Solution Guide

Zero Standing Privilege Starts Here

Enforce zero trust-based privileged access with high precision for every employee, contractor, and third party — verified, time-bound, and dynamic.

Most privileged access is managed through a dated workflow with ticketing, group-based access, a VPN connection, jump host, etc. There is also a frequent reliance on policies that, once created, are not reviewed. And access that is granted without real time risk context. The consequence is standing, over privileged access that persists long after business needs expire, leaving attack paths that can be exploited by bad actors. Contractor, partner, and vendor risk is compounded, as access is granted through manual processes, with no identity verification and no automatic expiration.

Together, Saviynt and Zscaler extend powerful zero trust enforcement to every session by combining industry-leading identity security with least privilege network enforcement. The result is privileged access that is always verified, always time-bound, and always auditable, with the precision to control exactly what is accessible within every session, for every user and third party.

Enforce Precise Least Privileged Control Over Privileged Access

Saviynt complements Zscaler's Privileged Remote Access (PRA) with granular privileged access controls based on policy and context. No manual handoff or lag between policy and enforcement. Prevent standing privilege from taking hold with just-in-time, just-enough access enforced automatically, for every session and every identity irrespective of app, endpoint or network.

User registration and third-party onboarding

Onboard contractors, partners, and vendors with a single governed workflow through delegated administration that gives partner organizations the ability to manage their own users while Saviynt maintains centralized policy control. Every third-party identity is registered, governed, and subject to the same controls as internal users from day one.

Identity proofing before access is granted

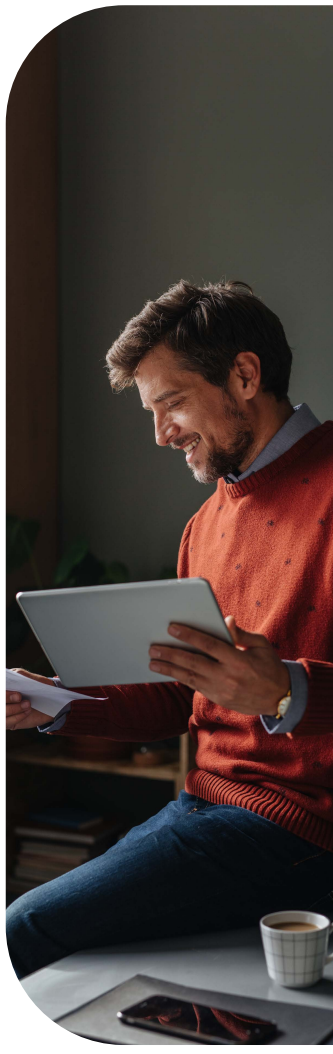
Saviynt verifies every identity before privileged access to Zscaler PRA environments is granted to ensure the right person is behind every request, not just a valid credential. Verification events are logged immediately, establishing the first link in a continuous, auditable chain of custody.

Precision Access, Not Just Privileged Access

Saviynt's deep PAM controls and fine-grained connectors deliver precision into what access is granted within a session down to a specific column in a database, a discrete policy in an application, or a single control within an enterprise system. Every approved session is provisioned with exactly the entitlements the work requires, scoped to the broadest ecosystem of applications, and revoked automatically when the window closes. No manual cleanup, no standing exposure, no forgotten entitlements.

Policy-validated access requests

Every access request is validated against separation of duties, risk thresholds, and ownership policy before it reaches Zscaler PRA. Saviynt determines who is entitled to a privileged session and for how long. If an entitlement was never granted or has expired, the Zscaler PRA session does not start.



Just-in-time, just-enough access, enforced automatically

Every approved session is provisioned with a defined expiration time. Privileged access exists for exactly as long as the work requires and disappears automatically when the window closes without manual cleanup, standing exposure, or forgotten entitlements. Zscaler PRA brokers, records, and terminates the session at the network layer the moment the governance window expires.

Zero Standing Privilege as an Operational Reality

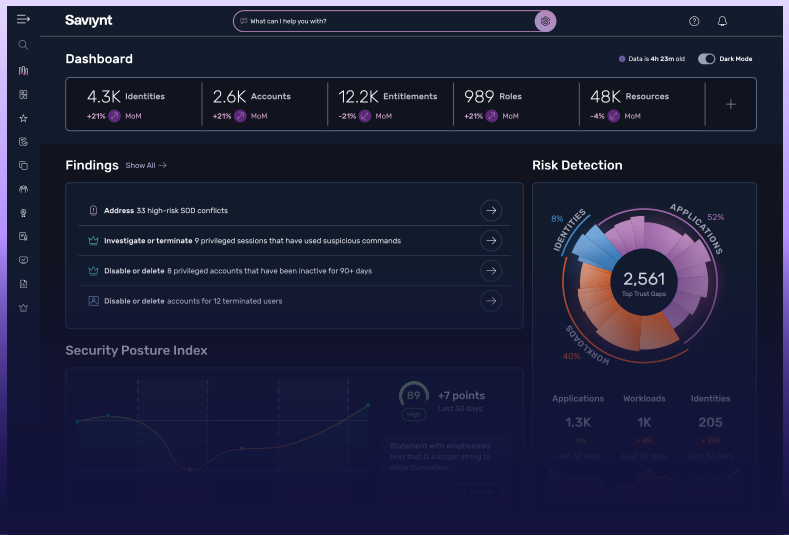
Every privileged access event (identity verification, access request, policy approval, session, and automatic revocation) is captured in a single, correlated audit trail. Compliance teams satisfy SOX, SOC 2, HIPAA, PCI DSS, and NIST 800-53 requirements from one continuous evidence chain without manually reconciling logs across disconnected systems. Zero Standing Privilege is demonstrable by design — not assembled manually before every audit.

Key Solution Benefits

- **Stop unauthorized sessions before they start.**
- **Eliminate standing privilege across every identity type**
- **Verify every identity before privileged access is granted**
- **Automatically enforce just-in-time, just-enough access**
- **Satisfy SOX, SOC 2, HIPAA, PCI DSS, and NIST 800-53 with a unified audit trail**

The Saviynt Identity Platform

Identity Security for AI. AI for Identity Security.™



Next Step

- Learn more by visiting **Saviynt.com/zscaler**
- **Schedule a demo** to experience posture-led security

About Saviynt

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is helping organizations safely accelerate their deployment and usage of AI today. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies, and government institutions. For more information, please visit **www.saviynt.com.**

Saviynt

Headquarters
1301 E El Segundo Blvd, Suite D El Segundo,
CA 90245 United States

310.641.1664
info@saviynt.com
www.saviynt.com