HOW AN AI SECURITY COMPANY BROUGHT CLOUD, SAAS AND EMERGENCY ACCESS UNDER A CENTRAL POLICY FRAMEWORK

About the customer

Industry
AI Security

Environment
Cloud infrastructure, SaaS applications, developer production access

Objectives

- Eliminate standing privilege
- Preserve fast developer workflows
- Improve audit readiness
- Scale to future AI agent use cases

Overview

A fast-growing AI security company needed a scalable way to govern privileged access across cloud infrastructure, SaaS applications and developer workflows. As the engineering organization expanded, so did the number of identities, systems and access paths that required central governance.

The company wanted to eliminate standing privilege without slowing down engineers, adding manual processes or replacing existing IAM investments.

Challenge

- Standing privilege existed across cloud infrastructure, SaaS platforms, developer tooling
- Long-lived credentials increased blast radius
- Emergency access was enabled with excessive and persistent privileges
- Audit preparation required manual evidence collection and identity correlation
- The team needed consistent governance without introducing user friction

> We needed to reduce standing access without creating another high touch process that engineers would inevitably work around. With P0, we could enforce policy across our existing workflows to minimize friction while making access more secure and easier audit."

Security Engineering Leader

AI Security Company

Solution

The company deployed P0 Security as a centralized runtime authorization layer across its existing identity infrastructure. Rather than replacing authentication systems, P0 evaluated every privileged request in real time, enforcing policy, limiting scope and automatically removing access when work was complete.

Key capabilities

- Policy-driven, just-in-time access
- Runtime authorization
- Okta integration
- PagerDuty integration
- Slack integration
- CLI workflows
- Complete audit history
- End-user accountability

Why it matters

The organization established a centralized policy foundation that governs privileged access consistently across people, infrastructure and applications. That same runtime authorization model is well positioned to extend naturally to AI agents and other machine identities as adoption expands.

Results

Minimized standing privilege

- Replaced persistent administrative access with policy-driven, time-bound access
- Applied the same access model consistently across cloud infrastructure and SaaS applications

Safer emergency response

- Preserved rapid on-call access through PagerDuty
- Engineers continued responding quickly during outages without the risk of broad, standing privilege

Simplified compliance

- Every request, approval, grant and revocation automatically recorded
- Eliminated manual audit evidence collection across multiple systems