PrivX PAM

Secure Non-Human Identities: Runtime Identity Control for the Machine-Driven Enterprise

Modern infrastructure is no longer operated primarily by people. Cloud workloads, Kubernetes clusters, CI/CD pipelines, automation platforms and APIs now perform a growing share of privileged operations. Traditional PAM solutions were built for privileged human users and static infrastructure. They struggle to secure dynamic, machine-driven environments without slowing automation or introducing operational friction.

PrivX PAM enables organizations to secure privileged access for non-human identities (NHIs) using identity-based controls, ephemeral credentials, runtime authorization, and centralized governance. As organizations expand automation, PrivX PAM extends Zero Standing Privileges beyond human users to NHIs operating across hybrid and cloud-native environments.

Benefits

Reduce Credential Risk

Eliminate long-lived machine credentials and replace them with ephemeral, identity-bound access that dramatically reduces the attack surface.

Accelerate Secure Automation

Enable cloud-native operations, DevOps pipelines, and AI-driven workflows without introducing friction for engineering teams.

Unify Identity Governance

Manage privileged access consistently across humans, workloads, services, and automation through a common policy framework.

1. NHI Governance

- Manage workloads, services, APIs, etc. as first-class identities
- Clearly distinguish human and non-human identities
- Centralize lifecycle and policy management
- Create a complete audit chain from identity to action

2. Workload Identity Security

- Replace static credentials with short-lived identities
- Support workload identities
- Secure Kubernetes, virtual machines, cloud instances, and containers
- Continuously verify workload identity before granting access

3. Runtime Authorization

- Apply fine-grained authorization at the action level
- Continuously evaluate identity, target, and context
- Enforce least privilege

4. Zero Standing Privilege

- Eliminate long-lived credentials
- Broker short-lived access when required
- Automatically revoke privileges
- Reduce credential sprawl across cloud infrastructure

5. Continuous Auditing

- Trace every privileged action from identity to target
- Correlate humans and workloads
- Centralize monitoring and compliance reporting
- Improve forensic investigations

6. Cloud-Native Control

- Secure Kubernetes, CI/CD, cloud, and hybrid infrastructure
- Integrate DevOps workflows
- Scale using cloud-native microservices
- Extend Zero Trust across human and machine identities

Why PrivX for NHIs?

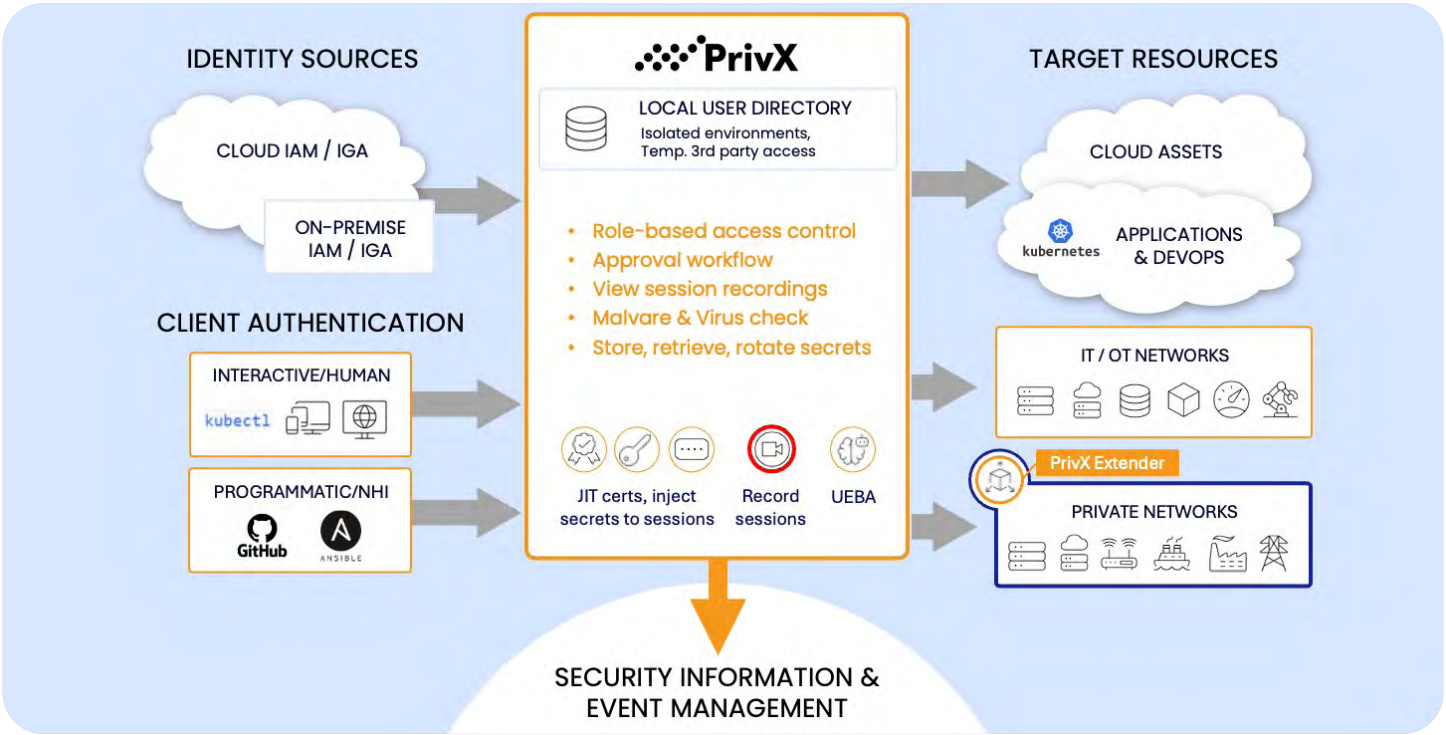
Built for modern, cloud-native infrastructure, PrivX PAM secures privileged access across workloads, services, automation platforms, Kubernetes and APIs without sacrificing operational agility.

Rather than extending legacy password vaults to machines, PrivX provides ephemeral access management using identity-bound sessions, ephemeral credentials, continuous authorization, and centralized auditing. This enables organizations to secure machine-driven privileged access and prepare for the next generation of NHIs.

50,000+

Non-human identities in a typical cloud-native 500-user enterprise*

* Modern organizations can manage between 5,000 and more than 50,000 non-human identities depending on cloud adoption, automation, and application architecture.



Global Enterprise Secures Non-Human Identities

Challenges

The organization relied on thousands of NHIs across cloud infrastructure, Kubernetes, CI/CD pipelines, APIs, and automation platforms. Long-lived credentials, service accounts, embedded secrets, and inconsistent workload identities created growing operational complexity and security risk. Existing PAM solutions focused primarily on human administrators and lacked the runtime controls needed for machine-driven environments.

Solutions

The organization deployed PrivX to secure workloads, automation platforms, and AI-enabled services using identity-bound authentication, ephemeral credentials, runtime authorization, and centralized policy management. By replacing standing credentials with short-lived identities and continuously enforcing access policies, the organization strengthened Zero Trust security without disrupting automation. Future workload identity support through SPIFFE/SPIRE further simplified machine identity management across dynamic cloud-native environments.

Results

The organization reduced credential sprawl, improved governance across thousands of machine identities, and established complete traceability from identity to action. Security teams gained centralized visibility into privileged machine activity, while engineering teams accelerated cloud automation without sacrificing agility. The organization is now positioned to securely adopt AI agents using the same solution that already governs privileged human and machine access.