BeyondTrust

Protéger les identités humaines, machines et agents IA contre les cybermenaces



Avec sa plate-forme **Pathfinder**, BeyondTrust est la seule plate-forme de sécurité des identités qui vous permet de détecter les menaces sur l'ensemble de votre parc d'identités – **humaines, machines et agents IA** – et de réagir en contrôlant les privilèges, les accès, les identifiants et les secrets. Grâce à des intégrations transparentes, une analyse incomparable et un ensemble de données axé sur l'identité, BeyondTrust offre une approche Zero Trust pour le moindre privilège, ainsi qu'une détection intelligente des menaces afin de renforcer en permanence votre stratégie de sécurisation de l'identité.

Avec **AI Agent Security**, BeyondTrust étend désormais ce modèle aux agents IA : découverte des agents présents sur les endpoints (y compris le shadow AI), contrôle de leurs actions à l'exécution et application du moindre privilège avant même que l'action ne soit réalisée.

Identités et accès intelligemment sécurisés

- Obtenez **une transparence totale des privilèges**
- Détectez **les menaces liées à l'identité** et répondez-y
- Proposez **un accès à distance sécurisé** à toute infrastructure
- **Protégez vos privilèges** à grande échelle
- **Sécurisez l'adoption de l'IA** en gouvernant les agents IA

Comment gérer les identités et les accès à privilèges sans altérer la productivité ?
Regardez la vidéo →



MIEL

Distribué en France par MIEL
01 60 19 34 52 - www.miel.fr

Secure Remote Access

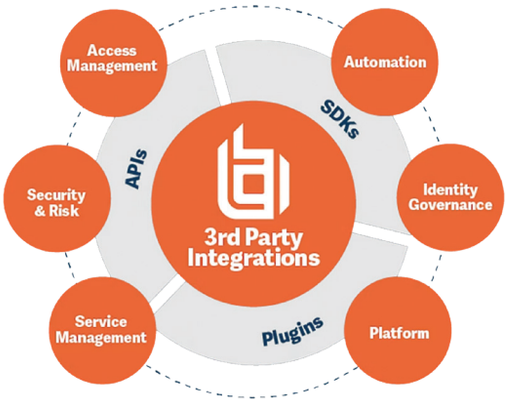
Privileged Remote Access – Gérez et auditez l'accès à distance des employés et des prestataires

Privileged Remote Access de BeyondTrust permet de donner l**e bon accès aux bonnes personnes** et **au bon moment** et offre **une visibilité et un contrôle complets sur tous les accès à distance**, qu'il s'agisse d'administrateurs, de prestataires externes, de développeurs ou d'ingénieurs CloudOps. Les entreprises peuvent utiliser cette solution pour étendre l'accès de manière transparente à des ressources informatiques cruciales tout en respectant des normes rigoureuses de sécurité et de conformité.

- **Un contrôle des accès privilégiés :** Abandonnez les accès à distance de type VPN et permettez aux employés et aux tiers de se connecter de manière transparente et sécurisée à n'importe quel device, où qu'ils se trouvent, avec un accès très contrôlé selon leur rôle et des paramètres de session prédéfinis.
- **Conçue pour aider les organisations à se conformer à la directive NIS2 :** Conformez-vous en toute simplicité grâce au principe clef de traçabilité et audit de session permettant de rejouer à n'importe quel moment les différentes sessions des techniciens.
- **Une sécurisation des outils choisis par l'utilisateur (Bring-Your-Own-Tools) :** Préservez la sécurité de vos activités quotidiennes tout en autorisant l'utilisation par le personnel technique d'outils familiers, tels que Putty et Azure Data Studio, le tout, sans VPN.
- **Des intégrations simples :** Intégrez à vos solutions SIEM existantes un accès à distance privilégié et sécurisé afin de créer un guichet unique pour les analystes et les techniciens dans le cadre de leurs workflows habituels.

Remote Support – Proposez une prise en main à distance fiable et instantanée aux utilisateurs finaux et clients, présents ou non sur votre réseau

Remote Support de BeyondTrust est la meilleure solution pour **accéder et supporter en toute sécurité n'importe quel device ou système et permet aux services support de se concentrer sur la résolution des tickets plutôt qu'à des problèmatiques liées à la sécurité.** Grâce à des options d'architecture adaptées aux exigences actuelles en matière de sécurité et de conformité, vous pouvez offrir **le meilleur des supports**, sans compromettre la sécurité ni les activités de l'entreprise.



- **Accès et contrôle à distance :** Contrôlez, diagnostiquez et supportez les appareils distants où qu'ils se trouvent et à tout moment, sur le réseau de votre entreprise comme en dehors.
- **Intégration :** Maximisez vos outils CRM, ITSM, SIEM et de gestion des mots de passe et créez des intégrations personnalisées avec l'API de BeyondTrust.
- **Efficacité et évolutivité :** Accompagnez sans effort la croissance de votre infrastructure grâce à une gestion efficace de tous les accès et à des intégrations d'annuaires externes, des packages d'installation de masse, des scripts standard et des fonctions d'escalade.
- **Gestion des équipes et des autorisations :** Renforcez la sécurité en appliquant le principe du moindre privilège et de l'accès just-in-time grâce à un contrôle granulaire des rôles, des autorisations et des politiques de session.

Endpoint Privilege Management

For Windows & Mac

Privilege Management for Windows & Mac permet aux entreprises de **supprimer les droits admins locaux** et d'appliquer de manière dynamique **le principe du moindre privilège sans compromettre la productivité des utilisateurs.**

Mettez en place **une stratégie Zero Trust** de manière transparente sur les endpoints Windows et macOS et bénéficiez d'**une protection avancée** contre les mouvements latéraux, les ransomwares et les menaces internes.

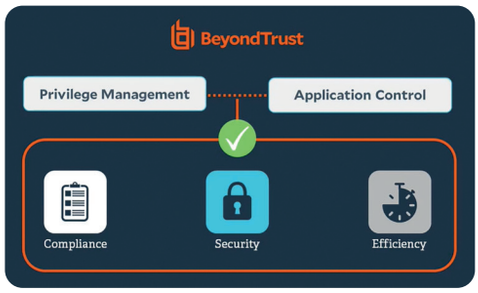
- Un vrai principe du moindre privilège
- Un contrôle précis des applications
- Des déploiements accélérés
- Une protection contre les ransomwares, le phishing et les attaques sans fichier

For Unix & Linux

Privilege Management for Unix & Linux est une solution pour la **gestion des privilèges** au sein des entreprises. Elle aide les services IT et les équipes de sécurité à **garantir la conformité**, **contrôler les accès privilégiés** ainsi qu'à **prévenir et contenir les intrusions** susceptibles d'affecter les systèmes Unix et Linux.

- Audit et gouvernance
- Politique granulaire du moindre privilège et des accès dynamiques
- Contrôle à distance des systèmes et des applications
- Vérification de l'intégrité des fichiers et des politiques

Découvrez la solution EPM en action.
Regardez la vidéo →



AI Agent Security

Encadrez ce que les agents IA sont autorisés à faire, avant qu'ils n'agissent

AI Agent Security permet d'**identifier les agents IA exécutés sur vos endpoints**, d'attribuer chaque action à un humain ou à un agent et de **contrôler ce que ces agents peuvent consulter ou exécuter**. Les politiques sont appliquées sur l'endpoint pendant l'exécution, avant la fin de l'action. La solution s'appuie sur Endpoint Privilege Management et sur l'expertise de BeyondTrust en sécurité des identités centrée sur les privilèges

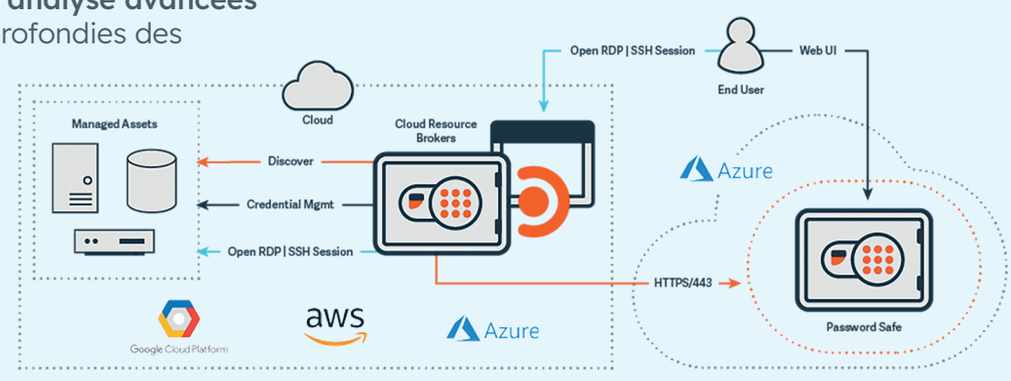
- **Découverte et attribution des agents IA :** Identifiez les agents, y compris le shadow AI, les sous-agents, les skills et les serveurs MCP, et distinguez l'activité humaine de celle des agents.
- **Contrôle à l'exécution :** Encadrez lancements de processus, modifications de fichiers, accès aux identifiants, connexions externes et commandes privilégiées ou destructrices.
- **Zéro privilège excessif des LLM :** Limitez les identifiants et fichiers accessibles aux agents, et gouvernez les connexions MCP et API.
- **Validation humaine :** Exigez une approbation pour les actions sensibles, même lorsque les agents fonctionnent de manière autonome.
- **Audit et simulation des politiques :** Enregistrezchaque session d'agent et testez une politique surl'activité passée avant de l'activer, à partir de modèles conçus par Phantom Labs™.
- **Gouvernance indépendante des éditeurs :** Des contrôles cohérents sur Claude Code, GitHub Copilot, Cursor, les modèles internes et d'autres outils agentiques.

Password Safe

Obtenez une visibilité et une maîtrise totales de vos secrets et identifiants privilégiés

Password Safe offre, en une solution unique, **une visibilité et un contrôle complets des secrets et des identifiants privilégiés.** Password Safe protège les identifiants dans un coffre-fort sécurisé et audité, permettant aux équipes IT, administrateurs et utilisateurs de les protéger ainsi que de **développer et déployer rapidement des solutions cloud. Options de déploiement flexibles :** Password Safe peut être déployé dans le cloud (AWS, Azure), ou on-premise sous la forme d'une appliance pouvant être virtuelle (vSphere, Hyper-V) ou physique.

- **Une gestion automatisée des identifiants :** Découvrez et intégrez automatiquement les comptes, gérez les secrets, enregistrez et renouvelez les mots de passe, le tout de manière automatisée.
- **Des fonctions d'audit et d'analyse avancées :** Tirez parti d'analyses approfondies des privilèges et des identifiants pour simplifier la mise en conformité, le suivi de benchmarks...
- **Une meilleure gestion des sessions :** Mettez en place un double contrôle permettant aux administrateurs d'enregistrer, verrouiller et documenter les activités des comptes privilégiés sans interrompre les sessions ou entraver la productivité.



Entitle

Permettez un accès granulaire, Just-in-Time au sein de votre infrastructure cloud et SaaS

- **Découverte automatisée des droits :** Éliminez les autorisations fantômes dans des comptes locaux, grâce à une source de référence centralisée.
- **Une demande, plusieurs autorisations :** Regroupez les rôles en une seule demande d'accès, qu'il s'agisse de dossiers SharePoint, de buckets S3 ou de tables MongoDB.
- **IaC et API robustes à l'échelle :** Personnalisez-le pour répondre à vos besoins exacts à l'aide d'API REST et d'un fournisseur Terraform.
- **Demandes d'accès et autorisations en libre-service :** Permettez aux utilisateurs d'accéder de manière transparente à ce dont ils ont besoin via Teams, Slack ou Jira.
- **Création de clés et de secrets JIT SSH :** Donnez aux utilisateurs, qui ont besoin d'accéder à des systèmes non fédérés, un nouveau compte temporaire doté uniquement des autorisations nécessaires.
- **Audit de la session complète et historique des demandes :** Simplifiez la conformité et la recherche de preuves grâce à une piste d'audit de toutes les activités de l'utilisateur.

Contactez-nous

Appelez le +33 1 60 19 34 52
reseausecu@miel.fr

Voir la page produit →

MIEL

www.miel.fr/beyondtrust