

The essential guide to
**NON-HUMAN
IDENTITY
MANAGEMENT**



ABSTRACT

This report covers and provides vital insights for the cybersecurity community regarding **Non-Human Identity Management (NHIM)**, which involves managing and securing of digital identities within organizational ecosystems. It explains the fundamental disparities between human and non-human identities, emphasizing the urgency for specialized NHIM solutions in today's dynamic threat landscape.

It highlights the decentralization, ownership, and operational risks associated with non-human identities and underlines the imperative for NHIM systems in mitigating potential cybersecurity incidents considering the heightened risks posed by compromised non-human entities.

Furthermore, the report explores the evolution from traditional Identity and Access Management (IAM) practices towards NHIM solutions, necessitated by the proliferation of cloud-based solutions and automation. Drawing from real-world incidents, it underscores the necessity for NHIM platforms to address existing gaps in security protocols.

Essential components of an effective NHIM system, including inventory discovery, posture assessment, contextual information provision, remediation plans, and lifecycle management are outlined. Additionally, it emphasizes seamless integration with existing workflows and systems to streamline operational processes and bolster cybersecurity resilience.

Table of CONTENTS

3	Introduction
4	What is Non-Human Identity Management
6	Examples of Non-Human Identities
7	How Non-Human Identities differ from Human Identities?
8	Why is NHIM Required?
10	What Should a Good NHIM system include and why?
11	Conclusion

Report CONTRIBUTORS



Andrew Wilder, Retained
CSO, Community Veterinary
Partners



Paul Carpenito, Head of
Information Security,
Loews Corporation



Bezawit Sumner, CISO, CRISP
Shared Services



Kapil Bareja, Digital And Cyber
Risk Governance Leader



INTRODUCTION

In one of the simplest definitions, in the context of access management, “digital identity is the recorded set of measurable characteristics by which a computer can identify an external entity. That entity may be a person, an organization, a software program, or another computer.” At the core of provisioning access, granting, and restricting permissions, and maintaining the full lifecycle of access management could define the strength and weakness of an organization.

Year after year, the most common attack vector in cyber incidents have been attributed to identity-based attacks. IBM's 2024 X-Force Threat Intelligence Index puts identity related incidents at 71%, proving the modern-day adage of how cyber criminals log in versus hack in to gain access to an organization's environment.

A successful compromise of a valid credential is the most attractive vector for cybercriminals to gain a foothold and execute an attack using legitimate identities in a network with little to no detection as their activities are seen as normal. Though the most visible of identities are human user identities, a 2023 report from CyberArk notes that machine identities “outweigh human identities by a factor of 45 to 1.”

These machine identities, also known as non-human identities, are steadily increasing as repeated tasks are frequently automated, which in turn allows for these identities that are granted privileges, often elevated, to carry out these tasks. Therefore, as human accounts rely on some form of a secret to be granted access, the non-human identities also rely on secrets to carry out their respective tasks.

This report sets out to explore what is non-human identity management, why it is required, and what makes a good non-human identity management system.

WHAT IS NON-HUMAN IDENTITY MANAGEMENT

Managing and securing digital identities within organizations has become a significant concern for the technology industry. Non-Human Identity Management (NHIM) seeks to address the complexity of managing identities in organizations not tied to humans. It involves the management and protection of identities associated with systems, applications, services, machines, Application Programming Interfaces (API's), Artificial Intelligence (AI) entities and any other automated systems or entities not associated with a human user.

The disparities between human and non-human identities emphasize the need for dedicated and advanced NHIM solutions to effectively mitigate emerging cyber threats.

NON-HUMAN IDENTITY MANAGEMENT (NHIM) INVOLVES THE MANAGEMENT AND PROTECTION OF IDENTITIES ASSOCIATED WITH SYSTEMS, APPLICATIONS, SERVICES, MACHINES, APPLICATION PROGRAMMING INTERFACES (API'S), ARTIFICIAL INTELLIGENCE (AI) ENTITIES AND ANY OTHER AUTOMATED SYSTEMS OR ENTITIES NOT ASSOCIATED WITH A HUMAN USER.

The exponential growth of cloud systems distributes the risk beyond enterprise borders and is often leveraged by threat actors in sophisticated attacks, which compounds the complexity and requirement of distinguishing between normal and abnormal behavior associated with identities, especially in automated systems.

While human identities are often characterized by a specific interaction and an expected or a reasonably defined behavior of a human, non-human identities operate autonomously and often lack ownership, clear visibility and typically, exist in the preverbally “set-it and forget-it” state, that cyber professionals are all too familiar with.



"As enterprise systems become increasingly distributed and interconnected, non-human identities have become the Achilles' heel of cybersecurity defenses. The compromise of even a single system account or secret can lead to catastrophic security breaches. It's imperative that CISOs recognize the urgency to adopt robust non-human identity management systems to protect their infrastructures and data effectively."

Emily Heath, General Partner at Cyberstarts and former CISO at Docusign, United Airlines, AECOM.

This report emphasizes the requirements for NHIM systems in addressing the decentralization, ownership, pervasive use, and operational risks associated with the existence and management of non-human identities. NIMH systems seek to fill gaps in security practices and enhance organizational cyber defenses against evolving threats. It also defines the components of an effective NHIM solution, agnostic to any specific cyber security solution provider, third-party vendor, or technology product. Practices include, but are not limited to, inventory, posture assessment, provisioning/de-provisioning, remediation, and lifecycle management.

Each process plays an important role in enhancing cybersecurity resilience of systems leveraging non-human identities. Proper integration of NIMH systems with existing workflows and systems will help streamline operational processes and enhance the cybersecurity posture of a system.

Through the exploration and definition of NHIM principles and practices, this report seeks to provide cybersecurity professionals with the state-of-the-art insights necessary to navigate the complexities of effectively managing and securing non-human identities within organizations.



EXAMPLES OF NON-HUMAN IDENTITIES

Non-human identities or machine identities, in the context of identity and access management, often take the form of:

- **Service accounts:** These are special types of accounts used by applications or services to interact with each other or with databases. They are not tied to a specific user but are used to run processes, tasks, or jobs.
- **API keys:** These are unique identifiers used to authenticate a user, developer, or calling program to an API. They are used to track and control how the API is being used.
- **Certificates:** These are used to secure the communication between different services. They authenticate the service's identity and encrypt the data being exchanged.
- **Tokens:** In the context of OAuth, tokens are used to grant applications limited access to user accounts on an HTTP service.
- **Bots:** In platforms like Slack or Teams, bots have their own identities and are used to automate tasks or responses. Often include integration with sophisticated Artificial Intelligence (AI) algorithms.



HOW NON-HUMAN IDENTITIES DIFFER FROM HUMAN IDENTITIES?

Machines far outnumber humans today. But far from any sci-fi notions of a dystopian robot-ruled future, machines help free us, from dangerous, time-consuming, or repetitive tasks.

Just like humans, each machine needs one or more unique identity to authenticate and securely communicate with one another or a system. Unlike their human counterparts, machine identities receive far less attention.

Human identities, in the scope of identity and access management, refer to unique identifiers, such as usernames, or credentials that are assigned to individuals to access and use resources within a system. These identities allow for the tracking of user activities, setting permissions and ensuring accountability.

Non-human identities, often referred to as service accounts, system identities, or machine identities, are used by applications or services to interact with each other. These identities also require management to ensure secure communication between different services, prevent unauthorized access, and facilitate accountability.

The key difference between human and non-human identities is that human identities are tied to individual users with personal characteristics, while non-human identities are used by systems or applications for interaction, not tied to personal characteristics or individual user behavior.

Unlike with human identities, the creation and control of non-human identities aren't centralized to IT or an identity team. In many cases, non-human identities are directly created by developers or even citizen developers in no-code, low-code who may not be aware of their usage, as they represent the only means for the code they need to interact with systems.

Securing non-human identities carries inherent operational risks. In the absence of a comprehensive understanding of all consumers, there is a potential for disrupting production systems. For example, efforts to rotate secrets may unintentionally disrupt established and vital business workflows.

Adding to the challenge is the lack of standardization of non-human identity types and formats across different cloud providers and technology stacks. For example, AWS service accounts differ from Azure service principals, which differ from GCP service accounts.

WHY IS NHIM REQUIRED?

Several trends, such as cloud, microservices, devops, have fueled the exponential growth of NHIs in enterprise environments. Industry research shows that NHIs now outnumber human identities by as much as 45x. With more and more business processes being automated via AI and accessed by AI enabled services, NHI growth is likely to accelerate even more and further increase the risk exposure.

Given their pivotal role, securing NHIs has consequently become a critical objective with high stakes, as a compromised NHI could easily lead to data exfiltration and compromised business operation. Attackers love NHIs because breaches are harder to detect, often going undetected for long periods of time. Due to the lack of MFA, NHIs can become long term backdoors with a large blast radius as they often have elevated privilege levels.

Solutions that seek to rotate passwords on a fixed cadence to a lengthy and random value may help to reduce the risk of an account compromise. Because NHIs often govern service to service access across an organization's infrastructure, once exploited they can also be leveraged for supply chain attacks.

It is not surprising to see attacks on NHIs on the rise. A few recent prominent examples are:

- **Mercedes-Benz** – The Mercedes-Benz breach occurred when a private key was inadvertently published in a public GitHub repository, granting unrestricted access to the company's source code.
- **Cloudflare** – The Cloudflare incident occurred as attackers exploited multiple unrotated and exposed secrets. The chain of events began with the Okta breach in October 2023, during which the attacker gained administrative access to Cloudflare's Okta system.
- **Microsoft AI Incident** – The Microsoft AI breach occurred as researchers, while publishing a bucket of open-source training data on GitHub, accidentally exposed 38 terabytes of additional private data – including a disk backup of two employees' workstations. The backup includes secrets, private keys, passwords, and over 30,000 internal Microsoft Teams messages.

Traditional IAM programs lack visibility and lead to NHIs unmanaged because traditional cybersecurity tools offer limited or no capability in this area.


IAM and PAM solutions focus on human identities. They are designed around a centralized management model where identities are provisioned and managed by a central team and are associated with an identifiable individual with the ability to leverage MFA.

Secret Managers focus on vaulting of secrets but are not identity aware. Consequently, they lack knowledge of ownership, usage, permissions and accessed resources. As a result, they can be used effectively to implement security policies or to automate processes like secret rotation.



Cloud Security Posture Management (CSPM) solutions can help but are focused on cloud instances and not all NHIs exist in the cloud – and take an infrastructure-first vs. identity-first approach. While CSPMs can show certain posture issues, they will not help to actually remediate the vulnerability. As a result, issues will just continue to pile up in the never-ending list that the security team needs to take care of, with no solution or fix.

Lack of visibility results in lack of action, which leads to increased breaches and operational paralysis. Lack of lifecycle automation results in continued ungoverned exposure as new NHIs are created and huge operational complexity when issues need to be addressed. In order to address the NHI attack surface without sacrificing operational efficiency, adding Non-Human Identity Management to enterprise IAM programs becomes essential.



WHAT SHOULD A GOOD NHIM SYSTEM INCLUDE AND WHY?

NHIs are a key enabler of modern distributed systems. The ability to rapidly create and deploy NHIs is critical for developers to build systems at a fast pace. This, however, comes often at the expense of implementing strong security best practices, such as least privilege, secret rotation, and reuse. At its core, a good NHIM solution needs to bridge the gap between agile operations and strong security, allowing developers to move quickly while also ensuring that security and identity teams maintain strong enterprise cybersecurity posture.

NHIs are fundamentally different from human identities, both structurally and from a lifecycle point of view:

- NHI are not centrally provisioned and managed. They are created by DevOps engineers and developers across the organization directly in infrastructure and applications.
- There isn't a single authoritative source of truth with a common data model that can provide visibility and context. Traditional IGA and PAM systems can't provide holistic view of NHIs with context because their architecture relies on the presence of a known single source of truth.
- The connection between NHIs, related applications, corresponding business processes and the level of criticality is typically unknown.

A good NHIM solution must:

- Connect with a wide range of NHI providers (IaaS, PaaS, SaaS, on-premise systems), secret managers and context enriching systems (DSPM, ASPM, CMDBs) to provide holistic visibility with rich contextual information on Ownership, Consumers, and Resources.
- Leverage powerful analytics to provide active posture assessment to identify, prioritize and remediate vulnerabilities.
- Use automation to drive alignment of processes to best practices and seamless enforcement of policies across the lifecycle of NHIs
- Empower organizations to establish robust cybersecurity governance by implementing policies and processes vital for managing cybersecurity risk effectively as articulated in the [NIST Cybersecurity Framework 2.0](#) with holistic approach that isn't just limited to vulnerability detection.





CONCLUSION

As demonstrated by recent breaches, the compromise of NHIs poses significant risks, often leading to significant cybersecurity incidents, operational disruptions, and even supply chain attacks. Traditional Identity and Access Management (IAM) solutions, primarily designed for human identities, fall short in addressing the unique challenges posed by NHIs, leaving organizations vulnerable to exploitation.

This report revealed how critical it is for organizations to inventory, document use, and protect non-human identities. Though it is a tedious task to build out NHIM for organizations as it might be an afterthought, there is an incremental approach to do so. There are an increasing number of tools and solutions focused on human identity protections and there is a need to work towards requiring the same for non-human-human identities.

The recent introduction of non-human identity management solutions in the industry are here to answer the call. These Non-Human Identities are out of sight and out of mind once they are created, making them easy to lose track and visibility. Unmanaged non-human identities have led to some of the most notable security incidents and breaches leaving valuable lessons and opportunities to live by cautionary tales, and the need to secure them. Hence the need for a strong partner in non-human identity management.

As virtual perimeters continue to evaporate through the pervasive use of hybrid & multi-cloud architecture and agile development methodologies, the adoption of NHIM becomes indispensable in safeguarding against evolving cyber threats. By prioritizing the implementation of comprehensive NHIM strategies, organizations can enhance their cybersecurity resilience and mitigate the risks associated with the proliferation of non-human identities.

ABOUT CYBER SECURITY TRIBE

At Cyber Security Tribe, we foster a vibrant and exclusive community for cybersecurity professionals to connect, learn, and network with their peers in a secure, private environment. Our online content platform is curated by experts in the field, offering valuable insights and practical knowledge to advance your cybersecurity expertise. Stay updated with the latest industry developments and news through our comprehensive resources. Join us at www.cybersecuritytribe.com to enhance your cyber security journey and access an invaluable network of peers.

