

Zero-friction escalation: Afresh automates privileged access with PO Security



About Afresh

Afresh is a San Francisco-based technology company that partners with grocery chains to reduce food waste. Their AI-powered forecasting and replenishment platform improves freshness and efficiency—while cutting climate impact.

Overview

Afresh is an AI-powered platform that helps grocery stores reduce food waste. They serve some of the largest grocery chains in the U.S., training machine learning models on terabytes of data each day.

With sensitive customer data flowing through Snowflake and other cloud systems, Afresh needed to demonstrate strong controls to maintain SOC 2 and internal security standards. At the same time, they couldn't afford to slow their engineering teams—especially during incidents.

AI-driven innovation depends on access to data—and control over it. At Afresh, that means ensuring engineers can move fast while minimizing risk to sensitive cloud systems.

Before adopting PO Security, the Afresh team struggled to balance developer productivity with strong access governance. Microsoft Entra PIM introduced friction and group sprawl that slowed developers down and required constant maintenance from the platform team.

They needed something better—a modern way to grant just-in-time access across systems like Azure, Snowflake, GitHub, and Kubernetes, without writing custom scripts or creating hundreds of brittle groups.

That's where PO came in.



Previously, to provide engineers safe access to critical resources in Snowflake and Kubernetes, we created a patchwork of static groups and roles, used Azure PIM to provide escalated access, and spent a lot of time managing group membership.”

Eugene Yedvabny,

Senior Staff Software Engineer,
Afresh

Challenge

Afresh attempted to implement least-privilege access using Microsoft Entra PIM, but it quickly became a source of overhead. Developers struggled to find the right roles, and escalated access often lingered after incidents.

As their environment scaled, the platform team faced:

- Too much static access across sensitive systems
- Constant permissions drift in Snowflake
- Hundreds of AD groups and manual scripts to manage escalation logic
- Delayed access for on-call engineers, often in the middle of critical incidents

Solution

PO replaced the complexity of Entra PIM with just-in-time automation and clean Slack-native workflows. Afresh now uses PO to govern access across their cloud stack:

- Short-lived access to Azure, GitHub, and Kubernetes via scoped AD groups
- JIT access to Snowflake—even down to specific SQL queries
- Automated drift remediation in production databases
- On-call auto-approvals powered by PO's PagerDuty integration
- Slackbot requests and approvals that keep engineers in flow

Implementation took just one Zoom call.



P0 is a game-changer. Before, we had to choose between access granularity and ease of use. Now we get both. I sleep well knowing long-standing escalated access isn't lurking in any group."

Eugene Yedvabny,

Senior Staff Software Engineer,
Afresh

Why it matters

Afresh's security posture has improved while eliminating manual overhead. P0 automates away the need for access cleanup scripts, reduces group sprawl, and ensures production access is right-sized and ephemeral by default.

More importantly, developer productivity has increased:

- On-call engineers get what they need instantly
- Mean-time-to-resolution has dropped from hours to minutes
- Engineers no longer have to guess which group to request

Results

- Reduced permissions sprawl across Snowflake, Azure, GitHub, and Kubernetes
- Hours of platform team time saved from group maintenance and scripting
- JIT access integrated directly into Slack and PagerDuty
- SOC 2 controls now automatically enforced—no screenshots required
- On-call access is instant—even at 2am