P0 SECURITY

Secure production access for every identity, every system, all the time

Redefining privileged access for the modern enterprise

The explosion of access paths in modern production infrastructure has outpaced traditional privileged access controls. With identity as the new perimeter, shared accounts, static credentials and standing access to these sensitive systems have become some of the largest risks for enterprises, with 74% of all breaches involving privileged credential abuse.

Shift to Zero Standing Privilege (ZSP)

P0 Security manages the entire privilege lifecycle for users, workloads and agents to programmatically replace standing access with least-privilege, short-lived and auditable production access. **Our mission is to ensure zero standing privileges with zero user friction.**

P0's closed-loop ZSP system

Every stage of this ZSP cycle is focused on optimizing and driving the automation of **just-enough-privilege (JEP) and just-in-time (JIT)** access controls. The combination of granular identity lineage, live posture assessment and runtime policy conversion creates a continuous model that informs and reinforces itself to achieve least-privilege as simply and sustainably as possible.

Global governance for users, workloads and agents

P0's modern Authorization Control Plane centralizes visibility, governance and access provisioning for humans, machines and AI agents. Delivering a consistent user experience and streamlined operations across production systems.

No vaults, static credentials, bastions or manual workflows

Eliminate standing privilege and static credentials

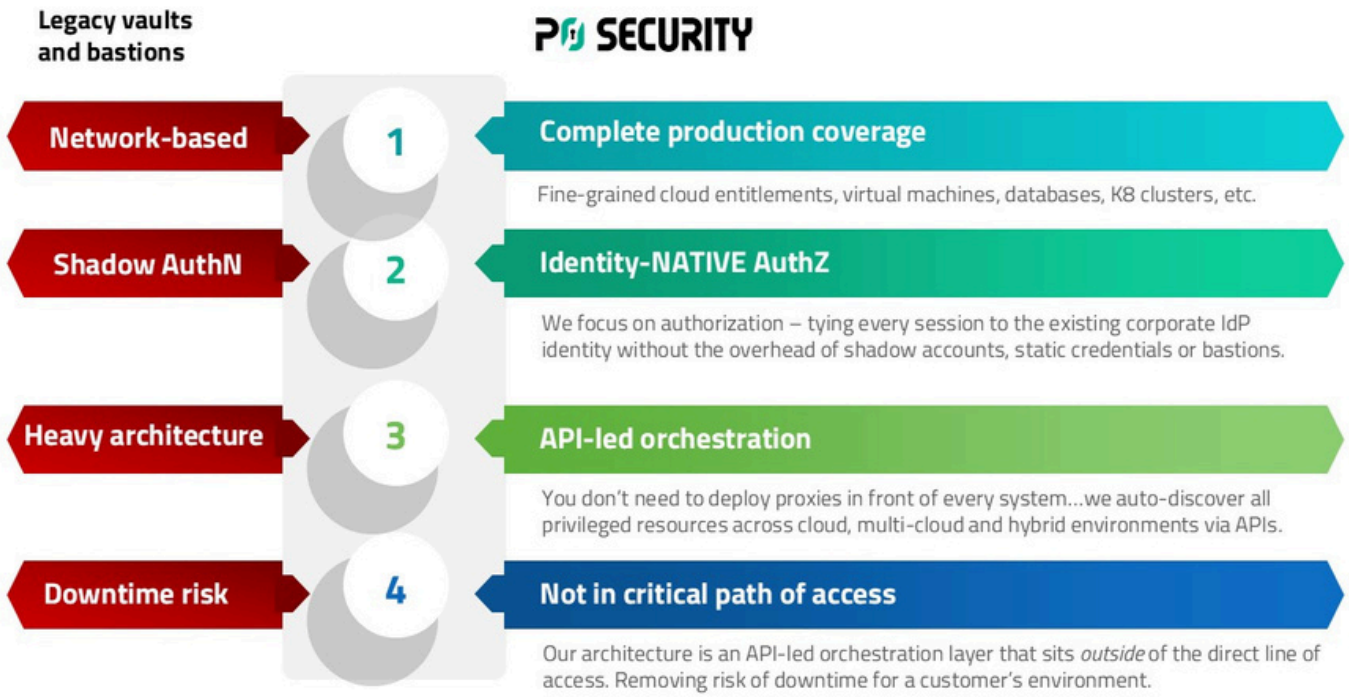
Enforce least privileged, JIT access natively in every system to eliminate standing access and static credentials.

Reduce governance overhead, save on audit prep time

Tie all user, machine and agentic access back to the IdP for end-to-end privilege visibility, informed policy design and continuous audit trails with session recordings.

Simplify operations and streamline developer workflows

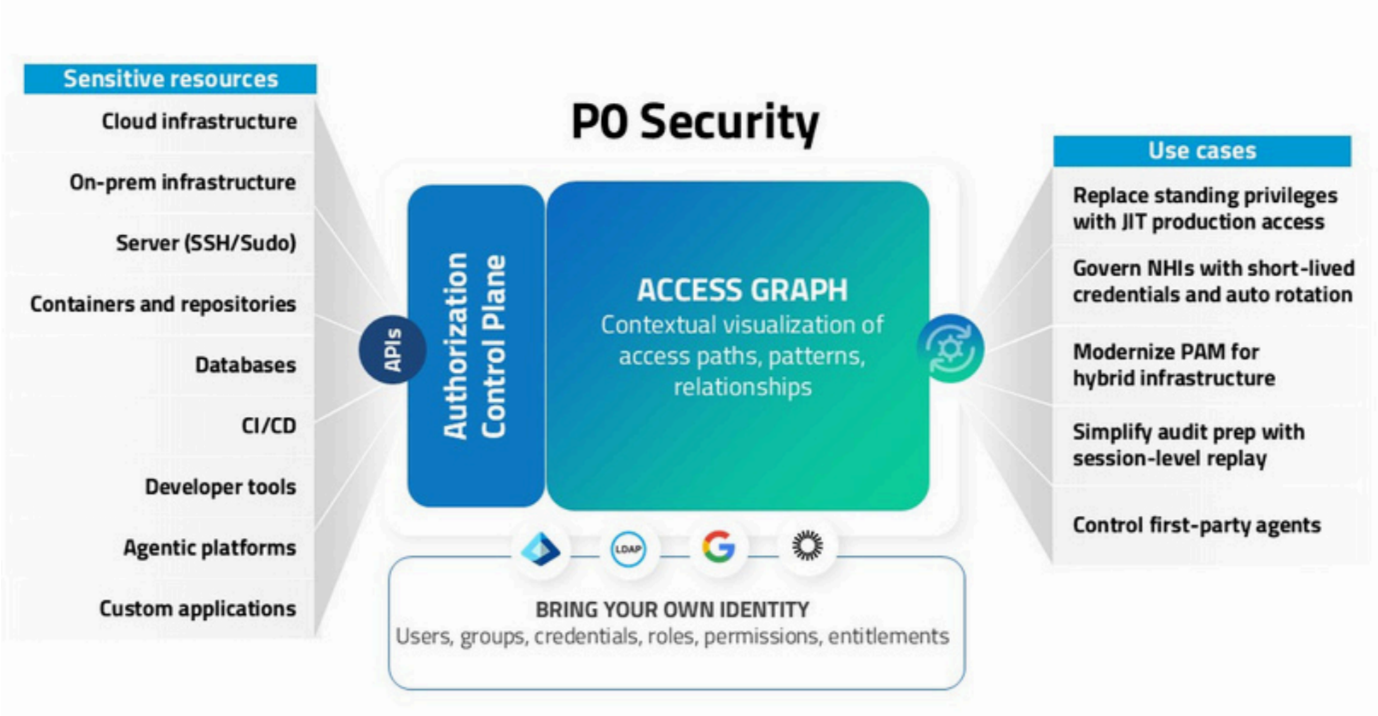
Consistent user experience across any multi-cloud or hybrid production environment that's embedded into existing ways of working via Slack/Teams, email, web console or the P0 CLI.



How it works

P0's identity-native architecture pulls all access related metadata across users, NHIs and agents into a single source of truth. Providing comprehensive context for determining and managing what's privileged across the entire production stack. From code repositories to K8 clusters and from multi-cloud to on-prem databases and servers.

The **P0 Authorization Control Plane** delivers centralized access workflow automations with just-enough-privilege and just-in-time controls to power zero standing privilege at scale.



Access Graph

Discover all privileged access and inform fine-grained policy design

Comprehensive visualization of access paths, patterns and relationships.

Policy Studio

Tailor P0 to your organization's exact policies and risk tolerance

Custom policy design lets teams proactively govern access for consistent, scalable control.

API-driven access

Enforce access governance directly within sensitive systems

Native APIs provision granular access and enforce policies directly in target resources.

P0 is built differently: Bring your own identity!

P0's "Bring your own identity" methodology speaks simply to our focus on provisioning privileged access, not relying on secondary authentication layers.

Identity-native authZ: IdP identities stay intact for complete visibility and granular audit logs.

No shadow authN: Eliminate static credentials, shared accounts, costly infrastructure and needless user friction.

> "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

Let's change the way you manage privileged access...

Extend PAM to multi-cloud and hybrid environments with a central authorization control plane for all users, NHIs and agents.

Access management

Automate least-privilege enforcement, eliminate standing access and static credentials:

- Least-privileged, JIT access
- Auto rotation of secrets for NHIs and service accounts
- IdP identity-native provisioning in any system

Privilege governance

Inform least-privilege policy design, shrink your identity attack surface and simplify compliance:

- Inventory and ownership of any access to production
- Access risk posture and continuous governance
- Session activity recording

Production coverage

Centralize control and streamline the access request user experience for multi-cloud and hybrid production environments:

- SSH/sudo access, databases, K8s, entitlements (AWS, GCP, Azure, OCI) and much more
- Fast and infrastructure free deployment

P0 SECURITY / www.p0.dev