PO SECURITY

PO Security transforms SSH/Sudo access for cloud and on-prem production servers

Organizations increasingly rely on a mix of cloud-native (AWS, GCP, Azure) and on-premises compute infrastructure. Yet traditional SSH/sudo access workflows remain rooted in vaults, static credentials and jump-hosts.

These legacy approaches lead to a proliferation of static credentials, standing privileged access and a poor developer experience that disrupts workflows and delays access. This simply does not meet the scale and flexibility required by modern hybrid environments.

PO's approach to SSH/Sudo

PO is redefining PAM for the modern enterprise, beyond vaults into identity-native, agent-free, API-led workflows. Eliminating static SSH keys or the need to route access through jump servers. **With PO users can:**

1. Grant short-lived, fine-grained JiT access to designated machines for a preset duration of time
2. Automatically expire access, eliminate static SSH keys and standing access
3. Provision SSH/sudo access that is always tied to the IdP identity and logs the session recording under that verified user identity

All with seamless developer workflows via Slack/Teams, web console, or the CLI.

Watch this video to see how PO eliminates the friction that comes with vaults.

Capabilities

- Provisioning short-lived SSH/sudo access to cloud or on-prem servers for users
- Granting or revoking Sudo (privileged) access dynamically
- Consistent user experience for requesting and gaining access to AWS, GCP, Azure, OCI or on-prem servers
- Logging all actions in a tamper-evident way for audit and compliance

Outcomes

- **Identity-native and JIT access:** Every SSH/sudo session is tied to a verified user IdP identity, access is granted just-in-time, automatically revoked after use
- **Infrastructure and maintenance-free:** PO is fully cloud-native, requiring no bastions, proxies, or jump hosts to deploy or maintain
- **Granular and flexible access control:** Roles and policies can be scoped to allow standard SSH or sudo access based on need, role, or environment
- **Unified governance at enterprise scale:** Manage SSH/sudo access, databases, Kubernetes, and cloud entitlements under a single policy framework
- **Fast deployment, measurable impact:** Configure and start using PO Security in hours...not weeks.

Getting started with P0 SSH/Sudo access

Setting up SSH/Sudo access with P0 takes just a few steps.

Simply connect your cloud account (AWS, GCP, Azure, OCI) in the P0 dashboard, link your compute instances, and sign in using your existing identity provider. Once configured, team members securely request and launch SSH/sudo sessions directly from the P0 CLI. No jump servers, VPNs, or long-lived keys required.

You can also define routing policies to direct access workflows based on roles, instance types, or environments, ensuring the right people get the right access through approved paths. The entire process takes under an hour and scales automatically as your environment grows.

Sample workflow