Talking to your auditor about Zero-Standing Privilege

01

Address the auditor's concerns upfront

02

Explain how policies replace group membership

03

Highlight the reduction in access review effort

04

Show how ZSP provides better audit evidence

05

Frame ZSP as a security and compliance improvement

Introduction

Auditors traditionally rely on role-based access control (RBAC), static group memberships, and quarterly user access reviews (UARs), which produce tangible artifacts like group rosters and signed-off reviews. **Zero-Standing Privilege (ZSP)** disrupts this approach by granting access only when justified, continuously evaluated, and applied in real time. This reduces standing access, lowers risk, and streamlines governance but challenges traditional auditing norms. To build confidence in ZSP, it's essential to explain how it meets or exceeds identity security requirements, even without traditional artifacts. Here's how to show auditors that ZSP meets or exceeds identity security requirements.

01

Address the auditor's concerns upfront

Auditors are responsible for ensuring that organizations comply with one or more standards. Traditionally, this verification process has depended on static evidence derived from role-based access control (RBAC) systems and periodic user access reviews (UARs). These approaches generate tangible artifacts, such as documented role assignments and formal review approvals, which auditors rely on to confirm that access controls are properly established and functioning as intended. However, compliance standards do not prescribe a specific type of evidence or enforcement mechanism. The key requirement is that organizations demonstrate their access policies are clearly defined, consistently enforced, and fully auditable. Instead of relying on static entitlements, ZSP ensures compliance by prioritizing real-time policy enforcement, allowing organizations to maintain continuous and dynamic control over access permissions.

How ZSP meets auditor needs

In ZSP, access is dynamic, tied to policies, with auditors focusing on two critical pieces:

- **Policy approval and review:** documentation that policies governing access have been reviewed and approved by the appropriate stakeholders.
- **Access logs:** detailed, real-time logs that show who accessed a system, when access occurred, and under which policy conditions.

Unlike RBAC, which samples roles, ZSP enables full review of access activity, ensuring precise compliance.

Why auditors prefer ZSP

ZSP provides auditors with stronger evidence of enforcement than RBAC systems:

- **Complete visibility:** instead of sampling a few roles or users, auditors have access to comprehensive logs of all access activity.
- **Real-time context:** access decisions are evaluated dynamically, ensuring they align with current business needs.
- **Fewer things to review:** auditors can review fewer policies instead of sampling countless role assignments and users, reducing complexity while ensuring strong compliance.

02

Explain how policies replace group membership

In an RBAC model, access is determined by static entitlements (e.g., group or role memberships), which are reviewed periodically to ensure alignment with job responsibilities. ZSP removes these static entitlements and replaces them with policy-driven access decisions.

- **Policies are explicitly defined:** they describe who can access what, under which conditions, and for how long.
- **Policies are evaluated in real time:** access decisions are made dynamically based on business context, such as ticket assignments, on-call rotations, or project requirements.
- **Policies create a clear audit trail:** every access decision is logged, including who requested access, why it was granted, and when it was revoked.

> “Instead of relying on static group memberships, we use policies that enforce access decisions in real time. These policies are tied to business processes, making them clear, specific, and justifiable. Each access decision produces a detailed, auditable log that answers who, what, why, and when.”

03

Highlight the reduction in access review effort

Traditional UAR processes are time-intensive, requiring validation of static group memberships for large user bases and many roles—most of which don’t involve critical systems. This not only consumes significant resources but also creates gaps where entitlements may linger unjustifiably.

ZSP reduces the burden of access reviews by removing standing access entirely:

- Since users no longer have persistent entitlements, there’s no need to validate static group memberships.
- Reviews focus only on the policies that govern access to critical systems, ensuring they remain appropriate and aligned with business needs.

> "By eliminating standing access, ZSP removes the need for static entitlement reviews. Instead, reviews focus on policy validation for critical systems, reducing effort while improving security and compliance."

04

Show how ZSP provides better audit evidence

The most significant auditor concern is often: “Where’s the evidence?” Traditional models rely on group membership lists and quarterly sign-offs, but these artifacts don’t reflect real-time access or the context in which access is granted. ZSP generates stronger evidence:

- **Policy logs:** every access decision is logged with who requested access, the conditions under which it was granted, and when it was revoked.
- **Real-time enforcement:** policies ensure that access is granted only when business conditions justify it—no lingering entitlements to review.
- **Improved accountability:** logs provide a detailed trail for auditors, showing that access decisions are consistently enforced and tied to policies rather than subjective manual approvals.

> “ZSP produces stronger audit evidence by logging every access decision in real time. Auditors can see exactly who accessed what, under what conditions, and for how long. This level of detail provides better accountability and transparency than quarterly reviews of static group memberships.”

05

Frame ZSP as a security and compliance improvement

Finally, it’s important to highlight that ZSP isn’t just a different way to manage access—it’s a better way. Traditional RBAC and quarterly reviews leave organizations exposed to standing access risks and stale entitlements. ZSP addresses these weaknesses head-on:

- **Reduces risk:** no lingering entitlements for malicious or compromised users to exploit.
- **Streamlines compliance:** focused, policy-based reviews replace broad, manual UAR processes.
- **Improves accountability:** detailed logs provide stronger evidence for audits, ensuring access is always justifiable and transparent.

> “ZSP aligns with the principles of least privilege and zero trust by removing standing access and enforcing policies in real time. This not only improves security but also ensures that access is always appropriate, justifiable, and fully auditable.”

A win-win-win scenario for auditors, security teams, and business owners

Zero-Standing Privilege may look different from traditional RBAC, but it addresses the same audit questions—who, why, and how—with greater accuracy, accountability, and security. By replacing static entitlements with real-time, policy-driven access decisions, ZSP eliminates the need for frequent, manual access reviews while generating detailed logs that auditors can rely on.

The result? A system that is not only more efficient but also more secure and transparent.

> "Would you rather review static group memberships that might be outdated—or see real-time evidence that every access decision is justified, logged, and aligned with business policies?"

By replacing static entitlements with real-time, policy-driven access decisions, ZSP eliminates the need for frequent, manual access reviews while generating detailed logs that auditors can rely on.

ABOUT SGNL

In today's era of persistent identity attacks, high-risk standing access is a serious threat to critical enterprise systems. Traditional IGA, RBAC, and PAM approaches fall short because they simply weren't designed for today's identity-centric security perimeter. SGNL's dynamic approach to access management achieves Zero Standing Privilege across your cloud applications like Azure, AWS, GitHub, and Salesforce, as well as on-prem systems.

It's why global enterprises and fast-growing mid-market companies alike are turning to SGNL to reduce their identity attack surfaces, and why SGNL is backed by top security technology investors including Cisco and Microsoft.

SGNL IS BACKED BY LEADING TECH INVESTORS

CISCO investments

M12 MICROSOFT'S VENTURE FUND

REQUEST A DEMO