JOINT SOLUTION BRIEF

zscaler™ + Saviynt

Identity-Centric Zero Trust Privileged Access Management

INTEGRATION HIGHLIGHTS

- Eliminate standing privilege across remote workforce, third-party, and contractor identities
- Verify every identity before privileged access is granted
- Satisfy compliance requirements with a unified audit trail

The Market Challenge

Most privileged access is managed through coordination across many disconnected systems with no unified governance or evidence chain. There is also a frequent reliance on policies that, once created, are not reviewed, along with access that is granted without real time risk context. The consequence is standing, over-privileged access that leaves attack paths that can be exploited by bad actors.

These risks are compounded for contractors, partners/vendors, and remote employees, as access is granted through manual processes, with no identity verification and no automatic expiration, leaving organizations open to even more risk. And with 80% of data breaches involve privilege access misuse or compromise it's imperative that organizations eliminate standing access before it's exploited.

The Solution

Together, Saviynt and Zscaler deliver a powerful, integrated approach that strengthens privileged access security by combining industry-leading identity governance with Zero Trust network enforcement for enhanced end-to-end visibility, accelerated remediation, and secure conditional access.

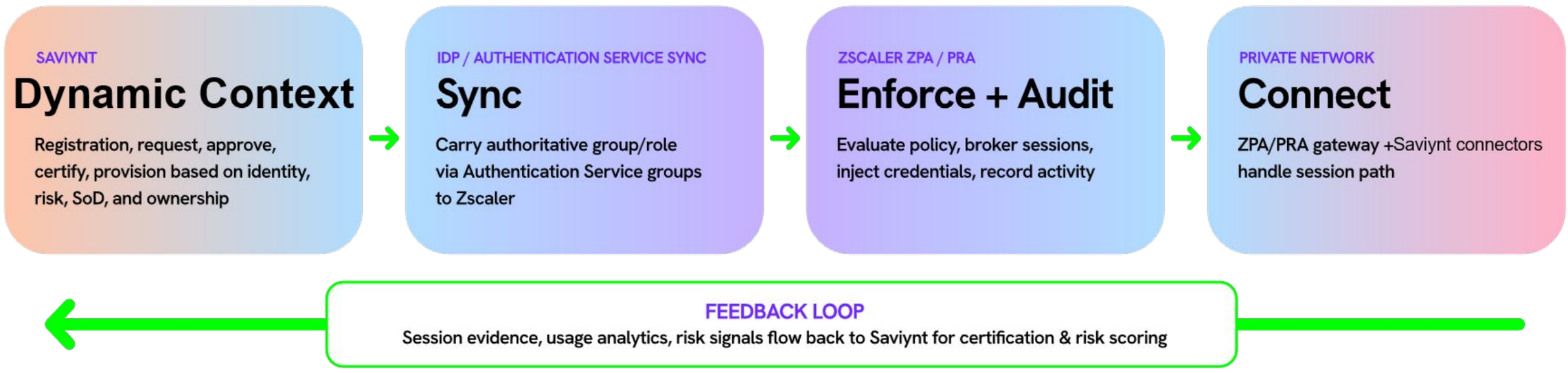
With seamless integration between Zscaler and Saviynt, security teams can enforce zero trust-based privileged access with extreme precision for every employee, contractor, and third party that is verified, time-bound, and dynamic. Stop unauthorized sessions before they start, remediate threats faster without pivoting between consoles, and maintain continuous compliance with a unified audit trail.

Together, Zscaler and Saviynt eliminate the risk of standing, over-privileged access by combining continuous, policy-validated identity governance with time-bound zero trust network enforcement for every user and session.

Solution Components Deep Dive

Precision Access, Not Just Privileged Access

Zscaler and Saviynt integrate for expanded visibility to provide security teams with a holistic understanding of threat context, user attributes, and permissions. While Zscaler Privileged Remote Access (PRA) provides secure, brokered application connectivity at the network layer, 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 automatically terminated the moment the governance window closes.



KEY USE CASES

User Registration and Third-Party Onboarding

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

Identity Proofing Before Access is Granted

Verify every identity before privileged access to Zscaler PRA environments are granted to ensure the right person is behind every request. Verification events are logged immediately, establishing the first link in a continuous, auditable chain of custody.

Policy-Validated Just-in-Time Enforcements

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

Zero Trust strategy is ultimately driven by the quality of identity decisions and how rigorously they are enforced. With Zscaler, we're helping customers move to a model where access is continuously verified, context-aware, and designed to expire. This marks an important step in delivering a Zero Trust approach to Identity Security.

Anirudh Sen
SVP of Products at Saviynt

Zscaler + Saviynt Benefits

ACTION	DESCRIPTION
Reduce the attack surface	Prevent standing privilege from taking hold with just-in-time, just-enough access enforced automatically for every session and identity irrespective of application, endpoint, or network. Stop unauthorized sessions before they start.
Prevent privilege creep	Provide a seamless, automated workflow where user access exists for exactly as long as the work requires. Zscaler PRA brokers and terminates the session at the network layer automatically when the window closes, requiring zero manual cleanup or administrative friction.
Achieve continuous audit-readiness	Bring compliance, identity, and network controls into a single architecture. Compliance teams can satisfy SOX, SOC 2, HIPAA, PCI DSS, and NIST 800-53 requirements from one continuous evidence chain without manually reconciling logs across disconnected systems.

Conclusion

Deliver better business results with Zscaler and Saviynt

Zscaler and Saviynt deliver an end-to-end zero trust solution that replaces traditional, dated security architectures that leverage legacy VPNs, jump hosts, and disconnected ticketing workflows. Instead of implicitly trusting identities or leaving standing, over-privileged access active indefinitely, connections are strictly authorized based on verified identity, business policy, and precise time-bounds. The net results are an operational reality for Zero Standing Privilege, a radically reduced attack surface, and a unified audit trail that makes compliance demonstrable by design.

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

[1] 2023 Forrester

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.

+1 408.533.0288

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

©2025 Zscaler, Inc. All rights reserved.