PO SECURITY

A PRACTICAL LOOK AT GOVERNING NON-HUMAN IDENTITIES (NHIS)

SECURING THE FASTEST-GROWING ATTACK SURFACE

Most identity programs stop at people. Modern infrastructure doesn't.

In today's environments, **non-human identities (NHIs)** such as CI/CD jobs, service accounts and AI agents outnumber employees by more than twenty to one. They deploy code, move data and interact with production systems every day. Yet most operate outside of corporate governance programs. They have credentials that never expire, access no one owns and permissions that collect quietly over time.

That's the latest identity risk gap.

THE RISK BEHIND EVERY UNATTENDED IDENTITY

Risk	What it means in practice
Static credentials	Long-lived tokens and API keys grant standing access with no expiration or oversight
No ownership	Few teams can say who is accountable for a service account or what its intended use is for
Over-permissioned roles	Most NHIs run with more broader roles than needed, widening the blast radius
Credential drift	Secrets get copied, reused and embedded into code without controls
Limited visibility	Vaults store credentials but don't govern how they're used or when they should expire

When a machine identity is compromised, there's often no way to easily trace access and no user session to lock out. It acts in blind trust and moves undetected through critical systems, with hidden drift and misconfigurations that remain until an attacker exploits and exposes them.

WHAT GOOD GOVERNANCE LOOKS LIKE

Effective NHI governance mirrors what you already do for people, just adapted for machines and agents.

01

Discover and inventory every NHI across clouds and tools

02

Assign ownership so each identity has an accountable person or team

03

Define scope with least-privilege policies tied to business intent

04

Enforce expiration so credentials are short-lived and just in time by default

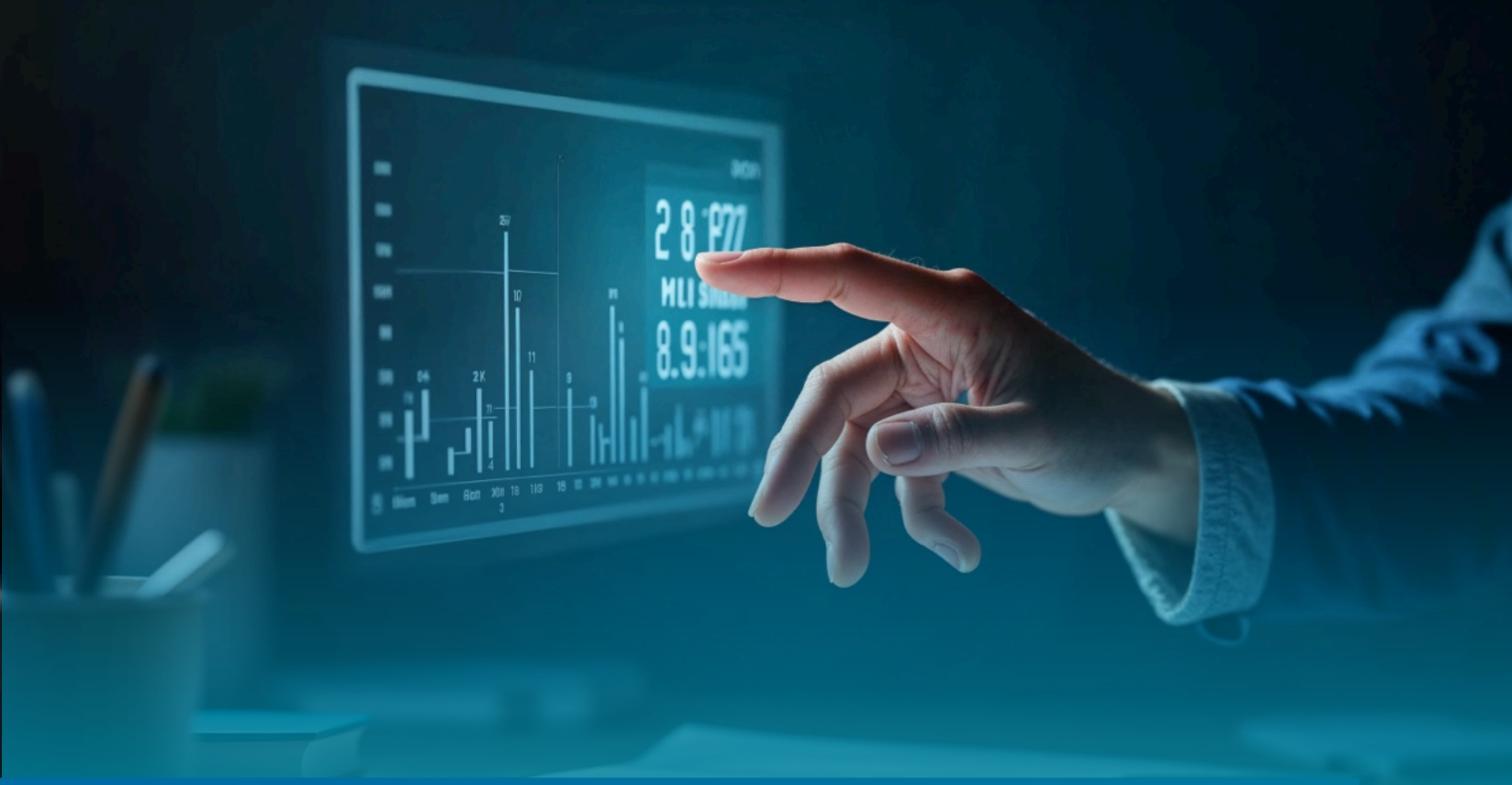
05

Automate rotation and revocation as and when access is no longer needed

06

Monitor for governance drift and flag policy violations automatically

Governance is not a one-time cleanup. It's an always-on process that treats every credential as an access-granting entity throughout its entire lifecycle.



A MATURITY PATH FOR GETTING CONTROL

Each phase builds on the last to shrink risk while reducing manual effort.

Phase	Focus	Outcome
Audit	Identify all NHIs and credentials using discovery or access control tools	Visibility into scope and exposure
Federate	Replace static, privileged credentials with role assumption and or identity federation	Removal of persistent secrets
Restrict	Block creation of new long-lived credentials through least-privilege policies and guardrails	Reduced credential sprawl
Automate	Rotate and expire remaining credentials through contextual policy enforcement	Consistent access hygiene
Govern	Manage access continuously through identity-native controls	Full lifecycle governance

HOW P0 SECURITY HELPS

P0 Security delivers continuous, identity-native access governance for human users, NHIs and AI agents.

Automated discovery across hybrid production environments

Ownership tagging at creation through existing IdP or active directories

Just-in-time and ephemeral access that eliminates standing privilege

Policy drift detection of any violations for new or unmanaged credentials

Native governance enforcement that embeds policies into workflows via API

With P0, every credential is created with purpose, scoped by policy and retired when no longer needed.

Let's change the way you manage privileged access...

Extend PAM to multi-cloud and hybrid environments with a central authorization control plane for all users, NHIs and agents.

Visit www.p0.dev for a demo or to start your free trial.

P0 SECURITY

Contact Us

Email: info@p0.dev
Web: www.p0.dev

P0 Security helps companies modernize Privileged Access Management (PAM) for multi-cloud and hybrid environments with the most agile way to ensure least-privileged, short-lived and auditable production access for users, NHIs and agents. Centralized governance, Just-Enough Privilege and Just-in-Time controls deliver secure access to production, as simply and scalable as possible.
Every identity. Every system. All the time.

P0's Access Graph and Identity DNA data layer make up the foundational architecture that powers privilege insights and access control across all identities, production resources and environments.

With P0, production access is least-privilege, short-lived and auditable by default, including the new class of AI-driven agentic workloads emerging in modern environments.

EB_GovNHIs_012026