BeyondTrust

SOLUTION BRIEF

# Secure Agentic AI

**Harness agentic AI with confidence—and with identity security that's built for it.**

While AI agents offer increased productivity, their widespread deployment, often mandated at the board level, has led to a proliferation of potential security risks. The ability for knowledge workers—not just developers—to create AI agents is also fueling "shadow AI"—AI agents used outside of official IT oversight.

AI agents often possess excessive privileges and access to sensitive data, making them prime targets for exploitation.

**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. Our solution is the industry's first generally-available offering for AI identity security.

We provide a unified security approach across human and non-human identities via the BeyondTrust Pathfinder Platform, which integrates our entire product portfolio.

## Key Security Outcomes

**Move fast, safely**
Accelerate AI adoption without compromising security.

**Gain total visibility**
Automatically discover and inventory AI agents alongside human and service identities.

**Prioritize real risks**
Identify over-privileged agents, secrets misuse, shadow AI, and hidden escalation paths.

**Seamlessly enforce governance**
Apply least privilege policies, including ZSP and JIT, to AI agents without disrupting workflows.

**Instantly act on guidance**
Flow findings discovered by the AI agent directly into the BeyondTrust control stack to trigger immediate remediation.

## The three core pillars of BeyondTrust's Secure Agentic AI Solution:

1. **AI Agent Security:**
   This feature provided by our Identity Security Insights® product empowers you with total visibility and integrated governance over AI agents. Auto-discover and inventory AI agents across cloud and SaaS environments, including those created on low-code platforms like Salesforce Agentforce. Detect "shadow AI" and assess privilege risk with the product's True Privilege™ graph. Leverage the shared Pathfinder console and integration with other BeyondTrust products to further reduce risk by applying just-in-time (JIT) access controls and removing standing access for AI agents.

2. **MCP Orchestration:**
   This orchestration layer facilitates secure workflows by brokering agentic AI actions across the BeyondTrust product portfolio via Pathfinder. This layer allows for privilege-safe actions, such as brokering JIT API requests via BeyondTrust Entitle, or triggering credential rotations in BeyondTrust Password Safe.

3. **On-demand AI-powered Intelligence:**
   Our AI assistant and identity expert is built into Pathfinder. The AI assistant provides real-time insights and guidance, helping customers make faster, more informed decisions by interacting directly with their identity security data.

**To see how BeyondTrust can help secure your AI initiatives, 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.**