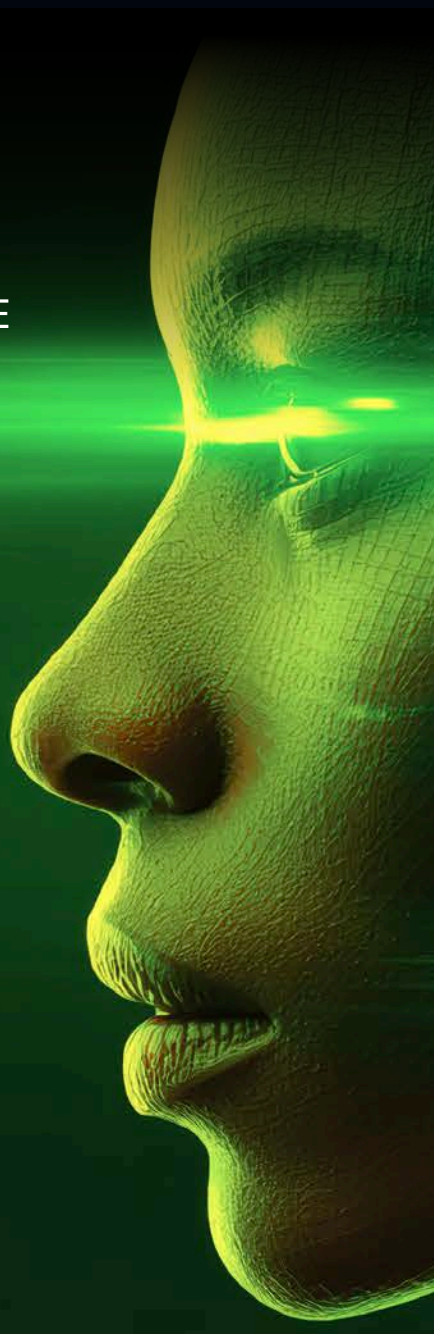
SECURING AGENTIC AI IDENTITIES

HOW SEKTOR AND SILVERFORT HELP
ANZ ORGANISATIONS GOVERN, CONTROL AND SECURE
AI-DRIVEN IDENTITIES AT SCALE.



www.sektorcyber.com

UNDERSTANDING THE IDENTITY RISKS BEHIND AGENTIC AI

Agentic AI is rapidly embedding itself into enterprise workflows across ANZ.

AI agents now write code, triage incidents, and orchestrate processes at machine speed.
But to operate, they authenticate, access systems, and interact with sensitive data — often with high privileges and minimal oversight.

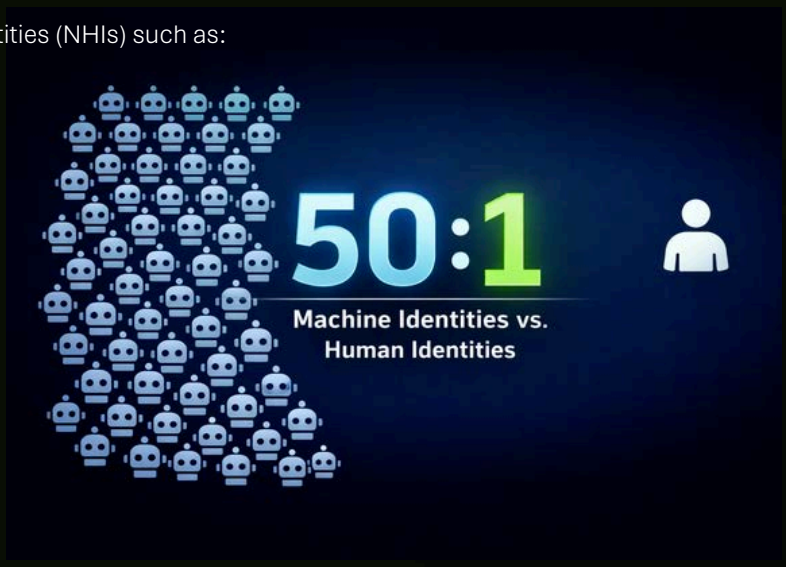
AGENTIC AI IS NOT JUST AN AUTOMATION CHALLENGE.
IT'S AN IDENTITY SECURITY PROBLEM.

THE NEW ATTACK SURFACE

AI Agents + Non-Human Identities = Expanding Risk

AI agents rely on a growing ecosystem of non-human identities (NHIs) such as:

- **Service accounts**
- **IAM roles & service principals**
- **API keys, tokens, certificates**
- **Cloud & SaaS identities**



Machine identities already outnumber humans 50 to 1 — and the gap is widening fast. Every AI agent, API, and automated workflow adds another identity with access to critical systems.

YOU CAN'T SECURE WHAT YOU CAN'T SEE

Without proper oversight, this explosion creates a powerful and largely invisible attack surface. If you don't have visibility, you can't answer:

- Which AI agents exist?
- What can they access?
- Who is accountable?

Traditional identity tools weren't designed for AI agents or NHIs.
This requires a new approach to identity security.

SILVERFORT: IDENTITY SECURITY FOR THE AI ERA

Silverfort connects via read-only APIs to identity providers, cloud platforms, and SaaS apps to automatically discover every AI agent — including shadow and rogue deployments — with no code changes required.

It also continuously maps all non-human identities across on-prem and cloud environments, including service accounts, IAM roles, API keys, tokens, and certificates.
Each identity is enriched with ownership, permissions, and risk context — transforming unmanaged machine accounts into fully governed assets.

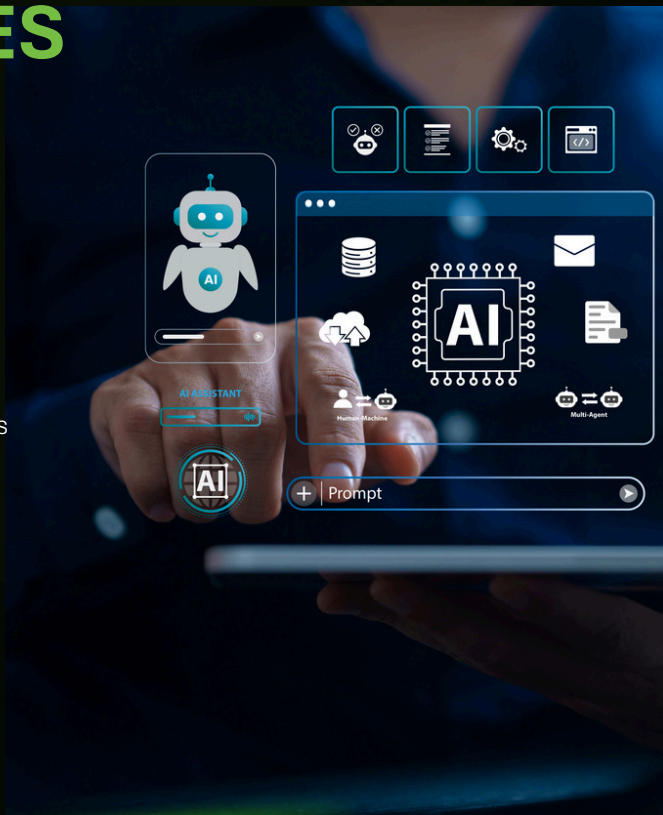
TURNING AI AGENTS INTO GOVERNED IDENTITIES

Silverfort links every AI agent to a human owner, ensuring full accountability for every action and closing the audit gap.

It then applies real-time, inline controls to:

- Enforce least privilege access
- Inspect and secure agent activity before it reaches systems
- Create a complete, tamper-proof audit trail

For non-human identities, Silverfort establishes behavioural baselines and applies “virtual fencing” to prevent misuse — stopping threats without disrupting automation.



WHY SEKTOR + SILVERFORT FOR ANZ

Sektor and Silverfort bring together local ANZ expertise and a leading identity security platform to help organisations take control of AI, human, and machine identities — all from a single, unified approach.

With Sektor and Silverfort, organisations gain:

Complete visibility

across human, non-human, and AI identities — on-prem and in the cloud

True control of AI agents

treated as governed identities, not black boxes

Robust protection

for the machine identities powering AI, DevOps, and automation

Agentic AI will keep accelerating. With Sektor and Silverfort, you can embrace that innovation while keeping every AI and machine identity in sight and under control.

www.sektorcyber.com

sektor Silverfort

Sources
Introducing AI Agent Security: Treat your AI agents as identities for accountability, inline protection, and accelerated innovation | Silverfort
Non-Human Identity Security | Silverfort
What is a Non-Human Identity? | Silverfort Glossary
Silverfort expands its Non-Human Identity (NHI) Security offering to the cloud for end-to-end identity security | Silverfort
AI Agent Security | Silverfort
NHI High Level Requirement Catalogue - vendor copy
Silverfort AI Agent Security | Silverfort
Silverfort unveils AI Agent Security to protect agentic identities, securing MCP deployments with inline, dynamic security controls | Silverfort
Silverfort expands its Non-Human Identity (NHI) Security offering to the cloud for end-to-end identity security | Silverfort
Silverfort Identity Security Platform | silverfort.com
Cloud Non-Human Identity (NHI) Security | Silverfort