



# Zscaler Deception

## Detect and eradicate compromised users and lateral movement

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 Ransomware and advanced threats:** Traditional defense approaches rely on signatures or malicious behavior to detect threats. However, human-operated threats such as ransomware, supply chain attack, and nation-state adversaries are adept at bypassing these defenses. The stealthy nature of these attacks makes it impossible to stop them early or limit the blast radius using traditional detection tools.

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

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

— Gartner

### Introducing Zscaler Deception

A pragmatic approach to de-risking the attack surface, detecting lateral movement, and stopping high-risk human-operated attacks.

#### Stop lateral movement

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

#### 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

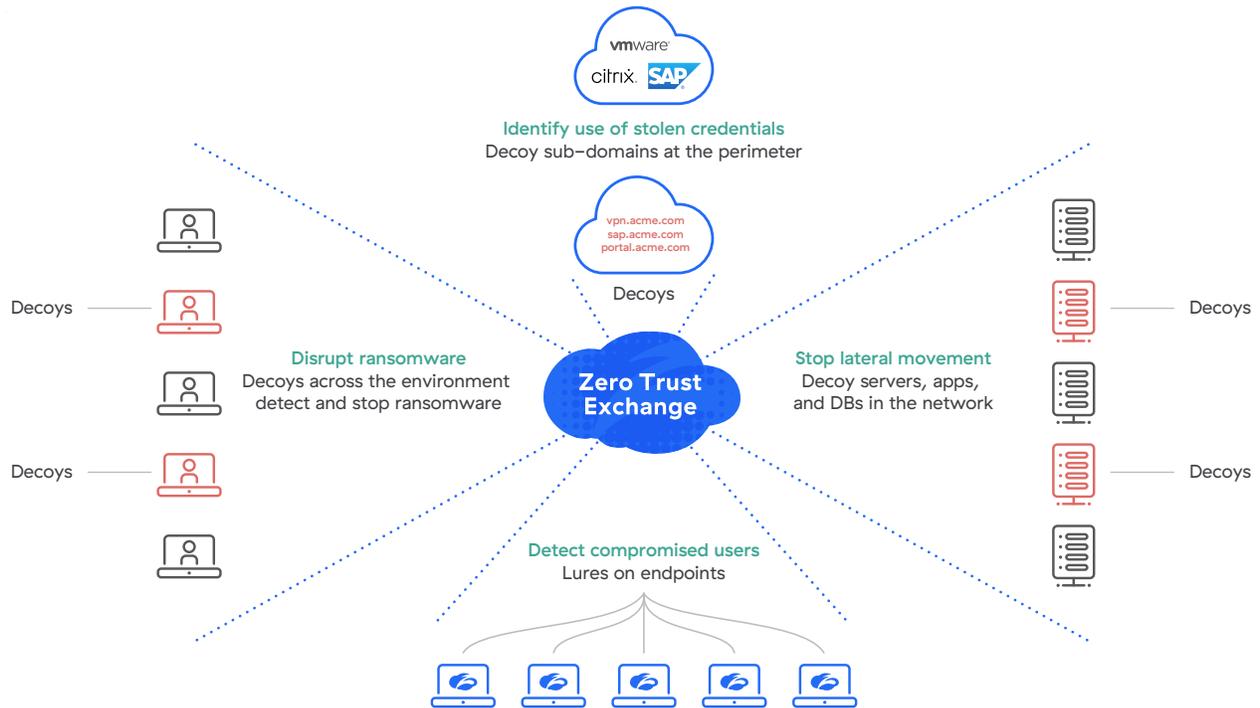
Decoy passwords, cookies, sessions, and bookmarks to decoy applications to detect compromised users when an attacker uses one of these deceptive assets.

#### Identify 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.

## 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.



- ✓ **De-risk your attack surface**  
Threat detection for endpoints, identity systems, networks, applications, and the cloud. Divert attackers away from targets and de-risks the attack surface.
- ✓ **Detect threats that matter, faster**  
Detect compromised users, lateral movement, and ransomware attacks. Deception alerts have little-to-no false positives and provide high-confidence IoCs.
- ✓ **Contain threats in real-time**  
Leverage zero trust network access enforcement policies to orchestrate response and contain threats without worrying about integrations.

“Actively detects and counters attackers’ measures to detect or bypass deceptions.”

— Gartner

## Features

- **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.
- **Golden image support:** Realistic high-interaction OS environments for deeper attack visibility.
- **MirageMaker:** Out-of-the-box decoy datasets for a variety of use cases to launch deception campaigns rapidly.

“Offers several unique deception types compared to other vendors.”

— Gartner

## 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 re-architecting 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 meantime to detect, know, and respond metrics.

## Zscaler Deception Plans

Zscaler Deception is available in the following two editions:

### Zscaler Deception Standard

For businesses starting with deception-based threat detection. Available exclusively as part of ZIA (Transformation and ELA) and ZPA (Business) editions.

### 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. Available as part of ZPA Transformation or as a standalone offering.

Capabilities	Zscaler Deception Standard	Zscaler Deception Advanced
<b>Includes</b>	<ul style="list-style-type: none"> <li>• 20 Application / Network decoys (includes perimeter decoys)</li> <li>• 1 decoy connector</li> <li>• 1 Active Directory decoy</li> <li>• Add-on decoys not available</li> </ul>	<ul style="list-style-type: none"> <li>• Up to 150 Application / Network decoys (includes perimeter decoys)</li> <li>• Up to 6 decoy connectors</li> <li>• 10 Active Directory decoys</li> <li>• Add-on decoys à la carte</li> </ul>
<b>Application / Network Deception</b>	<ul style="list-style-type: none"> <li>• Complete library of in-built decoys</li> </ul>	<ul style="list-style-type: none"> <li>• Complete library of in-built decoys</li> <li>• Customizable Decoys (VMs, containers)</li> </ul>
<b>Endpoint Deception</b>	<ul style="list-style-type: none"> <li>• Application lures, browser cookies, and beacon files</li> </ul>	<ul style="list-style-type: none"> <li>• Application lures, browser cookies, beacon files, ransomware detection, local scan detection, MiTM detection, privilege escalation detection, and defense evasion detection &amp; triage</li> </ul>
<b>Active Directory Deception</b>	<ul style="list-style-type: none"> <li>• Basic Active Directory integration for network and application decoys only</li> </ul>	<ul style="list-style-type: none"> <li>• Active Directory recon and attack detection</li> <li>• Active Directory decoy users</li> <li>• Multiple domains</li> </ul>
<b>SOC/Hunting Integration</b>	<ul style="list-style-type: none"> <li>• Email notifications only</li> </ul>	<ul style="list-style-type: none"> <li>• Email notifications, full SOC workflow, SIEM forwarding, orchestration and containment, SIEM dashboards, custom notifications, custom ThreatParse rules, cloud sandbox integration, and managed threat hunting integration</li> </ul>
<b>Enterprise Features</b>	<ul style="list-style-type: none"> <li>• Single sign-on, audit logs, and standard roles</li> </ul>	<ul style="list-style-type: none"> <li>• Single sign-on, audit logs, full RBAC, IP whitelisting, and API Access</li> </ul>
<b>Available with</b>	<ul style="list-style-type: none"> <li>• ZIA-TRANS EDITION or Higher</li> <li>• ZPA-BUS EDITION</li> <li>• 1000 Users minimum</li> </ul>	<ul style="list-style-type: none"> <li>• ZPA-TRANS EDITION</li> <li>• 1000 Users minimum</li> <li>• Also available as a standalone deception solution</li> </ul>

## 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 stops 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](#)



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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/](https://zscaler.com/legal/) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.