanced adversary groups across our security cloud. As ThreatLabz is also responsible for the security of Zscaler's cloud platform, they have unique insight into the most effective operations and policies for the Zero Trust Exchange, giving you an unparalleled edge in hardening your security posture. As a seamless extension of your team, ThreatLabz acts as a force multiplier for your security operations.

Unrivaled insight paired with expert assistance

Boost your security posture with insights from a small number of highly actionable, contextualized incident reports with clear action plans to further improve your Zscaler policy. In addition to prioritizing the most impactful attacks, our primary goal is to help you continuously reduce business risk through:

- Near real-time alerting for critical threats with full adversary context.
- Quarterly threat briefings including in-depth reviews of your local threat landscape, industry attack trends, ransomware risk, and in-depth policy reviews and recommendations for Zscaler Internet Access, Zscaler Private Access, and Zscaler Cloud Protection.
- Direct access to experts for in-depth questions on attacks, campaigns, payloads, or defense and response strategies.

Outcomes

- **Prevent future attacks:** continuously improve your security posture with ongoing policy review and recommendations.
- **Relentless threat hunting:** act with confidence against emerging threats with clear, prescriptive alerting and reporting with full context.
- **Cutting-edge detection:** early access to new and experimental detection rules used by threat hunters to catch the most sophisticated attacks.
- **Shut down attacks:** tight integration with the Zero Trust Exchange enabling direct action to contain attacks.
- **Force multiplier for security operations:** ThreatLabz acts as a seamless extension of your team, adding threat hunting, investigation, and response expertise to organizations of any size.

About Zscaler
Zscaler accelerates digital transformation with its Zero Trust Exchange, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network. Learn more at zscaler.com or follow us on Twitter @zscaler.

Zscaler, Inc. 120 Holger Way | San Jose, CA 95134 | +1 408.533.0288

zscaler™
www.zscaler.com