JOINT SOLUTION BRIEF

# zscaler™ + reco

Zero Trust for AI Agents: Across Your Network and Inside Every SaaS App



## INTEGRATION HIGHLIGHTS

- Unified shadow AI and shadow app discovery — across the network and inside every sanctioned app
- Unified identity view — Zscaler user data correlated with Reco's in-app activity and
- Unified security posture — Zscaler's network configuration correlated with Reco's SaaS findings

## The Market Challenge

87% of enterprise leaders believe AI agents operating with legitimate credentials pose a greater insider threat risk than human employees — and for good reason. AI agents are fast becoming the largest and fastest-growing identity class in the enterprise. They read data, take actions, move between SaaS apps, and operate at machine speed, often with standing permissions and no human in the loop.

At the same time, the SaaS estate keeps expanding. Shadow AI tools proliferate across browsers and unsanctioned accounts. Human users collect excess privileges. Third-party integrations, OAuth tokens, and non-human service accounts quietly accumulate access. Zero Trust at the network edge is necessary, but it stops at the front door, leaving the inside of every SaaS app — and every AI agent operating there — largely unseen.

Securing the agentic enterprise requires extending Zero Trust all the way from the network edge into every SaaS app and every AI agent operating inside it.

## The Solution

Together, Zscaler and Reco deliver Zero Trust across the full agentic enterprise, from the network edge to the SaaS runtime. Zscaler's Zero Trust Exchange secures how users, devices, and AI agents reach internet, SaaS, and private applications. Reco's Agentic AI & App Security platform secures what happens inside those apps — discovering every human and non-human identity, every AI agent, and every sensitive data action across your SaaS estate. The integration unifies both views in Reco: Zscaler ZIA's shadow app intelligence, user and identity data, security configuration, and audit activity flow continuously into Reco and correlate with its SaaS-resident findings. Security teams get one picture of every user, every app, and every AI agent — on-network and in-SaaS — without pivoting between consoles.

**Together, Zscaler and Reco extend Zero Trust from the network edge to every AI agent — across any network, any device, and every SaaS app.**



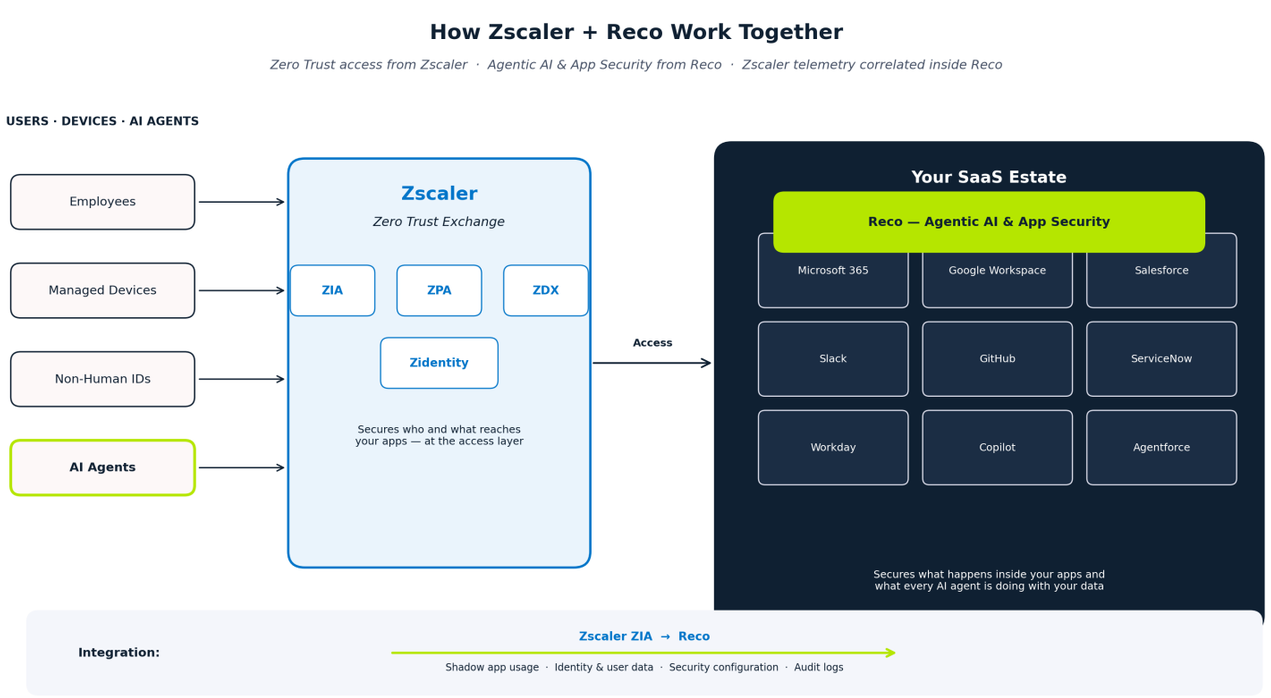
©2025 Zscaler, Inc. All rights reserved.

## Solution Components Deep Dive

Unified shadow AI and app discovery. Reco sees every AI agent, integration, and OAuth connection inside sanctioned SaaS apps. Zscaler sees unsanctioned AI tools employees reach directly from the browser. Together, no shadow hides.

Unified identity across network and SaaS. Reco scores every human and non-human identity on in-app activity, configuration, and permissions. Zscaler ZIA user data flows into Reco and anchors each identity across both layers — one record per human, service account, and AI agent.

Correlated security posture. Zscaler's network policy, security configuration, and audit logs flow into Reco, where they correlate with SaaS configurations, permissions, and agent behavior. Drift on either side is visible in one place, not split across consoles.




## KEY USE CASES

### Secure the AI agent wave

AI agents (Microsoft Copilot, Salesforce Agentforce, Glean, Gemini, custom GPTs, MCP connectors) are the fastest-growing identity class in the enterprise. Zscaler governs which destinations agents can reach and inspects what they send. Reco governs what those same agents can do inside each SaaS app — the data they access, the actions they take, and the privileges they accumulate. Together, every AI agent is observed, scored, and governed end to end.

### Zero Trust identity for every agent

Most SaaS breaches now start with an identity, often a non-human one. Zscaler secures the access path; Reco secures the SaaS runtime. Zscaler ZIA user data and shadow app activity flow into Reco and correlate with Reco's SaaS-resident findings — dormant admins, privilege drift, orphaned OAuth tokens, rogue AI agents — giving security teams a single view of every identity, human or machine, across both layers.

**Reco has transformed our relationship with our technology users. It's allowed us to be their partners as we work to build security into the business. We can implement strategic solutions that consolidate tools, improve resource efficiency, and reduce the attack surface.**

**Mike D'Arezzo, CISO**
**Wellstar Health**


©2025 Zscaler, Inc. All rights reserved.

## Zscaler + Reco Benefits

| ACTION | DESCRIPTION |
|---|---|
| **Reduce the attack surface** | Block unsanctioned AI tools at the network edge, lock down over-permissioned SaaS accounts, and shut down every path from a compromised identity to sensitive SaaS data — before an attacker or rogue agent ever reaches it. |
| **Improve the user experience** | Give employees safe, frictionless access to the apps and AI agents they need while automatically governing risky configurations and permissions in the background — no ticket backlog, no blocking what's safe. |
| **Increase agility and reduced TCO** | Consolidate network, identity, SaaS posture, and AI agent security into one operating model. Replace overlapping point tools and manual correlation between consoles with a single cross-layer Zero Trust fabric. |
| **Contain the AI agent wave** | See every AI agent across your SaaS estate (Copilot, Agentforce, Gemini, custom GPTs, MCP connectors). Zscaler governs which destinations agents can reach; Reco governs what they do inside each SaaS app. |
| **Close shadow AI and shadow app blind spots** | Unify Zscaler's network-observed discovery with Reco's SaaS-resident discovery to surface every integrated and browsed shadow app — eliminating the gaps that today's shadow inventories leave open. |

## Conclusion

### Deliver better business results with Zscaler and Reco

Zscaler + Reco deliver Zero Trust that finally reaches the agentic enterprise. Zscaler secures how users, devices, and AI agents reach every destination. Reco inspects what happens inside every SaaS app — every identity, every AI agent, every sensitive data action. Zscaler ZIA telemetry flows continuously into Reco, correlating network-observed shadow apps, user data, security configuration, and audit activity with Reco's SaaS-resident findings. Security teams get one view of the enterprise across network and SaaS. The net result: a smaller attack surface, faster detection and response, and a unified Zero Trust fabric that keeps pace with how AI is reshaping the enterprise.

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

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 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.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.