Understanding Zero-Standing Privilege (ZSP) in financial institutions

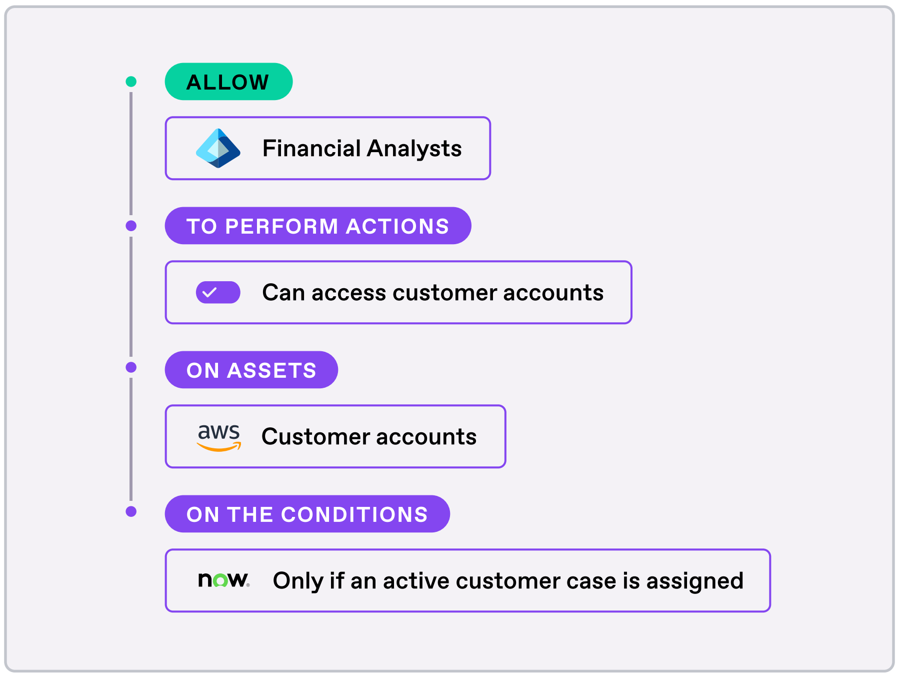
Introduction

Financial institutions are under constant pressure to protect sensitive information and comply with stringent regulatory requirements. While the transition to a zero-trust architecture at the network level has been a significant milestone, the next critical step is adopting Zero-Standing Privilege (ZSP) within Identity and Access Management (IAM) environments.

01

What is Zero-Standing Privilege (ZSP)?

Zero-Standing Privilege (ZSP) is a security approach that ensures no user or system has access to any resources unless it is required at that moment. This "just-in-time" access management model eliminates standing privileges, which can be exploited by malicious actors, and dynamically provisions access based on real-time business needs.



ALLOW

Financial Analysts

TO PERFORM ACTIONS

Can access customer accounts

ON ASSETS

aws Customer accounts

ON THE CONDITIONS

now. Only if an active customer case is assigned

02

The evolution of security in financial institutions

Financial institutions have been pioneers in adopting zero-trust principles, driven by the need to protect highly sensitive data. The shift from network perimeter security to identity-based security has led to the implementation of advanced authentication methods, including passwordless solutions and phishing-resistant MFA. However, securing authentication alone is not enough; standing privileges in cloud environments still pose significant risks.

	Traditional security model	Zero-Trust security model
Security perimeter	Network perimeter-based (firewalls, VPNs)	Identity and device-based perimeter
Access control	Role-based access control (RBAC)	Dynamic, just-in-time access control
Privilege management	Standing privileges granted permanently	Zero-standing privileges (ZSP)
Threat detection	Reactive threat detection (antivirus, IDS)	Proactive, real-time threat detection
Response to breaches	Post-breach analysis and mitigation	Continuous enforcement and instant response
Trust model	Trust based on network location or device	Trust based on continuous verification of identity and context

03

The importance of dynamic authorization

Dynamic authorization, also known as just-in-time access, is a core component of ZSP. This approach aligns with regulatory requirements, such as those set by the New York Department of Financial Services, which emphasizes the importance of context-aware access controls.

→ Dynamic authorization ensures that access is granted only when necessary and revoked as soon as the need expires, reducing the risk of unauthorized access.

04

Eliminating standing privileges: reducing risk

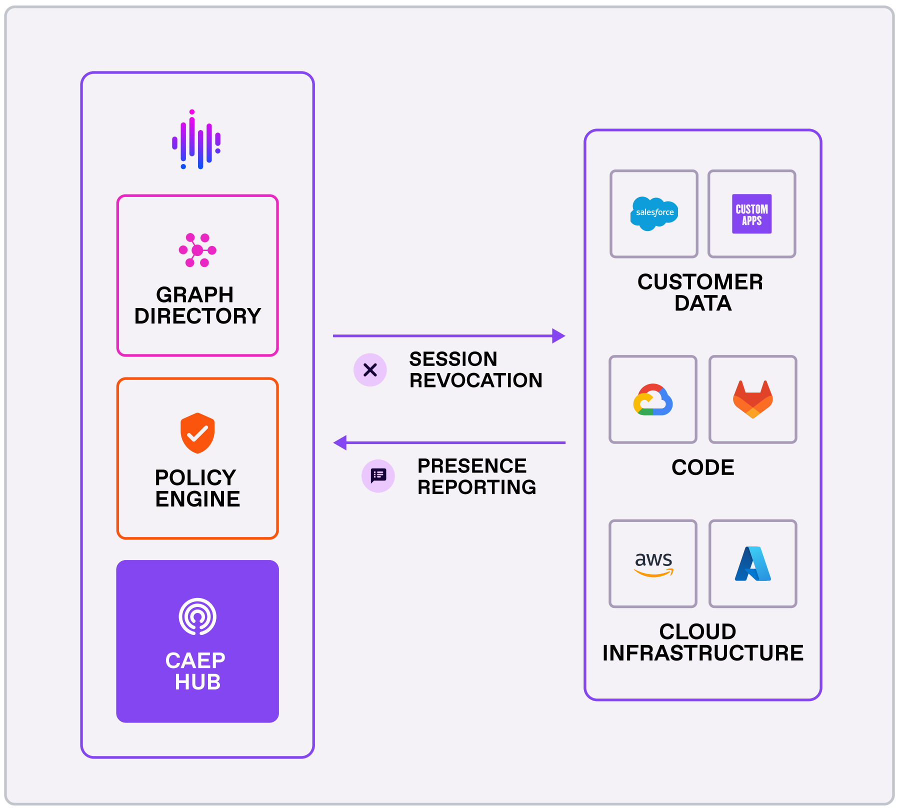
Traditional security models focus heavily on securing authentication processes. However, eliminating standing privileges is equally crucial. By granting access only when there is a legitimate business need, financial institutions can significantly reduce the potential impact of credential compromise.

→ The 2024 Verizon Data Breach Investigations Report indicates that over 80% of breaches involve stolen or compromised credentials. ZSP minimizes the damage from such breaches by making credentials less valuable.

05

Continuous enforcement with CAEP

Continuous enforcement of access policies is critical to maintaining security in a zero-trust environment. The Continuous Access Evaluation Profile (CAEP) enables real-time monitoring and enforcement of access policies, ensuring that any changes in context or behavior trigger immediate access revocation.



FAQ

Q What is the primary benefit of implementing ZSP in a financial institution?

A The primary benefit is enhanced security by ensuring that no standing privileges exist, reducing the risk associated with credential theft and misuse.

Q What is the primary benefit of implementing ZSP in a financial institution?

A The primary benefit is enhanced security by ensuring that no standing privileges exist, reducing the risk associated with credential theft and misuse.

Q Can ZSP be integrated with existing IAM systems?

A Yes, ZSP can be integrated with existing IAM systems, enhancing them with just-in-time access capabilities and continuous enforcement mechanisms like CAEP.

Conclusion

As financial institutions continue to advance their security strategies, moving towards a Zero-Standing Privilege model is essential. This proactive approach not only meets regulatory demands but also significantly strengthens the overall security posture. At SGNL, we are dedicated to guiding our clients through this transition, ensuring that access is always justified, secure, and temporary.

For more information and to see how ZSP can be implemented in your organization, request a demo at sgnl.ai/demo

As financial institutions continue to advance their security strategies, moving towards a Zero-Standing Privilege model is essential.

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