Infisign

Securing the Invisible Workforce

A CISO Playbook to Manage and Protect Non-Human Identities in 2026

Table Of Contents

- The New Frontier: Non-Human Identities in 2026
- How NHI Attacks Happen And Why Old Defenses Fail
- The CISO Playbook: Securing the NHI Lifecycle
- From Playbook to Practice
- How Infisign Secures the Invisible Workforce

Not every “user” in your business has a desk, a payroll number, or even a human heartbeat.

In fact, in 2026, most of them don’t.

They’re API keys, service accounts, security certificates, robotic scripts, and AI agents, quietly working behind the scenes to run your business. They move data, deploy code, connect systems, and process transactions. They don’t take lunch breaks. They don’t ask for a vacation. And you probably don’t have them all written down anywhere.

These are non-human identities (NHIs)—the fastest-growing category of accounts in your company. Most organizations don’t know exactly

How many exist, what they can access, or whether they’re still needed.

That’s not just untidy record-keeping. It’s a wide-open security risk. When left unchecked, NHIs become invisible backdoors into your systems, and attackers know it.

This playbook will show you:

- How attackers exploit NHIs in the real world
- Why legacy defenses fail to stop them
- The lifecycle approach CISOs are using to control the problem
- How Infisign can make this manageable at enterprise scale

The New Frontier:
Non-Human Identities in 2026

Non-human identities (NHIs) now make up the majority of accounts in most organizations. On average, there are 92 NHIs for every human identity, and their growth shows no sign of slowing. The problem isn't just the scale. Almost 97% have more access than necessary, and 71% go unrotated for months or years, making them prime targets for attackers. (source)

These identities aren't people, but they're just as powerful. They deploy your code, process your transactions, and connect your systems behind the scenes. And unlike human users, they rarely raise suspicion when they work outside of normal patterns.

Why They're Attractive Targets

Attackers love NHIs because they:

- Aren't tied to an employee record in HR systems.
- Rarely require multi-factor authentication.
- Are often created quickly for projects and never deleted.
- Sometimes have sweeping access to critical infrastructure.

A compromised NHI can function like a master key — one that opens many doors without raising alarms.

Type	Purpose	Risk If Compromised
API keys & tokens	API keys & tokens Let software components communicate	Direct access to services or sensitive data
Service accounts	Run background processes or jobs	Often have broad, persistent permissions
Certificates & SSH keys	Prove identity and secure connections	Can be used to impersonate systems
Bots & RPA scripts	Automate business or IT tasks	Could be hijacked to process fraudulent actions
AI agents	Make autonomous decisions, run code	May execute malicious instructions at scale

The Most Common Weaknesses

OWASP's 2025 Non-Human Identities (NHI) Top 10 lists the most critical risks, including:

1. **Improper Offboarding:** Accounts left active after their work is done.
2. **Secret Leakage:** Passwords, keys, or certificates exposed in code or stored unsafely.
3. **Over-Privileged NHI:** Broader access than the job requires.
4. **Long-Lived Secrets:** Credentials that never expire or rotate.
   NHI Reuse: The same credentials shared across multiple systems.

These aren't rare edge cases; they're everyday realities in environments where NHIs outnumber people. And in security, what you can't see is what can hurt you the most.

How NHI Attacks Happen And Why Old Defenses Fail

Attackers don't need to smash through your firewall or trick a person with a phishing email. They can just log in—as a machine.

Attack Path	Example	Impact
Leaked keys in code	A developer commits a file with an active access key. Automated bots find it within minutes.	Opens direct access to databases or services, often without triggering alerts.
Over-privileged accounts	Over-privileged accounts Run background processes or jobs Often have broad, persistent permissions	Gives attackers full control of systems far beyond the bot's intended scope.
Orphaned credentials	A retired service's login details remain valid for months, eventually discovered and abused by attackers.	Allows unauthorized access long after the service is decommissioned.
Pipeline compromises	Automation accounts in software build pipelines are hijacked to push malicious updates into production.	Inserts backdoors or malicious code directly into live systems
AI agent misuse	An AI tool with broad permissions is manipulated into running dangerous commands or stealing data.	Executes high-impact actions at speed, often without human review.

Why legacy defenses fail

Most identity tools and processes were built for people, logins you can see, track, and reset. NHIs break that model:

- They may never log in the "human" way, so behavioral detection doesn't trigger.
- Credentials can be valid for years if no one rotates them.
- Permissions often aren't reviewed, so excess access lingers.
- They're invisible in standard headcount and offboarding processes.

Without dedicated visibility and lifecycle management, you can't control them, and attackers know it.

The CISO Playbook:
Securing the NHI Lifecycle

NHIs need the same governance as human accounts and, in some cases, stricter. That's because they work faster, at a larger scale, and without the human sense of "something feels wrong."

That's why the most forward-thinking security leaders are adopting a lifecycle approach, managing every NHI from creation to retirement, with continuous checks in between.

You can't secure what you can't see. The first step is to identify every NHI in your environment, no matter where it lives. That includes:

- Cloud platforms (AWS, Azure, GCP)
- Software build and deployment pipelines (CI/CD)
- On-prem directories
- Code repositories
- Certificate and key stores

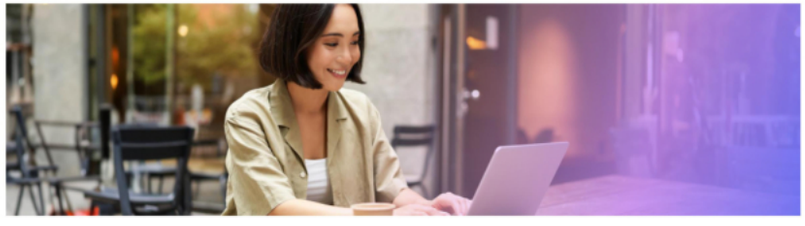
Once found, tag each identity with key attributes:

- Owner: Who is responsible for it?
- Purpose: What function does it serve?
- Permissions: What systems and data can it access?
- Creation date and last activity: How old is it and is it actively used?

Then, prioritize high-risk NHIs:

- Admin-level privileges
- Broad network access
- Access to sensitive or regulated data

This classification ensures your most dangerous identities are secured first, reducing the biggest risks early.



02 Govern & Control — Set Rules and Keep Everyone Accountable

Governance is about ownership and policy. Every NHI should have a named owner, a specific person or team, who is accountable for its creation, usage, and retirement.

Without this, "orphan" identities accumulate, creating unmonitored entry points for attackers.

Key governance practices:

- **Least privilege by default:** Give the NHI only the access it needs, and only for as long as it needs it.
- **Time-bound permissions:** Automatically expire access for temporary projects.
- **Avoid static credentials in code:** Replace with workload-based access (where systems prove their identity dynamically) or use centrally issued credentials.

With governance in place, you eliminate shadow identities, prevent over-privilege, and make it easier to track and audit every NHI.

03 Protect & Automate — Reduce Human Error and Close Gaps Faster

Once you've set governance, protection comes from strong controls, and automation ensures those controls are applied consistently.

Best practices include:

- **Centralize all credentials:** Store keys, tokens, and certificates in a secure vault with strict access controls.
- **Automate rotation:** Credentials should expire automatically, ideally within hours or minutes, so stolen ones become useless quickly.
- **Integrate security into development:** Use secret scanning in CI/CD pipelines to block any attempt to commit sensitive information into code.

Automation matters because manual processes simply can't keep pace with the number and turnover of NHIs in a modern environment.

04 Retire & Respond — End Access the Moment It's No Longer Needed

The fastest way to reduce risk is to remove unnecessary access. That's why retiring NHIs promptly is just as important as creating them securely.

Key actions:

- **Event-driven revocation:** When a bot, service, or agent is decommissioned, its credentials are revoked automatically, no exceptions.
- **Continuous monitoring:** Watch for unusual patterns, like a bot accessing systems it's never touched before.
- **Detailed logging:** Keep complete records of NHI activity for compliance audits and incident investigations.

A strong retirement process closes the "forgotten account" loophole — one of the top entry points attackers exploit.

From Playbook to Practice: How Infisign Secures the Invisible Workforce

Everything above takes constant monitoring, automation, and enforcement. Manual spreadsheets won't keep pace when NHIs can number in the tens of thousands.

That's where Infisign comes in.

Infisign is a unified identity security platform that treats non-human identities with the same seriousness and automation as human ones.

Key capabilities of Infisign:

Unified Discovery: Finds every identity, human or machine, across your systems.

Automated Lifecycle Management: Creates, rotates, and retires credentials without manual effort.

Zero Trust Enforcement: Ensures every NHI gets only the access it truly needs, and only for as long as it needs it.

Integration-Ready: Works with your existing tools, from cloud IAM to DevOps pipelines.

Continuous Monitoring: Flags suspicious activity in real time so you can respond before damage is done

How Infisign addresses the OWASP NHI Top 10 risks:

Improper Offboarding: Auto-removes NHIs when services retire.

Secret Leakage: Keeps keys out of code with secure vaulting.

Over-Privileged NHI: Enforces least privilege and reviews regularly.

Long-Lived Secrets: Rotates credentials automatically before they become stale.

NHI Reuse: Assigns unique identities to each service to prevent lateral compromise.

Making the Invisible Visible

Your invisible workforce isn't going away; in fact, it's growing daily.

The CISO playbook gives you the strategy to find, govern, and protect them. Infisign gives you the tools to do it at scale, automatically, across your entire environment, without slowing your business down.

Infisign was built for this challenge.

- See every NHI in your environment.
- Control their access with precision.
- Remove them instantly when they're no longer needed.

It's time to turn the invisible workforce into a secure, accountable one.

End NHI Security Gaps with an AI-Powered IAM

Ready to See How Infisign Protects Vulnerable Tech With AI-Based NHI Management?

Book a free trial now

www.infisign.ai