SOLUTION BRIEF

Zscaler™ Deception

The world's only deception-based threat detection solution built for a zero trust architecture. Zscaler Deception uses advanced lures and decoys to detect and disrupt sophisticated threats that consistently bypass traditional defenses, including organized ransomware operators, supply chain attacks, and APTs.

The Challenge

Attackers are getting better and better at exploiting organizations' growing attack surfaces. Security teams relying on traditional detection technologies are at a disadvantage because:

Sophisticated attacks are stealthy

Advanced adversaries use purpose-built playbooks and an in-depth understanding of their target's environment to get in and stay hidden. It takes 280 days on average to detect and mitigate a breach. Combine this with the fact that 91% of incidents don't even generate a security alert and you can see how some of the most well-defended and prepared organizations end up on the 9:00 news.

Advanced attacks are human-operated

Traditional defenses look for malicious code to keep adversaries out but 68% of attacks aren't even malware-based. Sophisticated adversaries are abandoning the malware strategy and instead using advanced tactics like legitimate credentials and built-in tools to achieve their objectives. These advanced maneuvers easily bypass traditional defenses and pose a challenge to security teams that don't have the means or time to hunt for threats.

Real threats hide in false positives

Security operations now default to collecting as much data as possible, pooling it in a SIEM, and then trying to find evil. The result? Analysts drown in security alerts and miss serious threats because 45% of alerts are false positives. 99% of security teams say that alert volumes are a problem. Look at some of the biggest breaches and you'll often find that a security control had flagged the activity but it got buried in all the noise.

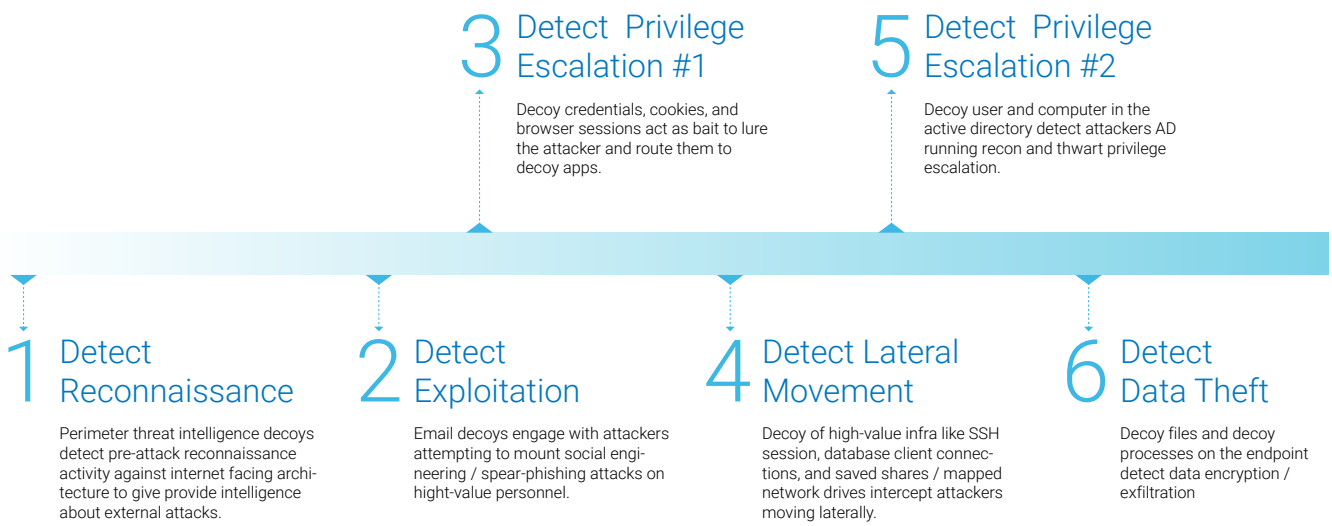
Enter Deception

Deception is a proactive defense approach that detects active threats by populating your environment with decoys: fake endpoints, files, services, databases, users, computers, and other resources that mimic production assets for the sole purpose of alerting you to adversary presence when they're touched.

Introducing Zscaler Deception

Zscaler Deception augments the Zscaler Zero Trust Exchange with deception technology to blanket your environment with decoys and false user paths that lure attackers and detect advanced attacks without operational overhead or false positives. It's the easiest way to add a powerful layer of high-fidelity threat detection to your entire enterprise.

Decoys to disrupt attacks at every stage of the kill-chain



Pre-breach warnings

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.

Lateral movement detection

Catch attackers that have bypassed traditional perimeter-based defenses and are trying to move laterally in your environment. Application decoys and endpoint lures intercept these adversaries and limit their ability to find targets or move laterally.

Defense against ransomware

Decoys in the cloud, network, endpoints, and Active Directory act as landmines to detect ransomware at every stage of the kill chain. Simply having decoys in your environment limits ransomware's ability to spread.

Real-time threat containment

Unlike standalone deception tools, Zscaler Deception integrates seamlessly with the Zscaler platform and an ecosystem of third-party security tools such as SIEM, SOAR, and other SOC solutions to shut down active attackers with automated, rapid response actions.

Outcomes and Benefits

Disrupt advanced threats

Detect and stop attackers across your security infrastructure, including low visibility paths like DC-to-DC and internal-traffic-to-DC.

167% – Average increase in 'Opportunity to Detect' advanced attacks like ransomware

No false positives

There is no legitimate business traffic to decoys, so any interaction with them is an immediate, high-confidence signal of an ongoing breach, alerting your security team to threats like ransomware, supply chain attacks, and APTs.

98% – Average reduction in alert volume compared to traditional detection controls

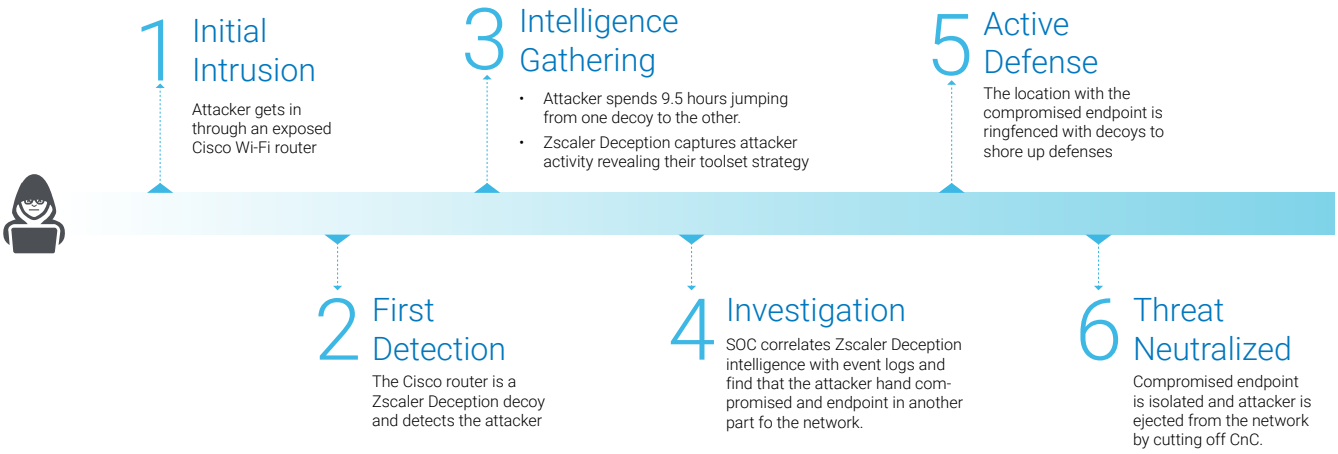
Part of the Zero Trust ecosystem

Integration with the Zscaler Zero Trust Exchange allows for seamless deployment and automatic response actions, including threat containment and policy updates. Fully deploy in days with no appliances.

50% – Average increase in visibility for targeted threats not found in threat intel feeds

Deception in action – Case study

One of the world's largest banks stops an unknown advanced threat early in the kill chain



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** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com