

NHI & AI Agent Security

NHIs & AI agents are transforming enterprise operations. Silverfort maps them to their human owners, assesses their risk and secures them at runtime, from one platform

Service accounts, cloud NHIs, and AI agents vastly outnumber your employees. Silverfort secures them **from AD to AI**, so business processes and innovation can keep scaling without expanding your attack surface. From a single control plane, Silverfort continuously discovers non-human and agentic identities, maps each one to the human who owns it, and remediates exposures. At runtime, **Virtual Fencing restricts AD service accounts inline**, **Geo-fencing limits where cloud NHIs can be used**, and **runtime policies control what AI agents can access and do**.

The challenge: More identities, less control

Identity security was built for people. Today, non-human identities, from legacy AD service accounts to API keys, OAuth tokens, cloud roles, and now AI agents, are multiplying faster than any team can govern. They're created ad hoc, spread across disconnected silos, and can't be protected with human-centric controls like MFA or traditional PAM.

- **Over-privileged by design:** NHIs and agents often hold excessive, long-lived permissions, which sets them up perfectly for credential abuse and lateral movement.
- **Fragmented visibility:** Identities are scattered across AD, IdPs, cloud, SaaS, and AI platforms, with no unified inventory, owner, or context.
- **Autonomy at machine speed:** Agents act independently, and stolen NHI credentials let attackers move at machine speed, with no human in the loop to stop them.
- **Alerts, not protection:** Legacy IAM and point NHI tools typically stop at visibility. They report risk after the fact instead of blocking it.

"94% of organizations are dealing with increased machine identities, largely driven by AI and AI agent deployments."

– Gartner, 2025 Machine Identity Management survey

From AD to AI: See, reduce, and stop non-human risk



See every identity, end to end
Discover every service account, cloud NHI, and AI agent across your environments. Trace each agent to the NHIs it runs on and the human who owns it, so you know what exists, what it can reach, and how it behaves.

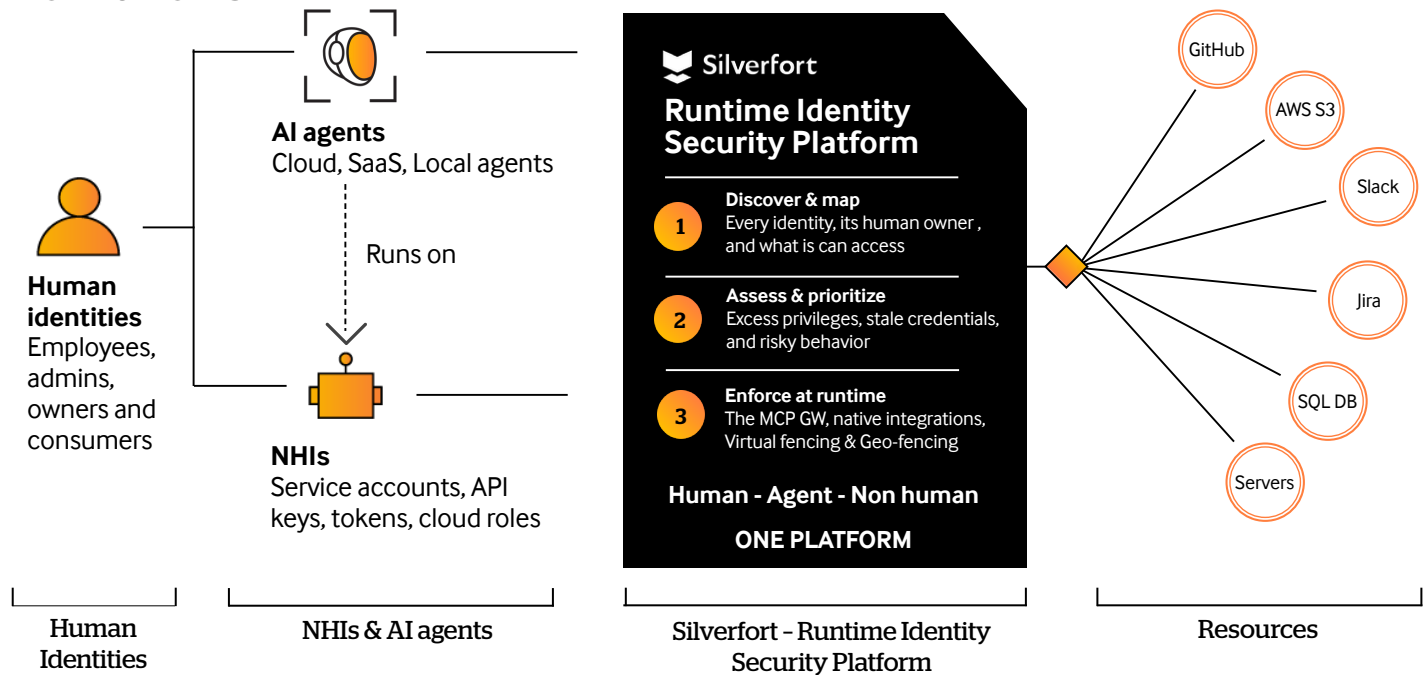


Fix the riskiest exposures first
Surface excess privileges, stale credentials, and risky behavior across every identity, ranked by impact. Then remediate with least-privilege policies recommended from each identity's observed behavior, so your team focuses where it matters.



Stop abuse at runtime
Lock AD service accounts to their approved sources and targets with Virtual Fencing, restrict cloud NHIs by location with Geo-fencing, and enforce runtime policies on every AI agent action. Block unauthorized access, lateral movement, and privilege escalation before damage is done.

How it works



Silverfort connects to a wide range of identity silos, including Active Directory, cloud identity providers, cloud infrastructure, SaaS applications, and AI platforms. It follows a three-step approach to unify visibility, prioritize risk, and enforce protection in real time, without modifying legacy systems or slowing developers down.

The full journey

Step 1 – Discover and map: Automatically identify every service account, cloud NHI, and AI agent across on-prem, cloud, SaaS, and agentic platforms. Map each to its human owner and related identities to establish full accountability and context.

Step 2 – Assess and prioritize risks: Analyze each identity's privileges, activity, and access paths to uncover excessive permissions, stale or exposed credentials, and anomalous behavior that may indicate misuse.

Step 3 – Enforce policies at runtime: Restrict non-human identities to only what they need, when they need it, and from where they should run, with Virtual Fencing for AD service accounts, geo-fencing policy automation for leading cloud platforms, and for AI agents via native integrations or the MCP Gateway.

Why Silverfort



End-to-end coverage:

Humans, machines, and AI agents, on-prem and cloud, in one platform rather than another point-solution.



Inline enforcement:

Stop attacks in real time, instead of getting more alerts to investigate.



Smart policies:

Learn your environment and NHIs legitimate behavior to scale remediation, apply protection and auto-generate policies for the scale of your business.



Proven at scale:

1,000+ customers secure their different identities with Silverfort.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.