KPMG

# Non-Human Identities Management



KPMG. Make the Difference.

June 2026



01 Executive Summary

02 What are NHIs?

03 Drivers and case for action

04 The current challenge and risk landscapes

05 The regulatory landscape

06 NHI Management strategy & Controls Framework

07 NHI vendor landscape and capability benchmark

08 From risk to resilience: The KPMG approach to NHI management

09 Case studies: Notable NHI related incidents

10 Glossary

# Overview

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Executive summary

01

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Executive summary

**Non-Human Identities (NHIs) are the digital credentials that allow machines to interact automatically. They now vastly outnumber human identities and represent the fastest-growing, least-secured attack surface in the modern enterprise.**

NHIs are the **digital credentials and identities assigned to machines, applications, services, scripts, automated pipelines, and devices** that **authenticate and authorise machine-to-machine interactions** without a person present.

In many enterprises NHIs **already outnumber human identities by 80:1**[1], with some environments reporting ratios **up to 144:1**[2] **.**



> Right now, businesses are turning a blind eye to one of the most dangerous threats they face. That innate, emotive and traditional desire we have to protect the human users and their identities is unquestionably important, but machine identities are just as valuable to attackers and need to be understood and protected to the same extent." Source
>
> **Rich Turner,** President of EMEA, CyberArk/IDIRA
>
> (a Palo Alto Networks Company)

> The main problem we're seeing in organisations, and the main problem we had at Microsoft, is that usually organisations don't really know how many NHIs and secrets they have and where they are. Where every misstep could lead to a breach, organisations need to be sure their NHIs are well-managed, well-protected, and well-governed." Source
>
> **Itzik Alvas, CEO** (Entro Security, part of SailPoint now)

> Every attack we've done involves some non-human identity compromise, whether that's during the "in and through" phases of the attack, or as part of the objective - the "out" phase. I can't think of a single job where we didn't compromise a NHI or aim to at one point or other"
>
> **KPMG UK Cyber Defence Services** (CDS) team

[1]Source: CyberArk, "Machine Identities Outnumber Humans by More Than 80 to 1: New Report Exposes the Exponential Threats of Fragmented Identity Security", 2025
[2]Entro Labs, "NHI & Secrets Risk Report H1 2025" Key Takeaways from The Non-Human Identity & Secrets Risk Report

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Executive summary

## The Strategic Imperative

NHIs enable systems to connect, exchange data, and perform operational tasks automatically across cloud, SaaS, and on-prem environments. The accelerated growth and heightened criticality has been driven by cloud-native architectures, persistent automation, and the emergence of agentic AI with Industry evidence now showing a severe lack of confidence in managing NHI risks:

**15%***

of organisations report high confidence in preventing NHI-driven attacks.

**69%***

of organisations are moderately to highly concerned about NHIs as an attack vector.

**When mismanaged, compromised keys or tokens effectively circumvent the MFA protections placed on human users.**

NHIs inherently cannot support MFA. When compromised, they **grant attackers' direct, unchallenged access** and **enable lateral movement at machine speed**.

Organisations must now treat NHIs as first-class identities with security requirements equal to, if not greater than, those applied to human users.



## The Evolving Threat Landscape

Cloud migration, automated pipelines, and Agentic AI are reducing human intervention – but also enabling attackers to automate at scale. AI is now being weaponised to orchestrate attacks with minimal human input.

An inflection point came in late 2025, when Anthropic disclosed a large-scale cyber-espionage campaign driven largely by an autonomous AI agent capable of chaining exploits and moving laterally at machine speed – marking one of the first documented cases of a largely autonomous cyberattack and signaling a major step-change in attacker capability.

Since then, advances in frontier models (e.g., Anthropic's Claude systems, including gated variants such as Mythos) highlight accelerating AI capability – reinforcing the need for equally autonomous, defense-first security models.



*Source: Baron, Hillary. 2024. The State of Non-Human Identity Security. Cloud Security Alliance (Sponsored by Astrix Security – now part of Cisco)

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# What are NHIs?

02

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Understanding NHIs



**Unlike human identities managed centrally by HR, NHIs are highly privileged, heavily fragmented, and generated programmatically at massive scale, requiring an entirely different governance approach.**

## What are NHIs?

- Digital constructs assigned to machines, applications, scripts, and automated processes that allow systems to authenticate reliably and automatically.
- Enable systems to connect, exchange data, and perform operational tasks automatically across cloud, SaaS, and on-prem environments.
- Accelerated growth and heightened criticality primarily due to cloud-native architectures, persistent automation, and the emergence of agentic AI.

## Human identities

Represent people.

vs

## NHIs

Represent machines, applications, scripts, and automated processes.

**Static constructs**

long-lived passwords, API keys, shared service accounts.

**Dynamic/ ephemeral constructs**

OAuth tokens, IAM roles, SPIFFE SVIDs.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Key features of NHIs

**Lifecycle fragmentation:**
Often lead to stale/ unused identities and weak off-boarding as they are created programmatically and sit outside standard Joiner/Mover/Leaver (JML) processes.

**High privilege by design and credential risk:**
High-privilege nature, coupled with common security failures like hard-coded secrets, lack of credential rotation, and misconfigured webhooks, create a highly vulnerable credential risk profile.

**Ownership ambiguity:**
Frequently orphaned or poorly mapped to accountable application or service owners – severely complicating audits and remediation.

**Scale and dynamism:**
Numerous, fast-growing and difficult to track – often exceed human identities by a ratio of 80:1[1].

**Operational usage patterns:**
Access is automatic, repetitive, and often occurs at high frequency to support integrations and automated workflows.

**The visibility gap:**
Often undocumented and entirely unknown to security teams as they are frequently created without clear ownership – not actively protected.

**Non-interactive authentication:**
Authenticate using API keys, tokens, or certificates – rendering traditional security controls like MFA non-enforceable.

**Audit and monitoring challenges:**
Need for specialised discovery, enrichment, and continuous monitoring to tie runtime behavior back to specific NHIs and their ultimate human/ service owners.

## NHIs create unique security challenges

Driven by how they're created, used, and governed.

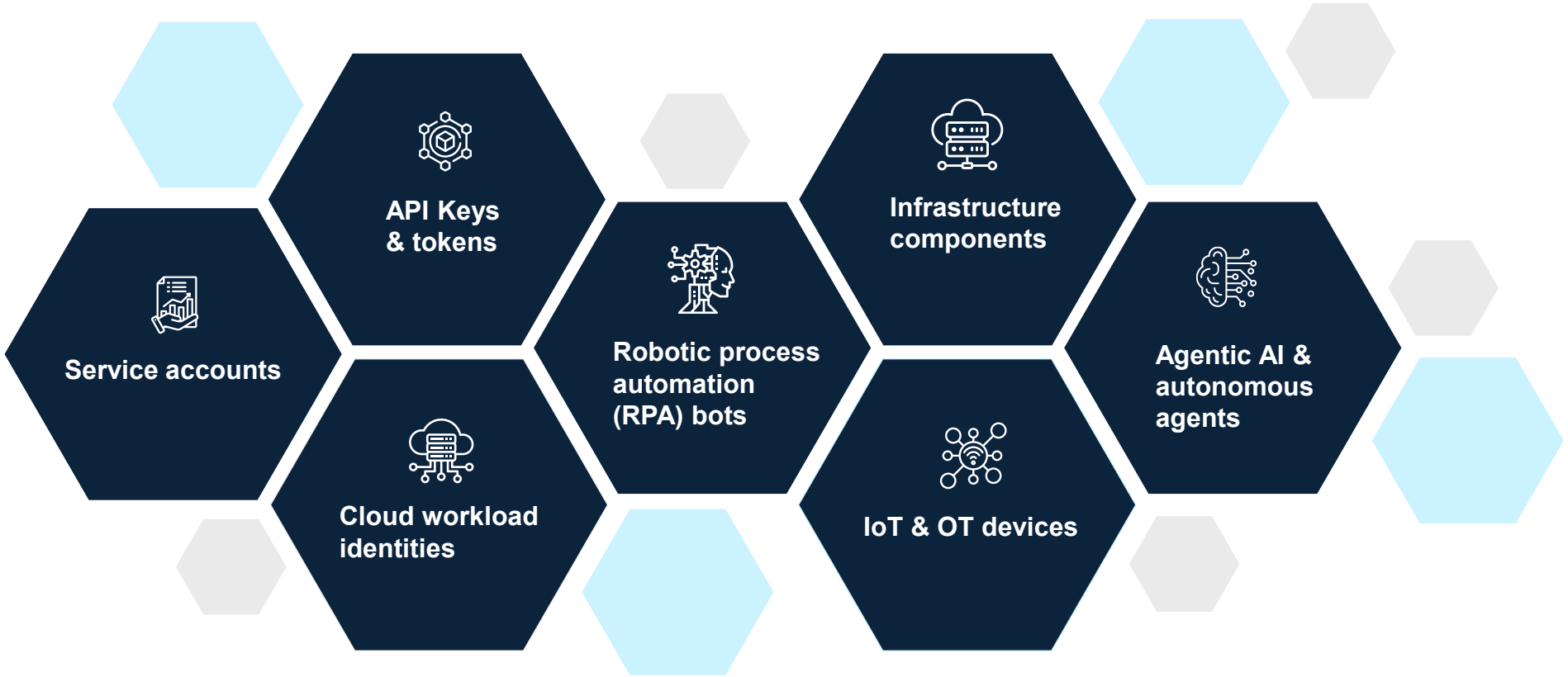
**NHIs are prime targets:**
Built to bypass controls | Enable machine-speed lateral movement

Source: [1]CyberArk, "Machine Identities Outnumber Humans by More Than 80 to 1: New Report Exposes the Exponential Threats of Fragmented Identity Security", 2025

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Common NHI categories




Source: KPMG Analysis

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Overview of common NHI categories

**The following table outlines the most prevalent types of Non-Human Identities, their primary functions, and the specific security risks they introduce to an environment**

| NHI category | Description | Typical security risks |
|---|---|---|
| **Service Accounts** | • Non-interactive accounts used by systems or automated services for backend processes, database interactions, or scheduled jobs.<br>• Often exempt from MFA and hold elevated privileges (e.g., domain admin). | • Hard-coded passwords in legacy scripts, rarely rotated credentials, difficulty identifying the true business owner, and the occasional misuse of these credentials as interactive accounts. |
| **API Keys & Tokens** | • Artifacts (OAuth tokens, JWTs) that allow services to authenticate with each other and cloud platforms, forming the backbone of system-to-system communication. | • Public GitHub leaks, over-permissioned tokens (e.g., granted the permission "all scopes"), and long-lived secrets that never expire. |
| **Cloud Workload Identities** | • Highly dynamic identities (e.g., AWS IAM Roles, Azure Managed Identities) assigned to cloud resources at massive scale in microservice architectures to access storage, secrets, or databases. | • Excessive trust relationships between workloads, inheritance of overly broad IAM roles, and unclear accountability. |
| **RPA Bots** | • Robotic Process Automation bots that run business processes by imitating human actions (logging into portals, etc.), often requiring the exact same access as the employee they replicate. | • Shared bot accounts, non-rotated secrets, and the lack of an audit trail to distinguish bot-initiated actions from human activity. |
| **Infrastructure Components** | • Machine credentials used by autonomous infrastructure (Containers, VMs, CI/CD pipelines) to pull images, deploy code, or read configurations.<br>• Containers create thousands of ephemeral identities daily. | • High-value secrets stored in plaintext pipeline variables, unsecured build agents, and compromised container images with embedded credentials. |
| **IoT & OT Devices** | • Identities for physical operational technology like sensors, industrial machines, medical devices, and building management systems.<br>• Crucial for physical operations but often running outdated firmware. | • Inability to support modern authentication protocols, leading to a total lack of identity governance applied to highly critical physical infrastructure. |
| **Agentic AI & Autonomous Agents** | • AI models and agents designed to autonomously execute tasks, retrieve data, and call third-party APIs (e.g., AI customer support bots querying CRM databases).<br>• Highly dynamic, chaining actions across trust boundaries without human prompting. | • Indirect Prompt Injection: Hijacking agent logic via malicious data to abuse NHI privileges.<br>• Non-deterministic Lateral Movement: Dynamically evolving attack paths that bypass static detections.<br>• Confused Deputy: High-privilege agents leaking data to unauthorised users.<br>• Shadow AI: Autonomous creation of untracked sub-identities. |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Drivers and case for action

03

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Why NHIs are a risk

## Explosive identity growth

NHIs now form the largest and fastest-growing identity class in cyberspace.

## Privileged but unmanaged

Despite their massive scale and elevated privileges – acting as deeply embedded "trusted actors" – they remain chronically under-governed and many exist without lifecycle management.

## A prime attack vector

Consequently, attackers actively target NHIs to bypass MFA and achieve lateral movement, data exfiltration, and ransomware propagation with minimal detection.

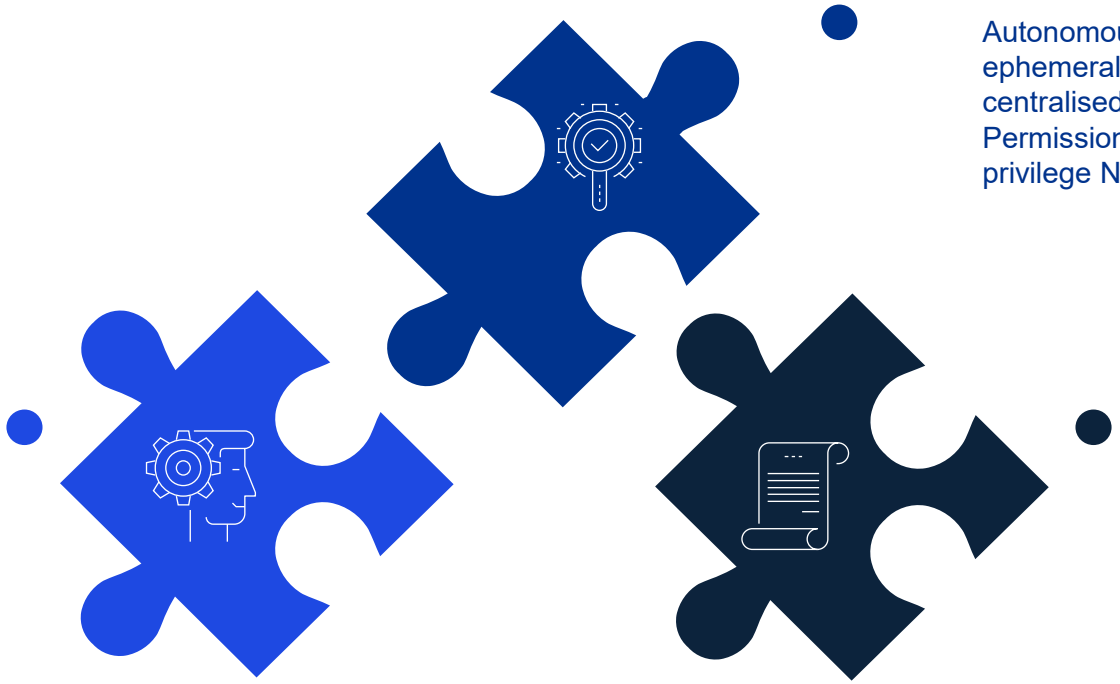


© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Why NHIs matter to organisations

## The "shadow AI" problem:

Autonomous agents can programmatically generate ephemeral sub-identities to complete tasks. Without centralised tracking, this leads to "Autonomous Permission Creep", creating a web of untracked, high-privilege NHIs that security teams cannot see or revoke



## Operational dependency:

Because critical flows depend on NHIs, a single misconfigured or revoked machine identity can disrupt payments, halt customer-facing services, or break integrations.

## Compliance pressure

Regulators increasingly expect organisations to demonstrate strong, auditable governance over machine identities to prevent operational disruption and non-compliance.

**Mismanaged NHIs break the business: Enabling breaches, halting operations, and exposing organisations to regulatory penalties.**

Source: KPMG Analysis

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# The current challenge and risk landscape

04

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# The current challenges



**While organisations generally understand how to manage human identities via established HR processes, NHIs present drastically different practical challenges. The traditional IAM toolkits and workflows simply do not map directly to machine identities.**

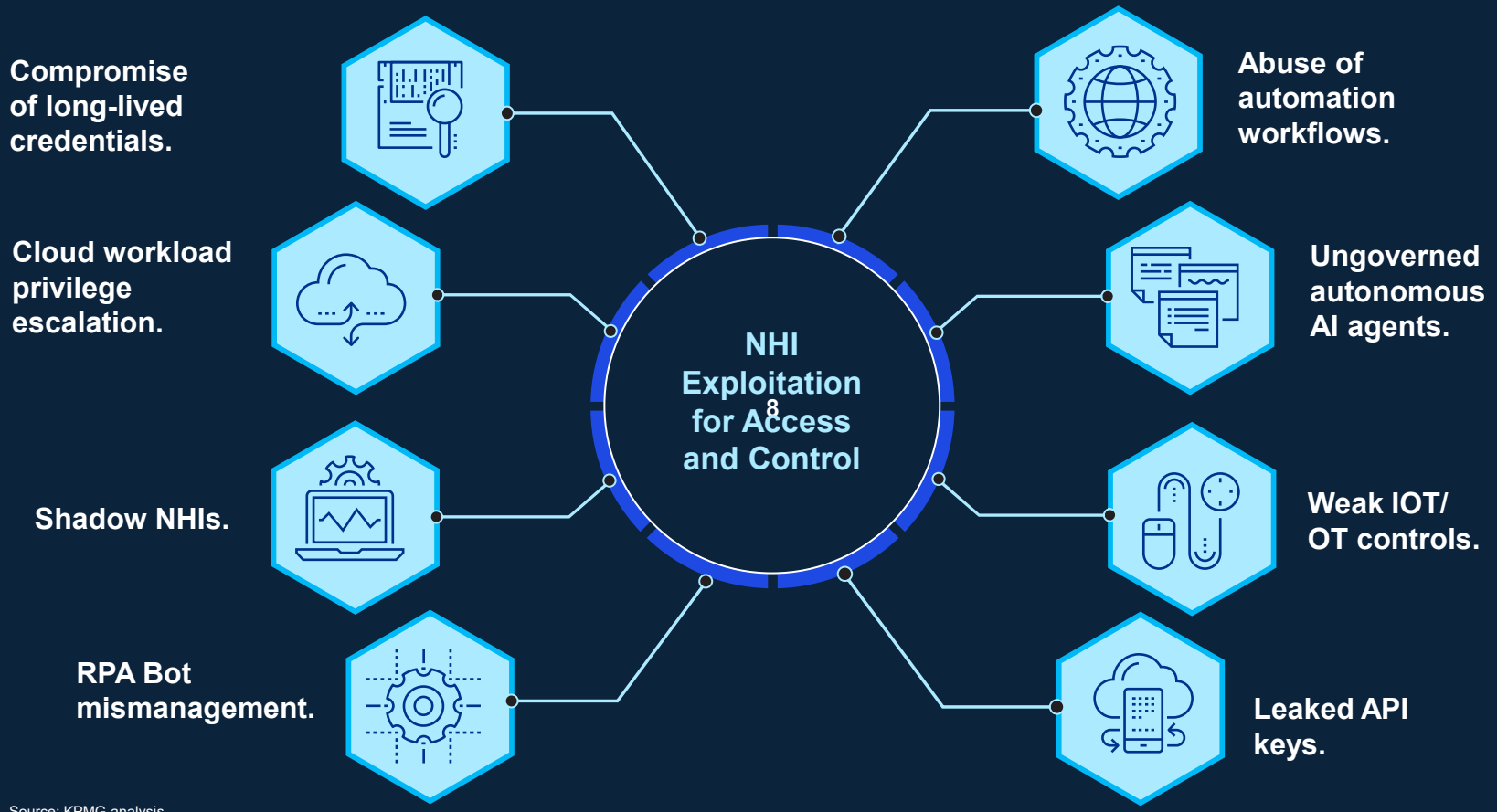
**Traditional, human-centric IAM tools do not secure machine identities with the same rigor as human identities, leaving organisations blind to their true attack surface and vulnerable to critical risks like improper offboarding and secret leakage.**

| Human identities | | NHIs |
|---|---|---|
| Centralised and triggered by HR (JML processes). | **Lifecycle Ownership** | Decentralised, created programmatically by developers/cloud engineers, or automated CI/CD pipelines.<br>Often completely bypass security teams. |
| Use interactive logins protected by MFA and Single Sign-On. | **Authentication** | Rely on programmatic, static secrets (API keys, tokens, certificates) that cannot prompt for MFA.<br>Highly vulnerable if leaked. |
| One primary corporate identity per human user. | **Visibility and Scale** | Massive scale and “shadow identities” as a single developer might spin up dozens of ephemeral microservices and containers.<br>Lack of sight, tracking and confident revocation (without breaking business-critical apps). |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Key NHI threat vectors




Source: KPMG analysis



© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Key NHI threat vectors and business impacts

| Threat vector | Vulnerability and governance gap | Business impact |
|---|---|---|
| **Compromise of long-lived credentials** | Hardcoded service credentials (API keys, certs) bypass MFA and remain unrotated. | 01 — Broad lateral movement. Severe data exfiltration. Large-scale compromise. |
| **Cloud workload privilege escalation** | Over-privileged IAM roles and unmanaged trust relationships. | 02 — Full environment compromise by attackers from escalated privileges across storage, databases, and secrets. |
| **Shadow NHIs** | Unmonitored machine identities automatically generated outside standard lifecycle processes by CI/CD systems, Infrastructure as Code (IaC) workflows, and scripts. | 03 — Orphaned and forgotten accounts become undetected backdoors into critical infrastructure. |
| **RPA Bot Mismanagement** | Informal governance of shared credentials used by RPA bots which are rarely rotated and difficult to distinguish from human activity. | 04 — Fraudulent transactions. Unaudited system activity. Inability to accurately attribute malicious actions. |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Key NHI threat vectors and business impacts (cont.)

| Threat vector | Vulnerability and governance gap | Business impact | | |
|---|---|---|---|---|
| **Leaked API Keys** | Exposure of API keys or OAuth tokens in code or logs enables unauthorised system access without authentication. | 05 | Unauthorised system access. | Rapid data extraction. | Complete internal services takeover. |
| **Weak IoT/OT Controls** | Outdated firmware incapable of supporting modern authentication. | 06 | Loss of control over physical operations. | Disruption of critical physical operations. |
| **Ungoverned Autonomous AI Agents** | Lack of frameworks to identify and constrain autonomously created credentials. | 07 | Uncontrolled actions with direct business impact. | Uncontrolled and rapid access expansion. | Untraceable system modifications. |
| **Abuse of Automated Workflows** | Systems reliant on critical data flows and automated workloads managed by NHIs. | 08 | Operational outages. | Breakdown of critical service delivery. | Halting of critical business processes (e.g., payments, customer service). |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Case studies: High impact NHI incidents

**NHI focus:** NHI's (legacy system-level access paths) remained active and unmonitored post Starwood Hotel acquisition, highlighting weak NHI governance during M&A integration.

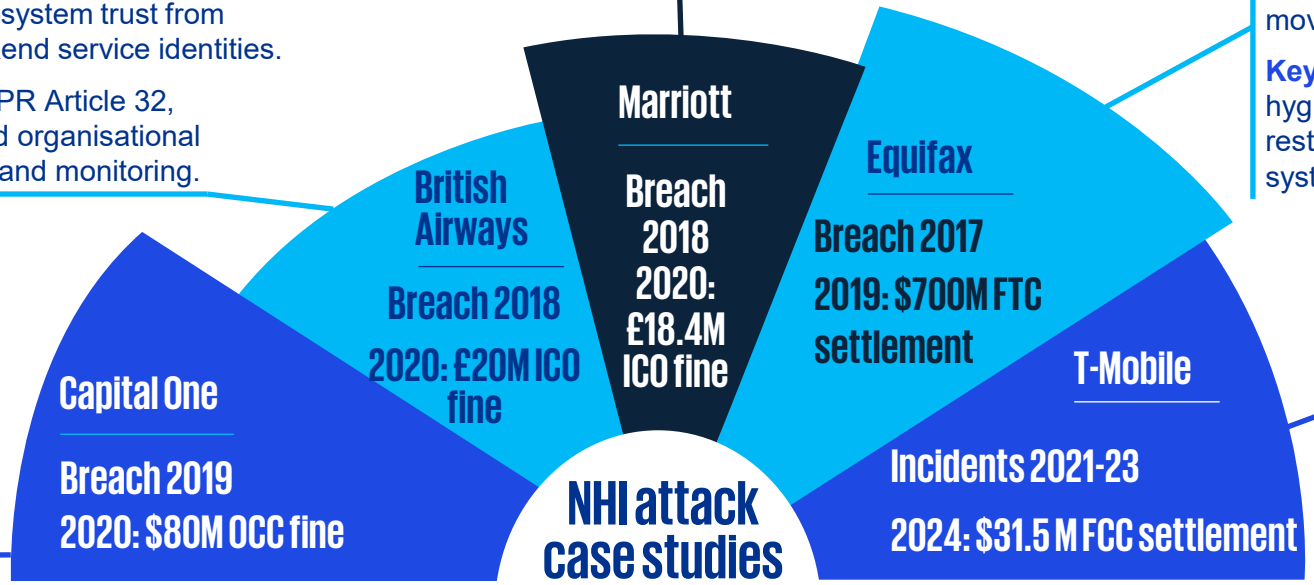
**Key control gap:** Poor access controls and inadequate backend monitoring allowed attackers to exploit inherited systems long after the acquisition, exposing gaps in post-merger security assurance.

**NHI focus:** Exploitation of system-to-system trust from implicitly trusted application and backend service identities.

**Key control gap:** Failures under GDPR Article 32, emphasising insufficient technical and organisational measures around automated access and monitoring.

**NHI focus:** Over-privileged, long-lived system and service account identities enabled attackers to persist and laterally move at scale without detection.

**Key control gap:** Failure to implement basic hygiene controls, including patching, access restriction, and monitoring of backend system activity.




**NHI Focus:** Misconfigured cloud permissions allowed exploitation of machine identity (IAM role) with over-privileged access.

**Key control Gap:** Deficiencies in cloud risk assessment and access control design.

**NHI focus:** Unauthorised access to customer data due to weak API and insufficient access monitoring.

**Key control gap:** Lapse in customer data protection, failed enforcement of least privilege, and inadequate API access monitoring.

Source: ACM, "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned", 2022; Huntress, "British Airways Data Breach", 2025; Epic, "Equifax Data Breach"; Huntress, "Marriott Data Breach", 2025; Huntress, "T-Mobile 2023 API Data Breach", 2025

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# MOVEit supply chain breach (2023)

## Why this breach matters for NHIs?

### Automation at scale

Automated file transfer platforms act as high-volume, trusted machine-to-machine data pipelines across organisations.

### Centralised trust mode

Single systems (e.g., MFT platforms) often hold privileged access to multiple internal and third-party environments.

### Third-party dependencies

Widely used across supply chains, amplifying blast radius when compromised.

### Key application areas

- Automated data exchange across partners.
- API-driven integrations.
- CI/CD and data pipelines.

## Where NHI controls broke down

**Uncontrolled automated data pipelines**

Machine-to-machine file transfers operated with implicit trust and lacked granular access controls or validation mechanisms.

**Unmonitored automated data flows**

Hardcoded credentials and insecure protocols in legacy OT systems expose NHIs to exploitation.

**Third-party trust exploitation**

Unmonitored and shadow NHIs lacking governance can enable unauthorised access and manipulation of sensitive operational data.

**Credential misuse at scale**

Stale credentials and reused access in dormant NHIs create persistent backdoors, increasing the risk of long-term compromise.

## Incident

A zero-day vulnerability in Progress Software's MOVEit Transfer platform enabled attackers to exploit trusted automated file transfer pipelines, impacting 2,700+ organisations and ~90 million individuals globally.

**NHI failure**

Uncontrolled machine-to-machine data flows and implicit trust in automated pipelines.

**Business impact**

One of the largest supply chain breaches, with ~$9 - 10B estimated global cost, widespread regulatory exposure, and downstream partner compromise.

**NHI failure pattern**

- Automated system-to-system data flows (MFT platform).
- No granular control over machine access.
- Centralised pipeline = single point of systemic failure.

**Timeline:**

- May 28, 2023 → first suspicious activity reported.
- May 31, 2023 → vulnerability publicly disclosed.
- June 2023 → mass exploitation confirmed globally.

**Links:**

- Techcrunch – MoveIt Mass Hack by the Numbers.
- Wikipedia – MOVEit Data Breach.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Typical NHI compromise pathway attack kill chain

| | Reconnaissance and Exposure | Initial access | Discovery and lateral movement | Privilege escalation | Action on objectives (impact) |
|---|---|---|---|---|---|
| **Attacker Action** | Scans public repositories (like GitHub), Pastebin, or unsecured S3 buckets for exposed secrets, API keys, or default service account credentials. | Uses the compromised token or API key to authenticate into the corporate network, cloud environment, or SaaS application. | Uses the NHI to scan the internal environment, in search of connections to production databases or adjacent cloud instances. | Leverages the service account to access a secrets vault, modify IAM policies, or assume a higher-level role (such as domain admin/ cloud root user). | Executes end goal at high speed to exfiltrate sensitive data, deploy ransomware across automated pipelines, or spin up crypto-mining infrastructure. |
| **NHI Vulnerability exploited** | **Hardcoded secrets:** Developers often embed credentials directly into source code or config files for convenience. | **Lack of MFA:** Because it is a machine identity, the system does not prompt the attacker for a second factor or CAPTCHA. The token is trusted implicitly. | **Stale/shared accounts:** Stale or shared NHIs often persist beyond their intended use, enabling broad internal access, while AI-driven agents dynamically identify and exploit lateral movement paths in real time. | **Over-provisioning (Violation of Least Privilege):** NHIs are given broad permissions to avoid breaking automated workflows, which are exploited to access sensitive areas and leak information. | **Lack of behavioural monitoring:** Machines operate rapidly and at odd hours due to which massive data transfers, or sudden resource spikes by NHIs often go unnoticed by standard user-behaviour analytics. |
| **MOVEit, 2023** | Exposed credentials and vulnerabilities in widely used file transfer services created an entry point into non-human identity. environments | Compromised service accounts and NHI credentials enabled unauthorised access to enterprise systems without human verification. | Trusted NHIs and automated processes were used to identify connected systems, databases, and data transfer pathways | Over-privileged NHIs allowed expansion into sensitive systems and access to large volumes of critical data. | Automated NHI access enabled rapid, large-scale exfiltration of sensitive data across multiple organisations. |

Source: KPMG analysis

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# The regulatory landscape

05

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Overview



**Regulators have recognised that unsecured machine identities pose a massive systemic risk. Modern frameworks now require organisations to apply the same IAM controls used for human identities – such as lifecycle management, vaulting, and least privilege – to service accounts, APIs, and workloads.**

**Regulators increasingly classify unsecured NHIs as a systemic risk, elevating NHI governance from a technical concern to a core compliance requirement, necessitating evaluation across three interconnected regulatory pillars.**

### Security: Safeguarding system access and resilience

Safeguards infrastructure and assets from unauthorised access, privilege escalation, and lateral movement arising from compromised machine credentials.

### Privacy: Protecting personal and sensitive information

Evaluates how non-human identities access and process sensitive data, including PII and PHI, from a privacy and data protection standpoint.



### Data: Governing data integrity, sovereignty, and machine access

Focuses on ensuring the secure flow, integrity, and sovereignty of data exchanged between systems, particularly in API-driven, cloud-native architectures, and AI ecosystems.

**Recent advancements in technology and artificial intelligence have increased regulatory scrutiny and heightened interest among industry and government bodies in the need for effective Non-Human Identity (NHI) management. Particularly, in the UK, this growing focus is being driven by three key factors:**

**01** NCSC UK PQC migration targets for enterprise PKI (quantum ready encryption for device certificates).

**02** CA/Browser Forum mandate to reduce SSL/TLS certificate lifecycle to 47 days by 2029 (automated digital certificates rotation)

**03** Emergence of frontier AI models with strong cyber capabilities (e.g., Anthropic's gated Claude Mythos), creating dual-use risks for attackers and defenders

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Key standards/frameworks, laws and regulations

## 01 Security frameworks and standards

Demand organisation eliminate long-lived credentials, enforce least-privilege access, implement proper secret rotation, and establish a verifiable lifecycle for every machine identity

### Key global regulations

- **OWASP NHI Top 10:** Serves as a de facto technical standard for mitigating NHI risks.
- **NIST SP 800-207:** Enforces continuous verification, micro-segmentation, and strict access governance across machine and human interactions.
- **ISO/IEC 27001:2022 (updated Annex A provisions):** Requires lifecycle management and least-privilege access controls for NHIs.
- **DORA and NIS 2:** Enforce strong access controls for automated functions, authentication mechanisms for cryptographic keys, and continuous monitoring of non-interactive service accounts.
- **NCSC CAF and Cyber Essentials:** Mandate comprehensive inventory, monitoring, and least-privilege governance of NHIs, including service accounts to prevent credential misuse and lateral movement.

## 02 Privacy laws and regulations

Mandate "data protection by default" for automated processes by requiring strict authentication, authorisation, and access limited only to the data necessary for their functioning

### Key global regulations

- **GDPR (Articles 25 and 32):** Mandate least-privilege access and strong technical controls for automated processing, with breaches from implicit trust or compromised secrets attracting significant penalties.
- **Personal Information Protection Law:** Requires stringent safeguards for automated personal data processing, enforcing strong authentication and monitoring of APIs and backend systems to prevent unauthorised exposure.
- **HIPAA (Security Rule):** Mandates robust authentication and access controls for systems and machine identities handling ePHI.

## 03 Data laws and standards

Enforce safeguards over machine-to-machine data access, continuous oversight, and demonstrable NHI governance (especially while interacting with restricted data) as per sovereignty policies

### Key global regulations

- **Cybersecurity Law and Data Security Law:** Mandate strict access controls and data localisation for network data processing, including API- and service account-led activities, with significant penalties on unmonitored cross-border NHI data flows.
- **Data Act:** Requires strong IAM and service identity controls for access to machine-generated data.
- **EU AI Act:** Establishes governance over autonomous AI systems, addressing risks from models that automatically access and process data using machine identities.
- **PCI-DSS:** Enforces robust access governance, secret management, and identity lifecycle controls for systems and associated machine identities handling cardholder data.

Source: KPMG Analysis; OWASP Non-Human Identities Top 10 [URL]; NIST SP 800-207 [URL]; ISO [URL]; DORA [URL]; NIS 2 Directive [URL]; Cyber Assessment Framework [URL]; Cyber Essentials [URL]; GDPR [URL]; PIPL [URL]; Security Rule [URL]; Cybersecurity Law (China) [URL]; Data Security Law of the People's Republic of China [URL]; Data Act [URL]; EU AI Act [URL]; PCI-DSS [URL]

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# NHI Management Strategy & Control Framework

06

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# NHI Risk mitigation priorities

**Start with these questions to uncover your most critical NHI risks.**

### Is there a NHI policy in place?

Ensure all NHI are created, approved, inventoried, monitored and decommissioned with risks and controls identified (orphaned accounts, credential rotation, privilege review and monitoring etc.).

### Do we have a full inventory?

Eliminate shadow identities across cloud, hybrid, and on-premise.

### Who is accountable?

Explicitly define owners for every account.

### Are credentials vaulted and rotated?

Ban hard-coded secrets.

### Are we avoiding long-standing credentials?

Shift toward short-lived, ephemeral tokens and Just-In-Time (JIT) access to minimise the window of opportunity if a credential is ever compromised.

### Are pipelines creating untracked NHIs?

Ensure CI/ CD integrates with identity tracking.

### Do our AI agents have 'Human-in-the-loop' gates?

Ensure manual authorisation is required before an agent uses NHIs with administrative or bulk-export privileges.

### Are you tracking key NHI metrics to measure effectiveness of NHI mitigation efforts?

Ensure key KPIs are tracked across aspects such as ownership, credential lifespan, pipeline hygiene and cleanup.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# From risk to control: Operationalising NHI management

**Non-Human Identity management requires both a risk-based lens to prioritise what matters and a lifecycle model to operationalise controls at scale. These two perspectives work together to ensure NHIs are not only understood, but continuously governed and secured across their full lifecycle.**

## Risk management: identifying, assessing, and prioritising NHI risk



**In practice, understanding the NHI attack surface requires a structured view of where exposure sits across the environment and how that risk accumulates across identities, access, and usage.**

### Identification (visibility & discovery)

The foundational step in risk management is achieving total visibility. Organisations must implement continuous discovery mechanisms – scanning code repositories, cloud environments, and SaaS platforms – to identify all static and dynamic NHIs. This process must specifically target "shadow" NHIs and orphaned service accounts that exist outside official IT governance.

### Assessment (contextual risk scoring)

Once identified, every NHI must be assessed for risk based on its context. This involves evaluating the identity's privilege level, its access to sensitive environments (e.g., databases containing PII or financial records), and its authentication strength (e.g., long-lived static key vs. dynamically rotated token). High-risk NHIs, such as over-privileged cloud workload identities or dormant accounts with domain admin access, must be flagged for immediate priority.

### Remediation & mitigation

Remediation strategies must be actionable and, where possible, automated to match the scale of machine identities. This includes right-sizing over-privileged accounts, vaulting plaintext secrets, and migrating legacy accounts to Just-In-Time (JIT) access models. Furthermore, organisations must map the operational "blast radius" of critical NHIs; this ensures that if an NHI is compromised, Security Operations (SOC) teams can confidently revoke the credential without inadvertently causing catastrophic outages to core business services.

## Lifecycle control: operationalising NHI governance and security



**Translating that understanding into control then depends on a consistent lifecycle approach, ensuring NHIs are governed, secured, and monitored throughout their use.**

### Continuous discovery & inventory

Security teams cannot protect what they cannot see. The solution requires automated scanning across code repositories (GitHub), cloud environments (AWS/Azure), and CI/CD pipelines to build a centralised, continuously updated inventory of all keys, tokens, and service accounts, effectively eliminating "Shadow NHIs".

### Context & ownership mapping

Every machine identity must be explicitly tied to a human owner, a specific application, or a business unit. Solutions must auto-discover usage patterns to suggest owners for orphaned accounts, ensuring accountability when a credential needs to be rotated or revoked.

### Posture management & threat detection (ITDR)

Applying strict Least Privilege by analysing actual usage versus granted permissions to remove excessive rights. Furthermore, integrating NHI telemetry into the SIEM/SOC enables real-time Identity Threat Detection and Response (ITDR) to instantly block anomalous machine behaviour.

### Lifecycle automation (provisioning to deprovisioning)

Moving away from manual ticket requests, the solution must integrate with developer workflows. This enables secure, automated provisioning of Just-In-Time (JIT) credentials and, crucially, automated revocation when a project ends or a microservice is decommissioned.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Organisational policies, standards, and accountability

**Technology alone cannot secure NHIs; establishing control requires integrated lifecycle management supported by clear governance, defined ownership, and a well-structured operating model.**

## What needs to be fixed (policies and standards)

Organisations must formally update their IAM policies to mandate explicit controls for Non-Human Identities. This includes prohibiting hard-coded secrets in code repositories, enforcing maximum credential lifespans (e.g., mandatory 30–90-day rotation), establishing a verifiable JML process for machines, and demanding a transition to short-lived, ephemeral tokens where feasible.

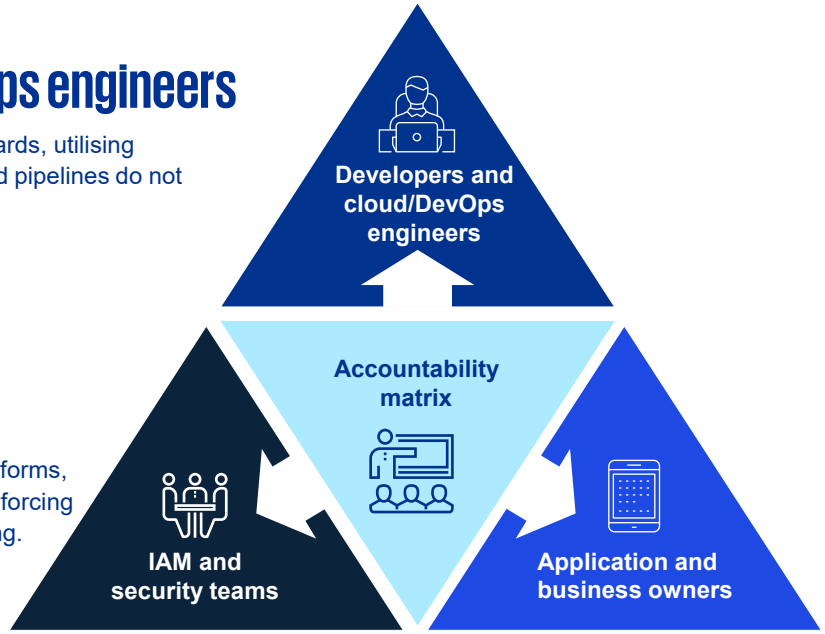
**Accountability for Non-Human Identity management cannot reside solely with the central security team. A matrixed approach is required to secure NHIs at scale:**

## Developers and cloud/DevOps engineers

Responsible for adhering to secure coding standards, utilising centralised secret vaults, and ensuring automated pipelines do not generate untracked "shadow" identities.

## IAM and security teams

Responsible for providing centralised identity platforms, defining the overarching policy guardrails, and enforcing compliance through continuous posture monitoring.




## Application and business owners

Responsible for regular access reviews, recertification, and approving decommissioning; must be explicitly documented as the accountable "human owner" of every NHI tied to their service

Source: KPMG Analysis

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# NHI lifecycle management

**Securing NHIs requires moving beyond manual spreadsheets to a fully automated lifecycle approach, encompassing continuous discovery, strict ownership mapping, JIT provisioning, and real-time threat detection.**

## Preventive controls

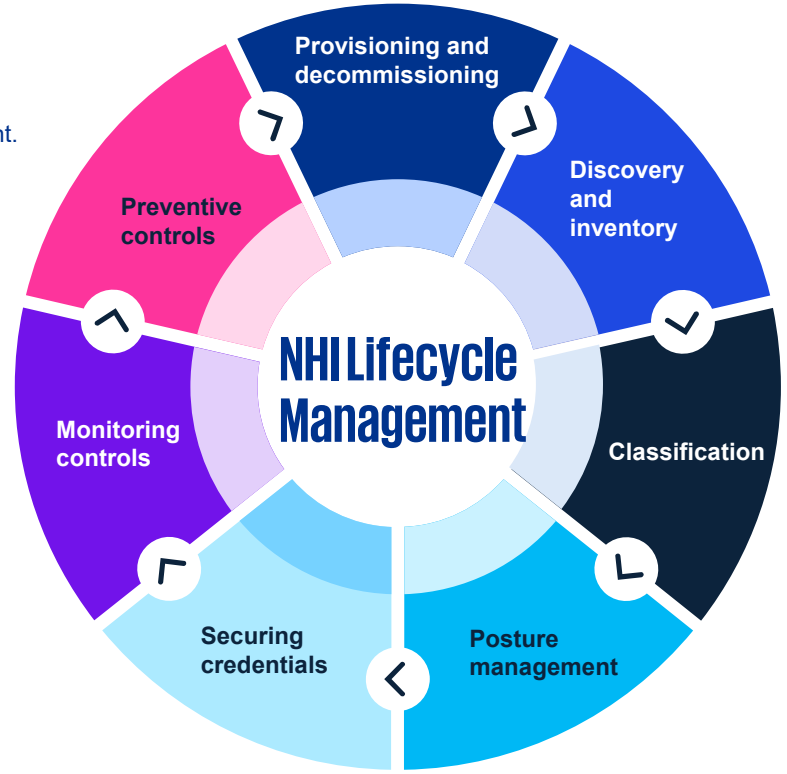
- Block check-in of secrets during the development phase.
- Enable real-time threat protection via automated policy enforcement.

## Monitoring controls

- Use behaviour analytics to detect misuse and anomalies.
- Differentiate between NHI and human usage to reduce false positives.

## Securing credentials

- Transition from plain-text to encrypted/password-less.
- Implement automated rotation via vaulting to uncover hidden dependencies.




## Provisioning and decommissioning

- Configure static NHIs into secret vaults.
- Use JIT methods for dynamic NHIs.
- Implement strong decommissioning and recertification.

## Discovery and inventory

- Identify NHIs across IdPs, SaaS, and hybrid-cloud.
- Scan source code and file systems for hard-coded credentials.
- Build a comprehensive, centralised inventory.

## Classification

- Assign ownership and assess permission levels.
- Evaluate breadth of access to prioritise remediation.

## Posture management

- Eliminate excessive permissions (Least Privilege).
- Remove inactive/shared accounts to prevent lateral movement.

Source: KPMG Analysis; Non-Human Identity Management Group [URL]

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Core NHI vulnerabilities and mitigation strategies

## Inadequate inventory and visibility

Shadow NHIs are underestimated risks. Organisations run thousands of service accounts, bots, and integrations, many of which are never tracked or reviewed. These identities accumulate over time and lead to massive breaches.

**Mitigation strategies**

- Implement a formal 'Machine JML' lifecycle, requiring approved ITSM tickets and assigned human owners for token creation (Joiner), continuous right-sizing access scopes (Mover), and automating revocation if the human owner leaves the company or fails to re-certify the NHI (Leaver).
- Use Identity Threat Detection and Response (ITDR) tools to detect anomalies.
- Integrate AI agent orchestration platforms with your central NHI inventory to automatically register and track any ephemeral sub-identities created during agent operations.

## Third-party integrations

Third party tools such as Slack and GitHub introduce their own NHIs, OAuth tokens, and webhooks, most of which are never reviewed after initial setup.

**Mitigation strategies**

- Use SaaS Security Posture management (SSPM) to monitor SaaS-to-SaaS integrations.
- Periodically rotate secrets and restrict scopes.
- Isolate third party NHIs in segmented environments with strict scope controls.
- Ensure code repositories are private and access restricted.

## Secrets sprawl is out of control

Security breaches often involve exposed secret keys, API tokens and credentials due to weak controls and monitoring. Increase in use of cloud-native architectures, CI/CD, containers and growing automation result in amplified secret sprawls.

**Mitigation strategies**

- Transition to secret-less architectures via use of Identity Federation (e.g., AWS IAM Roles, Azure Managed Identities) to natively integrate identities and eliminate the need for static credentials.
- Implement centralised secrets vaults.
- Integrate JIT access for NHIs.
- Regularly scan for secrets in CI/CD pipelines, repositories, and across cloud environments.
- Use short-lived credentials with automatic expiration and revocation policies.

## Overprivileged NHIs

NHIs operate with excessive privileges due to misconfigured IAM roles, shared service accounts with elevated rights, and an absence of role scoping and privilege boundaries.

**Mitigation strategies**

- Apply least privilege by default and escalate only on-demand.
- Audit NHI access scopes regularly.
- Ensure all sensitive data is encrypted at rest and in transit.
- Enforce strict role-based access control.
- Implement identity-aware output filtering, i.e., require agents to verify the requesting user's specific permissions before sharing any data retrieved via the agent's backend NHI credentials.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Core NHI vulnerabilities and mitigation strategies (cont.)

## Environment segregation

Breached environments fail to maintain strict separation across development, test, staging, and production, enabling lateral movement for attackers.

**Mitigation strategies**

- Implement strong boundary controls between environments.
- Use dedicated NHIs per environment.
- Enforce environment specific secrets vaults and audit trails.
- Monitor for cross environment activity, especially lateral movement indicators.
- Strictly segment AI agent identities into 'Identity Isolation Zones' to prevent them from cross-communicating with unrelated production environments or sensitive data stores (Model-Level Isolation).

## Cloud misconfigurations

Over permissioned IAM roles and long-lived secrets expose cloud platforms to persistence and unauthorised control.

**Mitigation strategies**

- Use Cloud Infrastructure Entitlement management (CIEM) to enforce least privilege and detect privilege creep.
- Enforce key rotation and expiration policies.
- Mandate MFA across all cloud accounts.
- Monitor cloud audit logs for anomalies like privilege escalation and cross region activity.

## Incident response and blast radius

Unlike a human identity breach, abruptly revoking a compromised machine identity during an attack can cause cascading outages across critical production services and payment gateways

**Mitigation strategies**

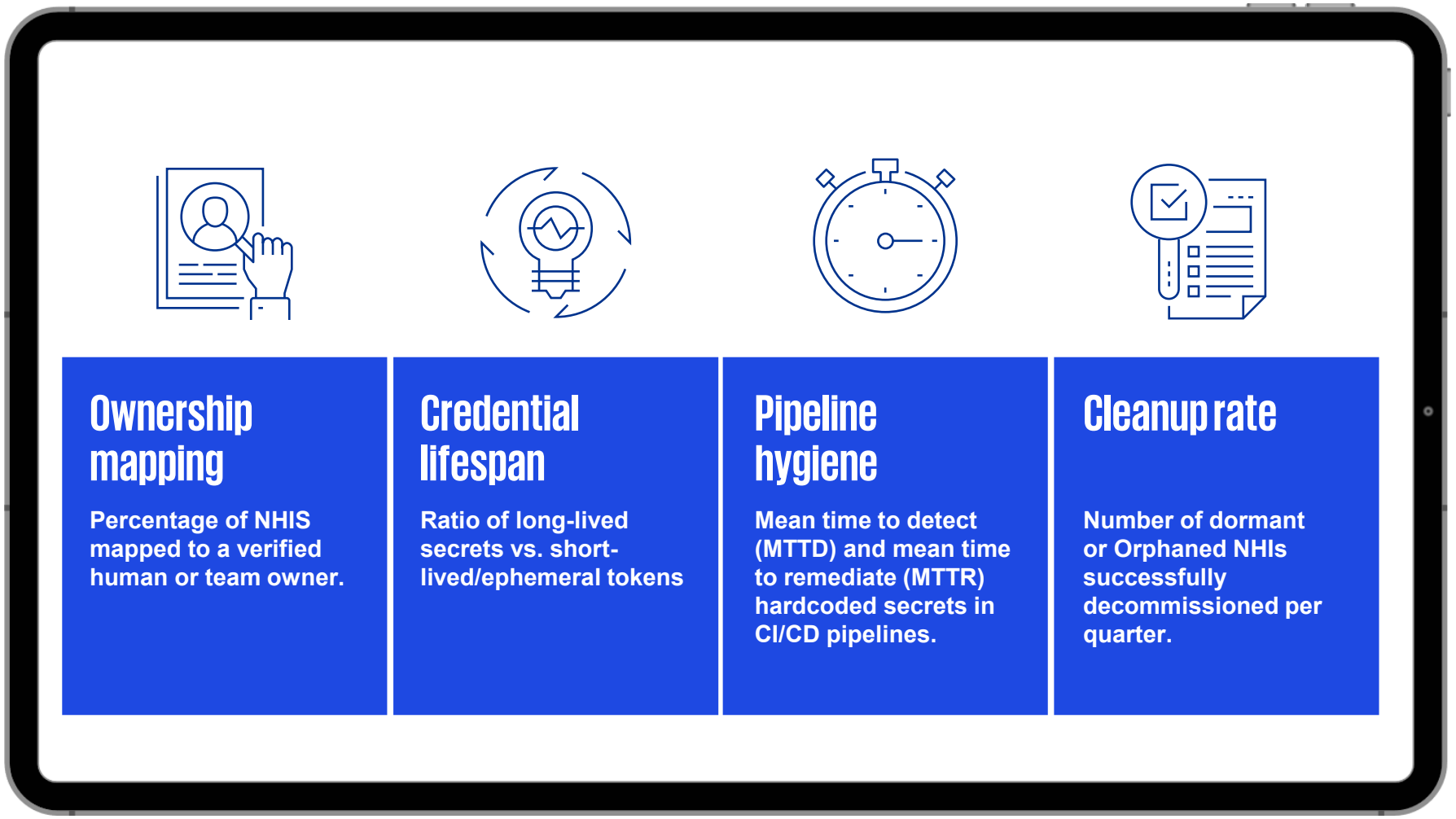
- Define NHI-specific response play books.
- Map NHI dependencies and blast radius.
- Test revocation in non-production environments.
- Enable controlled and staged response actions.




© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Measuring NHI maturity – Key KPIs

**Organisations should track specific machine identity metrics to measure effectiveness of NHI mitigation effort.**




© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# NHI Vendor landscape & capability benchmark

07

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Vendor Landscape

**Given the wide variation in Non-Human Identity types, a single solution is insufficient to address all associated risks. As a result, IAM vendors are rapidly extending their offerings to cover critical NHI use cases. Below is a view of the current vendor landscape.**



## Saviynt Identity Cloud

**Core focus:** Converged Identity Security and IGA: Extends unified governance to all NHIs, providing real-time discovery, ownership mapping, and risk-based controls for service accounts, bots, workloads, and AI agents.

**Ideal client use case:** Organisations wanting to centrally govern rapidly growing machine identities – especially in cloud, DevOps, and AI-driven environments—through a single identity security platform.

## SailPoint (Machine identity security)

**Core focus:** Governance and IGA: Extends human identity governance to machines. Excels at tying NHIs to human owners and running certification/recertification campaigns.

**Ideal client use case:** Organisations looking to extend existing enterprise identity governance to service accounts and bots.

## IDIRA[(a)] (Secrets management)

**Core focus:** Identity security platform with ZSP, JIT access, secrets management, session control, and AI identity security capabilities

**Ideal Client Use Case:** Enterprises requiring centralised control of privileged, machine, and AI identities across cloud, infrastructure, pipelines, and hybrid environments

## Entro Security[(b)]

**Core focus:** End-to-End NHI Lifecycle: NHI discovery, automated mapping to human owners, and real-time Non-Human Identity Detection and Response (NHIDR).

**Ideal client use case:** Cloud-native organisations struggling with shadow identities and needing lifecycle orchestration across. hybrid environments.

## Oasis Security

**Core focus:** Context-Aware Posture: Auto-discovers NHIs, analyses permissions to enforce least privilege, and automates remediation without breaking applications.

**Ideal client use case:** Enterprises with massive scale seeking to clean up legacy credentials and enforce Zero Standing Privileges.

## Astrix Security[(c)]

**Core focus:** App-to-App/AI Access: Specialised in securing third-party integrations (OAuth, API keys) and providing an "AI Agent Control Plane" to govern autonomous agents.

**Ideal client use case:** Organisations heavily utilising SaaS integrations, third-party marketplaces, and Agentic AI tools.

## GitGuardian

**Core focus:** Code and Supply Chain Security: Real-time secret detection; identifies hard-coded credentials in developer environments, GitHub, and CI/CD logs.

**Ideal client use case:** devsecops teams looking to shift-left and stop developers from pushing hard-coded secrets into production.

Note: (a) IDIRA acquired by Palo Alto Networks; (b) Entro has been acquired by SailPoint, (c) Astrix is now part of Cisco
Source: KPMG Analysis

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Vendor capability benchmarking

**There is no "one-size-fits-all" solution - each vendor addresses different parts of the NHI problem space.**

| Vendor and product | Governance and accountability | Lifecycle management | Secrets management | Least privilege /zero trust |
|---|---|---|---|---|
| **SailPoint**<br>Machine Identity Security | Ties machine identities to owners via IGA workflows; extends human governance policies to machines. | Automates provisioning and certification reviews for bots/service accounts. | Integrates with vaults but is primarily an IGA tool, not a vault itself. | Removes unused access through Certification campaigns and offers limited real-time enforcement. |
| **IDIRA**<br>Machine Identity Security | Centralised policy enforcement for privileged access; strong on defining safe access paths. | Comprehensive rotation and management of secrets; automates onboarding of privileged accounts. | **Leader.** Core strength in Conjur for securing, rotating, and managing secrets. | Specialised "JIT" access for cloud and on-prem; enforces zero standing privileges. |
| **GitGuardian**<br>NHI Security | Focuses on developer workflow; identifies who committed a secret (git blame) to assign ownership. | Primarily focuses on detection and remediation (rotation) of leaked secrets, not full lifecycle. | **Specialist.** Detects hard-coded secrets in code/logs; facilitates rotation but does not store them. | Not a primary feature (focus is on code security). |
| **Entro**<br>Security for NHIs | **Strong.** Auto-discovers NHIs and maps them to human owners/teams for accountability | Automates creation, rotation, and decommissioning of NHIs and secrets End-to-End. | **Agnostic.** Integrates with existing vaults (Hashi, AWS KMS) to enforce usage policies and rotation. | Analyses permissions to recommend rightsizing and removing over-privileged access. |
| **Oasis**<br>NHI Security Cloud | **Strong.** "Context-aware" governance that maps every identity to an owner and application. | End-to-End. Automates the full lifecycle (provision to retire) across hybrid cloud. | **Agnostic.** Manages secrets across various vaults; focuses on secret hygiene and rotation. | Continuously assesses privileges to enforce least privilege and detect drift. |
| **Astrix**<br>Security platform | **Strong.** Automated ownership assignment for tokens and keys based on behavioural usage. | End-to-End. Manages lifecycle for API keys, OAuth tokens, and service accounts. | **Agnostic.** Focuses on securing the access provided by secrets (tokens) rather than just storage. | Identifies over-privileged service accounts and unused tokens for reduction. |
| **Saviynt**<br>Identity Cloud | Unified governance for all NHIs with ownership mapping and risk-based controls. | Automatic NHI discovery, lifecycle tracking, and continuous posture assessment with AI-guided remediation. | Integrates with cloud-security partners (e.g., Wiz) to enrich credential-related risk but is not a vault. | Risk-driven access evaluation and anomaly detection to surface over-privileged NHIs. |

Note: IDIRA acquired by Palo Alto Networks; Entro has been acquired by SailPoint, Astrix is now part of Cisco
Source: KPMG Analysis

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Vendor capability benchmarking (cont.)

**There is no "one-size-fits-all" solution - each vendor addresses different parts of the NHI problem space.**

| Vendor and product | Monitoring | Cloud-Native/ AI-Ready | Automation |
|---|---|---|---|
| **SailPoint**<br>Machine Identity Security | Limited to governance data (who has what access); relies on integrations for behavioural analytics. | Evolving coverage for cloud workloads; strong on traditional enterprise apps. | **Lifecycle and discovery.** Automates discovery to expose blind spots and runs certification campaigns to validate machine access. |
| **IDIRA**<br>Machine Identity Security | Strong monitoring of privileged sessions and credential usage patterns. | Strong cloud portfolio; securing workloads and automated pipelines. | **Policy-Driven.** Scalable automation for rotation, certificate management, and securing workload identities to increase efficiency. |
| **GitGuardian**<br>NHI Security | Real-time alerting on secret leakage in public/private repos and CI/CD pipelines | Heavy focus on software supply chain, DevOps, and protecting codebases. | **Remediation and detection.** Automated workflows to detect secrets in code and trigger remediation (alerting devs, revoking keys). |
| **Entro**<br>Security for NHIs | **Real-time detection of anomalous NHI behaviour and active threats through NHIDR Engine.** | High AI-readiness, with specific focus on protecting AI agents and secrets in modern stacks. | **Context-Aware remediation.** Automates secret rotation and response to anomalies (NHIDR) to fix misconfigurations without breaking apps. |
| **Oasis**<br>NHI Security Cloud | **Continuous monitoring for anomaly detection and misuse of machine credentials.** | High cloud-nativity with purpose-built for hybrid cloud and massive scale of cloud-native identities. | **Lifecycle orchestration.** Automates the entire NHI lifecycle (provisioning to decommissioning) and offers one-click remediation plans. |
| **Astrix**<br>Security platform | **Behaviour-based threat detection (ITDR)** specifically for app-to-app connections. | High AI-readiness, with specialised "AI Agent Control Plane" to secure autonomous agent access. | **Rotation and cleanup.** Automates key rotation and the removal of unused/stale tokens to reduce the attack surface. |
| **Saviynt**<br>Identity Cloud | Real-time inventory, activity timelines, and contextual insights; deeper behavioral analytics via integrations. | Strong support for cloud workloads, DevOps identities, and AI agents. | **Lifecycle & Discovery**. Automated NHI discovery, posture evaluation, and AI-driven remediation workflows. |

Note: IDIRA acquired by Palo Alto Networks; Entro has been acquired by SailPoint, Astrix is now part of Cisco
Source: KPMG Analysis

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# From risk to resilience: The KPMG approach to NHI management

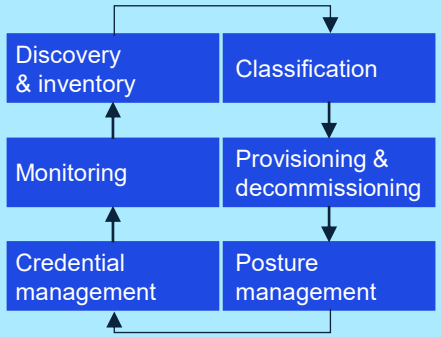
08

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

## KPMG's NHI Capability Offering

KPMG delivers Non-Human Identity (NHI) capabilities through a structured Target Operating Model (TOM), aligned to the NHI lifecycle and delivered through an authoritative service tier model.

All services, capabilities, and delivery artefacts are aligned to the KPMG NHI Target Operating Model (TOM), ensuring consistent governance, scalable implementation, and audit-ready outcomes across the full NHI lifecycle.




# Our capabilities

**Delivered through four service tiers aligned to the NHI Target Operating Model:**

### 1

### NHI discovery and maturity assessment

Establish visibility, baseline risk, and audit readiness across Non-Human Identities.

- **Discovery & assessment**
- **Secrets risk assessment**
- **Control mapping**
- **Regulatory readiness**

### 2

### Governance framework and operating model design

Define governance, lifecycle control, ownership, and workflows for Non-Human Identities.

- **Governance framework design**
- **Target operating model**
- **Ownership mapping**
- **Lifecycle (JML)**

### 3

### NHI transformation and implementation

Optimise credentials, enable secretless transformation, and reduce identity-related risk.

- **NHI operating model implementation**
- **Secrets platform implementation**
- **Workload identity & secretless**
- **Least privilege remediation**
- **DevSecOps automation**
- **Dynamic secrets migration**

### 4

### NHI monitoring and managed services

Monitor, detect, and operate NHI controls continuously across the lifecycle using ITDR and managed operations.

- **Monitoring & risk posture**
- **Secrets & certificate lifecycle**
- **Continuous compliance**

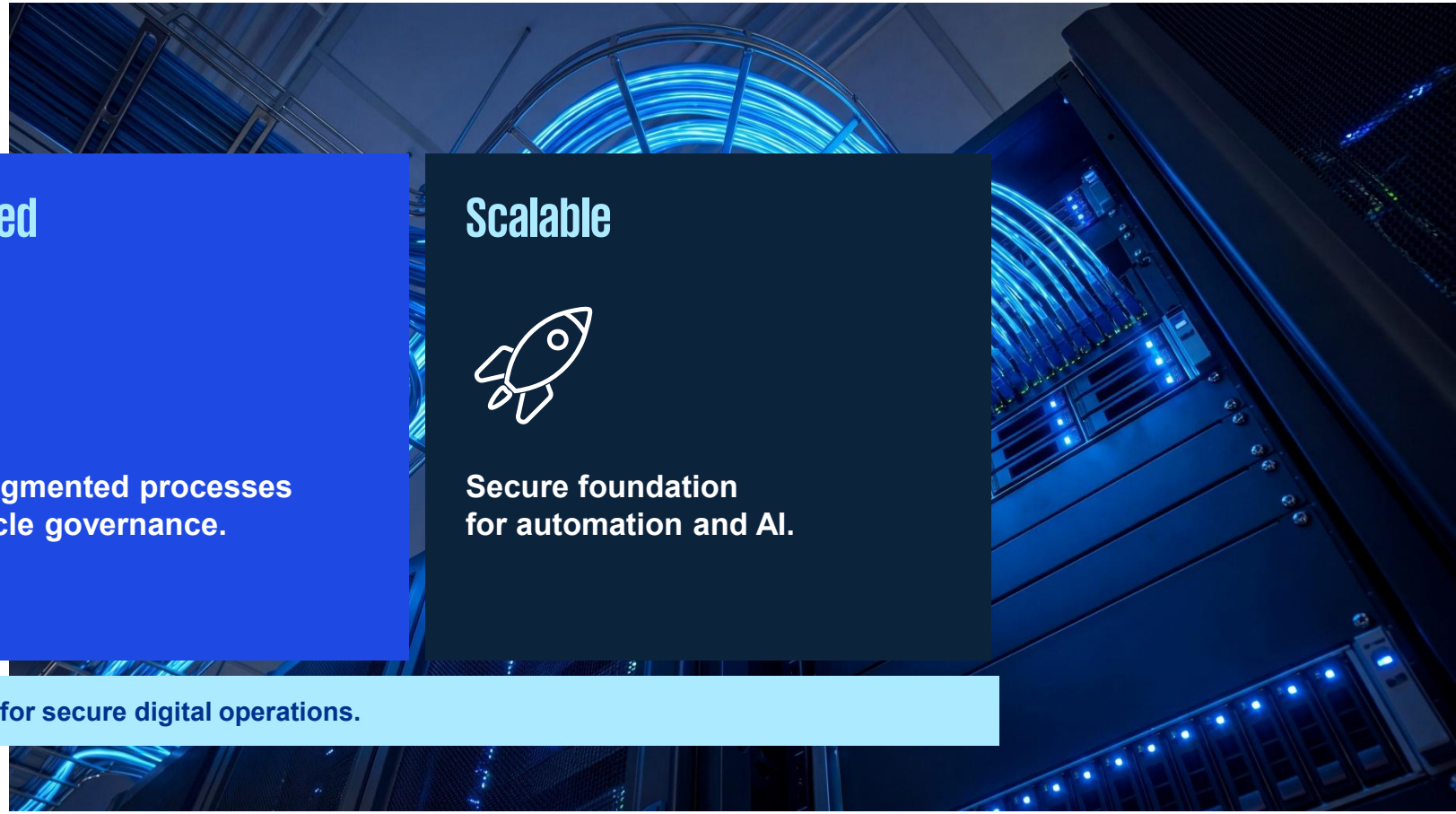
**KPMG transforms NHI risk into a secure business enabler through a multi-disciplinary approach, combining deep technical integrations with industry-leading vendor platforms, robust regulatory mapping, and strategic governance design.**

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Conclusion

## Expanding digital attack surface



### Unmanaged

Expanding, ungoverned NHI attack surface.

### Governed

From fragmented processes to lifecycle governance.

### Scalable

Secure foundation for automation and AI.

**NHI governance is no longer optional – it is a prerequisite for secure digital operations.**

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Why KPMG?

## What we offer:

**End-to-end Non-Human Identity (NHI) capabilities delivered through a lifecycle-aligned Target Operating Model (TOM).**

## How we do it:

**Combination of deep IAM expertise and business integration to move organisations from fragmented → governed → automated.**

## Our goal:

**Secure, scalable NHI ecosystem aligned to regulatory and operational requirements.**

**Serena Tejani**
Partner,
KPMG LLP Canada
E: serenatejani@kpmg.ca

**Kalpana Iyer**
Director,
KPMG UK
E: kalpana.iyer@kpmg.co.uk

**Harriet Burwood**
Senior Manager,
KPMG UK
E: harriet.burwood@kpmg.co.uk

**Pascal Fernandez Gomez**
Manager,
KPMG Germany
E: pfernandezgomez@kpmg.com

**Nail Baycan**
Assistant Manager,
KPMG Germany
E: nbaycan@kpmg.com

**Niall Donnelly**
Senior Consultant,
KPMG Ireland
E: niall.donnelly@kpmg.ie

**Daniel Garcia Suarez**
Specialist,
KPMG S.A. Spain
E: dgarcia14@kpmg.es

**Shreyash Pathak**
Manager,
KPMG LLP
E: shreyashpathak@kpmg.com

**To learn of any of our other IAM and Cyber offerings, get in touch.**
**Other related offerings: Identity Proofing | Deepfake Detection | CIAM | Workforce IAM | Zero Trust.**

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Case studies:
# Notable NHI related incidents

09

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Okta support system breach (2023)

## Why this breach matters for NHIs?

**Service account proliferation**

Modern SaaS systems rely heavily on non-human support and backend accounts.

**Token-based authentication**

Session tokens replace passwords and bypass MFA if compromised.

**Logging and monitoring gaps**

Sensitive credentials often stored in logs and support artifacts.

### Key application areas

- Identity providers (IdP).
- Customer support systems.
- API authentication flows.

## Where NHI controls broke down

**Weak service account governance**

Compromised non-human support account enabled attackers to access sensitive backend systems without sufficient restrictions.

**Exposure of authentication tokens in logs**

Session tokens stored in support logs created reusable credentials that bypassed MFA protections.

**Persistent and reusable credentials**

Tokens remained valid and could be replayed to maintain unauthorised access across downstream systems.

**Insufficient visibility into NHI activity**

Limited monitoring of service account behavior delayed detection and containment.

## Incident

Attackers accessed Okta's support system via a compromised service account, retrieving session tokens from HAR logs and enabling session hijacking across customer environments.

**NHI failure**

Weak governance over service accounts and authentication tokens.

**Business impact**

Potential exposure affecting 18,000+ enterprise customers, undermining trust in critical identity infrastructure.

**NHI failure pattern**

- Poorly managed service account (non-human identity).
- Sensitive artifacts (tokens) exposed via logs.
- Tokens used to bypass MFA entirely.

**Timeline:**

- Sept 28, 2023 → initial compromise begins.
- Oct 13, 2023 → suspicious activity discovered.
- Oct 19, 2023 → public disclosure by Okta.

**Links:**

- Okta Security Article – Okta's Support Case Management System Root Cause.
- The Hackernews – Okta's Support System Breach.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Microsoft storm-0558 token theft (2023)

## Why this breach matters for NHIs?

**Identity trust as foundation**

Cloud ecosystems rely on cryptographic keys to validate identity.

**Machine-issued authentication**

Tokens are generated and validated entirely without human interaction.

**Centralised identity infrastructure**

Compromise affects multiple tenants and environments.

### Key application areas

- Cloud identity providers.
- Enterprise email systems.
- API authentication and token validation.

## Where NHI controls broke down

**Compromise of identity signing keys**

Critical machine identity used to validate authentication tokens was exposed, enabling identity forgery.

**Breakdown of trust in authentication layer**

Systems inherently trusted forged tokens, allowing unauthorised access without triggering traditional controls.

**Cross-tenant identity exposure**

Centralised identity infrastructure increased the impact across multiple organisations and environments.

**Limited detection of token misuse**

Lack of deep inspection into token usage delayed identification of malicious activity.

## Incident

Attackers obtained a Microsoft signing key and used it to forge authentication tokens, enabling unauthorised access to enterprise and government email systems.

**NHI failure**

Compromised identity trust layer (machine signing keys) enabling token forgery.

**Business impact**

~60,000 sensitive emails accessed, including U.S. government accounts, triggering major regulatory scrutiny and investigations.

**NHI failure pattern**

- Long-lived signing key (machine identity) not properly secured.
- Token validation flaw allowed cross-boundary abuse.
- Represents “orphaned / uncontrolled NHI” at hyperscaler level.

**Timeline:**

- May 15, 2023 → attack activity begins.
- June 16, 2023 → detected via customer logging.
- July 11, 2023 → publicly disclosed by Microsoft.

**Links:**

- Microsoft – Analysis of Storm-0558.
- West Oahu Hawaii News – Storm-0558 Forensic Analysis.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Glossary

10

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Glossary

| Abbreviation | Definition | Context |
|---|---|---|
| **AI** | Artificial intelligence | Refers specifically to "Agentic AI" in the text – autonomous systems capable of executing complex tasks and attack lifecycles without human oversight. |
| **API** | Application programming interface | A set of rules allowing different software entities to communicate. APIs often require specific credentials – like keys or tokens – which are a common form of Non-Human Identity. |
| **AWS** | Amazon web services | A leading cloud service provider. NHIs such as IAM roles and access keys are fundamental to AWS security. |
| **CI/CD** | Continuous integration / continuous deployment | Automated pipelines used by DevOps teams to build, test, and deploy software. A major source of "shadow" NHIs. |
| **DevOps** | Development and operations | A methodology combining software development and IT operations. DevOps automation is a primary cause for NHIs outnumbering human identities. |
| **DORA** | Digital Operational Resilience Act | An EU regulation mandating that financial entities manage ICT risks, including the security of machine identities. |
| **EU Data Act** | European Data Act | Regulation creating a fair and innovative data economy, focusing on access to and use of data generated by connected products. |
| **GDPR** | General data protection regulation | European Union regulation that governs how personal data is processed, protected, and accessed. |
| **HIPAA** | Health Insurance Portability and Accountability Act | U.S. federal law that governs the protection, privacy, and security of health information, specifically electronic Protected Health Information (ePHI). |
| **IAM** | Identity and access management | The framework of policies and technologies for ensuring the right users (and machines) have the right access to the right resources at the right time. |
| **IaC** | Infrastructure as Code | The management and provisioning of computing infrastructure through machine-readable definition files (code) rather than manual processes. IaC tools (like Terraform or Ansible) rely on powerful NHIs to automatically deploy and modify cloud environments, making them a critical security focus. |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Glossary (cont.)

| Abbreviation | Definition | Context |
|---|---|---|
| **ICT** | Information and communication technology | An umbrella term for all technologies used to manage telecommunications and broadcast media. Used in DORA. |
| **IGA** | Identity governance and administration | The policy-based management of digital identities and access rights, typically focused on compliance and lifecycle. |
| **IoT** | Internet of Things | Physical devices (sensors, cameras, smart appliances) that connect to the internet and require machine identities. |
| **ISO 27001** | International Organisation for Standardisation 27001 | The leading international standard for information security management systems (ISMS). |
| **IT** | Information technology | The use of systems (computers, storage, networking) to process and manage data. |
| **ITDR** | Identity threat detection and response | A security discipline focused on detecting and reacting to credential theft and privilege misuse in real-time. |
| **JIT** | Just-In-Time (Access) | A security practice where access is granted only for the specific time it is needed, reducing the risk of standing privileges. |
| **JWT** | JSON Web token | A compact, URL-safe means of representing claims to be transferred between two parties, commonly used for API authentication. |
| **MFA** | Multi-factor authentication | A security system requiring more than one method of authentication. Notably, NHIs typically cannot use MFA, making them a prime target of attack. |
| **NIS 2** | Network and information security (directive 2) | EU legislation on cybersecurity that provides legal measures to boost the overall level of cybersecurity in the EU. |
| **NHI** | Non-human identity | A digital identity used by a machine, service, or application (not a person) to authenticate and access resources. |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Glossary (cont.)

| Abbreviation | Definition | Context |
|---|---|---|
| **NIST** | National institute of standards and technology | U.S. federal agency within the U.S. Department of Commerce that develops standards, frameworks, and guidelines for security, technology, and risk management. |
| **NIST CSF** | NIST cybersecurity framework | A widely adopted voluntary framework in the US consisting of standards, guidelines, and best practices to manage cybersecurity risk. |
| **NIST SP** | NIST special publication | A series of authoritative technical guidelines and standards used widely in cybersecurity, risk management, and IT governance. |
| **OAuth** | Open authorisation | An open standard for access delegation, commonly used for token-based authentication (e.g., "Log in with Google"). |
| **OT** | Operational technology | Hardware and software used to monitor and control physical industrial machinery and processes (e.g., factory robots, power grids). |
| **OWASP** | Open worldwide application security project | A nonprofit foundation that works to improve the security of software. It is essentially the global standard-bearer for application security. |
| **PAM** | Privileged access management | Cybersecurity strategies and technologies for exerting control over elevated ("admin") access and permissions. |
| **PCI DSS** | Payment card industry data security standard | Information security standard for organisations that handle branded credit cards. |
| **PII** | Personally Identifiable Information | Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred. |
| **PHI** | Protected health information | A subset of PII, that includes any representation of health-related information that can be linked to an individual. |
| **PQC** | Post Quantum Cryptography | Refers to new cryptographic algorithms designed to secure digital data against future, highly powerful quantum computers |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# Glossary (cont.)

| Abbreviation | Definition | Context |
|---|---|---|
| **RBAC** | Role-based access control | A method of restricting access based on the roles of individual users or machines within an enterprise. |
| **RPA** | Robotic process automation | Software technology that makes it easy to build, deploy, and manage software robots that emulate human actions. |
| **S3** | Simple storage system | A scalable, high-speed, web-based cloud storage service designed for online backup and archiving of data and application programs. |
| **SaaS** | Software as a service | A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted by the vendor. |
| **SIEM** | Security information and event management | A solution that provides real-time analysis of security alerts generated by applications and network hardware. |
| **SOC 2** | System and organisation controls | Assurance report developed by the American Institute of Certified Public Accountants (AICPA) with controls related to security, availability, processing integrity, confidentiality, and privacy. |
| **SOX** | Sarbanes-Oxley Act | U.S. federal law enacted to strengthen corporate governance, financial transparency, and internal controls. |
| **PCI DSS** | Payment card industry data security standard | Information security standard for organisations that handle branded credit cards. |
| **SVID** | SPIFFE Verifiable Identity Document | The document used by a workload to prove its identity to a resource or another workload. |
| **VM** | Virtual Machine | An emulation of a computer system. VMs require their own identities to interact with the network and other resources. |

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.




© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Create | CRT168300A | June 2026

**Document Classification: KPMG Public**