P0 SECURITY

Access control beyond vault limitations

When cloud entitlements, ephemeral workloads and NHIs demand more

Traditional vendors like CyberArk still play an important role for most enterprise environments where vaulting, rotation, session recording and host based privilege elevation are well established. Those capabilities are required for many on-prem systems. The challenge is that these platforms were built around static servers and shared credentials, not dynamic cloud resources, short-lived workloads or a proliferation of non-human identities (NHIs).

As organizations shift toward hybrid and multi-cloud architectures, these gaps become hard to ignore. Teams struggle to extend vault-centric models into environments that move faster than vaults can handle.

Why vaults can't keep up

As infrastructure becomes ephemeral and access patterns shift from the network layer to API-driven workflows, these traditional tools introduce friction, complexity and sizable coverage gaps.

- **Limited NHI inventory:** No unified view of human, workloads and agents with privileged access to resources. Limited visibility into what is privileged.
- **Unmapped privileged access:** Shared credentials block visibility into which users are taking actions, degrading accountability and audibility.
- **Static credentials:** Managing and rotating static credentials in ephemeral environments becomes an operational burden.
- **Governance overhead:** Approvals, audits, and provisioning are manual and inconsistent.
- **Developer friction and operational overhead:** Complex deployments and workflows introduce friction, delay access, and are often bypassed.
- **Maintenance overhead:** 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.

Every identity, whether human, workload or agent, is federated with your IdP

No static users, keys, or tokens exist anywhere. All credentials are short-lived and scoped to the minimum required privilege

Privileged access is auditable, policy-driven, and automated

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

P0 Security vs CyberArk

Why CyberArk customers are making the move

With P0 Security, organizations don't need to replace their vaults and start from scratch. Teams are able to close their governance gaps across modern production stacks by replacing standing privilege with just enough privilege and just-in-time access by default. Integrating seamlessly with the tools and workflows developer teams already use.

P0 customers gain specialized coverage for the modern parts of their environment while making existing vault 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	✗ Vault-based; static, manual rotation
Identity model	✓ Fully identity-native; tied to IDP identity	✗ Not identity-native; relies on static credentials and shared accounts often with vast privileges
Production coverage	✓ Cloud and on-prem servers, databases, Kubernetes, cloud entitlements and more	⚠ On-prem systems
Developer experience	✓ Fast, simple; works with CLI, Slack, Terraform	⚠ Heavy, slow deployments; poor integrations
Least Privilege posture	✓ 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

P0 Security: built for hybrid infrastructure and agile production

P0 is redefining PAM for hybrid and modern enterprises. P0 does not rely on vaults, static credentials or shared accounts. It integrates natively with your identity provider and cloud platforms through APIs. Every form of privileged access, whether an SSH session or a privileged entitlement, is tied to an identity and governed centrally.

Identity-native and JIT: Access is tied to a verified user IdP identity, granted just-in-time and automatically revoked after use. No shared accounts or credential handoffs.

Infrastructure and maintenance free: P0 integrates directly with APIs for fast, resilient, and reliable access, without the infrastructure overhead.

Least-privilege by default: All access is scoped, ephemeral, and policy-enforced.

Developer-first: Integrated with CLI, Slack, Terraform for low-friction adoption and developer-speed workflows.

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 and flexible access control so roles and policies can be scoped based on need, role, or environment.

Consistent user experience for requesting and gaining access to AWS, GCP, Azure, OCI or on-prem resources.

Session level recording and replay, logging all actions in a tamper-evident way for audit and compliance.

Unified governance at enterprise scale so teams can centrally manage SSH/sudo access, RDP access, databases, Kubernetes, cloud entitlements and cloud resources under a single policy framework.

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