P0 SECURITY

P0 Security

Secure sensitive systems with runtime access control

Most identity stacks were built around admin time, humans signing into privileged accounts using static credentials. As identity types have diversified to include workloads like AI agents, and environments have expanded across the cloud and SaaS, modern enterprises need security that keeps pace with the speed, sprawl, and flexibility of today's environments.

AI agents dramatically raise the stakes. They can operate across multiple systems, act at machine speed and use permissions inherited from humans, workloads or applications. **What was once a multi-year standing privilege cleanup is becoming a runtime requirement for every identity touching sensitive systems and enterprise data.**

The result is three access problems security teams need to solve:

Multiple identities, no traceability

Every agent action involves at least the originator and the agent. Often, the agent inherits permissions and assumes the identity of their originator, making it difficult to figure out what was done, by whom.

Too much standing access for too long

Originators and agents often have broad permissions or static credentials that exceed the task and remain available long after they are needed.

Lack of enforcement, accountability breakdown

Agent workflows span multiple control points. If identity and policy enforcement are not carried out across the action chain, agents can easily take rogue actions and create unintentional failures, making audit impossible.

Runtime access control for every identity

P0 Security delivers runtime access control by evaluating what an identity is trying to do in the moment, applying least-privilege policy using business context and authorizing just-in-time access directly in the target system.

For AI agents

Govern what agents can actually do by evaluating the agent, originator, delegated identity, target and requested action across the full action chain.

For human users

Replace standing production access with fine-grained, just-in-time permissions that are automatically provisioned and revoked.

For workloads

Discover service accounts, workloads and other machine identities, govern their access and reduce long-lived credentials through automated lifecycle controls.

P0 Security - one control plane for every identity

Discover

Know which identities exist and what they can reach.

- Inventory all agents, users and machines, as well as their permissions and access paths across local and remote environments
- Identify shadow agents, standing access and emerging risk

Control

Decide what an agent can do, when and based on the privilege overlap between the originator and agent.

- Issue a blended identity that preserves the originating user and acting agent for each session
- Enforce runtime policy based on originator, agent, action and resource context, with per-task JIT authorization in target systems to eliminate standing access

Prove

Understand what happened, who initiated it and why it was allowed.

- Capture the full action chain, provenance and attribution from originator through agent, tool and resource
- Monitor activity, access decisions and policy enforcement as actions occur, with audit history for governance, compliance, investigation and accountability

P0 connects directly to sensitive systems through native APIs, without requiring vaults, bastions, proxies or changes to the network path.

- **Agentic platforms -** Amazon Bedrock, Claude, Google Vertex AI, Microsoft Foundry and MCP-connected systems
- **Cloud infrastructure -** AWS, Google Cloud, Microsoft Azure and Oracle Cloud Infrastructure
- **Servers and databases -** Virtual machines, SSH/sudo, PostgreSQL, Amazon RDS, Snowflake and more
- **Workforace and developer applications -** Kubernetes, GitHub, GitLab, code repositories, CI/CD, SaaS and custom applications

Why P0 Security

Built for modern access workflows

Runtime enforcement
Enforce policy where the action happens using the native authorization controls of the target system.

Zero Standing Privilege (ZSP)
Replace persistent access with ephemeral, least-privilege entitlements that expire automatically when the work is done.

Identity-native authorization
Preserve enterprise identity, ownership and business context without creating shared accounts or any manual correlation burden.

API-led architecture
Discover, provision and revoke access through native APIs without the maintenance or friction of vaults, bastions and proxies.

What you can do with P0

- Replace standing production access with just-in-time (JIT) and just-enough privilege (JEP)
- Govern human, machine and AI agent access through one policy layer
- Control AI agents using delegated or inherited permissions
- Discover unowned identities and excessive access
- Centralize audit evidence across access decisions and activity

What makes P0 different

- Runtime enforcement in the target system
- One Authorization Control Plane across users, NHIs and AI agents
- Full originator-to-agent-to-target action-chain context
- No vaults, bastions or inline proxies
- Central revocation when identity or business context changes

Where P0 fits

01 AI agents are reaching sensitive systems
You need to govern what agents can actually do, not only which models, tools or MCP servers they can reach.

02 Engineers or administrators retain standing production access
You want to move to JIT access and ZSP without slowing down engineering or the business.

03 Service accounts and workloads have long-lived access
You need visibility, ownership and lifecycle controls across non-human identities.

04 Your existing PAM architecture does not extend to cloud and developer workflows
You need fine-grained control without forcing access through vaults, bastions or proxies.

05 Auditors are asking how privileged access is governed
You need evidence connecting identity, request, decision, permissions, activity and revocation.

Ready to rethink privileged access?

See how P0 applies runtime access control across agents, users and workloads.

p0.dev/get-a-demo