Omada

The Non-Human Identity Governance Gap

7 Security Control Questions Most Enterprises Struggle to Answer

Non-human identities (NHI) now represent the majority share of identities in enterprise environments. Service accounts. APIs. Automation scripts. Containers. Bots. AI agents.

They operate continuously. Many hold elevated access. Most were never designed to fit cleanly into workforce-centric governance models.

When ownership is unclear and lifecycle controls are inconsistent, identity exposure expands.

The questions below surface structural control gaps that directly affect exposure.

1. Can you produce a complete inventory of non-human identities?

Can you generate an authoritative inventory across cloud, on-premises, and SaaS environments without manual reconciliation?

If discovery is fragmented, blind spots exist.

2. Does every non-human identity or agent have a named accountable owner and a clear business purpose?

Each NHI should have a clearly assigned human owner responsible for purpose, access level, and lifecycle.

If ownership is shared, assumed, or undocumented, accountability gaps remain.

3. Are lifecycle controls enforced from creation to rotation to decommissioning?

Are NHIs approved before creation, assigned least privilege at inception, reviewed periodically, and automatically disabled when no longer required?

Persistence without review increases exposure.

4. Can you quantify privileged access held by non-human identities?

How many service accounts or automation identities hold administrative or elevated privileges?

Can each privilege be justified based on current function?

Unreviewed privilege accumulates risk.

Omada

5. Are non-human identities included in policy enforcement and segregation of duties?

Can you tell whether agents, automation identities, and other non-human identities act autonomously, through their own identity, or on behalf of a user?

NHIs should be evaluated against the same policy guardrails applied to workforce identities.

Exclusion creates silent control failures.

6. Do you monitor non-human identity behavior continuously?

Unusual access times, abnormal usage patterns, or unexpected privilege escalation from NHIs should trigger investigation as quickly as human anomalies.

Without monitoring, misuse persists undetected.

7. Can you isolate and revoke non-human identity access immediately across systems?

If a NHI is compromised, can you identify every connected system and suspend access centrally without delay?

Containment speed defines exposure impact.

Non-human identities are not peripheral to identity security. They are central to it.

As automation and AI expand, NHIs are scaling faster than the traditional governance models built to control them.

Balanced identity security governance requires unified visibility, enforced least privilege, clear ownership, and continuous control across both human and non-human identities.

If these questions are difficult to answer with precision, the exposure gap is measurable.