



HOW A FORTUNE 50 COMPANY MINIMIZED RISK

How a leading company eliminated standing access and significantly reduced its blast radius.

Overview




One of the world's largest companies selected SGNL to lock down access management for the critical infrastructure that supports 10s of billions in revenue annually. By eliminating standing privilege to AWS, the company has drastically reduced its potential blast radius while preventing costly employee errors and maintaining compliance with established security policies.

The challenge of limiting damage from identity compromises

As one of the company's largest business units achieved double-digit revenue growth and employed over 100,000 people, ensuring constant availability for its customer-facing websites and back-end systems became a top priority. Despite employing enterprise security tools and the best DevOps and Infrastructure teams in the industry, the company's standing access to cloud production environments posed a serious risk.

If one identity became compromised—or one employee made a mistake—operations could grind to a halt. The financial and reputational damage to a serious business disruption or data exfiltration could be irreversible.

SGNL's impact on the company

-  Achieved **Zero Standing Privilege**
-  Drastically **reduced risk of outages** and data leaks
-  Improved **policy adherence** across systems

These lingering concerns intensified in September 2023 when MGM Resorts suffered a major identity breach that shut down numerous aspects of its business, including electronic payments, ATMs, and customer-facing systems. MGM reported a \$100 million revenue loss over just 10 days of disrupted operations¹.

With nearly 80% of high-profile outages from identity breaches attributable to excessive standing privileges², the Fortune 50 company's Identity Security team endeavored to stop threat actors from compromising user identities and gaining access to critical systems as they did at MGM.

¹ [MGM Resorts cyberattack cost could exceed \\$100M](#)

² [CrowdStrike 2024 Global Threat Report](#)




The solution to standing access: SGNL's modern Privileged Identity Management system

The head of Identity Security singled out AWS as the most critical environment to protect. His team searched for a Zero Standing Privilege (ZSP) solution to:

- Remove standing AWS role assignments from all employees
- Provide on-call staff with appropriate, business-justified, and privileged access to protected systems and applications running in AWS only when ServiceNow tickets for critical incidents or planned changes are properly logged

Manually escalating and rescinding privileges proved far too cumbersome and resource-intensive. The company's existing privileged access management (PAM) and identity governance & administration (IGA) platforms couldn't accommodate this use case and the required workflows to achieve Zero Standing Privilege. Even adding a variety of homegrown identity tools to complement PAM and IGA failed to reduce standing access as intended.

Must-have technical requirements

-  **Systems of Record (SoR)** integration with Ping, Okta, ServiceNow, and AWS
-  **Dynamic assignment of privilege in AWS** based on ServiceNow ticket justification and additional context from a custom data source
-  **Automated session revocation** once the context has changed

The company then turned to SGNL for its modern Privileged Identity Management system that completely eliminates standing access to critical systems and automatically revokes privileged sessions when context changes. From the first discovery call, SGNL's team demonstrated a detailed understanding of the company's environment and their expertise with leading identity and access management (IAM) systems and enterprise SaaS tools.

The head of Identity Security initiated a proof of concept (POC) for a specific use case to ensure SGNL could fully automate sensitive AWS access and achieve Zero Standing Privilege. The process involved the following steps:

1. SGNL verifies that the access comes from valid Okta users attached to a ServiceNow group that's assigned to a specific incident.
2. After the policy is confirmed, SGNL grants access to a custom AWS role with the minimum required privileges for the user. This access would be restricted to the specific AWS account associated with the ServiceNow ticket.
3. Once the ticket is closed or the timeframe specified in the ticket has expired, SGNL immediately revokes the AWS access.

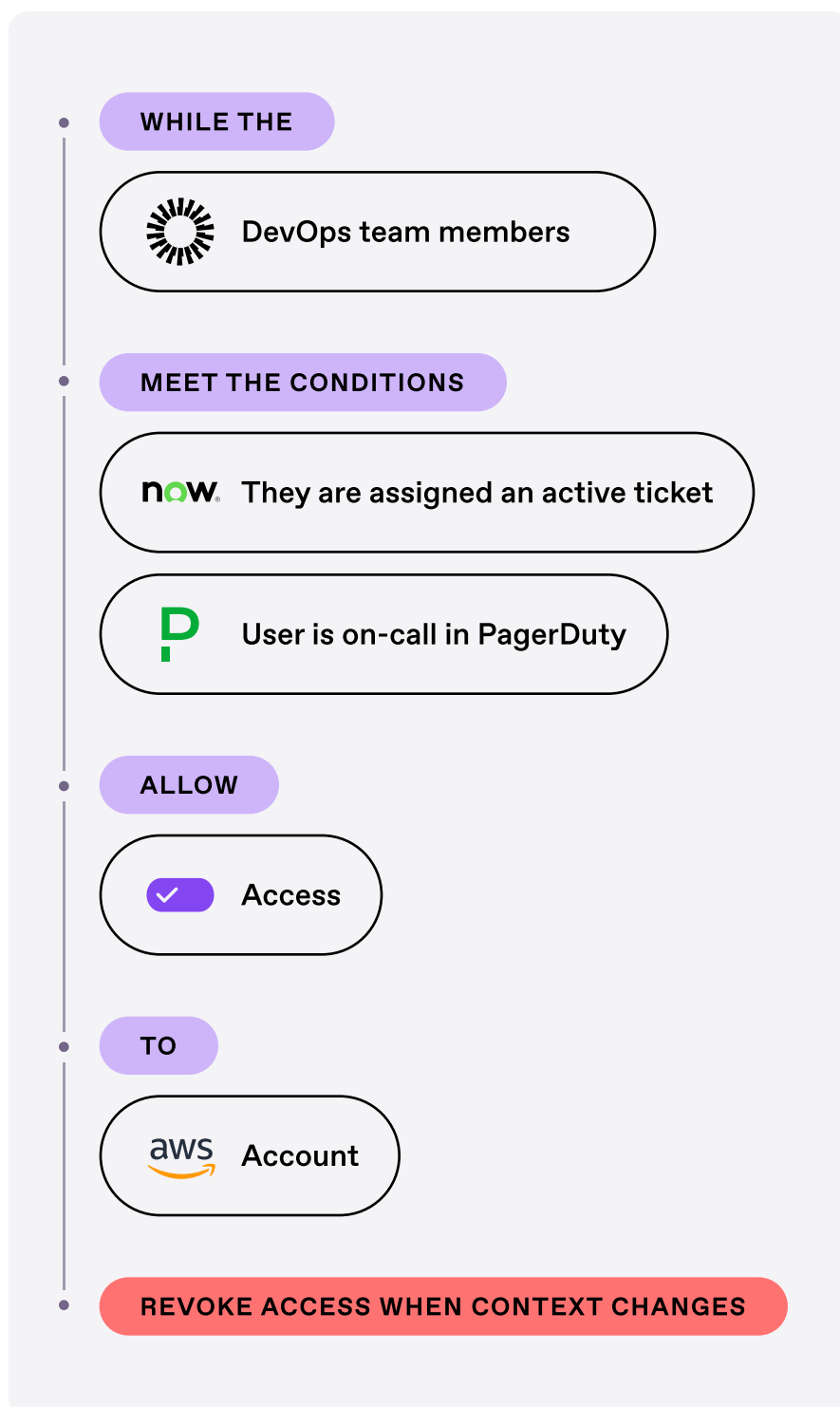


Figure 01. How the company uses SGNL to ensure only valid Okta users with relevant ServiceNow tickets are granted limited access to corresponding AWS environments.

Within several weeks, the POC was deemed a complete success, fulfilling the use case requirements exactly as specified. The positive feedback from the Identity Security, DevOps, and Infrastructure teams — coupled with the SGNL's responsiveness and depth of knowledge — easily convinced the company's leadership to move forward.

Identity security after SGNL's implementation

In a matter of several days, SGNL ingested the relevant data from systems of record, providing exceptional time-to-value. With SGNL's solution now in place, the company can restrict AWS access to users who have a justified business need — and only while that need remains valid.

By eliminating standing access, the likelihood of a compromised identity ever gaining AWS access is negligible. Employees are far less likely to make mistakes in production environments as their access is tied to finite, assigned tasks. The company has reduced its blast radius and odds of an outage or data exposure substantially.

To ensure compliance with corporate security policies across AWS and relevant systems of record, the Identity Security team streamlined policy management in SGNL. Now, technical experts and business leaders alike can understand access policies and modify them as necessary.

Over the next few years, the company will continue rolling out its strategic identity management initiative for key security areas such as dynamic authorization, privileged session revocation, identity-threat detection and response (ITDR), and continuous access management. SGNL's solution for Zero Standing Privilege in AWS will serve as the foundation for many of these planned improvements.

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



[REQUEST A DEMO](#)