OASIS

White Paper

Financial Services

Securing Non-Human Identities for Financial Services

Overview

Introduction 02

Understanding the Risks 03

Common Breach Scenarios Involving NHIs 04

The Role of NHI Security in Top Technology Priorities For Banking 05

How Financial Services Organizations Can Fail to Secure NHIs 09

Building an Effective NHI Security Strategy 10

Choosing the Right NHI Management Solution 11

Key Takeaways 12

Appendix 13

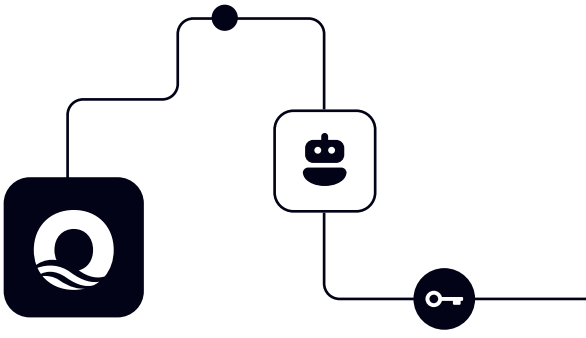
Introduction

Digital transformation is driving a massive shift in the financial services industry. Everything is evolving—from how financial transactions are conducted to how data is handled and how relationships with clients are maintained.

None of this would be possible without Non-Human Identities (NHIs), such as service accounts, secrets, API keys, and more, which are the critical elements that enable modern infrastructure and services to connect with each other.

However, as reliance on these NHIs grows, so does the risk associated with their potential misuse or compromise. In 2023, the finance sector surpassed healthcare as the most breached industry, according to the Risk and Financial Advisory firm Kroll. Recent breaches have shown that the threat is real for even the most security-aware organizations. For example, the Cloudflare breach in October 2023 exposed how attackers exploited multiple unrotated & exposed secrets, leading to unauthorized administrative access. Similarly, the Microsoft AI breach revealed how sensitive data, including secrets and private keys, was accidentally exposed while publishing a dataset on GitHub.

In this white paper, we'll dive into the top tech trends in banking these days, examine how they relate to non-human identities, and explore how new cybersecurity solutions can help manage these identities securely and efficiently.

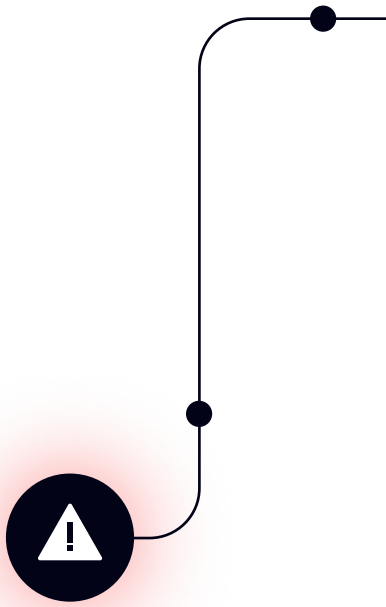


Understanding the Risks

Non-human identities are fundamentally different. Unlike human identities, NHIs are not tied to a specific individual, and they typically do not utilize Multi-Factor Authentication (MFA) or benefit from regular password resets. They are often created in a decentralized manner by different departments, lacking centralized control and clear ownership. This decentralization makes them harder to manage, more prone to being forgotten, and therefore more vulnerable to exploitation by attackers.

NHIs are pervasive in modern environments. They are a foundational element for leveraging any cloud service (IaaS, PaaS, and SaaS), connecting to APIs, running microservices architectures, and more. This widespread use significantly enlarges the attack surface (estimated to be at least 10x greater than the human perimeter), thereby exponentially increasing the risk of security breaches.

Unsecured NHIs also exponentially increase the blast radius of a breach, as they are frequently granted high privileges and are often shared among multiple users or systems. Since NHIs underpin access with third-party systems, the blast radius rapidly expands beyond the enterprise perimeter across the supply chain, significantly increasing the reputational risk and the potential financial consequences for a financial institution.



Common Breach Scenarios Involving NHIs

- **Misconfiguration and Exposed Secrets:** This occurs when credentials or private keys are accidentally exposed due to misconfigurations. For example, Microsoft AI researchers inadvertently exposed 38 TB of data when a misconfigured Shared Access Signature (SAS) token was published in a public repository.
- **Exploitation of Unrotated Secrets:** Often exploit old or unrotated credentials to gain unauthorized access. A notable case involved Cloudflare, where four NHIs were left unrotated after a breach at Okta by mistake (approx. 5K were properly rotated), leading to potential unauthorized access.
- **Privilege Escalation:** Attackers gain unauthorized access to systems due to inadequate identity and access controls, often stemming from poor visibility and management of NHIs. An example includes a breach at AWS, where attackers accessed .env files containing privileged credentials. This access allowed them to exploit email services, leave ransomware notes, and attempt the provisioning of compute-optimized instances.

Referring to the MITRE ATT&CK Matrix for Enterprise, NHIs are involved in various adversary tactics and techniques, including Valid Accounts (T1078), Cloud Accounts (SSH Authorized keys [T1078.004]), and Credentials from Password Stores (T1555).

According to IBM's Cost of a Data Breach Report 2024, the global average cost of a data breach increased by 10% within just one year, reaching USD 4.88 million—the largest annual rise since the pandemic. With breaches increasingly linked to identity-related incidents (accounting for 71% of incidents), the financial services sector faces heightened risk due to unmanaged NHIs, which can result in data exfiltration, regulatory penalties, and damage to brand reputation.

The Role of NHI Security in Top Technology Priorities For Financial Services

Financial Services organizations are among the most highly regulated and cybersecurity-aware organizations due to the critical nature of their role and the sensitivity of the data they handle in modern economies. NHIs are key enablers of all major technology priorities for banks, facilitating secure access and authentication between services at every layer of the technology stack. Having a strong and effective security program for NHIs is a foundational requirement for financial institutions to adopt all major technology priorities successfully.

Initiatives

- Artificial Intelligence (AI) and Machine Learning (ML)
- Blockchain and Distributed Ledger Technology (DLT)
- Big Data and Analytics
- Robotic Process Automation (RPA)
- Open Banking
- Mobile and Digital Wallets
- Cloud Migration
- Identity Security
- Regulatory Technology (RegTech) and Auditing

Initiative	Why it's a priority	The role of NHIs
Artificial Intelligence (AI) and Machine Learning (ML)	Banks invest in AI and ML for predictive analytics, personalized customer experiences, fraud detection, and risk management. AI-powered chatbots and virtual assistants are also becoming more common, improving the speed and efficiency of customer support. With the increasing adoption of LLMs (Large Language Models) and RAG (Retrieval Augmented Generation) architectures, many companies are choosing to outsource these technologies rather than develop them in-house, often leveraging open-source solutions.	Non-human identities play a crucial role in this outsourced environment, ensuring secure access to grounding data, managing retrieval processes, and maintaining the integrity of responses generated by AI systems. In RAG architecture, NHIs facilitate the secure retrieval of relevant information from external databases, which is then used by large language models to generate more accurate & contextually relevant responses.
Blockchain and Distributed Ledger Technology (DLT)	Blockchain is considered for its potential to improve security, reduce fraud, and streamline processes like cross-border payments, trade finance, and know-your-customer (KYC) protocols.	Blockchain heavily relies on microservices architecture & API-based connectivity with third parties. NHIs, such as API keys, secrets, and system accounts, are the core digital constructs that ensure secure intra-service connectivity. In the blockchain ecosystem, tokens function similarly to currency, representing ownership or value within the network. These tokens are programmable assets, enabling seamless transactions & interactions within the decentralized environment.
Big Data and Analytics	Banks leverage big data to gain insights into customer behavior, optimize operations, and develop targeted marketing strategies. Advanced analytics also play a crucial role in credit scoring and risk assessment.	NHIs handle data ingestion, manage data processing pipelines, execute analytics jobs, and ensure secure access to big data platforms. They are essential for secure and effective big data analytics.

Initiative	Why it's a priority	The role of NHIs
Robotic Process Automation (RPA)	RPA is used to automate repetitive tasks such as data entry and processing, with the goal of increasing efficiency and reducing human error.	RPA bots use NHIs, such as service accounts, to perform automated tasks, access and update systems, handle data entry, and ensure compliance with security policies.
Open Banking	Open banking initiatives allow customers to securely share their financial data, including Personally Identifiable Information (PII), with third-party providers. This access enables third parties to develop innovative apps and services, offering account holders greater transparency and control over their financial information. A common use case is found in the insurance industry, where companies leverage this shared data to build more accurate and personalized client profiles.	Open banking uses APIs to share data between financial institutions. NHIs authenticate & authorize API calls, ensuring secure data exchange between banks and third-party providers. They manage access controls and monitor API interactions for security and compliance. When a third party connects to your infrastructure using an NHI, that identity effectively becomes your new perimeter.
Mobile and Digital Wallets	Banks are developing mobile and digital wallets to deliver seamless online & mobile banking services. This transformation includes integrating digital wallets, enabling contactless payments, and implementing biometric authentication to enhance security and convenience. In many cases, banks are collaborating with FinTech solutions to co-develop innovative financial services, significantly improving customer experiences.	NHIs facilitate secure authentication, authorize transactions, and ensure data integrity during communication between users, banks, & third-party services. They also support the micro-services architecture that underpins these digital wallets, enabling secure, scalable, & efficient service-to-service communication.

Initiative	Why it's a priority	The role of NHIs
Cloud Migration	Banks are accelerating the adoption of cloud services to improve scalability, reduce costs, and enhance flexibility. Cloud-based solutions are also critical for the deployment of AI and big data analytics.	NHIs are core components of all cloud infrastructure services. Service principles in Azure, Service accounts in Google, and IAM Roles in AWS are essential to managing cloud resources, controlling access to cloud services, orchestrating cloud-based applications, and securing data storage and processing in the cloud. Furthermore, most developers take advantage of native secret managers —such as Azure Key Vault, Google Secret Manager, and AWS Secrets Manager—to store secrets, keys, and other forms of authentication. Cloud is a primary driver for the exponential growth of non-human identities in an enterprise environment.
Identity Security	Banks operate in a highly regulated environment that demands strict adherence to Anti-Money Laundering (AML) procedures and robust safeguards for personal data protection. Mismanagement of user identities and accounts can expose both individuals and institutions to cybercriminal activities, including identity theft and fraud.	NHIs manage the secure access and authentication processes for various services and applications within the bank's infrastructure. Properly managing NHIs is essential to ensure that bad actors do not exploit these digital entities to bypass security controls.
Regulatory Technology (RegTech) and Auditing	RegTech empowers banks to streamline compliance and auditing by automating key processes such as reporting, monitoring, and compliance management, making adherence to regulatory standards more efficient and effective.	As regulations like PCI 4.0 begin to mandate the monitoring and reporting of non-human identities, including controls over system and application accounts, it is becoming critical to properly manage these accounts.

How Financial Services Organizations Can Fail to Secure NHIs

Despite their critical role in enabling finance operations, many enterprises fail to secure NHIs effectively. This failure stems from several interconnected issues.

Underestimating the Risk and Attack Surface	Many enterprises overlook the extensive attack surface that NHIs create. They often underestimate the number of NHIs within their environment and the complexity of managing them. This ignorance leads to a lack of focus on securing these identities, leaving the organization exposed to significant cyber risks. The assumption that traditional security measures for human identities can be applied to NHIs often results in inadequate protection.
Relying on Human Identity Management Processes	Enterprises frequently depend on Identity and Access Management (IAM) processes and technologies designed for human users, which are ill-suited for managing NHIs. Traditional Identity Governance and Administration (IGA) tools are typically built around authoritative human identity sources, such as HR databases or Active Directory. However, NHIs are distributed across multiple environments—cloud platforms, on-premises systems, and various applications—where traditional tools struggle to provide the necessary visibility, control, and security measures.
Failure to Recognize Operational Challenges	Many organizations struggle to operationalize the management of NHIs effectively, leading to error-prone practices and security gaps. Without standardized processes, managing the complexity & volume of NHIs across various environments becomes overwhelming. As seen in the Cloudflare incident, where the failure to rotate just four out of thousands of secrets left critical NHIs exposed. The absence of clear, repeatable processes for handling NHIs across platforms, cloud services, and on-premises systems results in inconsistent practices and fragmented oversight.
Failure to Bridge the Gap Between Security Teams and Developers	There is often a gap between security teams and developers, where security teams lack the ability to enforce practices effectively—having a policy does not guarantee it will be followed or implemented, especially when security measures are seen as obstacles that slow down development. This misalignment can cause developers to bypass security protocols, resulting in protection gaps. Balancing the needs of both security and development is essential to ensure that both teams can achieve their objectives without feeling hindered or compromised.
Lack of Designated Responsibility for NHI Security	Often, no single team is responsible for the security of NHIs, leading to a lack of accountability and oversight. The responsibility for securing NHIs is fragmented across multiple teams—such as cloud, IAM, and development teams—creating gaps in coverage and increasing the likelihood of security issues. Without a clear mandate & ownership, NHIs can easily be neglected, leading to mismanagement and potential security breaches.

Building an Effective NHI Security Strategy

Implementing a successful strategy to manage and secure NHIs needs to be a top priority for cybersecurity and IAM programs. While identity has become the new security perimeter, focusing only on humans alone is no longer enough because the identity perimeter is now mostly Non-human.

There are three critical steps to achieve:

1. **Visibility:** The first step is gaining a comprehensive understanding of your environment and all identities within it, beyond just the data provided by your Identity Provider (IdP), by incorporating multiple sources of information for deeper visibility into all an identity's critical usage characteristics.

2. **Security:** The second step is about understanding your perimeter risk exposure. This means developing security policies tailored to your specific business needs, utilizing tools with advanced analytics to identify potential gaps, and finally establishing a process for continuous review and assessment of your security posture.

3. **Governance:** The last step is about taking control of the lifecycle without creating operational headaches and minimizing the response time to issues. This means moving beyond slow email-based processes for remediation and adopting a more efficient policy-based automation model that can orchestrate workflows across existing infrastructure and services without disruption.

Choosing the Right NHI Management Solution

Financial services organizations need specialized solutions designed specifically for the unique requirements of non-human entities. While several new solutions have been announced, not all solutions are born equal, and it can be hard to sort through the noise.

Checklist of capabilities to choose the right NHIM solution:

- ☐ **Identity Centric: Architecture**
  Understand all aspects of NHIs. NHIs are the primary asset the solution manages and secures.
- ☐ **Classification**
  Categorizes identities as humans or non-human and resolves ambiguities.
- ☐ **Discovery**
  Scans the environment and automatically creates an inventory across all identity sources.
- ☐ **Usage Contextualization**
  Adds context to identities based on consumers, users' permissions, roles, and resources.
- ☐ **Ownership Assignment**
  Assigns clear ownership to each NHI.
- ☐ **Risk Posture**
  Evaluates security risks and vulnerabilities.
- ☐ **Toxic Combinations**
  Detects concurrent risk combinations.
- ☐ **Threat Detection**
  Identifies suspicious activities in real-time.
- ☐ **Remediation**
  Automates the resolution of security incidents and posture violations.
- ☐ **Compliance**
  Ensures adherence to regulatory requirements.
- ☐ **Workflows**
  Automates security processes and incident management.
- ☐ **Provisioning**
  Manages creation & assignment of identities.
- ☐ **Rotation**
  Regularly updates secrets and credentials based on policy.
- ☐ **Offboarding**
  Remove access to NHI for identities that no longer need exposure & for former employees.
- ☐ **Decommission**
  Safely removes inactive or obsolete identities.
- ☐ **Policy-Based Automation**
  Automates tasks using predefined policies.
- ☐ **Cloud-Native Orchestration**
  Integrates seamlessly with diverse cloud-native services & does not require proprietary systems.
- ☐ **Cross-Cloud**
  Supports all major clouds
- ☐ **Cross-Vault**
  Supports cloud-native and 3rd party cloud vaults.
- ☐ **DevOps Tool Integration**
  Connects with DevOps tools for secure workflows.

By implementing a robust NHIM platform equipped with the integration to the necessary ecosystem & capabilities, organizations can effectively manage non-human identities, strengthen their security posture, and fully leverage the benefits of automation and interconnected systems.

Key Takeaways

- **NHIs are the new digital perimeter:** NHIs like API keys & service accounts are now critical to digital infrastructure. Managing them is essential to protect your organization's perimeter.
- **Traditional tools can't keep up:** Existing identity management tools weren't built for NHIs, leaving organizations exposed in today's decentralized, multi-cloud environments.
- **Vulnerabilities are everywhere:** Due to misconfigurations, unrotated secrets, & poor controls, NHIs are prime targets for attackers, driving the need for specialized management.
- **The cost of inaction is high:** Breaches involving NHIs are costly and damaging. Unmanaged NHIs heighten financial risks and regulatory exposure.
- **A new approach is required:** Organizations need a purpose-built NHIM solution to ensure visibility, control, and security across all environments.
- **Regulations are tightening:** Compliance requirements, like PCI 4.0, are increasingly focusing on NHIs (see appendix).

Discover how Oasis can enhance your organization's efficiency and security by managing non-human identities. Read our white paper: Oasis Security for Financial Services

Appendix: PCI 4.0

The Payment Card Industry Data Security Standard (PCI DSS) was launched in 2006 to provide a framework for securing cardholder data (CHD) and sensitive authentication data (SAD). It applies to all entities involved in the storage, processing, or transmission of CHD and/or SAD or those that could impact the security of such data. This includes merchants, processors, acquirers, issuers, & other service providers. The current version is PCI DSS 4.0, released in March 2024. While some new requirements are considered best practices until March 31, 2025, they will become mandatory for all PCI DSS assessments thereafter.

Key Requirements for Non-Human Identities

Non-Human Identities, referred to as system and application accounts (also known as "service accounts"), are critical elements under PCI DSS v4.0. These accounts execute processes, perform automated tasks, & often require elevated privileges, which makes them significant from a security perspective. The following are the primary requirements related to NHIs:

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

- **Requirement 7.2.5**: All application and system accounts and related access privileges are assigned and managed as follows:
  - Based on the least privileges necessary for the operability of the system or application.
  - Access is limited to the systems, applications, or processes that specifically require their use.
- **Requirement 7.2.5.1**: All access by application and system accounts and related access privileges are reviewed as follows:
  - Periodically (defined in the entity's targeted risk analysis, which is performed according to Requirement 12.3.1)
  - The application/system access remains appropriate for the function performed.
  - Any inappropriate access is addressed.
  - Management acknowledges that access remains appropriate.

Requirement 8.6: Management of Application and System Accounts: The use of application & system accounts and associated authentication factors is strictly managed to ensure they are used only for the intended purpose and are not misused

- **Requirement 8.6.1**: If accounts used by systems or applications can be used for interactive login, they are managed by:
  - Preventing interactive use unless necessary for an exceptional circumstance.
  - Limiting interactive use to the time necessary for the exceptional circumstance.
  - Documenting business justification and explicitly approving it by management.
  - Ensuring all actions are attributable to an individual user, confirming their identity before access is allowed.
- **Requirement 8.6.2**: Passwords for any application & system accounts that can be used for interactive login are not hard-coded in scripts, configuration/property files, or bespoke or custom source code.
- **Requirement 8.6.3**: Passwords for all application & system accounts are protected against misuse by:
- Changing passwords periodically and upon suspicion or confirmation of compromise.
- Constructing passwords with sufficient complexity appropriate for how frequently the entity changes the passwords.

By adhering to these requirements, entities can ensure that NHIs are properly managed and secured, aligning with PCI DSS v4.0 standards to protect cardholder data and sensitive authentication data.

OASIS

Simple. Smart. Effective.

Our mission is to fortify cybersecurity defenses by enabling enterprises to efficiently secure non-human identities throughout their lifecycle.

Get a Demo

Get a Free Assessment

Learn more

Contact us at sales@oasis.security or visit our website at oasis.security