Just-in-Time Access for DevOps

Privileged Orchestration and Infrastructure Automation Security

Keep your organization secure and your engineers productive with Zero Standing Privileges, ephemeral credentials, and secure infrastructure automation.

Modern infrastructure is operated by CI/CD pipelines, Kubernetes clusters, automation platforms, and machine identities. Traditional PAM solutions were built for static infrastructure and struggle to secure high-velocity cloud-native operations without introducing operational friction.

PrivX PAM enables organizations to secure privileged access for DevOps teams across GitLab, Kubernetes, Ansible, and cloud infrastructure using identity-based controls, ephemeral access, and centralized governance.

Benefits

Reduced attack surface

Eliminate static credentials and overprivileged access within the automation tooling environment.

Improved engineering velocity

Reduce deployment friction while maintaining strong security controls and fine-grained access control.

Centralized governance

Improve auditability, compliance readiness, and infrastructure visibility.

1. Secure CI/CD

- Remove standing privileges from GitLab pipelines
- Dynamically inject credentials
- Apply fine-grained policy controls to CI/CD runner execution
- Centralize policy enforcement

2. Ephemeral Kubernetes access

- Give Just-in-time access for kubectl
- Enable R/O vs R/W cluster access via the API endpoint
- Full session recording of Kubectl activity
- Securely manage secrets using the PrivX K8s Secrets Operator

3. Secure automation governance

- Secure Ansible Orchestration Workflows
- Remove static credentials (ephemeral certificates)
- Control playbook execution
- Manage secrets in a secure Vault

4. Zero Standing Privilege

- Elevate access only as needed
- Automate approval workflows
- Automatically revoke privileges
- Authorize based on identity

5. Infrastructure access control

- Secure access across cloud and hybrid environments
- Enforce RBAC for infrastructure operations
- Centralize governance for machine identities
- Reduce privileged credential exposure

6. Cloud-native architecture

- Secure Kubernetes and CI/CD environments
- Scale easily with microservices architecture
- Deploy quickly Hybrid and multi-cloud deployment support
- Enable engineering teams

Why PrivX PAM for DevOps?

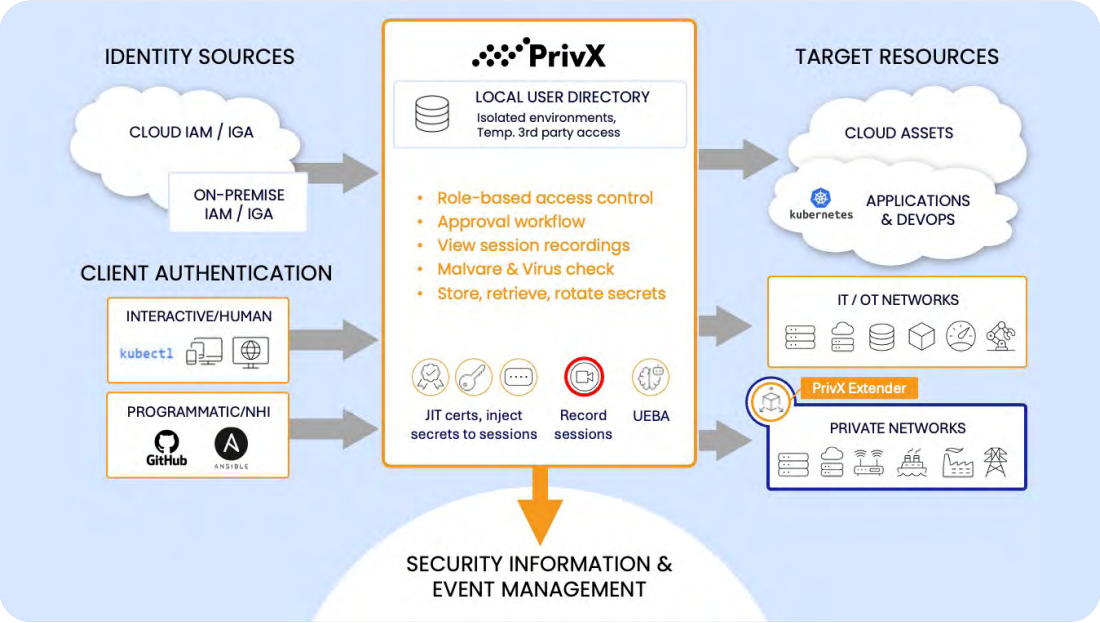
Built for modern, ephemeral infrastructure operations, PrivX PAM helps modern organizations secure privileged access across GitLab, Kubernetes, Ansible, and cloud environments without compromising engineering productivity and velocity.

Stay secure.

Stay competitive.

1.5M

SSH authorized keys removed and migrated to ephemeral certificates in a customer's environment



Global enterprise modernizes privileged access for DevOps and CI/CD automation

Challenges

The company relies on CI/CD pipelines, automation frameworks, and configuration management tools to manage production infrastructure at scale. Static SSH keys, embedded secrets, and long-lived credentials across DevOps workflows created operational and security risks. Traditional PAM solutions introduced too much friction for engineering teams and failed to support the speed and agility required for cloud-native infrastructure operations.

Solutions

The organization implemented modern PAM controls using ephemeral certificates, identity-based authentication, and Just-in-Time access workflows across their CI/CD and automation environments with PrivX. By integrating directly into DevOps and configuration management processes, the organization eliminated standing credentials while improving governance and auditability across infrastructure operations.

Results

They strengthened their security without introducing friction for engineers, reduced credential sprawl and operational complexity, and improved deployment efficiency and visibility. Engineering gained streamlined access workflows without sacrificing productivity and security teams strengthened governance through centralized auditing, reduced standing privileges, and improved control over machine-driven access to production systems.