BeyondTrust

SOLUTION BRIEF

Agentic AI Identity Security

Secure agentic AI with confidence—and improve compliance posture.

As organizations race to adopt AI, they are inadvertently creating a massive, invisible attack surface that can also undermine their compliance posture. Non-human identities are estimated to already outnumber human identities by 80:1[1], and 96% of enterprise IT leaders worldwide plan to expand their use of AI agents in the next 12 months[2].

Yet, many are experiencing security drawbacks, with one study reporting 75% of organizations incurred an AI-related data breach over the past year. In addition, 86% of organizations reported delaying AI deployments by up to a year due to such security concerns.[3]

BeyondTrust's Approach to a Secure AI Future

We believe AI should be a part of a company's identity program, not an unmanaged exception. BeyondTrust provides a comprehensive defense against the explosion of unmanaged machine identities and autonomous AI agents.

Our integrated solution ensures:

Visibility:
Solves for agentic AI blind spots by illuminating the entire identity estate—on-premises, cloud, and SaaS—to detect identity-based risks, including anomalous machine behavior.

Intelligence:
Provides the intelligence layer to discover non-human identities and distinguish legitimate business automation from malicious agents.

Compliance:
Offers MITRE ATT&CK and NIST 800-53 dashboards and reports to make risk mitigation actionable and efficient.

Control:
Moves beyond traditional PAM to address True Privilege™, identifying the service accounts, bots, and AI agents that silently hold elevated access.

Remediation:
Enables IT Security and DevOps to identify, prioritize, and remediate risks.

Key Security Outcomes

Reduce the agentic AI attack surface
Shift from reactive detection to preemptive exposure management.

Mitigate AI sprawl
Auto-discover and inventory all machine identities, so they can be onboarded or blocked.

Eliminate hardcoded secrets
Remove a major vector for AI compromise.

Evaluate AI agent risk
Leverage risk scoring and real-time dashboards and reporting to prioritize impactful remediations.

Act on integrated remediation recommendations
Flow findings discovered by Identity Security Insights™ directly into the BeyondTrust control stack and other security tools to trigger immediate remediation.

[1]SASE/SSE Platforms Must Adapt to Secure the Rise of Agentic AI and (NHI) Non-Human Identity Access. Gartner. By Charanpal Bhogal, Charlie Winckless, Neil MacDonald, & John Watts. December 2025.
[2]The Future of Enterprise AI Agents. Cloudera. April 2025.
[3]The State of AI. AvePoint. October 2025.

To see how BeyondTrust can help secure your AI initiatives and improve compliance, we invite you to access a complimentary Identity Security Risk Assessment. Or get in touch with us at https://www.beyondtrust.com/contact to learn more.