

Securing the rise of non-human identities

How well do you know your new (non-human) coworkers?











The rise of agentic AI has turbocharged the prevalence of and dependence on Non-Human Identities (NHIs). While protocols like Model Context Protocol (MCP), agent-to-agent (A2A) interactions, and machine-to-machine (M2M) communication boost efficacy, this cross-boundary coordination creates a critical governance gap that demands organizations unify their identity security fabric to automate oversight across every identity, use case, and resource.

This infographic gives a brief overview of the roles and risks of NHIs. Read through to make sure you're not overlooking this critical new attack surface.

50:1

NHIs outnumber human identities by as much as.

CSO Online, "What are non-human identities and why do they matter?"

NHI type	Description	Potential controls	Associated OWASP categories
 Service Accounts	Used by apps or services to interact with other systems automatically.	 Minimize standing privileges Certify privileges. Enforce trust policies.	NHI1:2025 Improper Offboarding
 API keys and tokens	Provides secure, programmatic access between apps, services, or integrations.	 Zero long-lived credentials Automate credential rotation. Secure inter-app comms.	NHI5:2025 Overprivileged NHI
 Machine identities	Certificates or cryptographic keys used to authenticate VMs, containers, or devices.	 Unique, governed device trust Detect unmanaged accounts. Automate detail-rich audit trails.	NHI3:2025 Vulnerable Third-Party NHI
 Cloud workload identities	Auto-generated credentials for serverless functions and containerized workloads.	 Scoped, ephemeral access Vault secrets for high-impact tasks. Surface hidden risks.	NHI4:2025 Insecure Authentication
 Automation scripts and bots	Credentials accessed by scripts that execute CI/CD pipelines, infrastructure codes, or RPA tasks.	 Attested, time-boxed automation Automate access requests. Enforce accountability.	NHI7:2025 Long-Lived Secrets
			NHI9:2025 NHI Reuse
			NHI10:2025 Human Use of NHI

Data exfiltration risk

Imagine a scenario in which a trusted engineer leaves your organization. Their account is properly offboarded and permissions removed. But what about the many NHIs and automations they created while they were active? Now, let's say the credentials for one of these overlooked NHIs are accidentally shared in a public repository. It could become the perfect vehicle for data exfiltration—able to operate quickly, broadly, and perhaps evade detection for many days.

Below are a handful of attributes and examples of why NHIs are uniquely attractive to threat actors, any combination of which could be at play in a breach.







66%

of enterprises have experienced a successful cyber attack resulting from compromised NHIs.

Portnox, "Navigating the growing challenges of non-human identities in IT"

What attributes could be exploited?

Permissions	Authentication	Lifecycle	Governance
Overprivileged access 	Hardcoded credentials 	Improper offboarding 	Misuse by humans 
Often given to NHIs for convenience. Attackers can exploit these excessive permissions for lateral movement or to escalate an attack.	Secrets that do not expire pose a significant danger if compromised, as attackers can exploit them undetected for long durations, providing persistent access.	When offboarding a human, the NHIs they created or managed can become orphaned. Dormant accounts without oversight are at risk of being hijacked.	Developers sometimes use NHIs to manually access systems, bypassing the controls intended for human users and introducing monitoring blind spots.

What prevention methods could avert an incident?



Automatically deprovision all associated identities when personnel leave



Apply frameworks for preventing the use of hardcoded credentials



Discover evolved accounts and flag orphaned identities

Okta product key

The Okta Platform delivers comprehensive visibility into NHI security

Identity Security Posture Management

Provides continuous discovery and risk analysis of NHIs. It detects unmanaged accounts to curb sprawl, surface hidden risks, and guide effective threat remediation.

Okta Privileged Access

Helps secure NHI privileges by vaulting secrets like API keys and shared accounts. It automates credential rotation and enforces individual accountability.

Okta Identity Governance*

Provides automated access requests and periodic certification for NHIs and agent identities, establishing a comprehensive audit trail for every agent action and decision to help enable compliance with federal mandates.

Workflows

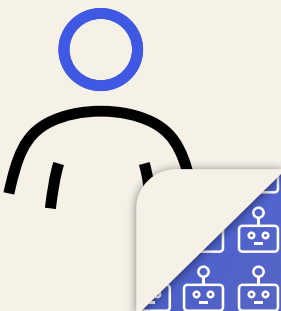
For public APIs, enables automated remediation and lifecycle actions for non-human identities, such as disabling users and orchestrating cross-system responses. It helps reduce manual effort and ensures consistent enforcement of security policies.

Get in touch or watch the on-demand webinar

Don't wait for a breach. Intervene now and keep NHIs working for you, not against you. You can talk to one of our experts or learn more in our NHI webinar by clicking on the links below.

→ Contact

→ Webinar



*This product feature is currently in development and not yet available for purchase. Feature specifications and release dates are subject to change without notice. Please refer to Okta's official product announcements for the most current information. To learn about the respective product milestones for our compliance offerings, please reference the [Okta US Public Sector resource page](#).