

zscaler™ + Oasis Security

Securing Non-Human & Agentic Identities
across the Zero Trust Exchange

OASIS



INTEGRATION HIGHLIGHTS

- ✓ Govern every non-human identity in a Zscaler estate
- ✓ Surface AI agents and MCP servers on endpoints
- ✓ Rotate the secret, scope access, retire the identity.

The Market Challenge

Enterprise traffic is no longer dominated by humans. Service accounts, API keys, IAM roles, OAuth tokens, and AI agents make up the majority of the components that touch modern infrastructure. Zero Trust assumes an authenticated identity behind every connection, but when that identity is a non-human, the lifecycle controls built for human users break down. Non-human identities are created in code, shared across teams, and persist long after their owner has left.

Agentic AI compounds the problem. Delegated agents call APIs, access data, and chain tools across cloud environments on behalf of users. Without governance, every new agent risks exposing the business to data loss and business continuity challenges. Identity and Security teams are left with two disconnected views: network traffic lacks identity context; identities and accounts lack real-world behavior.

The Solution

Together, Zscaler and Oasis Security unify enforcement and identity governance across cloud, SaaS, and on-premises, bringing end-to-end visibility, ownership, and lifecycle control to machine and agentic access. Oasis Security, the platform for Non-Human Identity Management and Agentic Access Management, continuously discovers, attributes, scores, and governs every machine identity and AI agent.

The Zscaler Zero Trust Exchange inspects, brokers, and enforces every connection for all users, workloads, and agents from any location, with inline AI-powered traffic inspection and advanced threat protection.

With Oasis feeding identity context into Zscaler, security teams can attribute each non-human identity to an owner, then rotate, scope, or decommission its access without writing or maintaining brittle custom scripts. Identity and security teams reconcile every non-human and agentic access once, in one place, with greater speed and confidence.

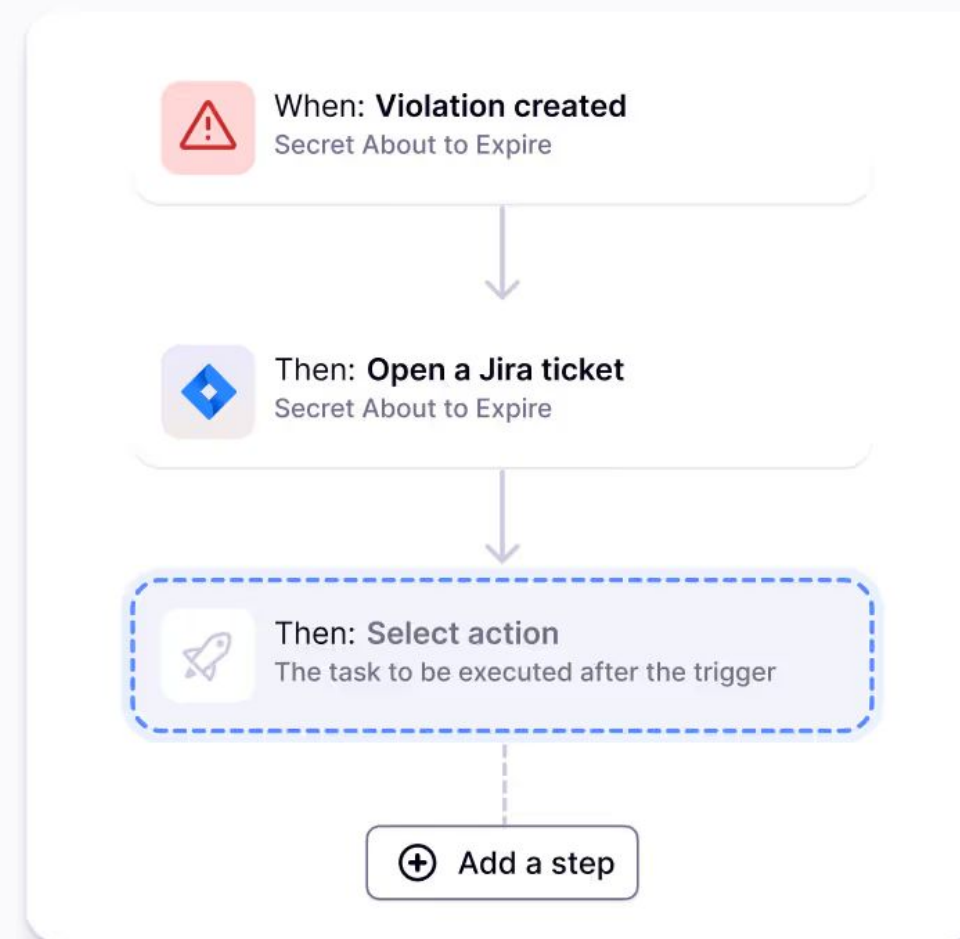
Together, Zscaler and Oasis Security deliver a single, end-to-end zero trust solution that governs every non-human identity touching the Zero Trust Exchange: service accounts, API keys, OAuth tokens, IAM roles, secrets, and AI agents.

Solution Components Deep Dive

Govern every machine identity touching ZIA and ZPA: discover each service account, API key, OAuth token, and IAM role across your estate. Attribute each to an owner, and score its real risk.

Score the risk of every non-human identity by access scope. Surface which secrets it carries and what systems those credentials can reach. If over-scoped, drive it to rotation or retirement.

Continuously surface the AI agents and MCP servers running on your managed enterprise endpoints. For example, the Zscaler Client Connector exposes a locally running agent, and Oasis ties it to the credentials and access paths it carries. Reduce risk by revoking or scoping access when an agent's standing privilege exceeds what its purpose requires. Oasis attributes every detected agent to its owning human or team. If an access path is over-scoped, Zscaler enforces inline, blocking, isolating, or shaping the traffic. Standing access is rotated or removed once the agent no longer needs it to operate.



KEY USE CASES

Govern Every Machine Identity

Zscaler and Oasis integrate to give security teams a complete view of every non-human identity behind Zero Trust Exchange traffic, including who created it, what it can reach, and whether it is still owned.

While Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) broker and enforce every connection, Oasis discovers each identity, attributes ownership, scores risk, and drives lifecycle action across the estate.

Secure AI Agents

Zscaler and Oasis integrate to govern the AI agents and MCP servers appearing on enterprise endpoints, surfacing the secrets each carries and the systems it can reach. While the Zscaler Client Connector detects and contains agents inline, Oasis ties each to an owner, scores its standing access, and drives rotation, scoping, or decommissioning.

Zero Trust only works when you know the identity behind it. Zscaler + Oasis are core to our security stack, finally giving non-human and agentic identities a real owner. Together, Zscaler + Oasis turn "we found a secret" into "we rotated it and retired the identity," so a small team can govern thousands of NHIs with confidence.

Director of IAM

Global Market Leader in the Food Industry

Zscaler + Oasis Security Benefits

ACTION	DESCRIPTION
Close the NHI visibility gap	Surface and govern every non-human identity touching the Zero Trust Exchange.
Give every connection an accountable owner	Zscaler brokers the connection; Oasis names the non-human identity behind it, its owner, and its blast radius. No more traffic without identity context, and no identities without real-world behavior.
Eliminate stale and standing privilege	Move from “secret found” to “secret rotated” with full lifecycle governance; no orphaned access, no stale credentials, no off-boarded identity surprises.
Enforce identity-aware policy inline	Push high-confidence NHI threat signals to ZIA for inline blocking, without writing custom integrations or maintaining brittle scripts.
Govern AI agents with the same control plane	Apply the same discovery, ownership, and enforcement model to delegated AI agents and MCP servers as the rest of the identity estate.

Conclusion

Deliver better business results with Zscaler and Oasis Security

Zscaler + Oasis Security deliver one operational model for human, machine, and agentic access, replacing stale assumptions about who owns each identity. Instead of trusting non-human identities by default, every connection is tied to a real owner and purpose, scored for risk, and driven to lifecycle action; rotating the secret, scoping the access path, and decommissioning the identity. The net results are reduced blast radius, agents shipped with guardrails, and identity reconciled once.

Learn more at www.zscaler.com/partners/technology



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 in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

©2025 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ 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.