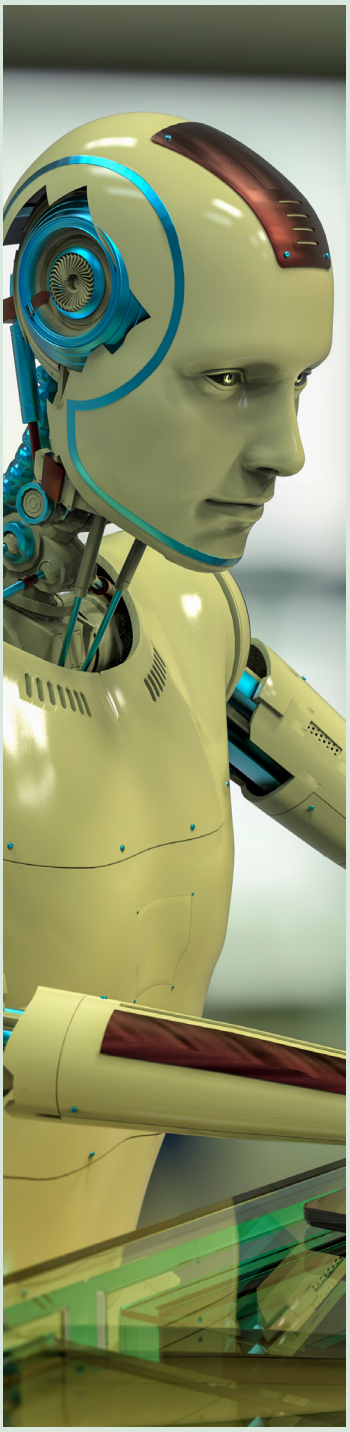
WHITE PAPER



NON-HUMAN IDENTITY MANAGEMENT
— SECURING THE GROWING DIGITAL WORKFORCE

Abstract

Non-human identities (NHIs)—encompassing service accounts, API keys, machine credentials, IoT devices, and automation scripts—now dominate digital ecosystems, averaging 45 NHIs per human employee. This explosion, driven by cloud adoption, microservices, and AI, introduces unprecedented security risks. Unmanaged NHIs create massive attack surfaces, with 97% exhibiting excessive privileges and 44% of tokens exposed in collaborative tools like Teams or Jira. This whitepaper details a proactive framework for NHIM, combining governance, automation, and Zero Trust principles to mitigate risks like credential theft, compliance violations, and large-scale breaches.

Infosys®
Navigate your next

Introduction

What Are Non-Human Identities?

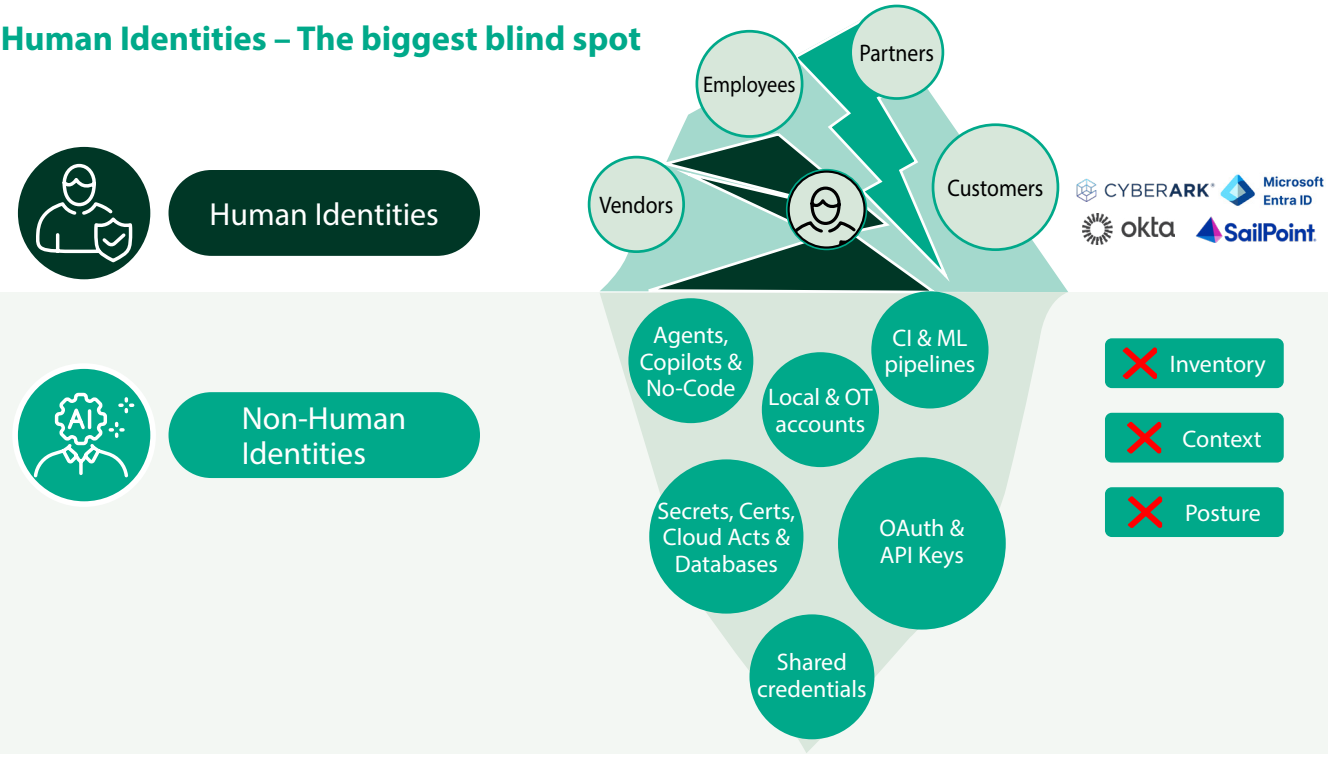
Non-human identities are digital entities that authenticate and authorize machines and software to interact with systems and data autonomously. Unlike human users, NHIs do not use passwords or biometrics; instead, they rely on API keys, OAuth tokens, service accounts, certificates, or cryptographic credentials.

Common types of NHIs include:

- **Service Accounts:** Used by applications to access databases or services.
- **API Tokens and OAuth Credentials:** Facilitate communication between SaaS tools and internal systems.
- **Automation Scripts and Bots:** Run scheduled jobs, CI/CD pipelines, or Robotic Process Automation (RPA).
- **AI Agents:** Automated systems with persistent privileges can be exploited at scale without human intervention.
- **Machine Identities:** Assigned to containers, virtual machines, serverless functions, and IoT devices.

NHIs are created primarily to enable automation, cloud infrastructure provisioning, application integration, and internal microservices communication without human intervention.

Non-Human Identities – The biggest blind spot



Finance & Banking	Trading BOTs	KYC/AML checks	Insurance/Loans	**Payment Gateways**
Healthcare	Device Integration	Lab Automation	EHR Systems	**Data Exchange**
Supply Chain	IoT Sensors	Real-time Reporting	Inventory Mgmt.	**EDI – PO, Invoices**
Retail	Customer Profiler BOT	Chatbots	**Inventory**	**Virtual Assistants**

Non-Human Identity Management (NHIM) is the discipline of discovering, governing, securing, and auditing these identities to mitigate risk, enforce least privilege, and maintain compliance. This whitepaper explores the nature of NHIs, the challenges they pose, and best practices for effective NHIM across modern hybrid and cloud environments.

Key Risks associated with NHIM

Scale and Complexity:
NHIs outnumber humans **45:1**, complicating visibility and governance.

Lifecycle Neglect:
91% of orphaned tokens stay active post-employment, while **71%** lack rotation.

Excessive Privileges:
97% of NHIs have unnecessary permissions, broadening attack surfaces.

Third-Party Exposure:
92% of organizations share NHIs externally, often without aligned security practices.

Non-Human Identity Types

- Service Accounts
- Service Principals
- Storage Account
- Access Keys
- Roles
- RDS Users
- Snowflake Roles
- Batch Process Users
- Document DB Users
- M2M Accounts
- RPA Accounts
- IDaaS Apps – Okta/ Entra etc..
- DB Warehouse Access Credentials

Authentication Methods

- Secret Manager
- Vaults
- SAS Token
- JSON Web Token
- Service-Service Certificates
- GitHub Token
- Storage Account Keys
- OAuth Token
- Encryption Keys
- HMAC Keys
- GitHub API Keys
- KMS Keys

NHI Sources

Why attackers like NHIs

- KMS Keys
- Long Lifespans
- Hidden Backdoors
- Broad blast radius
- Hard to detect unauthorized activities
- Supply chain attacks

The Overlooked Complexity of NHI Lifecycle Management

Managing the lifecycle of Non-Human Identities (NHIs) is one of the most underrated challenges in enterprise security. While Identity and Access Management (IAM) programs have significantly matured for human identities—enforcing onboarding, access control, monitoring, and offboarding processes—NHIs often lack the same level of governance.

Common Exploitation Methods:

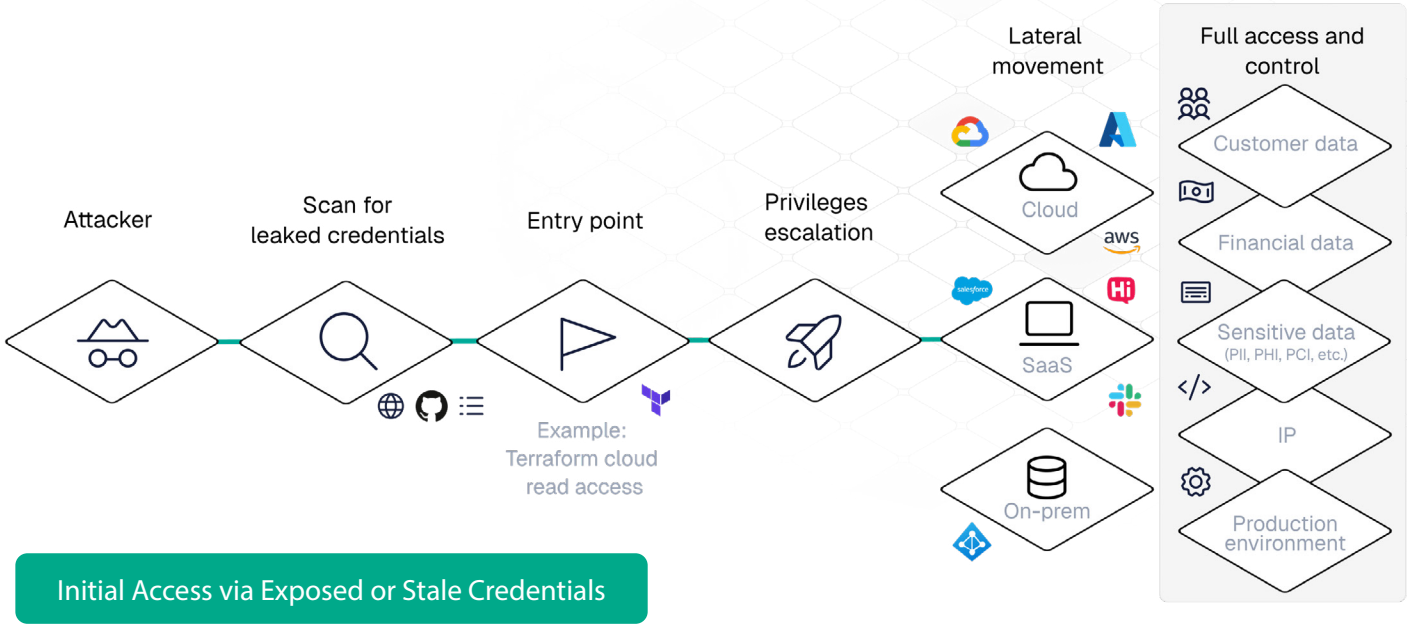
Stale or Unrotated Credentials: Privileged NHIs with unchanged or expired secrets are highly vulnerable to exploitation due to lack of credential rotation and ownership.

Secrets Leakage: Credentials accidentally exposed in source code repositories, developer forums, or public clouds are frequent entry points for attackers.

Overprivileged and Orphaned Accounts: NHIs with excessive permissions or no clear owner increase the risk and facilitate lateral movement within networks.

Third-Party and Supply Chain Risks: Compromised NHIs in third-party integrations or SaaS platforms can propagate attacks across supply chains.

Sample Attack Vector



Initial Access via Exposed or Stale Credentials

Credential Abuse and Lateral Movement

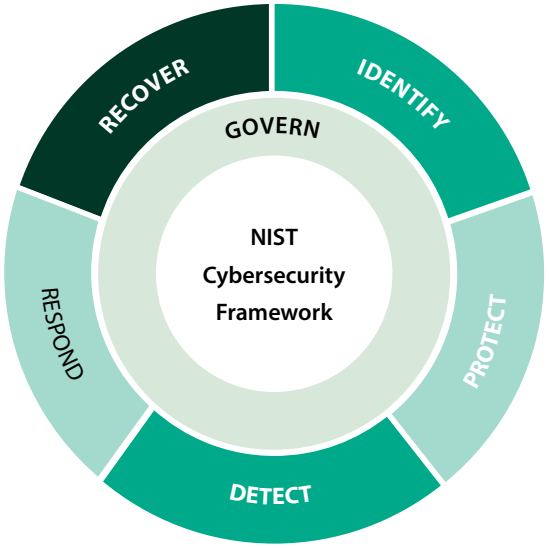
Data Exfiltration and Impact

Persistence via Orphaned or Unmonitored NHIs

Delayed Detection and Response

The Path Forward: Securing Non-Human Identities

The **NIST Cybersecurity Framework (CSF) 2.0** provides a comprehensive and updated approach to managing cybersecurity risks, including specific guidance for securing **Non-Human Identities (NHIs)** such as machine identities, service accounts, AI agents, and workload identities. Applying NIST CSF 2.0 to non-human identity security involves integrating Identity and Access Management (IAM) principles into the framework's core functions to mitigate risks associated with these increasingly critical identities.



CSF 2.0 Function	CATEGORY	CATEGORY IDENTIFIER
Govern	Define NHI ownership, policies, and align with enterprise risk management	**Asset Accountability (GV.AM)** **Asset Compliance (GV.CM)** **Asset Oversight (GV.OV)**

Identify	Inventory and classify NHIs; map access to roles and risk profiles	**Asset Management (ID.AM)** **Identity Management (ID.IM)**
Protect	Use dynamic access controls, credential vaulting, MFA for NHIs	**Access Control (PR.AC)** **Data Security (PR.DS)** **Awareness & Training (PR.AT)**
Detect	Continuous monitoring, behavioral analytics, logging of NHI activities	**Anomalies & Events (DE.AE)** **Security Continuous Monitoring (DE.CM)**
Respond	Incident response plans for NHIs, rapid revocation and remediation	**Response Planning (RS.RP)** **Mitigation (RS.MI)**
Recover	Recovery and post-incident review including NHIs	**Recovery Planning (RC.RP)**

Infosys NHIM deployment framework encapsulates the key directives from **NIST Cybersecurity Framework (CSF) 2.0** which includes the aspects of discovery, ownership, dynamic access control, continuous monitoring, and governance, making it a robust foundation for managing the complex landscape of non-human identities today.

Below are the essential stages and pointers for each foundational element, with a focus on Discovery & Ownership, Posture & Remediation, and Lifecycle Management.

Discovery & Ownership:

Continuously scan, inventory, and classify all non-human identities across environments, mapping them to their functions, assets, and owners for full visibility.

Assign accountable owners to each NHI, ensuring periodic attestation and stakeholder engagement for governance and risk assessment.

Posture & Remediation:

Assess privileges, risks, and policy compliance for all NHIs, enforcing the least privilege through automated policy frameworks and secret management.

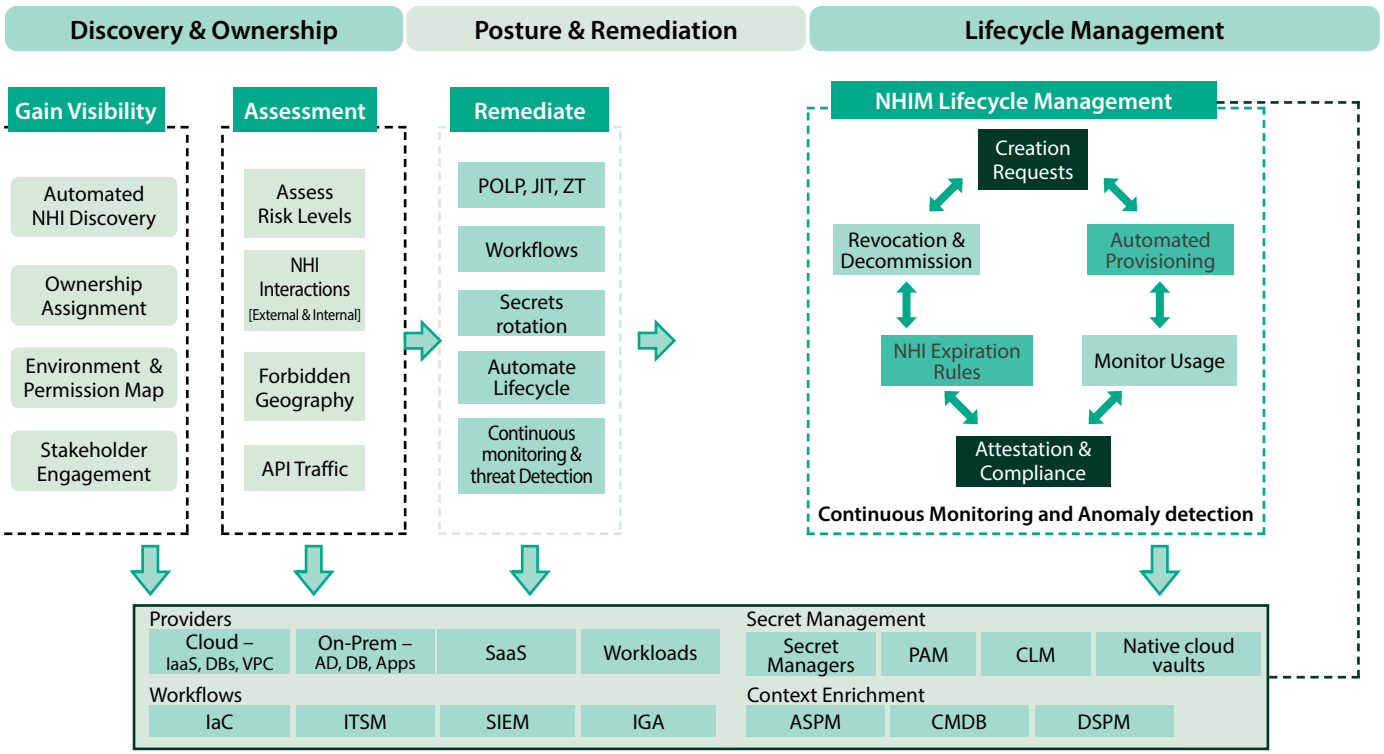
Continuously monitor activity, triggering alerts for anomalies and automating remediation—such as credential rotation or decommissioning—when necessary.

Lifecycle Management:

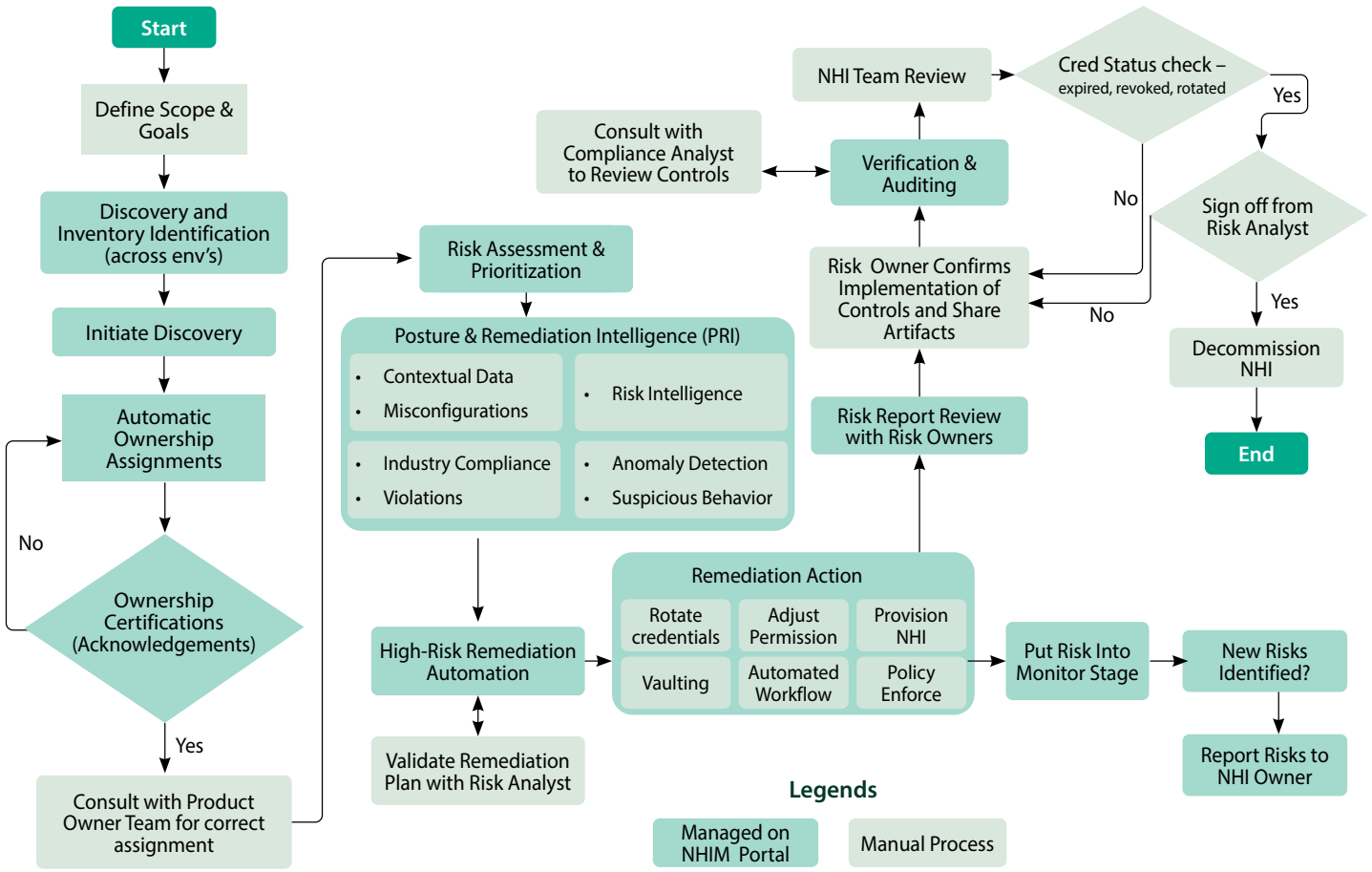
Automate secure provisioning, credential storage, rotation, and access reviews for NHIs, maintaining rigorous control from creation to decommissioning.

Promptly detect and retire unused or orphaned identities, with full audit trails to ensure compliance and minimize operational risk.

Infosys NHIM Framework



NHIM Process workflow to achieve the required result of risk remediation

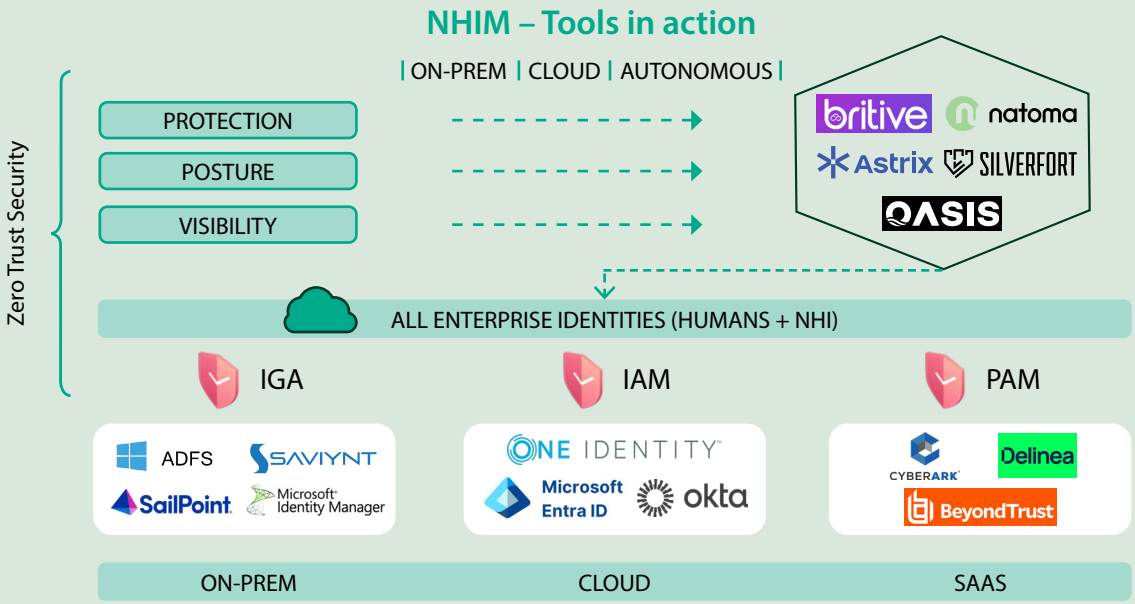


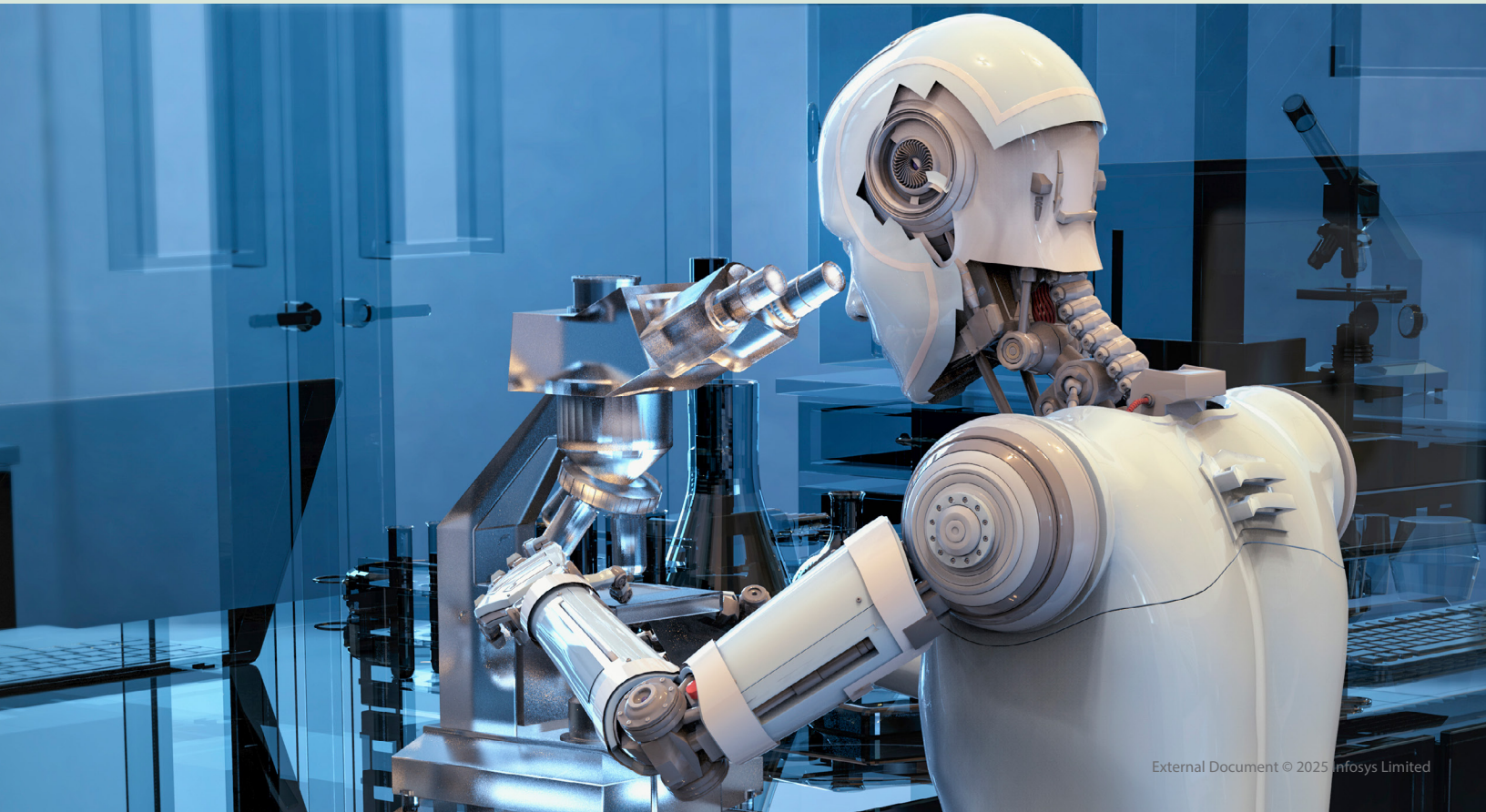
Deriving Benefits & Adopting Best Practices

The framework's emphasis on ownership, dynamic access control, continuous monitoring, and governance makes it a robust foundation for managing the complex landscape of non-human identities today. **Infosys has adopted a comprehensive, multi-vendor strategy to address the complex risks associated with Non-Human Identity Management (NHIM) across cloud and hybrid environments. This approach leverages best-of-breed tools and deep integration to deliver proactive security, compliance, and operational efficiency.**

- Automatically discover and map all NHIs with a contextualized inventory
- Effortlessly manage NHIs lifecycle and address governance gaps
- Drastically reduce the attack surface by mitigating NHI-based risks
- Immediately detect and respond to suspicious NHI behavior to reduce threats impact
- Aspire to operationalize Zero Trust: Aim for Zero Trust everywhere but be practical about making incremental progress

NHIM – Tools in action





Conclusion

By integrating identity management for NHIs into a comprehensive cybersecurity program—guided by leading frameworks such as NIST Cybersecurity Framework (CSF) 2.0—organizations can address unique challenges associated with machine identities.

Ultimately, organizations must treat non-human identities with the same rigor as human identities, recognizing that cyber adversaries increasingly target these digital identities to gain privileged access or enable lateral movement. A risk-based, automated, and well-governed approach to NHI management enables organizations to safeguard critical systems, support compliance objectives, and confidently advance digital transformation initiatives.

References

- The NIST Cybersecurity Framework (CSF) 2.0
- Cybersecurity Framework | NIST
- Non Human Identity Resources
- Security for non-employee identities - White Paper
- The Ultimate Guide To Non-Human Identities

About the Author

Atul Sharma

Principal Consultant

Atul Sharma is an accomplished IAM Architect with over 16 years of specialized experience in Identity and Access Management architecture and engineering. He brings deep expertise in designing and delivering end-to-end IAM solutions, ranging from on-premises deployments to modern, cloud-based platforms.

Atul maintains a forward-thinking approach to shaping the future of digital identity and is deeply engaged in exploring how AI/ML and Agentic Automation can transform access management and security governance.

For more information, contact askus@infosys.com

Infosys®
Navigate your next