Zscaler Deception

Detect attacks that bypass existing controls

DATASHEET

Zscaler Deception is a deception-based threat detection platform delivered as part of the Zscaler Zero Trust Exchange. This integrated capability uses decoys/honeypots to detect advanced in-network threats that have bypassed existing defenses. Organizations use Zscaler Deception to detect compromised users, stop lateral movement, and defend against human-operated ransomware, hands-on keyboard threats, supply chain attacks, and malicious insiders.

Today's Top Security Challenges

1. **Compromised users:** With credentials being actively stolen using phishing attacks and kits from the dark web, identity compromise is a key challenge. Once attackers assume a trusted identity, they get the same access to IT assets as the identity they have compromised. The fact that the identity has legitimate access makes this kind of attack difficult to detect.

2. **Lateral movement:** Modern networks are extremely complex and provide limited visibility. Once attackers compromise a trusted identity, they leverage this lack of visibility to move laterally and find high-value targets to exploit. Attackers stay hidden in the network for an average of 280 days, making lateral movement the longest phase of an attack.

3. **Attacks against GenAI apps:**
Attackers are increasingly going after GenAI chatbots, GenAI applications, and LLM APIs with attacks including prompt injection, data poisoning, jailbreaking, adversarial suffixes, training data extraction, and more. These post-compromise attacks are difficult to detect using traditional threat detection controls and aid adversaries to move laterally, exploit GenAI infrastructure, and exfiltrate data.

> Enterprises use deception platforms to identify ransomware attacks during the initial access, which is quite early in the ransomware kill chain. The endpoint decoys detect any ransomware attack, such as attempts to encrypt files and credentials stealing across different stages of the ransomware kill chain, making it easier to prevent the endpoint against such attacks.
>
> GARTNER

What can Zscaler Deception do?

- **Detect pre–breach attacks**
  Get alerted when threat actors are scoping out your environment before mounting an attack. Block these threats and use telemetry to correlate the presence of attacker activity in your environment.

- **Detect compromised users**
  Decoy passwords, cookies, sessions, and bookmarks to decoy applications to detect compromised users when an attacker uses one of these deceptive assets.

- **Identity use of stolen credentials**
  Decoy web apps resembling vulnerable testbed applications and remote access services, like VPN, intercept attackers using stolen credentials to log in.

- **Detect privilege escalation**
  Detect and block adversaries that have compromised your environment and are now enumerating Active Directory to find high value targets for privilege escalation.

A 360° Approach To Targeted Threat Detection

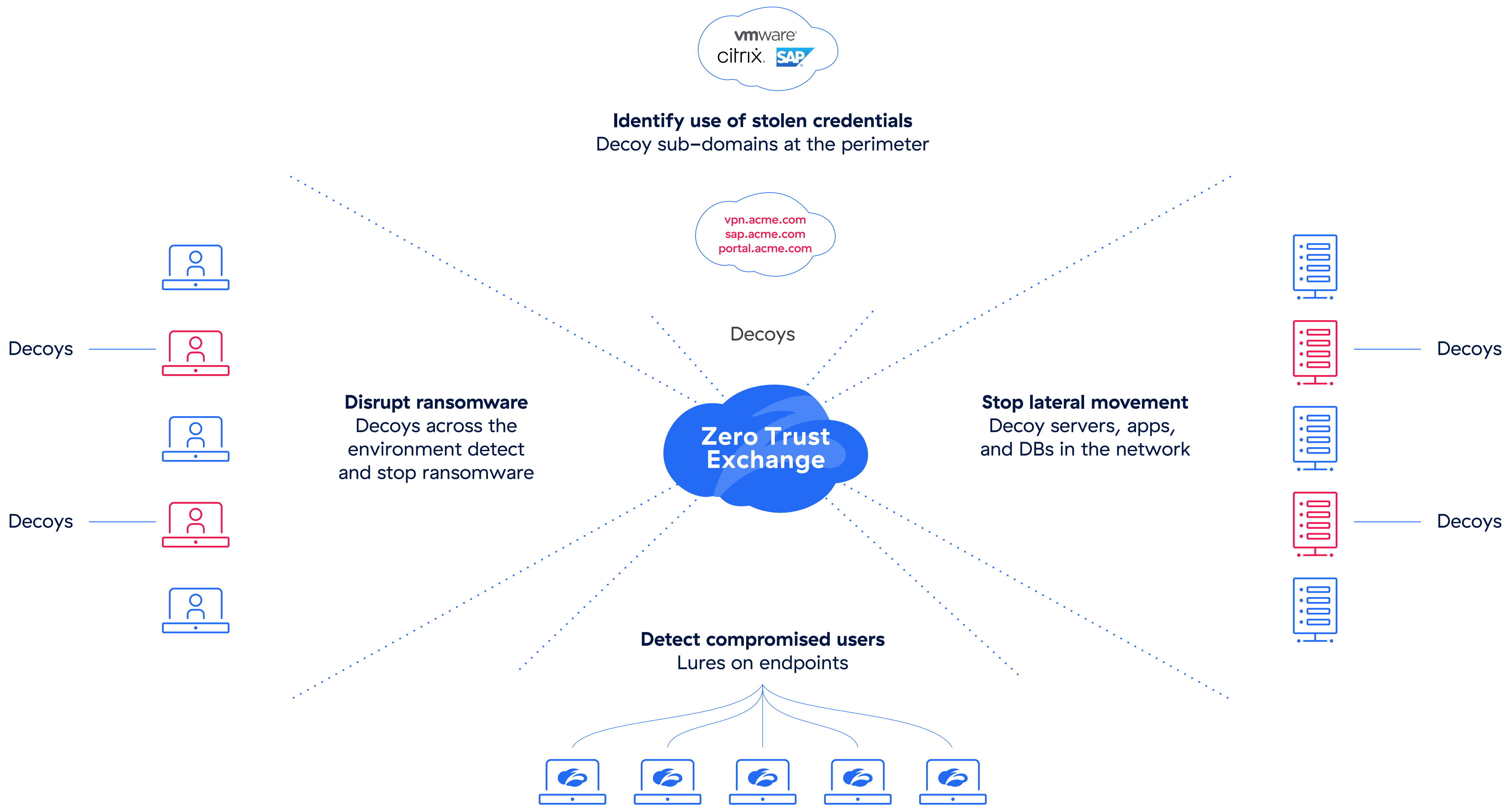
Zscaler Deception places decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.

The only vendor offering Private Threat Intelligence, a rare form of deception defense.

GARTNER

Actively detects and counters attackers' measures to detect or bypass deceptions.

GARTNER



- **Detect lateral movement**
  Decoy servers, applications, and databases planted in the network detect attackers attempting to move laterally and cut them off.

- **Detect cloud attacks**
  Detect attackers targeting your cloud workloads in AWS and Entra by accessing S3 buckets, IAM keys, etc. Stop cloud lateral movement and exploitation with high fidelity alerting.

- **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 attacks against GenAI apps**
  Detect attackers attempting to exploit GenAI applications including chatbots and API using attacks like prompt injection, data poisoning, jailbreaking, adversarial suffixes, training data extraction, and more.

Capabilities

- **GenAI decoys**
  Use decoy chatbots, decoys LLM APIs, adaptive decoys, and decoy agents to detect attackers targeting GenAI infra in your environment.

- **Threat intel deception**
  Internet-facing decoys that heuristically detect pre-breach threats that are specifically targeting your organization.

- **Endpoint deception**
  A minefield for your endpoints. Includes decoy files, decoy credentials, decoy processes, etc.

- **Cloud deception**
  Decoys web servers, databases, file servers,

etc. that detect lateral movement in your cloud environments.

- **ThreatParse**
  Automated forensics and root-cause analysis in two clicks. Extracts insights from logs.

- **Application deception**
  Server system decoys that host services like SSH servers, databases, file shares, and more.

- **Active Directory deception**
  Fake users in active directory that detect enumeration activity and malicious access.

- **RDP decoys**
  Realistic high-interaction OS environments for deeper attack visibility.

Additional Capabilities

- **Early warning system**
  Get early warning signals when sophisticated adversaries like organized ransomware operators or APT groups are scoping you out. Perimeter decoys detect stealthy pre-breach recon activities that often go unnoticed.

- **Active Directory security**
  Fixing Active Directory misconfigurations is not always possible. Zscaler Deception provides a pragmatic solution to detecting threats leveraging Active Directory. It's the next best thing to rearchitecting your identity strategy.

- **SOC optimization**
  Leverage low false positives and identity intelligence to support your SOC with high fidelity alerting that enables threat hunting and meaningfully reduces your mean time to detect and respond metrics.

> Offers several unique deception types compared to other vendors.
>
> GARTNER

Zscaler Deception Plans

Zscaler Deception is available in the following two editions:

- **Zscaler Deception Standard**
  For businesses starting with deception-based threat detection.

- **Zscaler Deception Advanced**
  For businesses looking to implement a comprehensive deception-based active defense solution to detect advanced threats and secure critical parts of their environment.

Capabilities	Zscaler Deception Standard	Zscaler Deception Advanced
Sizing	• 20 decoys • No add-on decoys	• Starts at 50 decoys (additional 50 per 5000 users, up to 300) • Add-on decoys
Application lures, cloud lures, browser cookies, beacon files	• Full decoy library	• Everything in Standard, plus: • Customizable decoys (VMs, containers)
Endpoint Deception	• Application lures, browser cookies, and beacon files	• Everything in Standard, plus: ransomware detection, MiTM detection, brute force detection, Kerberoasting detection, detect use of in-memory credentials, defense evasion detection, triage
Active Directory Deception	• Active Directory recon and attack detection • Active Directory decoy users • Single domain	• Active Directory recon and attack detection • Active Directory decoy users • Multiple domains
SOC/Hunting Integration	• Email notifications only	• Full SOC workflow includes everything in Standard, plus: SIEM forwarding, orchestration and containment, custom notifications, custom ThreatParse rules, Zscaler Sandbox integration
Enterprise Features	• Single sign-on, audit logs, and standard roles	• Custom RBAC, static IP whitelisting, API access
Available with	• Zscaler Platform	• Add-on SKU — Zscaler Risk Management

Why Zscaler Deception?

- **Seamless, cloud-native deployment**
  Zscaler Deception integrates with Zscaler Private Access (ZPA) to create, host, and distribute decoys with no additional VMs or hardware needed.

- **Zero network configuration**
  Say goodbye to VLAN trunking/SPAN ports/GRE tunnels to route traffic to decoys. Zscaler Deception routes malicious traffic as a transparent extension of the Zero Trust Exchange.

- **Integrated into the Zero Trust Exchange**
  The world's only zero trust architecture with integrated deception detects and stop the most advanced attackers, compromised users, and insider threats without adding complexity or compounding alert fatigue.

START DETECTING ADVANCED THREATS

Whether you're just starting your Zero Trust journey or are already a Zscaler customer, learn more about Zscaler Deception and request a demo to understand how you can leverage this capability to accelerate and secure your shift to Zero Trust.

REQUEST A DEMO

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line 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**

zscaler™

Zero Trust Everywhere.™