SOLUTION BRIEF

Zscaler Deception

Detect and stop frontier AI attacks

Frontier AI has changed the speed, scale and economics of attacks

AI-driven attacks follow very different patterns than human adversaries use. They probe environments in parallel, adapt to failed attempts, chain vulnerabilities, use stolen credentials, and move across environments at machine speed.

That changes the detection problem. Security teams no longer have the luxury of waiting for multiple weak signals to accumulate into a high-confidence incident. By the time traditional workflows collect enough evidence and then correlate, triage, and escalate the threat, an autonomous or AI-assisted attacker will likely be several steps into your environment.

To stop machine-speed attacks, defenders need alerts that confirm attacker presence instantly, before traditional investigation workflows can catch up.

Deterministic detection for the era of AI-powered attacks

Zscaler Deception turns attacker exploration into high-fidelity detection. By placing realistic decoys and lures across your environment, Zscaler creates a defense surface that is indistinguishable from real attack paths and a blanket of tripwires that AI can't help but stumble into.

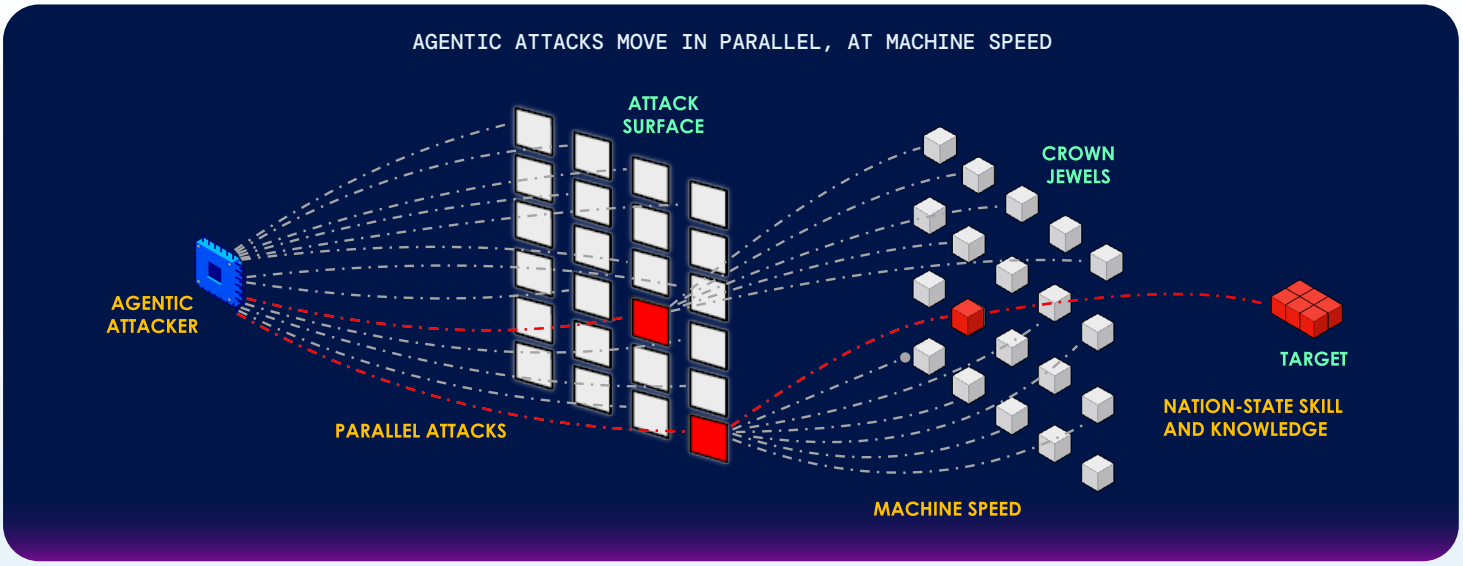
When an attacker interacts with a decoy, the signal is deterministic: no legitimate user or process should touch that asset. That certainty makes deception uniquely effective against AI-driven attacks, where adversaries move fast, probe broadly, and act on every path they discover.

AI attackers are forced into a no-win scenario:

- **If they move quickly and exhaustively, they hit decoys and expose themselves.**
- **If they slow down to avoid detection, they lose the speed advantage that makes them dangerous.**
- **If they try to map the environment first, that can trigger deception controls such as AI-specific detections in Zscaler Deception.**

These properties explain why the Cloud Security Alliance cited deploying deception technology as a critical priority in their strategy briefings on Mythos and the Hugging Face incident.

With one-click deployment in Zscaler Private Access, Deception gives security teams immediate protection against AI-driven attacks.



©2026 Zscaler, Inc. All rights reserved.

High-fidelity detection and response for AI-driven attacks

Attacker probes environment

Attacker engages decoy

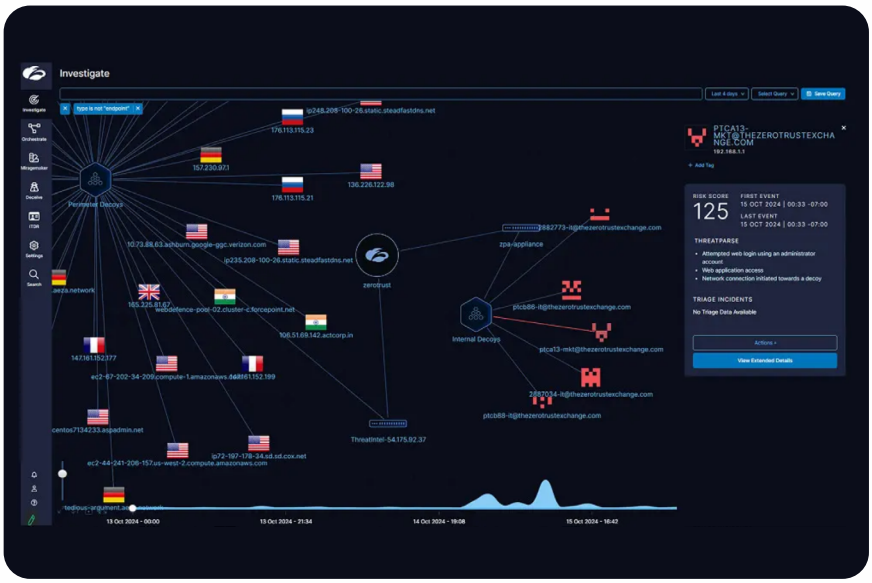
Deception triggers high-fidelity alert

Automated response initiates containment

Attacker telemetry captured

Detect Frontier AI attacks with high-fidelity signals

- Confirm attacker intent instantly when adversaries touch decoy assets, credentials, identities, or services that legitimate users should never access.
- Identify agentic AI probing from autonomous agents, LLM-driven crawlers, and AI-assisted tools as they interact with hidden decoy paths.
- Turn AI speed and parallelism into a liability by forcing autonomous attackers to either trigger decoys or slow down and lose their speed advantage.



Protect every surface that attackers pursue

- Deceive attackers on endpoints with lures and breadcrumbs that expose reconnaissance, credential theft, and early lateral movement.
- Reveal identity and Active Directory attacks such as credential misuse, Kerberoasting, brute force, and escalation attempts.
- Expose cloud, workload, and AI infrastructure attacks including cloud reconnaissance, suspicious data access, prompt injection, jailbreaks, and agentic probing.

Contain threats at machine speed

- Trigger response from confirmed alerts to isolate hosts, restrict access, revoke credentials, or initiate response workflows.
- Use Zscaler Zero Trust Exchange policy enforcement to limit lateral movement before damage spreads.
- Pre-authorize containment actions to enable automatic containment without waiting for manual triage.

Learn more at 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**.

© 2026 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/trademarks 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.

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