ZSCALER DECEPTION FOR MYTHOS-LEVEL ATTACKS

Defense in Depth with ZPA and Deception

AT-A-GLANCE

The Cloud Security Alliance says to build a deception capability in 90 days. ZPA customers need only minutes.

Mythos-Ready Threat Detection

In response to Mythos-level AI attacks, and the CSA's 90-day mandate to deploy deception, one-click deployment of Zscaler Deception activates a full deception strategy across your zero trust environment, with no new agents or hardware, and no network reconfiguration. Deception is enabled through your existing infrastructure, with no changes to users, so you can:

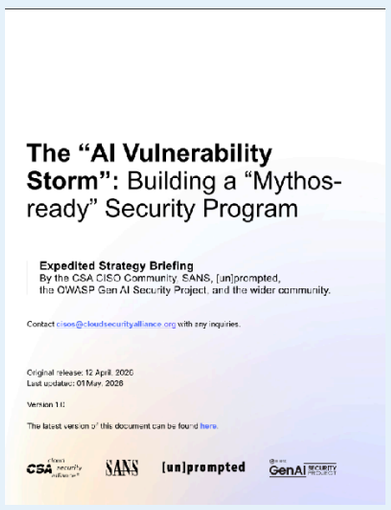
- **Stop lateral movement:** Decoy applications appear alongside your real private apps in Zscaler Private Access. Attackers attempting to pivot hit decoys instead of real resources.
- **Redirect attackers with endpoint lures:** Decoy credentials and bookmarks deployed via Zscaler Client Connector lead compromised identities straight to decoys, away from real resources.
- **Trap attackers probing unauthorized services:** Decoy services on real apps catch anyone scanning ports that legitimate users would never touch.

Deterministic Alerts Against AI

AI-orchestrated attacks move through kill chains in minutes using legitimate tools your traditional controls like EDR won't flag. Deception sidesteps the signature and behavioral detection problem entirely. No legitimate user has any reason to touch a decoy, so every interaction is confirmed malicious, with no ambiguity. Whether it's an agentic AI attacker or a compromised insider, the signal is the same: deterministic proof of compromise.

Automated Containment via ZPA

The moment a decoy is triggered, Deception automatically revokes the compromised user's access to private applications via ZPA, across every device they're signed into. A pre-authorized response means an analyst does not have to manually approve the block so the attacker is cut off before they pivot, eliminating lateral movement at the speed of the attack, not the speed of your SOC queue.



The Cloud Security Alliance convened 250+ CISOs and security leaders—including former CISA, NSA and White House cyber leaders—to help companies prepare for Mythos-enabled attacks.

The result: an emergency strategy briefing with **11 priority actions** for a Mythos-ready security program.

#9: Build a Deception Capability

Classified as HIGH risk with a mandate to implement in the next 90 days.

"Deception is attack-tool and vulnerability independent, identifying attacks and attackers based on their TTPs."

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

Zero Trust Everywhere