BeyondID

AI AGENTS: THE NEW INSIDER THREAT?

Why non-human identities are poised to replace humans as the top cybersecurity vulnerability.

EXECUTIVE SUMMARY

AI is reshaping enterprise operations, and with it, the identity landscape. As organizations embed AI agents across workflows, a new class of security risk is emerging. These agents increasingly interact with systems, data, and users in ways that mirror human behavior, yet most identity and access management practices haven't evolved to match.

This report explores how non-human identities are creating blind spots in enterprise security strategies, why current frameworks fall short, and what steps organizations must take to mitigate this growing risk. A dedicated spotlight on the healthcare sector highlights how rapid AI adoption without corresponding identity controls can amplify exposure.

KEY FINDINGS

AI is acting like a user. Security teams aren't treating it like one.

AI agents are performing tasks once limited to humans (logging in, accessing sensitive systems, and triggering actions), yet most security teams still treat them like static infrastructure. This disconnect creates serious risk: without the right identity governance, AI can operate unchecked with elevated access.

Confidence is high, controls are weak.

Over 50% use AI to detect threats, but fewer apply access monitoring to AI systems themselves, service accounts and bots are often over-permissioned and persist beyond their intended use, and behavioral monitoring is rarely extended to non-human actors. This overconfidence spells big problems for IT professionals.

AI threats are identity threats.

AI impersonation of users is the top concern for 37% of security leaders, followed by worries about AI-powered credential stuffing (15%) and deepfake-based social engineering (15%). Despite these risks, only 6% rank securing non-human identities as their most difficult challenge.

Only **30%** of organizations regularly map non-human identities like AI agents to critical assets.

Of organizations say that they're ready for AI in security, but far fewer are actively managing the risks.

Securing non-human identities ranks among the **top 5 hardest challenges** in cybersecurity today.

BeyondID

ZOOMING IN ON THE HEALTHCARE INDUSTRY

A Sector at the Forefront of AI and Under Pressure to Keep Up

Healthcare is among the fastest adopters of AI, integrating it into diagnostics, scheduling, and patient engagement. But its identity practices haven't kept pace.

AI agents are now handling Protected Health Information (PHI), accessing medical systems, and interacting with third parties often without strong oversight.

61%

Of healthcare organizations reported at least one identity-related attack (above average).

42%

Failed an identity-related compliance audit.

17%

List compliance as a top concern (a surprisingly low share).

23%

Offer passwordless authentication (well below other sectors).

34%

Name AI impersonation of users as the top emerging threat.

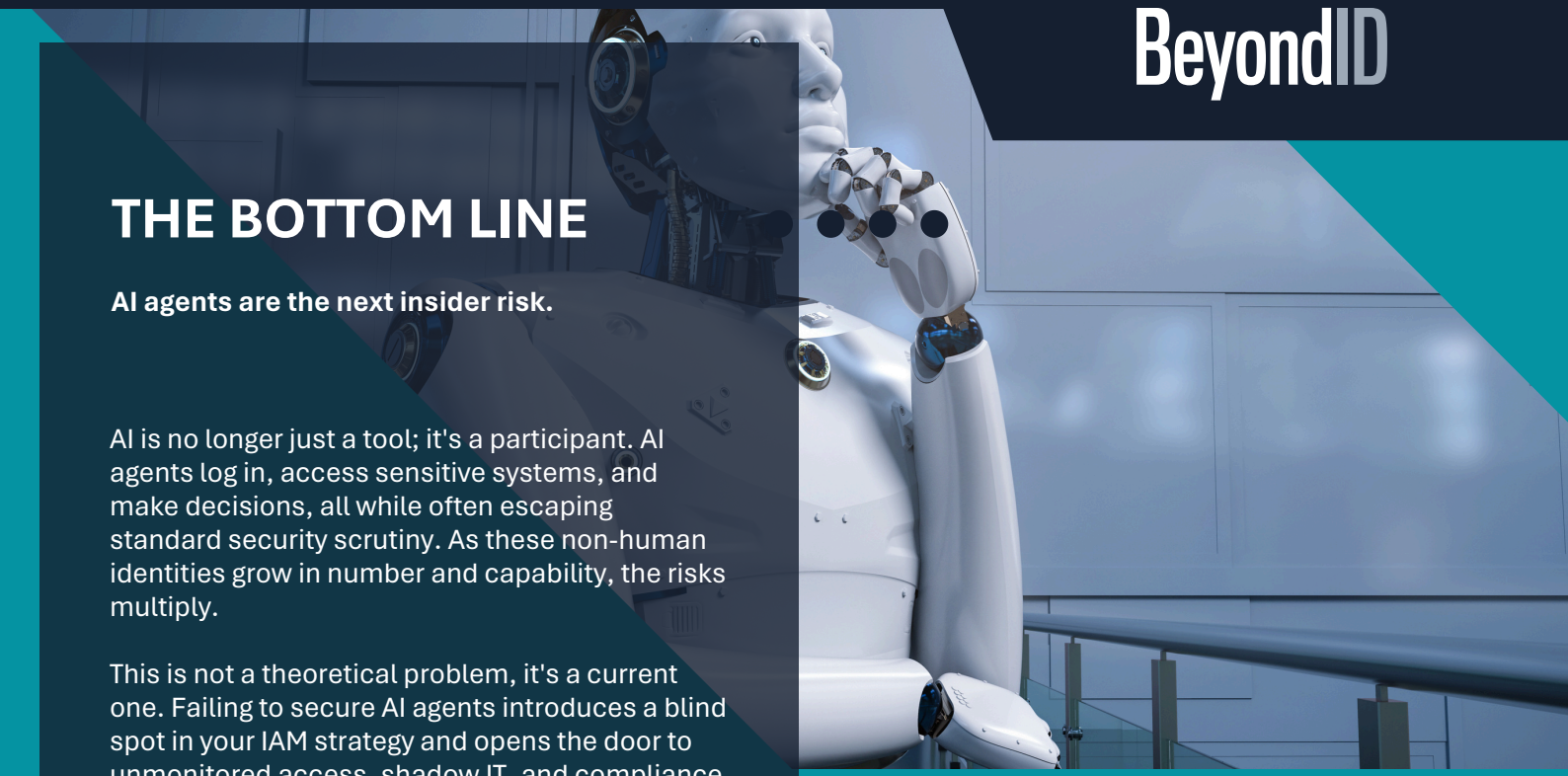
25%

Are concerned about automated discovery of identity misconfigurations.

ANALYSIS

These numbers reveal a troubling pattern: healthcare is moving fast on AI, but lagging on identity maturity. In a sector where privacy and uptime are paramount, these gaps introduce systemic risk.

BeyondID



THE BOTTOM LINE

AI agents are the next insider risk.

AI is no longer just a tool; it's a participant. AI agents log in, access sensitive systems, and make decisions, all while often escaping standard security scrutiny. As these non-human identities grow in number and capability, the risks multiply.

This is not a theoretical problem, it's a current one. Failing to secure AI agents introduces a blind spot in your IAM strategy and opens the door to unmonitored access, shadow IT, and compliance violations. Whether in healthcare or finance, public sector or tech, any organization using AI should treat these agents like any other high-risk user.

RECOMMENDATIONS

How to Treat AI Agents Like Users:

1. Map AI Identities to Critical Systems
2. Enforce Least Privilege Access
3. Monitor Behavior Continuously
4. Include AI in Your IAM Lifecycle
5. Align with Compliance Frameworks

WHAT'S NEXT?

This special report is part of BeyondID's ongoing research into the future of identity security. Want to go deeper or see how your organization compares?

Contact us today to start the conversation.

Schedule a consultation

ABOUT THE DATA

The numbers and insights featured in this report are based in the findings of a 2025 BeyondID survey of US-based IT leaders, including vice presidents, directors, and managers.

Respondents represented a range of industries such as healthcare, finance, and technology, offering a broad view into the current state of identity security.