SOLUTION BRIEF

Zscaler Deception

Get high-fidelity alerts about bad actors in your environment, right now.

Advanced Threat Actors Are Bypassing Your Traditional Defenses

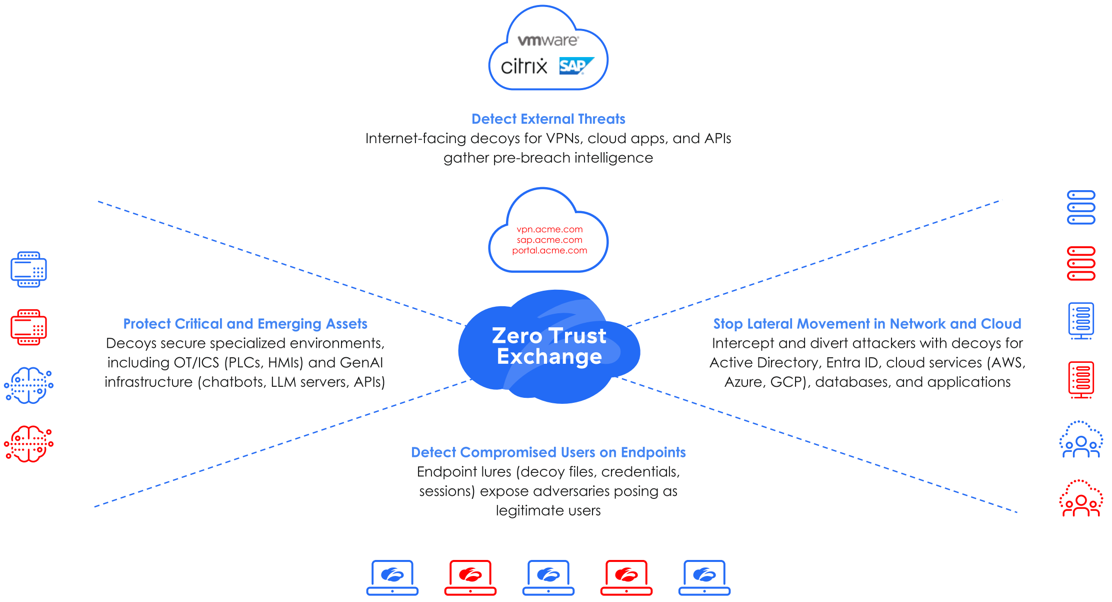
Today's security teams are inundated with a high volume of security events, and nearly half of all alerts are false positives. Sophisticated adversaries exploit this operational noise, using it as cover to conduct their initial breach. Their campaigns often begin by compromising a legitimate identity through stolen credentials. Because these attackers operate using a trusted identity's legitimate access, their activity is nearly indistinguishable from normal user behavior, allowing them to easily bypass traditional, signature-based security controls and gain an initial foothold completely undetected.

Once inside, the real attack begins. Threat actors leverage the poor visibility inherent in modern networks to move laterally, hunting for high-value targets. According to the IBM Cost of a Data Breach report, attackers can dwell in hybrid environments for an average of 276 days—a massive, undetected window to discover crown jewels, exfiltrate data, and ultimately deploy ransomware. This post-compromise threat surface is also rapidly expanding to include GenAI applications, with adversaries targeting LLMs with attacks like prompt injection and data poisoning. These novel attacks, hidden within benign text, are also designed to be invisible to legacy defenses, leaving security teams blind to critical stages of the attack kill chain.

Turn the tables on advanced attackers inside your network

Zscaler Deception is a threat detection platform delivered as part of the Zscaler Zero Trust Exchange. While tools like EDR and firewalls are designed to block initial attacks, Zscaler Deception specializes in exposing the post-compromise activity they miss—like attackers moving laterally with stolen credentials. Deception fills this critical gap, enabling organizations to detect compromised users, stop lateral movement, and defend against human-operated ransomware, hands-on keyboard threats, and malicious insiders.

Zscaler Deception places decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets:



Detect External Threats
Internet-facing decoys for VPNs, cloud apps, and APIs gather pre-breach intelligence

Protect Critical and Emerging Assets
Decoys secure specialized environments, including OT/ICS (PLCs, HMIs) and GenAI infrastructure (chatbots, LLM servers, APIs)

Stop Lateral Movement in Network and Cloud
Intercept and divert attackers with decoys for Active Directory, Entra ID, cloud services (AWS, Azure, GCP), databases, and applications

Detect Compromised Users on Endpoints
Endpoint lures (decoy files, credentials, sessions) expose adversaries posing as legitimate users

Why Zscaler Deception?

Stop lateral movement
Endpoint lures and application decoys are planted in the network to detect attackers attempting to move laterally and cut them off with containment actions.

Disrupt ransomware
Decoys placed across the environment detect and slow down ransomware at every stage of the kill chain and limit its blast radius.

Detect compromised users
Any use of decoy passwords, cookies, or sessions is a high-fidelity signal of compromise, as legitimate users have no reason to interact with them.

Secure your GenAI adoption journey
Detect attacks such as prompt injection, data poisoning, jailbreaking, adversarial suffixes, and training data extraction that target GenAI chatbots and LLM APIs.

Identify use of stolen credentials
Decoy web apps resembling vulnerable testbed applications and remote access services (like VPNs) intercept attackers attempting to log in.

Reduce Mean Time to Respond (MTTR)
Leverage zero trust network access enforcement policies and integrations with EDR, SIEM, SOAR tools to orchestrate response and contain threats.

Deploy in one click
Integrates with Zscaler Private Access (ZPA) to create, host, and distribute decoys with no additional VMs or hardware needed.

Establish an early warning system
Perimeter decoys detect stealthy pre-breach recon activities that often go unnoticed.

A Comprehensive Deception Portfolio

- **GenAI:** High-interaction GenAI decoys and decoy dataset files that mimic GenAI assets like chatbots, LLM servers, and APIs.
- **Threat intelligence:** Internet-facing decoys heuristically detect pre-breach threats that are specifically targeting your organization.
- **Endpoint:** A minefield for your endpoints, which includes decoy files, decoy credentials, decoy processes and more.
- **Cloud:** Decoy web servers, databases, file servers, and more that detect lateral movement in your cloud environments.
- **Application:** Server system decoys that host services like SSH and RDP, databases, file shares, and services on custom ports.
- **Active Directory:** Fake users in Active Directory that detect enumeration activity and malicious access.
- **OT/Industrial controls:** Decoys that replicate critical industrial assets (HMIs, PLCs, engineering workstations) to safely detect threats in SCADA and ICS environments without disrupting physical operations.

For more information, visit **zscaler.com/deception**

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**.

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