opentext™

WHITE PAPER

Conquering the non-human identity explosion

Rethinking the perimeter: identity at the core of your defense

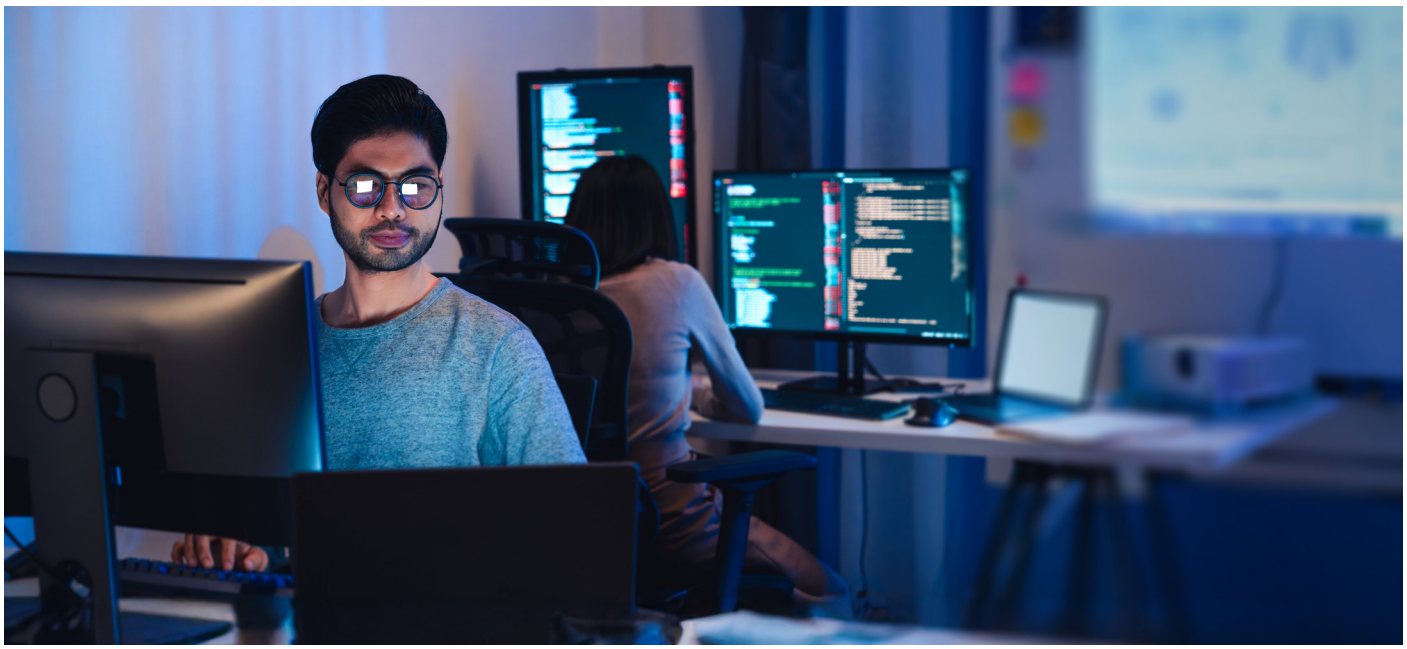
Contents

Executive summary

Non-human identities (NHIs)—the service accounts, bots, APIs, and AI agents running today's digital enterprises—now vastly outnumber human users, in some cases by more than **100 to 1**.[1] And its growth is accelerating. **This surge has created the single largest unmanaged attack surface in modern IT**. Unlike employees, NHIs are often created without oversight, rarely retired, and frequently carry excessive privileges. The result is a sprawling, invisible workforce that attackers increasingly exploit to gain persistence and access sensitive data.

Traditional identity systems, designed around human lifecycles, are failing to keep pace. Securing NHIs requires a new approach: Non-human identity management (NHIM). This strategy requires that zero trust principles be applied to every identity—human or machine. It means that organizations need to equip themselves with automated discovery, centralized governance, continuous monitoring, and secrets management across all their identity stores, not just the precious few that are typically done today. The goal is clear ownership, least-privilege access, and rapid credential rotation to close the gaps left by static and orphaned accounts that saturate many organizations' digital environment.

The message is urgent but actionable: NHIs are no longer a background concern, they are the dominant population in the enterprise. Treating them with the same rigor as human identities is now a strategic priority, critical to building resilience and ensuring security in an AI-driven future



1 Forbes, *OWASP's Top 10 NHI Risks: A Wake-Up Call For Modern Cybersecurity*, March 2025

Managing the identity explosion

Managing digital identities has become one of the defining challenges of the modern enterprise. What once meant tracking employee logins to a handful of business systems has exploded into an ecosystem of interconnected users, applications, devices, and services, each requiring secure and seamless access. The rise of cloud computing, SaaS platforms, mobile workforces, and hybrid infrastructures has forced organizations to rethink identity not as a narrow IT function, but as the very fabric of digital trust. Every new application brought into the enterprise adds another layer of complexity, multiplying the number of credentials, entitlements, and security considerations that leaders must govern.

It's this growing reliance on cloud infrastructure, automation, and artificial intelligence that has quietly cultivated a new, dominant population of digital entities: Non-human identities (NHIs).[2] These identities, which include service accounts, API keys, and automated bots, now vastly outnumber their human counterparts. And each of these types of services carries greater loads and higher levels of interaction. This exponential growth has created the largest and most dynamic unmanaged attack surface, posing a critical and urgent challenge to traditional cybersecurity paradigms.

Traditional identity and access management (IAM) strategies, originally designed for human users and their predictable lifecycles, are proving to be fundamentally inadequate for securing NHIs. This inadequacy is a primary driver behind a significant percentage of modern cyberattacks, as attackers increasingly target these digital entities, which often operate with elevated privileges and without foundational security controls. The pervasive issues of overprivileged access, poor credential hygiene, and a lack of centralized visibility have transformed NHI sprawl into a crisis of governance and security.[3]

A comprehensive solution requires a strategic pivot to a unified, identity-centric security model that treats all identities—human and non-human—with the same rigorous standards of a zero trust framework. NHIM necessitates purpose-built capabilities for automated discovery, continuous monitoring, and secure identity governance and administration. By implementing these measures, organizations can close critical security blind spots, mitigate a top-tier cyber risk, and build a resilient foundation for the automated, AI-driven future.[4]

2 GitGuardian, *OWASP Top 10 Non-Human Identity Risks for 2025: What You Need to Know*, January 2025

3 CRTInsights, *Why Managing Non-Human Identities (NHIs) Must Be a Central Concern for Identity Access Management*, August 2025

4 AppViewX, *Key Takeaways from the 2024 ESG Report on Non-Human Identity (NHI) Management,* October 2024

The unseen workforce: A new frontier of digital identity

The rapid evolution of digital infrastructure, marked by the adoption of cloud services, microservices, and automated workflows, has led to a fundamental shift in how organizations operate. This technological progression has given rise to an unseen workforce, a vast network of machine-to-machine processes that execute mission-critical tasks without direct human intervention.5 This new digital workforce is the engine of modern business, powering everything from CI/CD pipelines to customer-facing applications and data synchronization processes.[5]

For decades, the central focus of cybersecurity has been on protecting human users, their access, and their data. The security perimeter was largely defined by the individual user and their credentials. However, the sheer volume and distinct operational nature of non-human identities (NHIs) now demand a profound re-evaluation of this security paradigm. The pivotal challenge of modern cybersecurity has transitioned from simply securing people to comprehensively securing machines. This shift is not merely a technical adjustment; it represents a new frontier of digital identity, requiring a complete overhaul of security strategies to address an identity population that is, in many cases, already far larger and more active than the human workforce it serves.

The anatomy of a non-human identity

A non-human identity (NHI) is a digital credential that represents any machine, application, service, software component, or automated process that needs to authenticate itself to access data or resources within a digital environment. Unlike human identities, which are tied to individual users, NHIs are designed to facilitate automatic, machine-to-machine operations. They prove their identity not through passwords, multi-factor authentication (MFA), or biometrics, or other common passwordless methods but through cryptographic credentials, such as API keys, tokens, certificates, and secrets. These credentials serve as a digital “passport,” enabling secure communication and data exchange across complex, distributed systems.

5 Cyber Security Intelligence, *Sprawling Non-Human Identities Are the Next Big Cyber Risk*, August 2025

The demographics of machine processes

The population of NHIs is diverse and expanding. While often discussed as a single group, these identities represent distinct classes of digital entities, each with a specific purpose. The primary types of NHIs include:

- **Workloads:** These are identities assigned to software workloads, such as service accounts that connect applications to databases, APIs, and other systems to automatically execute tasks.6 They are the backbone of automated application functions.
- **Machine identities:** Secure digital identities for devices and systems, including virtual machines, containers, and Internet of Things (IoT) devices. They are crucial for network communication and device-level security.
- **API tokens and OAuth tokens:** These credentials authenticate data exchanges between applications, ensuring that only authorized services can access sensitive information.
- **Bots and scripts:** This category includes automation scripts and bots that execute tasks such as CI/CD pipelines, infrastructure as code (IaC), and robotic process automation (RPA).
- **Agentic AI:** An emerging and high-risk category of NHIs, agentic AI systems operate autonomously across applications and services. They can be granted wide-ranging permissions and may even generate new credentials to complete tasks, leading to an unpredictable and self-reinforcing sprawl.

NHI's exponential growth and its drivers

The proliferation of NHIs is occurring at an astounding rate, far outpacing the growth of human identities.[6] The trend is not merely linear but exponential, as previously stated, in some environments NHIs outnumber human users by as much as 100 to 1. Other studies have shown that NHIs routinely significantly exceed human identities. The primary drivers fueling this expansion are deeply embedded in modern digital transformation initiatives.

The mass adoption of **cloud computing** is a significant catalyst, as NHIs are essential for facilitating secure communication across distributed cloud services and Software as a Service (SaaS) environment.[7]

6 Forbes, *OWASP's Top 10 NHI Risks: A Wake-Up Call For Modern Cybersecurity*, March 2025

7 GitGuardian, *Non-Human Identity Security in the Age of AI*, February 2025

DevOps and CI/CD (continuous integration/continuous deployment) pipelines generate NHIs in seconds to manage and deploy infrastructure and applications. This rapid, ad-hoc creation often occurs outside of traditional identity management processes, contributing to an unmanaged sprawl.

The most recent and significant driver is the rapid integration of cloud services and autonomous systems into the enterprise.[8] AI agents, in particular, can be granted broader permissions than traditional bots and can autonomously create credentials to complete their assigned tasks. This creates a self-reinforcing cycle where the NHI population compounds with every new automation and AI-driven process, making it difficult for organizations to even quantify the scale of the problem.

The creation of NHIs is often a rapid, ad-hoc process driven by developers to meet immediate project needs. This lack of centralized oversight is consistently identified as a major management challenge. The consequence is not just a technical problem of credential management but a fundamental issue of organizational accountability and governance. When a developer creates a service account for a temporary project and then leaves the company or moves to another team, that account can become "orphaned," with no clear owner responsible for its security or lifecycle. This systemic ownership gap is a critical prerequisite for the vulnerabilities that define NHI sprawl. Addressing this issue requires a strategic shift to "shift left" with security, embedding identity governance into the DevOps process and establishing clear accountability structures to bridge the operational gap between development and security teams.

Characteristic	Human identity	Non-human identity
Authentication method	Passwords, MFA, biometrics, SSO	API keys, tokens, certificates, secrets
Lifecycle management	Structured onboarding and offboarding tied to HR processes	Often ad hoc creation; may persist indefinitely, leading to orphaned accounts
Behavior	Interactive and varied; tied to an individual's work patterns	Repetitive and predictable; operates continuously at machine speed
Ownership	Tied to a specific individual	Often lacks a clear owner or accountability
Primary goal	Enables human access to systems and data	Facilitates machine-to-machine communication and automated workflows
Monitoring	Traditional tools, SIEM, behavior analytics	Often low visibility; generates high levels of activity that can obscure threats

Non-human identities may impose additional challenges to an organization's identity fabric

8 ConductorOne, *Identity Lifecycle Management for Non-Human Identities*, March 2025

The looming crisis: Traditional IAM's blind spots

Traditional identity and access management (IAM) deployments were architected with a default and exclusive focus on human identities and their associated lifecycles. These systems are designed for users who log in interactively, use multi-factor authentication, and are subject to formal, HR-triggered onboarding and offboarding processes. However, this model is fundamentally ill-equipped for the unique characteristics of NHIs. For example, unlike what people commonly do today, a machine cannot receive a multi-factor authentication code on a cell phone. Furthermore, because NHIs operate continuously in the background at machine speed, traditional behavioral monitoring and oversight tools often fail to distinguish legitimate actions from malicious ones, often rendering them ineffective.

IAM weak spots exposed by NHI sprawl

Often, organizations develop a combination of automated and manual processes to achieve their identity management objectives; however, the proliferation of NHIs typically scales beyond what this approach can handle. Without a corresponding evolution in identity and access management strategies NHI will expose critical weak spots. Vulnerability that has become prime targets for attackers.

- **Lack of centralized visibility and governance:** One of the most significant challenges is the absence of a comprehensive, centralized inventory of NHIs across hybrid and multi-cloud environments.[9] This creates massive security blind spots, making it virtually impossible for security teams to assess exposure, enforce policy, or even quantify the scale of the problem.
- **Weak credential hygiene and secrets sprawl:** A pervasive weakness is the reliance on static credentials, such as hard-coded API keys, tokens, and secrets that are rarely, if ever, rotated. This lack of credential hygiene leads to "secrets sprawl," a top risk cited by the OWASP Top 10 for 2025. Attackers actively target these insecure credentials to gain unauthorized access.[10]
- **Identity sprawl and improper offboarding:** Without a formal lifecycle, NHIs are frequently created and then forgotten, persisting long after their intended purpose has ended. This results in a growing population of "zombie NHIs" that are unmonitored and vulnerable to exploitation, serving as persistent backdoors for adversaries.
- **Overprivileged access:** Poorly designed or followed security practices lead to NHIs receiving broad, excessive, and persistent privileges, largely because their roles are not clearly defined.[11] This practice violates the principle of least privilege (POLP) and dramatically expands the "blast radius" in the event of a compromise, allowing an attacker to move laterally and access sensitive data far beyond the initial entry point.

While identity and access management specialists will recognize the list above as some of the most prioritized scenarios to manage, their importance multiplies with the proliferation of NHIs. In that most breaches are identity based, managing them across all your edge identity stores is fundamental to protecting against them. An approach that most organizations short cut against.

9 AppViewX, *Key Takeaways from the 2024 ESG Report on Non-Human Identity (NHI) Management,* October 2024

10 GitGuardian, *OWASP Top 10 Non-Human Identity Risks for 2025: What You Need to Know,* January 2025

11 GitGuardian, *Non-Human Identity Security in the Age of AI*, February 2025

The architectural and operational barriers to secrets management

Even organizations with top-branded IAM solutions often fail to implement effective secrets management because the tools and workflows were not designed for the complexities of the modern, cloud-first world. This problem is a matter of both architectural limitations and operational friction.

Onboarding friction and developer workflows

The rapid, ad-hoc creation of NHIs is a major source of the problem.[12] In the fast-paced world of DevOps and CI/CD, developers often create and provision NHIs and their credentials to meet immediate needs. This results in secrets being hardcoded directly into source code, scripts, or configuration files, a significant risk cited by the OWASP Top 10.[13] This practice is common because if a security solution or process adds friction, developers will simply find a way to circumvent it to get their work done. Any secrets management processes that rely on manual distribution and static credentials are bottlenecks that cannot scale to NHI levels. Furthermore, any decentralized approach with result in silos that lack consistent identity security fabric. Rather secrets are scattered, fragmented, and typically out of date across the organization's identity stores.

For most organizations, identity security teams struggle to enforce IAM standards without disrupting development or overall productivity, making it even a further stretch to provide those services to developers in a timely manner. Beyond providing a core set of identity-based APIs, they need to be able to automate identity governance and administration while keeping developer friction to a minimum.

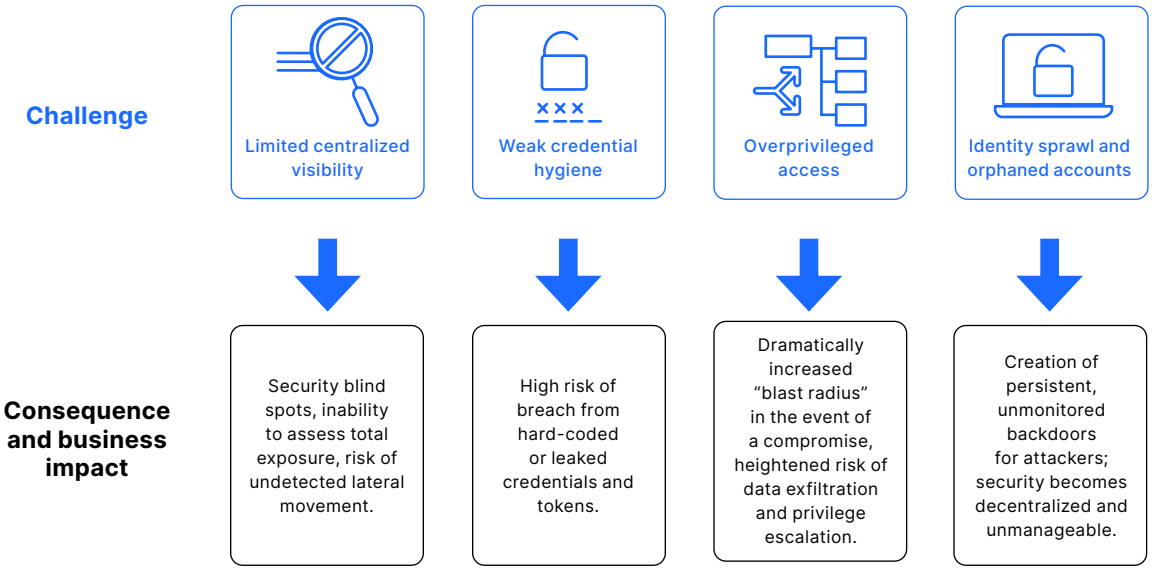
12 Cyber Security Intelligence, *Sprawling Non-Human Identities Are the Next Big Cyber Risk*, August 2025

13 ConductorOne, *Identity Lifecycle Management for Non-Human Identities*, March 2025

Legacy tooling and visibility gaps

Traditional IAM tools and processes are fundamentally limited in their ability to govern NHIs at scale. While many can detect some NHIs, discovery alone doesn't solve the accountability gap because they lack the ability to onboard and manage their full lifecycle. The core architectural limitation is a dynamic credential blind spot that exists outside the scope of traditional configuration analysis tools.[14] This problem is compounded in organizations that use manual tools designed to monitor for misconfigurations and policy drift on static assets that lack visibility into the ephemeral, machine-speed rotation and use of credentials. This creates a fundamental mismatch: ephemeral infrastructure protected by persistent, hardcoded credentials that attackers can exploit long after the original workload has been decommissioned.[15] Furthermore, legacy IAM systems struggle with the scalability and flexibility required to unify access policies across multi-cloud and SaaS platforms, leading to security gaps and a lack of real-time access monitoring. A single compromised service account can provide unfettered access across systems with little to no monitoring in place.

Non-human identities are not merely a new type of identity; they represent a fundamental expansion of the attack surface. The core issue is a dangerous combination of their sheer volume, their privileged access, and their functional invisibility to established identity onboarding and management. Extending the IAM security model to behavior analytics, because NHIs operate at machine speed and continuously in the background, their legitimate activity can obscure malicious actions, making it difficult for security teams to distinguish a threat from normal operations. This lack of monitoring and oversight turns them into security blind spots.[16] A compromised NHI with broad, persistent privileges can quietly move through a network and access sensitive data without raising the alarms designed for human-like behavior, posing a far more dangerous threat than a single compromised user account.



Managing non-human identities poses new challenges

14 OWASP, *Non-Human-Identities Top10*, 2025

15 ConductorOne, I*dentity Lifecycle Management for Non-Human Identities*, March 2025

16 Forbes, *OWASP's Top 10 NHI Risks: A Wake-Up Call For Modern Cybersecurity*, March 2025

Redefining the perimeter: The evolving role of IAM

As identities become the new security perimeter, enterprises must move beyond human-centric IAM to a unified platform securing both people and machines. A successful deployment of NHIM needs to deliver automated discoveries, lifecycle governance, continuous monitoring, and secrets management to address the risks of sprawling NHIs. This evolution expands focus from just access to broader identity security, making NHI protection a strategic imperative for building resilient defenses in an AI-driven enterprise.

The imperative for a unified identity platform

As the identity landscape becomes the new security perimeter, an exclusive focus on human identities is no longer a viable strategy. The future of enterprise security relies on a unified identity platform that can comprehensively secure all digital entities, both human and non-human. The goal is to manage all identities with automated processes that keep sensitive resources secure while logging all types of access to them. By eliminating these emerging security blind spots created by NHIs organizations can enforce governance policies consistently across the entire environment, regardless of whether the identity belongs to a person or a machine. This necessitates an evolution from traditional IAM to a new model of comprehensive identity security.

Core capabilities of modern non-human identity management

NHIM is the specialized practice of discovering, securing, and automating the lifecycle of NHIs. A purpose-built NHIM platform must include core capabilities designed to address the unique challenges of this new identity population:

- **Automated discovery and classification:** The foundational requirement is the ability to automatically find and catalog all NHIs across on-premises, cloud, SaaS, and hybrid environments. This is the critical first step in gaining the necessary visibility and creating a comprehensive inventory of the digital workforce.[17]
- **Centralized lifecycle management:** A modern solution must govern the entire lifecycle of an NHI, from its automated creation and provisioning to its timely retirement and decommissioning. This eliminates the problem of orphaned accounts and ensures that identities do not persist long after their purpose ends.[18]
- **Active posture management and continuous monitoring:** An effective platform must continuously assess the security configuration of NHIs in real time. This includes identifying misconfigurations, excessive privileges, and suspicious activity by establishing behavioral baselines and detecting anomalies.[19]
- **Automated secrets management:** To move beyond the risk of manual token and certificate management, a NHIM solution must provide a secure, automated system for storing, rotating, and expiring secrets. This eliminates the risk of hard-coded credentials and long-term credential exposure.[20]

17 AppViewX, *Key Takeaways from the 2024 ESG Report on Non-Human Identity (NHI) Management*, October 2024

18 GitGuardian, *OWASP Top 10 Non-Human Identity Risks for 2025: What You Need to Know*, January 2025

19 Cyber Security Intelligence, *Sprawling Non-Human Identities Are the Next Big Cyber Risk*, August 2025

20 Crowdstrike, *What are non-human identities?*, January 2025

The proliferation of NHIs and how they are used is fundamentally shifting the security conversation from access management to identity security. It has long been claimed that identity has become the new security perimeter, and the proliferation of NHI has taken that discussion to a whole new level. As a result, the increasing number of organizations that plan to increase their spending on NHI security is a clear signal that this has become a top-level business priority.[21] This is not simply a technical investment but a strategic one, aimed at building a resilient, adaptable security architecture for the automated, AI-driven enterprise of the future. The conversation has evolved from **"how do we manage NHIs?"** to the more critical question of "how do we secure our entire digital landscape where NHIs are the dominant population?"

The blueprint for action: A strategic framework for securing NHIs

Organizations seeking to address the challenges of NHI sprawl must adopt a strategic framework that goes beyond traditional security practices. This blueprint for action is built on foundational principles and purpose-built capabilities.

Embracing a zero trust model for all identities

The foundation of an effective NHIM security strategy is to upgrade IAM environments so that a zero trust model can be applied to them. The core principle of never assume trustworthiness must be universally applied, to every identity, human or non-human. This model requires continuous identity management across even the most dynamic identity environment. This prevents a compromised identity from being able to bypass security controls and move freely through the network.

Applying the principle of least privilege (POLP)

The principle of least privilege (POLP) is a cornerstone of any robust security posture of any and all environments, which means that it needs to be applied universally to NHIs as well. So, while organizations have spent years implementing and maturing POLP processes for their carbon-based identities, the same level of focus also needs to be applied to the NHI ones as well. Just as for humans, implementing POLP for NHIs is crucial for minimizing the attack surface and limiting the potential impact of a compromised account.

Continuous secrets management and rotation

For all the same reasons they are rotated for humans, moving away from static, long-lived credentials is a top priority for mitigating risk of NHI's as well. Instead of hard-coded credentials, organizations should implement a secrets management system that automatically rotates credentials on a regular schedule and expires them when they are no longer in use. This approach eliminates the risk of hard-coded credentials and prevents long-term credential exposure, a major vulnerability cited in the OWASP Top 10.[22]

21 Forbes, *OWASP's Top 10 NHI Risks: A Wake-Up Call For Modern Cybersecurity*, March 2025

22 OWASP, *Non-Human-Identities Top 10*, 2025

Essential IAM principles for NHI

While the following list applies to all identities, the scale needed to manage the sheer number of NHIs exposes identity weaknesses often masked by manual closing of security gaps. A successful NHI management strategy integrates foundational principles with a proactive, disciplined approach to governance and operations. The following recommendations provide a practical path to building a resilient defense:

- **Assign clear ownership:** Every NHI must have a designated owner or a responsible team. This is a crucial non-technical step that addresses the accountability gap and ensures that someone is responsible for the lifecycle and security posture of the identity.[23]
- **Regular audits and reviews:** Organizations must implement routine audits of NHIs to identify overprivileged, unused, or misconfigured accounts. These reviews ensure that access privileges remain aligned with current needs and security policies.[24]
- **Align with OWASP's NHI Top 10:** Organizations should leverage the OWASP Top 10 for 2025 as a critical roadmap for understanding and prioritizing the most significant risks associated with NHIM. This framework provides a clear, industry-recognized guide for addressing vulnerabilities and strengthening security.[25]

23 CRTInsights, *Why Managing Non-Human Identities (NHIs) Must Be a Central Concern for Identity Access Management*, August 2025

24 Crowdstrike, *What are non-human identities?*, January 2025

25 OWASP, *Non-Human-Identities Top 10*, 2025

OWASP Risk ID	Risk description
NHI1:2025 Improper Offboarding	NHIs remain active with valid credentials long after they are no longer needed, creating "zombie NHIs" that are ripe for exploitation.
NHI2:2025 Secret Leakage	The leakage of credentials, such as API keys and tokens, into insecure data stores like code repositories or plain-text files.
NHI3:2025 Vulnerable Third-Party NHI	Security risks stemming from vulnerabilities in third-party services and applications that are integrated into the organization's workflows.
NHI4:2025 Insecure Authentication	The use of obsolete, weak, or easily crackable authentication methods for NHI access.
NHI5:2025 Overprivileged NHI	Granting an NHI more privileges than are necessary for its function, dramatically expanding the potential damage in a breach.
NHI6:2025 Insecure Cloud Deployment Configurations	The insecure storage of credentials within CI/CD pipelines, leaving them exposed to attackers.
NHI7:2025 Long-Lived Secrets	The use of credentials with distant or non-existent expiration dates, providing attackers with persistent access if compromised.
NHI8:2025 Environment Isolation	The failure to use separate NHIs for different phases of the software development lifecycle (e.g., using the same key for both testing and production environments).
NHI9:2025 NHI Reuse	Using the same NHI and its associated credentials across multiple, different applications or services.
NHI10:2025 Human Use of NHI	A human actor misusing an NHI credential for manual tasks, blurring audit trails and increasing the risk of privilege misuse.

By combining ownership, audits, and OWASP-aligned practices, organizations forge a disciplined NHIM strategy that strengthens governance, eliminates blind spots, and ensures resilience against evolving identity-driven risks.

Conclusion – NHI requirements will increasingly mature IAM practices

The exponential proliferation of non-human identities has irrevocably altered the landscape of enterprise security. NHIs are now the dominant population in most digital environments and, if left unmanaged, represent the single greatest unmanaged attack surface. The data is clear: attackers are aware of this blind spot and are increasingly targeting NHIs to achieve lateral movement and persistent access.[26]

Organizations that have relied on manual processes to fill in the gaps in onboarding NHIs required for identity management at scale. Until they solve this problem, they'll continue to fall short in implementing governance and lifecycle management of machine-to-machine processes.

The future of enterprise security relies on a unified, identity-centric approach that applies the same rigorous governance to all identities—human and machine. This requires a strategic investment in a comprehensive NHIM platform that can provide automated discovery, continuous monitoring, and secure lifecycle management.

By embracing a zero trust model, all types of identities, and adopting best practices like the PoLP and automated secrets management, organizations can begin to close the critical security gaps created by NHI sprawl. As each organization works its way through its own digital transformation journey, they've often settled with various degrees of Identity management automation. NHI raises the bar on IAM automation. The long-held view of partial identity management coverage lets attack surfaces expand, rather than shrink. And most importantly, in the coming years, organizations won't be able to afford settling for IAM solutions that fall short.

The time for organizations to elevate NHIM from a background concern to a central strategic priority is now, and there is no way that can happen without full ILM automation.

26 Forbes, *OWASP's Top 10 NHI Risks: A Wake-Up Call For Modern Cybersecurity*, March 2025

opentext™