INDIGO
CONSULTING

Beyond the Obvious: Securing the Invisible Identities in Your Digital World - A Unifying Framework for the Management of Human and Non-Human Identities

Author: Roberson Etienne

Date of Publication: July 2025

indigoconsulting.ca

Best Workplaces™ in Quebec
Great Place To Work® CANADA 2025 ™

Best Workplaces™
Great Place To Work® CANADA 2025 ™

Best Workplaces™ in Technology
Great Place To Work® CANADA 2025 ™

Table Of Contents

Executive Overview

Identity and Access Management (IAM) is the backbone of an organization's security infrastructure.

As enterprises speed up their digital transformation initiatives, new risks emerge in areas that are often overlooked: legacy installations, dormant accounts, and a class of access agents gaining new attention called Non-Human Identities (NHIs). This white paper is an exploration of the intersection of two critical dimensions of threat: the operational threats that are propelled by machine identities and the strategic deficits that are revealed by the "unknown unknowns" of Identity and Access Management (IAM).

It offers a comprehensive, lifecycle-oriented, and observability-focused solution designed to secure both human and non-human elements of digital identity.

1. Introduction: When the Silent Threats Become Severe

Emerging Threats: The Age of Unknown Unknowns

In 2024, the World Economic Forum warned us of the rising danger of "unknown unknowns" — threats that we don't anticipate and are not aware of. Originally characterized in climate policy, its cybersecurity analogues are strikingly familiar. IAM is our **digital climate**, managing who gets to view what, when, and why. Yet just like natural systems, IAM is prone to tipping points, cascade failure, and silent entropy.

IAM in a Cloud-First World

Most particularly, as organizations strengthen their automation procedures and cloud deployment models, Identity and Access Management (IAM) complexity grows exponentially.

Rethinking IAM Strategy

To **future-proof IAM**, this discussion argues that organizations must embrace the inherent risks of non-human identities, actively hunt for IAM blind spots, and manage IAM as a dynamic and evolving system.

2. The Emergence of Non-Human Identities

What exactly are NHIs?

Non-Human Identities, also referred to as machine identities, are credentials that are utilized by applications, APIs, bots, and scripts, along with service accounts, virtual machines, containers, Internet of Things (IoT) devices, and Continuous Integration/Continuous Deployment (CI/CD) tools, such as automation agents. These identities enable exception-free machine-to-machine (M2M) communication and tend to outmaneuver human users by a staggering ratio of 80 to 1[1]. They are a fundamental component of the infrastructure that underpins cloud-native architectures, DevOps pipelines, and artificial intelligence (AI) systems.

Why They Matter

Non-Human Identities (NHIs) are now a part of the fabric[2] of the digital business today. As companies adopt on cloud-native design patterns, mature their DevOps initiatives, and head towards automation and artificial intelligence on a larger scale, machine credentials are ever more representative of the majority of active identities within an environment.

They drive mission-critical infrastructure, powering primary operations in CI/CD, SaaS integrations, microservices, and AI agents, and therefore are vital to business continuity. However, NHIs are often highly privilege-rich by design, configured for convenience with persistent and high-level access, and therefore pose catastrophic risk in the event of a breach. NHIs operate in the background and anonymously, since their persistent, autonomous nature makes them difficult to identify with conventional tools, in contrast to human activity.

Furthermore, NHIs span hybrid and multi-cloud, reaching across all domains from on-prem data centers to SaaS applications and edge devices, where visibility and control are harder to achieve. They're also beyond traditional controls; machine identities don't use MFA, can't attend user training, and require alternate authentication methods. Finally, their lifecycle is ignored, being spun up ad hoc and rarely terminated, which leads NHIs to remain as abandoned or zombie identities long after initial use.

In fact, over 80%[3] breaches are related to identities, as the attackers gain access through a compromised User account. In several scenarios lateral movement or privilege escalation occurs through the use of NHIs, thus remaining a primary attack vector.

Lastly, NHIs are not a technical nicety, they're a strategic matter. Securing them is the key to limiting breach exposure and enabling safe, scalable automation.

[1] https://www.cyberark.com/press/machine-identities-outnumber-humans-by-more-than-80-to-1-new-report-exposes-the-exponential-threats-of-fragmented-identity-security/

[2] https://omadaidentity.com/resources/blog/what-is-identity-fabric

[3] https://spycloud.com/resource/report/spycloud-annual-identity-exposure-report-2025/

3. The Unknown Unknowns of IAM

IAM's greatest vulnerabilities lie not in what we monitor but in what we don't question sufficiently. This section exposes significant blind spots using environmental metaphors.

3.1 IAM's Invisible Insects: Service Components overlooked

Minor elements, such as deprecated connectors or unchecked scripts, can lead to disastrous failure. A recent example of this was an old SSO connector that brought about a worldwide outage in a Fortune 500 business.

3.2 Dormant Accounts: IAM's Ancient Pathogens

Legacy credentials are often still embedded in old systems.

3.3 Zombie Access: IAM's Underground Fires

Unexpectedly, old accounts are being revived by scripts or jobs.

3.4 IAM Tipping Points: Misconfigurations that Cascade

Excessively permissioned roles or Segregation of Duties (SoD) violations can lead to compounding failures in environments.

4. Critical Risks in NHI and IAM Blind Spots

The following table summarizes key risk areas:

RISK AREA	DESCRIPTION
Secrets Sprawl	Credentials embedded in code, cloud configurations, or public repositories are difficult to track and rotate[4].
Orphaned or Zombie Identities	Long-forgotten accounts left active; prime targets for attackers.[5]
Over-Privileged Access	Excessive permissions violate the principle of least privilege, opening pathways for lateral movement[6].
Inability to Trace	NHIs generate automated logs with no human intervention.
Supply Chain Weaknesses	Third-party integrations and OAuth tokens enlarge blast radius.
Policy Failures	IAM misconfigurations often go unnoticed until cascading failure occurs.

[4] https://checkmarx.com/blog/secret-sprawl-the-silent-threat-to-enterprise-security

[5] https://www.strongdm.com/what-is/zombie-accounts

[6] https://www.pingidentity.com/en/resources/blog/post/what-is-principle-of-least-privilege-polp.html

5. Preserving The Living IAM system's security and the need for NHI management

Both systemic and tactical threats need to be tackled by organizations through a **resilience-first**, **identity-based solution** covering every phase of the identity lifecycle. The end-to-end solution begins with centralized discovery and inventory where automatic discovery of both human and non-human identities in hybrid environments is followed by tagging, classification, and ownership mapping. This is then followed by robust Lifecycle Management, where ownership and application mapping of non-human identities is followed by automatic deactivation and purging of inactive accounts.

Effective **secret management** and rotation are another core pillar, including secure storage of credentials in vaults and regular rotation via **short-term certificates or tokens**. Least privilege enforcement is also essential, requiring strong **role-based access controls (RBAC)** and **attribute-based access controls (ABAC)** to ensure permissions are given only as absolutely required, with regular review mechanisms in place. Additionally, **behavioral monitoring and observability** are made necessary by defining Identity and Access Management (IAM) telemetry as a type of critical infrastructure data and thus allowing careful observation of identity behavior to detect any anomalies. Integration with **zero trust** principles and IAM governance therefore forces organizations to implement zero trust frameworks for continuous verification of access, carefully evaluating each request and simulating IAM policy changes while meeting strict governance criteria.

Another challenge in achieving the Zero Trust objective is the **"bootstrapping"** or **"Secret Zero"** problem, which raises a fundamental question: how can a system be trusted securely from the outset without embedding secrets directly into code? Zero Trust requires verification of identity at every layer. Emerging identity technologies such as **SPIFFE** and similar frameworks address this challenge by enabling **identity-based service-to-service** trust without relying on static credentials or deprecated secret management techniques. These foundational components allow organizations to build secure, scalable, and automated architectures that uphold Zero Trust principles in a dynamic digital environment.

The sheer volume and complexity of Non-Human Identities pose a threat level that cannot be effectively managed using **traditional Identity and Access Management (IAM)** products in isolation. Properly managing the complete machine identity lifecycle creation through **credentialing, access control, and deprovisioning** requires a response that goes beyond traditional **human-centric** thinking. Tailored Non-Human Identity Management (NHIM) solutions therefore not only seem beneficial but are also strategically requisite.

Experts like Gartner[7] always highlight the urgent need for advanced Non-Human Identity (NHI) solutions to protect modern digital businesses. Their findings confirm that full-fledged Non-Human Identity Management (NHIM) platforms provide the essential visibility, control, and automation to address the **'unknown unknowns'** of machine-to-machine communication. These solutions are carefully crafted to address the unique requirements of Non-Human Identities (NHIs). They include functionality like centralized discovery, automated secrets management, dynamic least privilege enforcement, and real-time behavior pattern monitoring.

Those organizations that invest in bespoke NHIM platforms, generally offered by market leaders, are in a much better position than their peers. By doing this, they can turn a risky environment into one that is managed and predictable, thus allowing their cloud-native designs, DevOps pipelines, and AI engines to develop securely, without threatening their precious assets due to unknown risks. What is more, by working with vendors that have insight in this area, organizations can accelerate their digital projects and create a truly resilient identity framework.

[7] 2024 Magic Quadrant for Privileged Access Management (PAM)

6. Recommendations

The adoption of a program aimed at "Non-Human Identity Management" involves assigning ownership, managing lifecycle events, and applying security controls to non-human identities (NHIs), such as service accounts, APIs, and **machine credentials**. Some vendors that offer solutions to protect and orchestrate non-human access in hybrid environments are **CyberArk Conjur, Saviynt Non-Human Identity Governance, and Ping Identity**, which is known to specialize in API and application federation.

Form an "IAM Unknowns" Task Force and bring together a cross-functional team that is charged with identifying and remediating hidden risks such as **over-entitled identities**[8], legacy credentials, orphaned accounts, and inactive integrations. The capabilities offered by **SailPoint Identity Security Cloud, BeyondTrust Discovery**, and **PingOne Risk Management** enable continuous visibility into entitlements and risk-adaptive access control decisioning.

Investment in Observability Platforms assists in establishing real-time and behavioral telemetry baselines. Solution such as PingOne with integration potential with identity analytics programs help to provide identity-monitoring and outlier-detecting capabilities. It expands Gartner's "identity-first security[9]" concept, taking identity signals into account to be important telemetry sources.

To enlighten stakeholders and executives, it is essential to move the IAM conversation from a purely **compliance-driven** narrative to one that is anchored in **operational risk** and **business impact**. Tangible ways to achieve this include:

Executive risk dashboards that map identity signals to financial exposure, operational disruption potential, and regulatory stance leveraging tools such as **Saviynt Analytics, Okta Identity Governance, Ping Identity.**

Quarterly identity risk reports presented in business language, highlighting trends like privilege creep, contractor lifecycle gaps, or unused admin accounts with actionable remediation recommendations and business consequences[11] of inaction.

Scenario-based training or tabletop exercises for identity compromise scenarios (e.g., lateral movement from a service account that has been orphaned), based on industry-specific threats, to educate leadership on how IAM failures can cascade into generalized security incidents.

Risk heatmaps and identity maturity benchmarks, aligned to business units or application portfolios, which enable executives to prioritize investment and intervention.

IAM impacts narratives for internal audit and compliance committees, linking technical findings to risk register entries and control effectiveness ratings.

[8] https://www.britive.com/resource/blog/gartner-cloud-infrastructure-entitlement-management

[9] Gartner, "Top Trends in Cybersecurity 2022–2024" (Gartner ID: G00758140)

[11] https://deloitte.wsj.com/riskandcompliance/beyond-numbers-critical-role-of-cybersecurity-in-m-a-deals-6aba020c

In summary, it is necessary to plan for Identity and Access Management (IAM) Failure Modes by incorporating IAM misconfigurations, identity abuse, and access compromise into traditional tabletop exercises. Those exercises should model actual attack vectors and test the organization’s ability to detect, respond to, and recover from identity-based threats. Prioritizing identity-focused threats in the incident response planning process greatly strengthens the organization's overall readiness and resiliency.

7. Conclusion: A Future-Proof Approach to IAM

The next big security breach will not likely originate from the things we are aware of today. Rather, it will probably be from an unused service account, a misconfigured connector, or an unmonitored token.

The New Threat Landscape

In an age of automation and artificial intelligence that allows for large scale, **non-human identities** have transformed from supporting actors to main threat agents.

A New Vision for IAM

IAM must be re-envisioned, not as a static control, but as a **living entity dynamic**, fluid, and prone to entropy. The organizations that will thrive in the future are the ones that shine a light into the **shadows of IAM** and bring the invisible under management.

References / Bibliography

- World Economic Forum. (2024). *The global Risks*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
- World Economic Forum. (2024, July). *Five strategies to help you stay relevant in the age of AI*. https://www.weforum.org/agenda/2024/07/five-strategies-ai-relevance/
- Oasis Security. *What Is Non-Human Identity Management?* https://www.oasis.security/blog/what-is-non-human-identity-management
- Portnox. *What Are Non-Human Identities (NHI) & Why Should You Care?* https://www.portnox.com/blog/non-human-identities/
- Gartner, "Top Trends in Cybersecurity 2022–2024" (Gartner ID: G00758140)
- Machine Identities Outnumber Humans by More Than 80 to 1: New Report Exposes the Exponential Threats of Fragmented Identity Security

  https://www.cyberark.com/press/machine-identities-outnumber-humans-by-more-than-80-to-1-new-report-exposes-the-exponential-threats-of-fragmented-identity-security/
- https://spycloud.com/resource/report/spycloud-annual-identity-exposure-report-2025/
- EM360Tech. *Non-Human Identity Management: What Is It and Why It Matters?* https://em360tech.com/cyber-security/non-human-identity-management-what-is-it-and-why-it-matters/
- https://deloitte.wsj.com/riskandcompliance/beyond-numbers-critical-role-of-cybersecurity-in-m-a-deals-6aba020c
- https://www.britive.com/resource/blog/gartner-cloud-infrastructure-entitlement-management
- Keyfactor. *What is Machine Identity Management? Everything You Need to Know*. https://www.keyfactor.com/blog/what-is-machine-identity-management-everything-you-need-to-know/
- KuppingerCole. *Machine Identity Management: Understanding the Market and Solutions*. https://www.kuppingercole.com/reports/71408
- Non-Human Identity Management Group (NHIMG.org). https://www.nhimg.org/
- Aembit. *What are Non-Human Identities*. https://www.aembit.io/blog/what-are-non-human-identities
- https://aembit.io/blog/key-takeaways-on-non-human-identity-security-from-gartners-pam-report
- The New Stack. *Why the Rise of Machine Identities Demands New Security Strategies*. https://thenewstack.io/why-the-rise-of-machine-identities-demands-new-security-strategies/