



AI Agent Security pour les endpoints

Appliquez le principe de moindre privilège aux agents IA qui s'exécutent sur vos endpoints.

Chaque agent IA est une nouvelle forme d'identité non humaine (NHI) qui s'exécute avec tous les privilèges de vos utilisateurs, mais sans aucune de leurs responsabilités. BeyondTrust AI Agent Security vous permet d'adopter l'IA à grande échelle, sans créer votre prochaine menace interne.

Avec AI Agent Security, vous contrôlez les actions des agents IA sur vos endpoints grâce à des politiques distinctes de celles que vous appliquez aux humains. Qu'il s'agisse d'un assistant de bureau qui travaille sur des fichiers locaux, d'une automatisation créée et exécutée par un collaborateur, ou d'un assistant de codage comme Claude Code, Cursor ou Copilot, vous pouvez appliquer les principes du moindre privilège pour limiter ce que ces agents peuvent consulter, exécuter et modifier.

En complément, découvrez chaque agent IA et chaque serveur MCP présent sur chaque endpoint, y compris les installations non déclarées (« shadow installs »). Enregistrez toute l'activité des agents IA avec une attribution action par action et des transcriptions complètes de session.

« Les recherches contrôlées menées par notre équipe de recherche en sécurité Phantom Labs® sur l'IA agentique et les vers autonomes ont mis en évidence une faille critique : les agents IA peuvent agir, s'adapter et se propager à la vitesse d'une machine. Dès lors qu'un agent IA se voit accorder un accès, des autorisations et une autonomie, il devient de fait un nouveau type d'identité. Les contrôles de sécurité traditionnels partent du principe qu'un être humain est à l'origine de chaque décision. Cette hypothèse n'est plus valable. Nous avons développé AI Agent Security précisément pour apporter visibilité, principe de moindre privilège et contrôle à cette nouvelle catégorie d'identité numérique. »

—Kinnaird McQuade, Chief Security Architect, BeyondTrust

AGENTS PRIS EN CHARGE :



- ✓ Visibilité : favorisez une adoption sécurisée de l'IA**
 Transformez le « non » catégorique en un « oui » encadré, afin que vos équipes profitent de la productivité de l'IA sans risque non maîtrisé.
- ✓ Intelligence : attribuez chaque action d'un agent**
 Chaque action d'un agent est consignée et les transcriptions complètes des commandes qu'il exécute fournissent des preuves d'audit et des éléments d'investigation pour répondre aux exigences de conformité telles que la loi européenne sur l'IA, les normes NIST et la norme ISO 42001.
- ✓ Protection : réduisez les risques grâce à des contrôles conçus pour les agents IA**
 Restreignez l'accès de l'IA aux identifiants sensibles, limitez la communication des agents avec certaines API externes et certains serveurs MCP, et imposez une validation humaine avant toute action de l'agent. Cela permet d'empêcher l'exfiltration d'identifiants, de bloquer les commandes destructrices et de garantir que l'EDR n'ait rien à nettoyer a posteriori.