P0 SECURITY

Closing CyberArk's cloud access gap

When cloud entitlements, ephemeral workloads and AI agents demand more

Traditional PAM vendors like CyberArk still play an important role for most enterprise environments where secrets vaulting, credential rotation, session recording and host-based privilege elevation are well established.

Those capabilities are deeply ingrained for most on-prem systems. The challenge is that these platforms were built around static environments and credentials, not dynamic cloud environments, fine-grained entitlements, ephemeral workloads or a proliferation of non-human identities (NHIs).

As organizations decidedly shift toward hybrid and multi-cloud architectures, these gaps become hard to ignore. Teams struggle to extend vault-centric models into environments that expand and evolve faster than static control methods can handle.

Vaults can't keep up

As infrastructure has become ephemeral and access patterns shift from the network layer authentication to authorization layer controls, these traditional tools introduce friction, complexity and sizable coverage gaps.

- **Standing privilege:** Any human or non-human with privileged credentials has persistent access to production, inherently expanding your attack surface.
- **No fine-grained cloud controls:** Enforcement operates at the network layer with course-grained roles, leaving large portions of modern cloud access outside of the vault's control plane.
- **Audit blindspots:** Shared credentials block visibility into which users are taking what actions, degrading accountability and audibility. Approvals, audits, and evidence gathering are manual and inconsistent.
- **Operational overhead and friction:** Heavy, complex infrastructure demands constant engineering effort, delays user access and is often bypassed by developers. Every new system requires costly deployment and management.

Modern environments require purpose-built capabilities

If you're moving from static infrastructure to cloud-native or hybrid workloads, your access strategies must also evolve. The following critical capabilities will augment existing PAM programs to ensure closed-loop zero standing privilege enforcement across hybrid production resources for users, NHIs and agents.

All production access is ephemeral and least-privileged by design.

Privileged access is auditable, policy-driven and automated.

Every identity, whether human, machine or agentic, is tied to a verified IdP user.

Developers have an integrated, frictionless experience when requesting or obtaining access.

P0 Security vs CyberArk

Why CyberArk customers are making the move

Most organizations don't want to rip out their CyberArk vaults and start from scratch nor should they. P0 enables teams to compliment their existing programs by closing their governance gaps across modern production stacks while moving towards Zero Standing Privileges (ZSP). With just-enough and just-in-time access integrated seamlessly into the tools and workflows developer teams already use.

P0 customers gain specialized coverage for the parts of their environment vaults can't cover, while making existing investments more efficient and effective. This allows teams to reduce the friction, risk and costs of legacy PAM solutions over time, without slowing down operations or compromising compliance with standards like ISO 27001 and SOC 2.

Capability	P0 Security	CyberArk
Infrastructure fit	✓ API by design; handles cloud and hybrid environments and ephemeral workloads	✗ Built for static, on-prem environments
Credential model	✓ IdP provisioned, ephemeral	✗ Shared, static, manual rotation
Access model	✓ Fully identity-native; tied to IDP identity	✗ Network-layer controls
Production coverage	✓ Cloud and on-prem servers, databases, Kubernetes, cloud entitlements and more	⚠ On-prem systems
Developer experience	✓ Fast, low touch, integrated with CLI, Slack, Terraform	⚠ Disjointed experience, clunky integrations
Least privilege	✓ Enforced by default via policy	⚠ Manually scoped; least privilege poorly retrofitted
Deployment speed	✓ Get started in hours, see value in days	✗ High overhead due to vaults and connectors
Governance scope	✓ Human, NHI and agentic access governance	⚠ Primarily focused on vaulting and compliance

Why P0 Security

The authorization control plane for modern environments

P0 Security replaces the risk and friction of legacy PAM with it's unified **Authz Control Plane** that secures access across your entire production stack. Instead of managing credentials, *P0 manages the privilege itself,* automating the full lifecycle of access for human users, non-human workloads and AI agents.

Identity-native and agentless: Provision access directly to IdP-federated identities, eliminating shared accounts and manual workflows.

Zero Standing Privileges: Enforce just-enough and Just-in-Time access, replacing static credentials and standing privilege.

Fast and scalable coverage: P0 integrates directly with APIs for fast, resilient and reliable access without proxies, bastions or gateways.

Consistent user experience: Developers can seamlessly request and gain access to any production resources across AWS, GCP, Azure, OCI or on-prem systems.

Addressing your next generation PAM requirements

P0 deploys in minutes, allows security teams to gain full visibility into who's accessing your cloud environments, and empowers DevOps teams with frictionless, fast, developer-friendly workflows.

Granular, flexible authorization controls so roles and policies can be scoped based on need, role or environment.

Global governance enforcement to centrally manage human users, NHIs and AI agents under a single policy framework.

Developer-friendly integrations with CLI, Slack, Terraform for low-friction adoption and developer-speed workflows.

Session-level recording and replay, logging every action in a tamper-evident way for streamlined audit and compliance.

Ready to upgrade your vaults?

CyberArk and BeyondTrust were build for an on-prem world, P0 is built for today's reality.

No vaults. No static credentials. Just seamless, secure, identity-native access, all delivered at DevOps speed.

Get a demo