

Decoding AI agents in the workplace

The rise of digital labor

AI agents are rapidly becoming part of the enterprise workforce. From processing invoices to managing infrastructure, AI agents are already executing real business tasks and their role is expanding fast.



45B+

Non human identities worldwide¹



40:1

Machine identities vs. human identities in many enterprises²



15%

Of daily work decisions may be made by AI agents by 2028³

Security was built for humans

Most enterprise security frameworks assume:



Stable identities



Predictable behavior



Clearly defined roles

AI agents challenge these assumptions. They operate at machine speed, scale dynamically and can execute thousands of tasks autonomously. This creates a fundamental question for enterprises.

What exactly is an AI agent in the enterprise – a tool or a worker?

The two emerging identity models

The Marionette

The AI agent acts on behalf of its human creator, inheriting that user's permissions.



Advantages:

- Easy to implement
- Compatible with existing IAM systems
- Clear human accountability

Challenges:

- Inherits all user permissions
- Creates over privileged automation
- Access may persist even if the user leaves

The Ghost

The AI agent is treated as a governed digital identity with its own permissions.



Advantages:

- Least privilege access
- Central governance and oversight
- Fully auditable activity

Challenges:

- Identity sprawl
- Lifecycle management complexity
- New accountability considerations

Creating identity at machine scale

If AI agents become digital workers, enterprises must manage them like a workforce. In cloud native environments, machine identities can outnumber humans by thousands to one.

Security teams must now handle:



Agent provisioning and deprovisioning



Continuous access reviews



Identity lifecycle governance

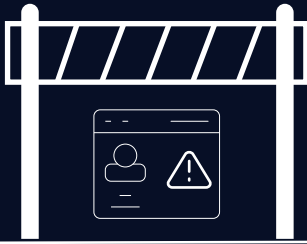


Monitoring agent behavior

Identity has moved beyond users to ecosystems. Security exposure is expanding rapidly.

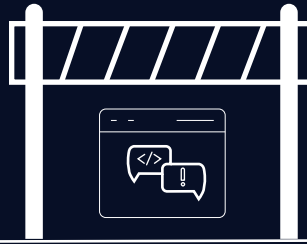
New enterprise attacks surface

AI agents introduce new attack surfaces and security risks.



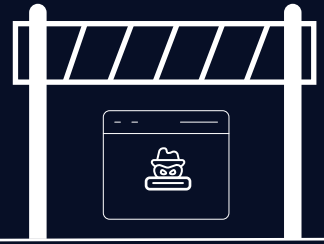
Credential hijacking

Compromised identities enable machine speed access.



Prompt injection

Malicious inputs manipulate agent behavior.



Agent swarm risks

Compromised agents can influence others and cascade failures.

Securing the digital workforce

Enterprises must evolve their security architecture to manage digital workers.

Identity based governance

Treat every AI agent as a unique identity.



Just in time access

Grant permissions only when needed for specific tasks.



Reasoning transparency

Audit not just what an agent did, but why it made that decision.

Human in the loop oversight

Maintain checkpoints for high impact decisions.



Driving trust at machine speed

Human security teams alone cannot monitor thousands of agents executing millions of actions. The solution? Agentic security operations. Specialized security agents can:

Detect swarm risks

Manage
permissions
automatically

Simulate attacks

Respond
to threats
in real time

Notably, organizations implementing AI-driven security operations have seen faster incident response times.

As AI agents scale, governance becomes critical.
Security must evolve to keep pace.

To know more, explore our latest
whitepaper “Marionette and ghost?
When AI agents join you in the workplace”.

Download

References

1. World Economic Forum. [Unsecured AI Agents Expose Businesses to New Cyberthreats](#). World Economic Forum. September 2025.
2. CyberArk. [AI Surge Drives a 40-1 Ratio of Machine to Human Identities](#). CyberArk.
3. Gartner. [Gartner Predicts Over 40 Percent of Agentic AI Projects Will Be Canceled by End of 2027](#) Gartner Press Release. June 25, 2025.

Visit nttdata.com to learn more.

NTT DATA is a \$30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.

