BeyondTrust

Il est essentiel de pouvoir mettre en place facilement une gestion des accès à privilèges ainsi qu'une sécurisation efficace des identités.

> **Pour commencer.**

PAM Buyer's Guide *pour* une **gestion complète des accès privilégiés**

TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE

L'identité constitue le nouveau périmètre et la gestion des accès à privilèges (PAM) est la pierre angulaire d'une sécurisation moderne des identités et des accès.

La sécurisation des identités -humaines ou machines- dotées d'un accès à privilèges aux systèmes, données, applications et autres ressources sensibles est une priorité.

Le PAM est également essentiel pour protéger l'ensemble de votre infrastructure liée aux identités, notamment vos outils IAM/IGA (gestion des identités et des accès/administration et gouvernance des identités).

Aujourd'hui, les privilèges sont omniprésents, qu'il s'agisse de systèmes d'exploitation, de systèmes de fichiers, d'applications, de bases de données, d'hyperviseurs, de plates-formes de gestion dans le cloud, d'outils DevOps, de processus d'automatisation robotique et plus encore.

Le développement du télétravail et du cloud signifie que les organisations doivent faire face non seulement à des identités de plus en plus nombreuses, mais également de plus en plus complexes.

Ce qui n'a pas changé, ce sont les cybercriminels qui convoitent toujours les privilèges et les accès à privilèges parce qu'ils leur permettent d'accéder plus rapidement aux cibles les plus sensibles d'une organisation.

En disposant d'identifiants et d'accès à privilèges, un cyberattaquant ou un logiciel malveillant devient essentiellement un « initié ». Les acteurs des cybermenaces ont également inclus dans leurs cibles les outils utilisés pour gérer les identités. Cela entraîne le besoin de sécuriser les identités pour tous les comptes.

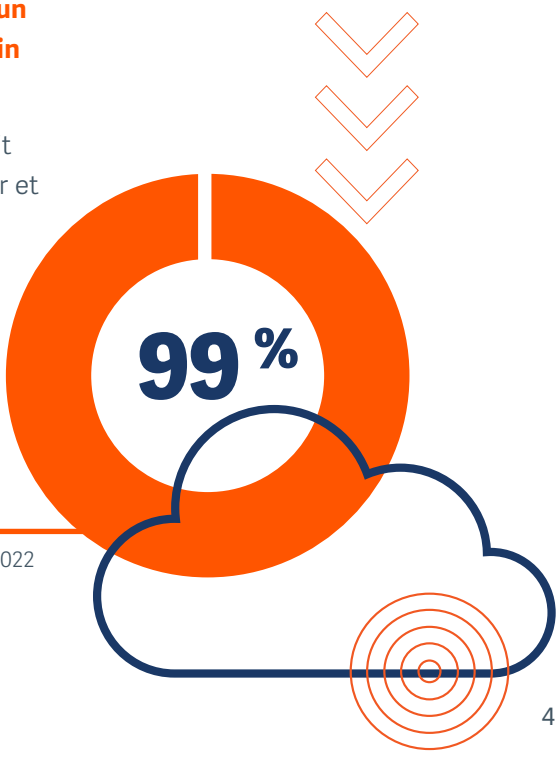
Bien que de nombreuses failles peuvent être éliminées en appliquant des principes de base en matière de sécurité, les attaquants gagnent rapidement en flexibilité en allant au-delà d'une simple automatisation. L'apprentissage machine et l'intelligence artificielle (IA) sont en train de changer la donne, étoffant considérablement le nombre d'outils mis à la disposition des attaquants et rendant de plus en plus possibles les attaques d'origine humaine.

L'IA générative n'en est qu'à ses débuts. Cependant, elle aide déjà les attaquants à agir plus rapidement et à opérer de façon mieux ciblée et sophistiquée, par exemple en exploitant des mécanismes d'ingénierie sociale à plusieurs facteurs pour usurper des identités et leurs attributs. Bien évidemment, il est tout aussi important pour les organisations de protéger leurs propres données issues de l'apprentissage machine et de l'intelligence artificielle contre le vol ou la manipulation.

Pour autant, le fait est que presque toutes les attaques nécessitent un privilège pour l'exploit initial ou pour se déplacer latéralement au sein d'un réseau.

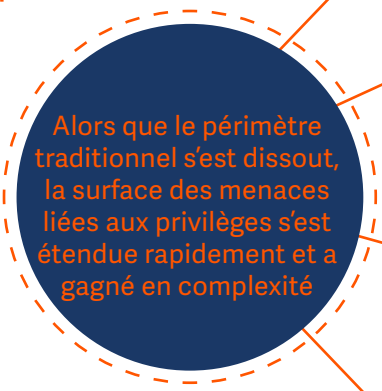
Alors que la surface d'attaque continue de s'étendre et d'évoluer, le fait le plus notable est la façon dont les privilèges continuent de proliférer et d'être exposés de nouvelles manières. Les vecteurs d'attaque des identités n'ont jamais été aussi nombreux.

>>> Il a été constaté dans **99 % des tests de pénétration** menés par l'équipe X-Force Red d'IBM que **les identités cloud étaient surprivilégiées**, permettant aux testeurs de rapidement compromettre les environnements cloud clients.



SOURCE : IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022

La surface d'attaque s'étend



Cloud et cloud hybride
Plates-formes de gestion dans le cloud (AWS, Azure)
Environnements virtualisés (VMware, Microsoft)
Machines virtualisées (Unix, Linux, Windows)
Applications SaaS (Facebook, LinkedIn, personnalisées)

Sur site
Comptes admin partagés
Ordinateurs (Windows, Mac)
Serveurs (Unix, Linux, Windows)
Systèmes de contrôle industriels
Sécurité et infrastructure réseau
Applications et bases de données
Identifiants machines (application à application)
Hyperviseurs et machines virtuelles

DevOps et infrastructure backend
DevOps et outils SecDevOps
Environnements virtuels dynamiques
Conteneurs
Microservices

Technologie opérationnelle (OT)/ Internet des objets (IoT)/IIoT industriel
Stations de travail itinérantes
BYOD
Caméras
Capteurs
Imprimantes
Tout appareil doté d'une connectivité Internet intégrée

Défis pour la sécurité basés sur l'identité

En bref

Plus de cloud, de multicloud et de Bring Your Own Cloud (BYOC)
Plus de 40 000 types d'autorisations cloud à gérer[1]

Plus de vulnérabilités
540 % d'augmentation des vulnérabilités du cloud au cours des six dernières années[2]
159 % d'augmentation des vulnérabilités Azure et Dynamics 365 au cours de 2022[3]

Plus d'accès distants
76 % des comptes cloud proposés à la vente sur le dark Web sont liés à un accès RDP[4]

Plus d'identités (humaines, machines, etc.)
98 % des professionnels de la sécurité déclarent que le nombre d'identités augmente, principalement en raison de l'adoption du cloud, des relations avec des tiers-mainteneurs et des identités machines[8]

Plus de privilèges
95 % des identités machines sont surprivilégiées[5]
Il a été constaté dans **99 % des tests de pénétration** que les identités cloud étaient surprivilégiées[6]

Plus de connectivité à toutes choses
93 % des professionnels de la sécurité OT indiquent que leur organisation a subi au moins un incident d'intrusion dans un système OT au cours des 12 derniers mois ; 78 % en signalant 3 ou plus ; **61 % des intrusions ont eu un impact sur leurs systèmes OT**[7]

Plus d'incidents et de violations liés à l'identité
90 % des professionnels de la sécurité ont déclaré avoir subi un incident lié à l'identité au cours de l'année écoulée[8]

1. 2023 State of Cloud Permissions Risks Report. Microsoft Security. Mars 2023.
2. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022.
3. Microsoft Vulnerabilities Report. BeyondTrust. Mars 2023.
4. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022.
5. Gartner. Innovation Insight for CIEM, juin 2021.
6. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022
7. 2022 State of Operational Technology and Cybersecurity Report. Fortinet. Juin 2022.
8. IDSA 2023 Trends in Securing Digital Identities. 30 mai 2023

Les attaquants utilisent des outils plus intelligents. Vous devriez faire de même.

Le PAM est au cœur de la sécurisation des identités.

De nos jours, une sécurité efficace contre les menaces liées aux privilèges et celles basées sur les identités nécessite de combiner des fonctionnalités de prévention et de détection. Ainsi, une solution PAM complète doit actuellement prévenir les menaces, mais aussi fournir des fonctionnalités de détection intelligentes. Pour comparer cet état de fait avec la sécurité domestique, il ne s'agit plus seulement d'utiliser des serrures et des codes d'accès, mais aussi des capteurs de mouvement intelligents.

Par où commencer ?

Contrôler, surveiller et auditer les privilèges et les accès privilégiés -pour les employés, les fournisseurs, les systèmes, les applications, l'IoT et tout le reste qui interagit avec vos environnements IT- est essentiel pour vous protéger des vecteurs d'attaque externes et internes, ainsi que pour répondre à des exigences de conformité qui ne cessent de croître.

Mais par *où* commencer ?

L'accès à distance constitue-t-il le plus grand risque ? Ou bien les identifiants privilégiés ? Qu'en est-il des machines des utilisateurs finaux ? Peut-être les serveurs Linux où vos données et opérations sensibles, y compris votre propre IA, sont hébergées ?
Après avoir entrepris votre démarche, comment savoir où concentrer votre attention lors des étapes suivantes ?

Ce PAM Buyer's Guide vous aidera justement à y répondre - par où commencer votre projet de gestion des accès à privilèges (PAM), comment améliorer votre stratégie de sécurité et quels résultats attendre sur le plan de vos activités. Nous commencerons par les bases du PAM qui atténueront la plupart des risques. Nous aborderons ensuite d'autres cas d'usage significatifs et conclurons par les cas d'usage émergents que vous devriez connaître.

Les enseignements que nous avons tirés de plusieurs milliers de déploiements indiquent que la plupart des clients adoptent une démarche assez similaire, mais finalement, vos prochaines décisions concernant le PAM seront fondées sur le risque et les besoins de votre organisation. En ayant les bons fournisseurs et partenaires à vos côtés, vous devriez aboutir assez facilement à une gestion des accès à privilèges efficace.

Problèmes liés à la gestion des accès, des identités et des privilèges dans les environnements sans PAM	→	**Objectifs de sécurité liés à l'état final du PAM**
Processus manuels de gestion des mots de passe privilégiés, notamment des feuilles de calcul ou des coffres-forts physiques		Gestion automatisée des mots de passe et des sessions pour tous les comptes privilégiés
La plupart des utilisateurs disposent d'un accès administrateur sur leurs machines		Le principe du moindre privilège basé sur des règles est appliqué à l'échelle de l'organisation, sur l'ensemble des systèmes et des machines
Manque d'audit et de contrôle concernant les comptes root et les comptes privilégiés		Contrôle complet et responsabilisation appliqués aux utilisateurs privilégiés sur n'importe quel système, éliminant l'accès root ou les méthodes insuffisantes telles que sudo
Aucun suivi de session ni enregistrement concernant l'utilisation associée à des privilèges		Enregistrement automatique des frappes clavier/vidéos/activités observées
Accès tiers-mainteneurs non contrôlé ou restreint en interne « tout ou rien »		Un contrôle granulaire et flexible garantit que l'accès distant n'est accordé qu'aux ressources requises pour les fournisseurs et les employés autorisés
Aucune image claire ou particulière des menaces ou des moyens de les contrecarrer		Panorama complet des identités et des vecteurs d'attaque pour atténuer les menaces de manière proactive
Infrastructure des services d'annuaire désorganisée et chaotique, avec plusieurs connexions requises et des politiques incohérentes sur Windows, Unix, Linux, etc.		Authentification unique (SSO) pour des systèmes hétérogènes tirant parti d'une infrastructure familière
Lacunes dans la gestion des identités privilégiées et non privilégiées		Gestion rationalisée des identités privilégiées et non privilégiées pour une couverture exhaustive, sans aucune lacune
Productivité des utilisateurs entravée et volume élevé de tickets de support		Les utilisateurs ont les moyens d'accomplir ce qu'ils doivent faire. Le service support reçoit moins de tickets en raison de la diminution des problèmes de sécurité
RISQUE TRÈS ÉLEVÉ POUR LA SÉCURITÉ		**RISQUE POUR LA SÉCURITÉ FORTEMENT RÉDUIT**

Le fait d'aller au-delà des bases pour améliorer les contrôles PAM optimisera la sécurité, l'auditabilité et les opérations commerciales. La réduction des risques gagnera en vigueur, votre surface de vulnérabilité se réduira et votre stratégie de sécurité se renforcera à mesure que vous vous rapprocherez de l'état final.

Principes intemporels de la sécurité PAM et sécurité des identités et des accès de nouvelle génération

En faisant évoluer votre PAM et vos capacités en matière de sécurisation des identités, non seulement vous réduisez votre surface de vulnérabilité, améliorez vos capacités réactives aux attaques et rendez possibles une meilleure conformité et une qualification accrue à la cyberassurance. Vous dissuadez également de nombreux attaquants qui cherchent à exploiter les proies les plus faciles.

La section suivante de ce document décrit une **approche en six étapes** pour que votre programme de gestion des accès à privilèges soit plus efficace.

1. **Améliorez** la responsabilisation et le contrôle des identités, des comptes et des mots de passe privilégiés
2. **Sécurisez** l'accès distant pour les employés, les fournisseurs, les sous-traitants et l'infrastructure
3. **Mettez en place** le principe du moindre privilège et un contrôle des applications pour Windows et macOS
4. **Mettez en place** le principe du moindre privilège et un accès aux fonctions d'audit pour les serveurs et les postes de travail Unix et Linux
5. **Rationalisez** la gestion des identités et la sécurité en intégrant Unix et Linux dans Windows
6. **Obtenez** une visibilité et des informations sur les menaces pour toutes les identités afin d'atténuer les risques de manière proactive

Les six étapes clés *pour* une gestion des privilèges complète

Cette section du livre blanc identifie les aspects essentiels de la gestion des accès à privilèges et présente les fonctionnalités principales que vous devez rechercher dans chacun d'eux pour sécuriser les identités et les accès tout en répondant aux objectifs de conformité.

Chaque aspect essentiel, une fois mis en place, vous fournira plus de moyens de contrôle et de responsabilisation pour les identités, les comptes, les ressources, les utilisateurs, les systèmes et les activités dans votre environnement, tout en éliminant et en atténuant de nombreux vecteurs de menace. Vous pouvez aborder tous ces aspects en même temps, ou, ce qui est plus fréquent, mettre en place des contrôles pour un ou plusieurs aspects du PAM à la fois. À mesure que vous mettrez en place ces aspects, vous constaterez une augmentation des synergies du PAM ainsi qu'une réduction des risques et une amélioration des opérations grandissantes pour votre entreprise.

Alors que vous procéderez à la sélection et au déploiement de votre solution de gestion des accès à privilèges, **gardez à l'esprit ces exigences**, car elles vous aideront à démontrer la valeur de ce programme auprès de ceux situés plus haut dans la hiérarchie de l'organisation :

Coût total de possession
Cela vous permet-il de gagner du temps (par exemple en remplaçant des processus manuels par une automatisation) et de redéployer des ressources en faveur d'autres initiatives ?

Rapidité de constatation des bénéfices
Dans quel délai cela vous permet-il d'améliorer de manière mesurable les contrôles de sécurité et d'atténuer les risques ?
Combien de temps vous faudra-t-il pour atteindre vos objectifs liés à l'état final du PAM avec la solution ?

Intégrations
Comment cela s'intègre-t-il au reste de votre écosystème de sécurité (gestion des accès et des identités, SIEM, assistance, analyse) ? Cela vous aide-t-il à prendre des décisions mieux informées quant aux risques et à profiter de meilleures synergies avec vos solutions de sécurité existantes ?

Longévité
Le fournisseur de votre solution évoluera-t-il avec vous ? Ira-t-il jusqu'à vous faire progresser grâce à la mise en place de mécanismes de sécurité ? Le fournisseur dispose-t-il des ressources nécessaires pour faire évoluer les capacités afin de répondre aux cas d'usage futurs du PAM ?

1

Améliorez la responsabilisation et le contrôle des identités, des comptes et des mots de passe privilégiés

Le point de départ le plus logique pour mieux contrôler les privilèges est d'améliorer la responsabilisation concernant les identités privilégiées, ainsi que les comptes et les identifiants qui y sont associés. Les identifiants privilégiés comprennent les mots de passe des comptes privilégiés, les secrets des outils DevOps et CI/CD, les clés SSH, les certificats et tout fichier nécessaire au démarrage et à la maintenance des systèmes DevOps, tels que les fichiers JSON et XML. Selon Forrester Research, ces identifiants privilégiés sont impliqués dans 80 % des fuites de données[9].

Les admins partagent fréquemment des mots de passe, ce qui rend presque impossible l'obtention d'une piste d'audit nette. De nombreux systèmes, applications et appareils (IoT, périphériques réseau, etc.) comportent des mots de passe intégrés ou codés en dur, créant des opportunités d'utilisation abusive. Des mots de passe sont nécessaires pour l'accès d'application à application et d'application à base de données. Des identifiants privilégiés sont rapidement générés lorsque de nouvelles instances virtuelles ou dans le cloud sont lancées. La liste ne s'arrête pas là.

Les mesures manuelles de gestion des identifiants privilégiés (découverte, renouvellement, propagation, application des meilleures pratiques de sécurité) sont notoirement peu fiables, complexes, chronophages et difficiles à mettre à l'échelle. Il est même impossible d'adopter certaines meilleures pratiques, par exemple en éliminant et en gérant de façon centralisée certains types de mots de passe intégrés, si on ne dispose pas d'outils d'entreprise.

Comment les organisations peuvent-elles assurer la sécurité et la responsabilisation pour tous les différents types d'identifiants permettant un accès à privilèges, sans pour autant perturber la productivité des administrateurs, les workflows et les processus ?

9. The Forrester Wave™: Privileged Identity Management, T4 2020

Objectif

Une solution automatisée et exhaustive pour facilement découvrir la liste toujours croissante des types de comptes et d'identifiants privilégiés dans votre environnement (tant humains que machines), placer ces comptes et identifiants sous gestion et répondre de façon satisfaisante aux demandes des auditeurs.

Une telle solution éliminera directement certains vecteurs d'attaque privilégiés tout en atténuant beaucoup d'autres, réduisant ainsi considérablement les risques pour la sécurité de l'entreprise. Cela nécessite une solution de gestion des mots de passe ou des identifiants privilégiés adaptée aux besoins de l'entreprise, capable d'automatiser chaque phase du cycle de vie des mots de passe en conformité avec vos politiques de sécurité.

Solution

Password Safe de BeyondTrust unifie la gestion des identités et des sessions privilégiées, des comptes, des mots de passe, des clés SSH, des clés API, des secrets DevOps et plus encore — le tout dans un seul produit.

Password Safe offre des **fonctionnalités exhaustives de découverte automatique, de gestion, d'audit et de contrôle** pour tout compte ou identifiant privilégié — humain, application, machine, etc. — en réduisant de façon importante le risque que des identifiants privilégiés soient utilisés de façon abusive et en respectant les exigences de conformité.

La solution fournit des moyens inégalés d'analyse des menaces (tels que la mise en corrélation entre des comportements anormaux des utilisateurs privilégiés et des données tierces pour déterminer la dangerosité des menaces), des fonctionnalités de reporting sophistiquées et des capacités d'adaptation incomparables pour l'entreprise.

Les trois principaux cas d'usages

Gestion des identifiants, des clés et des secrets
Découvrez et intégrez automatiquement les comptes. Enregistrez, gérez et effectuez des rotations de mots de passe privilégiés tout en éliminant les identifiants intégrés dans les scripts et le code.

Gestion des sessions en temps réel
Consignez et contrôlez toutes les sessions et les activités liées à des identifiants privilégiés à des fins de conformité et d'investigation.

Fonctionnalités d'audit et d'investigation avancées
Tirez parti d'analyses approfondies des privilèges et des identifiants pour simplifier la mise en conformité, le suivi de benchmarks, et bien plus encore.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

Autres points à considérer

À quel point la capacité d'évolution est-elle importante ? Disposez-vous de quelques milliers ou de centaines de milliers d'identifiants privilégiés ?

Seul un nombre limité de solutions PAM peut être en mesure de gérer des dizaines de milliers, voire des centaines de milliers d'identifiants d'utilisateurs privilégiés. Peu d'entre elles peuvent également gérer un grand nombre de clés SSH ou de secrets exploités par des utilisateurs non humains. S'il est important que vous puissiez contrôler et gérer toutes les sessions privilégiées (ce qui devrait être le cas), il vous faut réaliser que seule une poignée de fournisseurs est en mesure de contrôler/gérer des centaines de milliers de sessions en simultané. Seul BeyondTrust offre toutes ces fonctionnalités et répond aux besoins d'évolutivité de votre entreprise dans tous ses aspects et dans tout environnement.

À quel point la complexité de la sécurité, le chevauchement des solutions et la redondance des fournisseurs de sécurité vous rebutent-ils ?

De nombreux fournisseurs de sécurité vendent séparément différents composants pour la gestion des comptes et des identifiants privilégiés, chacun s'accompagnant de sa propre console de gestion. Bien sûr, il existe aussi des fournisseurs de sécurité spécialisés qui proposent des fonctionnalités autonomes pour la gestion des clés SSH, des mots de passe d'application ou des secrets.

Mais qu'en est-il de tous les autres mots de passe d'applications utilisés par les employés ?

Justement, Password Safe de BeyondTrust est également un outil formidable pour sécuriser les mots de passe des applications d'entreprise qu'utilisent les employés. Bien que les identifiants privilégiés présentent le plus de risques, la frontière tend à s'estomper de plus en plus entre ce qui doit être soumis à des privilèges ou non dans les environnements modernes. Les employés dans toute votre organisation ont besoin d'accéder à des dizaines, ou parfois même à des centaines, d'applications pour s'acquitter de leurs tâches et cela implique souvent de définir des niveaux de sensibilité en ce qui concerne les accès et les données. Password Safe est associé à un module Workforce Passwords qui applique une sécurité de niveau entreprise aux mots de passe utilisés par vos employés. Cela signifie que les utilisateurs n'ayant pas de privilèges peuvent utiliser Password Safe pour enregistrer rapidement les identifiants d'applications métiers nécessaires pour leur travail quotidien impliquant traditionnellement d'effectuer des stockages dans des dossiers et d'utiliser des extensions de navigateur. Cette fonctionnalité offre aussi une prise en charge complète des fonctions d'audit et de reporting, y compris le suivi granulaire des identités, des identifiants et des accès aux applications.

BeyondTrust propose une solution unique et complète pour une gestion, un contrôle et un audit de tous les types d'identifiants privilégiés qui se distingue par ses capacités de centralisation et d'unification, tout en offrant aux utilisateurs sans privilèges un moyen simple et sécurisé d'enregistrer leurs mots de passe d'applications métiers.

À titre de comparaison, il faudrait acheter jusqu'à six solutions différentes en passant par d'autres fournisseurs de premier plan !

« C'est bien la première fois que nous mettons en œuvre une solution de sécurité qui facilite autant le travail de l'utilisateur final. Nos responsables d'immeubles géraient auparavant des dizaines d'identifiants différents pour le personnel et les fournisseurs. Password Safe gère l'ensemble des identifiants de manière centralisée, de sorte qu'ils n'ont besoin que d'un seul mot de passe pour eux, un pour les fournisseurs, un autre pour leur équipe. »

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

ÉTAPE CLÉ

2

Sécurisez l'accès distant pour les employés, les fournisseurs, les sous-traitants et l'infrastructure

Les chemins d'accès distants constituent depuis longtemps les points faibles pour la plupart des organisations. L'époque actuelle marquée par l'augmentation du télétravail et la décentralisation des équipes offre de grandes opportunités aux attaquants. Des chercheurs ont constaté qu'entre 50 et 80 % des attaques de type ransomware débutent systématiquement par un exploit au niveau du RDP (Remote Desktop Protocol). Selon un rapport IBM X-Force, 76 % des comptes cloud proposés à la vente permettent des accès RDP[10].

Les tiers-mainteneurs tout comme les employés internes (y compris les ingénieurs des opérations cloud, les développeurs et les autres collaborateurs décentralisés) ont besoin d'un niveau d'accès approprié pour s'acquitter efficacement de leurs tâches. Les admins IT doivent être en mesure de gérer, d'accorder et d'élever efficacement les privilèges.

Les organisations manquent souvent de visibilité sur ce que font les fournisseurs et les employés à distance lorsqu'ils accèdent à leur réseau. Les VPN procurent un accès bien trop étendu par rapport aux besoins, ce qui expose les réseaux et les identités à un risque. La plupart des autres solutions d'accès à distance présentent les mêmes faiblesses que les VPN, notamment :

- Accès tout ou rien, avec une trop faible granularité du paramétrage de la sécurité
- Aucune visibilité ni aucun enregistrement en ce qui concerne l'activité des utilisateurs, ce qui signifie une absence de pistes d'audit
- Un manque de compatibilité entre les différents systèmes d'exploitation et cas d'usage

En raison de ces lacunes, un seul compte compromis peut rapidement et facilement perturber l'ensemble de votre réseau.

Lorsque vous considérez l'échelle de votre organisation et le risque pour la sécurité que représentent des dizaines ou des centaines de tiers utilisant votre réseau, la dangerosité de ces faiblesses devient évidente.

Avec autant de points d'accès distants - et généralement une visibilité, des fonctionnalités d'audit et des contrôles de sécurité insuffisants les concernant - ce n'est qu'une question de temps avant qu'un point faible de la surface d'accès à distance ne soit compromis par un employé ou un fournisseur.

10. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022

Comment les organisations peuvent-elles mieux contrôler les accès distants des utilisateurs privilégiés sans affecter la souplesse opérationnelle ?

Objectif

Éliminez le principe « tout ou rien » de l'accès à distance pour les fournisseurs et les télétravailleurs en mettant en place des droits granulaires basés sur des rôles pour accéder à des systèmes spécifiques avec des paramètres de session définis. Autorisez les fournisseurs ou les utilisateurs internes à accéder à certains systèmes pendant une période donnée, pour des objectifs ou des applications spécifiques. Les administrateurs sont en mesure d'approuver ou de refuser des demandes d'accès, quelle que soit leur origine et pour tout périphérique sur l'ensemble des plateformes traditionnelles.

Solution

Privileged Remote Access de BeyondTrust permet aux professionnels de l'IT et de la sécurité de contrôler, de gérer et d'auditer les accès distants à privilèges aux systèmes IT critiques sur la base d'identités et de comptes autorisés, notamment pour les employés, tiers-mainteneurs et fournisseurs — sans utiliser un VPN.

Privileged Remote Access répond aux besoins d'accès à distance des utilisateurs tout en protégeant les données sensibles et en assurant la conformité (PCI, HIPAA, ISO, RGPD, etc.).

Vous pouvez déployer la solution Privileged Remote Access sur site via une appliance virtuelle ou physique renforcée, ou bien au travers d'un cloud sécurisé. Accordez des accès vers et depuis des machines, des ordinateurs portables, des dispositifs mobiles et des endpoints OT (technologie opérationnelle).

Cette solution comprend aussi un coffre-fort de gestion des identifiants privilégiés dotée de fonctionnalités de détection, de gestion, de rotation, d'audit et de contrôle pour les comptes à privilèges (d'un administrateur local ou de domaine partagé à un compte admin personnel d'un utilisateur), y compris des comptes avec clés SSH, dans le cloud ou de médias sociaux.

Basée dans le cloud, cette solution peut gérer plus de 5 000 identifiants Windows et en stocker jusqu'à 10 000. **Privileged Remote Access s'intègre en parfaite harmonie avec Password Safe de BeyondTrust afin d'offrir des fonctionnalités plus complètes de gestion des identifiants.** Ces produits peuvent être groupés pour constituer **l'offre PASM totale** la plus puissante et la plus appréciée du marché.

Les trois principaux cas d'usages

Accès sécurisé pour les employés, où qu'ils soient
Maximisez la productivité des employés et la sécurité avec l'injection d'identifiants et l'accès à distance sécurisé aux systèmes autorisés.

Vendor Privileged Access Management (VPAM)
Offrez un accès simple et sécurisé pour les fournisseurs de confiance se connectant à vos systèmes, tout en éliminant le besoin de VPN et des identifiants connus.

Accès à l'infrastructure
Donnez à vos développeurs cloud et vos ingénieurs DevOps une connectivité, une authentification et une auditabilité sécurisées sans faille à travers toute l'infrastructure.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

BeyondTrust offre une solution unique dotée de fonctionnalités éprouvées de gestion des accès à privilèges ou de sécurisation des identités afin d'appliquer les meilleures pratiques en la matière aux fournisseurs, aux tiers-mainteneurs et aux employés travaillant à distance.

Nos concurrents les plus proches n'ont que récemment commencé à créer ces fonctionnalités PAM essentielles.

« Privileged Remote Access de BeyondTrust nous offre l'assurance que chaque partie de notre infrastructure est inaccessible, à moins que nous n'en décidions autrement… Nous pouvons appliquer le principe du moindre privilège en accordant un niveau d'accès pertinent en fonction du rôle et planifier le moment et la durée de l'accès des fournisseurs à des systèmes spécifiques. »

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

ÉTAPE CLÉ

3

Mettez en place le principe du moindre privilège et un contrôle des applications pour Windows et macOS

Une fois que les identifiants et les comptes privilégiés sont continuellement détectés, intégrés et gérés, l'étape suivante consiste à appliquer le principe du moindre privilège pour atteindre une gestion complète des accès associés. Comment ? En éliminant les droits admins locaux sur les machines des utilisateurs finaux. Si vous disposez de serveurs Windows, le principe du moindre privilège requiert aussi de mettre en place des accès à privilèges appropriés pour vos divers comptes administrateur, notamment en ce qui concerne le réseau, Microsoft Exchange Active Directory, la base de données, les développeurs, le service support, les utilisateurs de l'équipe IT/avancés, etc.

En adoptant une approche basée sur le moindre privilège, les utilisateurs ne reçoivent que les autorisations nécessaires selon leur rôle pour accéder aux systèmes, aux applications et aux données. Les privilèges, au lieu d'être toujours activés (et donc toujours susceptibles d'être utilisés à mauvais escient ou de manière abusive), ne sont élevés qu'en fonction des besoins. En faisant en sorte que la plupart des utilisateurs soient standard par défaut et en n'élevant les privilèges qu'en cas de besoin, vous réduisez fortement la surface d'attaque ainsi que votre vulnérabilité aux mouvements latéraux tout en minimisant le risque posé par le phishing et le ransomware. Vous contribuez à assurer la protection des ressources les plus sensibles de votre entreprise en contrôlant et en auditant minutieusement les accès admins.

Les outils natifs ou développés en interne pour restreindre ou activer les privilèges des utilisateurs finaux sont coûteux en temps et financièrement. En outre, bien que les utilisateurs ne devraient pas être dotés en premier lieu de privilèges utilisateur avancé ou admin local, certaines applications nécessitent parfois une élévation des privilèges pour fonctionner.

« Historiquement, 75 % des vulnérabilités critiques Microsoft auraient pu être atténuées en supprimant les droits admins. »

Microsoft Vulnerabilities Report 2023, **BeyondTrust**

Comment les services IT peuvent-ils réduire le risque posé par des utilisateurs surprivilégiés sans entraver la productivité ou surcharger le service support avec des demandes de privilèges ou d'autorisations ?

Objectif

Supprimez efficacement les droits admins locaux dans les environnements Windows et macOS, contrôlez et auditez minutieusement les accès admins aux serveurs et aux systèmes sensibles, et supervisez en détail les applications : le tout sans affecter la productivité des utilisateurs finaux. Les solutions d'entreprise de gestion des privilèges des endpoints doivent être en mesure de supprimer les privilèges des utilisateurs finaux tout en appliquant une technologie d'automatisation de l'élévation des privilèges liés aux applications sur la base de règles, sans jamais élever les privilèges des utilisateurs eux-mêmes.

Solution

Privilege Management pour Windows et Mac de BeyondTrust applique le principe du moindre privilège et facilite la conformité au niveau des environnements de bureau Microsoft Windows physiques et virtuels, des serveurs et des environnements de bureau macOS, tout en favorisant la productivité des utilisateurs finaux.

Les trois principaux cas d'usages

Sécurité Zero Trust sur Windows et macOS
Supprimez les droits admins locaux et assurer un vrai principe de moindre privilège pour les serveurs et postes de travail Windows et macOS.

Protection contre les attaques et les menaces sans fichier
Réduisez l'exposition aux cyberattaques et protégez-vous contre les attaques par malware, ransomware et phishing.

Audit et assurance de la conformité
Répondez rapidement aux exigences de conformité et de cyberassurance grâce à une piste d'audit unique et irréprochable pour toutes les activités nécessitant des privilèges.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

Autres points à considérer

À quel point est-il important pour vous de constater rapidement les bénéfices apportés par la solution ?
Certaines solutions exigent une réorganisation complexe des services, tandis que d'autres parviennent à démontrer une réduction des risques et des demandes auprès du service support en quelques semaines seulement.

Disposez-vous d'un parc de serveurs Unix ou Linux ou d'autres endpoints non traditionnels qui interagissent avec votre réseau ?
De nombreux fournisseurs proposent des fonctionnalités de gestion des privilèges sous Windows qui n'ont pas d'équivalent pour Unix, Linux et macOS, sans parler des endpoints non traditionnels. Ne vous semble-t-il pas plus utile d'avoir un fournisseur offrant un produit unique capable d'appliquer le principe du moindre privilège et les meilleures pratiques de contrôle des applications pour tous vos endpoints - y compris les dispositifs Windows, Unix, Linux, macOS, ICS, SCADA, IoT et réseau ?

BeyondTrust est le seul fournisseur capable d'offrir une gestion des privilèges pour l'ensemble de votre parc IT.

La solution Privileged Management pour Windows et Mac offre un ROI solide en remédiant aux failles de sécurité des accès et des identités, en diminuant les demandes adressées au service support concernant la sécurité et en accélérant la réalisation de vos objectifs de conformité.

Les règles QuickStart prêtes à l'emploi élaborées à partir de milliers de déploiements permettent aux organisations de progresser rapidement et fortement dans la réduction des risques. La fonctionnalité unique Trusted Application Protection de la solution (sous Windows uniquement) parvient même à bloquer les attaques sans fichier insidieuses en supervisant les DLL et les processus enfants, et en tirant parti de mécanismes de contrôle intégrés basés sur le contexte pour repérer les scripts dangereux et les pièces jointes infectées.

Privilege Management pour Windows et Mac peut être mis en œuvre plus rapidement que les solutions concurrentes, tout en offrant des fonctionnalités plus poussées. Vous en verrez rapidement les bénéfices dès que votre équipe en prendra possession.

« Nous disposons d'une équipe de six ingénieurs qui gèrent l'ensemble du parc mobile et de bureau. Nous avions donc besoin d'une solution leur permettant de s'acquitter de leurs tâches aussi rapidement et efficacement que possible. Il est indéniable que Privilege Management pour Windows et Mac nous a permis d'y parvenir. »

Ryan Powell, Operations & Response Centre Manager,
University of Derby

ÉTAPE CLÉ

4

Mettez en place le principe du moindre privilège et un accès aux fonctions d'audit pour les serveurs et les postes de travail Unix et Linux

Les applications de niveau 1 essentielles aux activités s'exécutant sur des serveurs Unix et Linux sont des cibles de choix pour les cyberattaquants. Les identifiants d'utilisateurs privilégiés liés à ces ressources peuvent permettre d'accéder aux données d'e-commerce, aux systèmes ERP contenant des renseignements sur les employés, aux informations sur les clients et aux données financières sensibles.

Les administrateurs IT ont parfois besoin de disposer de mots de passe root, d'un statut de « superuser » ou d'autres privilèges avec élévation des droits pour accomplir leur travail. Cette pratique pose malheureusement des risques importants pour la sécurité en raison d'une éventuelle utilisation à mauvais escient des privilèges, que ce soit de façon intentionnelle, accidentelle ou indirecte.

Des outils natifs, open source et ad hoc sont souvent utilisés par souci de simplicité. Cependant vous finissez par payer un prix élevé pour ces outils « gratuits » de multiples façons dans des environnements de serveurs, même peu complexes. Certaines des vulnérabilités de sudo et d'autres outils de base incluent :

- Déficiences en matière de supervision, d'investigation et d'audit, notamment un manque de contrôle de l'intégrité des fichiers, de sécurisation des logs ou de capacité à enregistrer les sessions et les frappes de clavier.
- Sérieuses lacunes en matière de sécurité. Ces outils ne prennent pas en compte l'activité au sein des scripts et des applications tierces, offrant des raccourcis à des applications non approuvées. Les outils natifs des systèmes d'exploitation sont également incapables de déléguer une autorisation sans avoir à divulguer des mots de passe.
- Complexité administrative et manque d'évolutivité. Les règles doivent généralement être gérées sur chaque serveur individuel lorsque sudo ou d'autres outils de base sont utilisés.
- Absence d'un support d'entreprise.
- Aucun moyen de migration efficace pour abandonner sudo, s'il est utilisé.

Avec sudo et d'autres outils, il est quasiment impossible de maintenir les meilleures pratiques de sécurité et de conformité dans tous les environnements informatiques, sauf les plus primitifs. Pour faire simple, les conséquences de contrôles d'accès à privilèges inadéquats dans vos environnements Unix et Linux sont bien trop élevées.

Objectif

Gagnez en visibilité et en contrôle sur l'ensemble de vos activités privilégiées sous Unix et Linux, appliquez uniformément le principe du moindre privilège, bénéficiez d'une délégation efficace des privilèges et autorisations Unix et Linux, le tout sans avoir à divulguer des mots de passe pour des comptes root ou autres. Soyez en mesure d'abandonner totalement sudo, ou d'en tirer le meilleur parti en superposant les fonctionnalités d'entreprise qui résolvent les déficiences en matière de sécurité et d'audit pour rendre l'administration plus simple et moins sujette aux erreurs.

Solution

BeyondTrust Privilege Management pour Unix et Linux est la solution de premier plan pour gérer la sécurité des accès à privilèges sous Unix et Linux. Cette solution vous aide à contrôler les privilèges des comptes root Unix/Linux au moyen de fonctions d'analyse centralisée, de reporting et d'enregistrement de la frappe clavier. Utilisez-la pour réduire les risques et atteindre la conformité plus rapidement qu'avec sudo ou des outils natifs.

Les trois principaux cas d'usages

Contrôle de l'accès root
Établissez des règles granulaires d'élévation de privilèges afin d'exécuter seulement des tâches ou commandes spécifiques.

Suivi et audit des activités
Protégez-vous contre toute modification non autorisée de fichiers, de scripts et de registres avec un audit avancé de toute activité utilisateur.

Surveillance de session en temps réel
Détectez les activités suspectes des utilisateurs, des comptes et des ressources en temps réel avec le suivi de tous les logs et de toutes les sessions.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

Autres points à considérer

Disposez-vous également de serveurs et de postes de travail Windows ? Préférez-vous disposer d'un fournisseur et d'une plateforme uniques pour mettre en œuvre le PAM parmi tous vos endpoints ?

Est-il important que vous ayez la possibilité d'activer l'authentification unique (SSO) dans l'ensemble de votre infrastructure hétérogène et d'unifier la gestion des règles sous Unix, Linux, macOS et Windows ?

Seule une poignée de fournisseurs peuvent satisfaire vos besoins si vous avez pour priorité d'améliorer votre couverture PAM et de réduire la complexité.

En mettant en place une gestion « just-in-time » des privilèges (et donc en éliminant les accès à privilèges persistants), Privilege Management pour Unix et Linux limite fortement la durée pendant laquelle un compte est doté de privilèges et de droits d'accès accrus.

Cela réduit drastiquement la période de vulnérabilité au cours de laquelle un cyberattaquant peut exploiter les privilèges d'un compte. Cette solution PAM pour Unix/Linux, qui est de loin la plus puissante du marché, offre également un coût total de possession faible par rapport aux alternatives. Cela est dû à la centralisation de la gestion des comptes privilégiés depuis une seule interface, réduisant ainsi fortement le temps et les efforts nécessaires pour atteindre les objectifs de sécurité et d'audit.

Privilege Management pour Unix et Linux renforce la sécurité, la responsabilisation et la productivité pour tous les utilisateurs et les administrateurs de serveur, sans les risques posés par les logiciels open-source sudo.

« Plutôt que de considérer Privilege Management pour Unix/Linux comme un ensemble de règles drastiques tentant de verrouiller tout le monde, pensez plutôt à ce que permet cette solution pour vos utilisateurs, à la rapidité avec laquelle vous pouvez accorder un accès en ligne à quelqu'un, lui permettre d'accomplir sa tâche et de résoudre les incidents sur le système. C'est ainsi que nous utilisons Privilege Management pour Unix et Linux. »

Chad Erbe, Sr. Staff Engineer,
ServiceNow

5 Rationalisez la gestion des identités et la sécurité en intégrant Unix et Linux dans Windows

Une fois que vous disposez d'un meilleur contrôle sur les accès à privilèges dans les environnements Unix et Linux, il est dans la logique des choses de placer ensuite ces systèmes dans un cadre uniformisé de gestion, de règles et d'authentification unique. Historiquement, Unix et Linux ont été gérés sous la forme de systèmes indépendants, chacun constituant un silo avec son propre ensemble d'utilisateurs, de groupes, de règles de contrôle d'accès, de fichiers de configuration et de mots de passe à mémoriser. La gestion d'un environnement hétérogène contenant ces silos - en plus de l'environnement Microsoft - entraîne une administration incohérente pour l'IT, une complexité inutile pour les utilisateurs finaux et un risque accru pour l'entreprise.

Comment les services IT gèrent-ils les politiques de manière uniforme sur différentes plateformes et fournissent-ils une expérience utilisateur rationalisée qui réduit le temps consacré à l'administration et les erreurs ?

Objectif

Authentification centralisée pour les environnements Windows, Unix et Linux qui réduit les risques et la complexité liés à la gestion d'un environnement hétérogène. Améliorez l'efficacité en réduisant la quantité d'informations de connexion (et par ricochet, le nombre d'appels au service support lorsqu'elles sont oubliées) ainsi que le nombre de systèmes, de configurations et de règles à gérer. Cela requiert une solution Active Directory Bridging afin de rationaliser la gestion des identités d'utilisateurs.

Solution

Active Directory (AD) Bridge de BeyondTrust rationalise la gestion des identités et le contrôle des accès dans l'ensemble de votre environnement hybride en étendant l'authentification Microsoft AD, les fonctionnalités d'authentification unique et la gestion de la configuration des politiques de groupes aux systèmes Unix et Linux.

En centralisant la gestion des informations de connexion et des configurations, et en tirant parti de votre infrastructure Windows Active Directory, AD Bridge de BeyondTrust accélère la réalisation de vos objectifs en matière de sécurité des identités et d'audit, tout en stimulant la productivité des utilisateurs et des administrateurs de serveurs.

Les trois principaux cas d'usages

Gestion unifiée des identités
Établissez des règles granulaires d'élévation de privilèges afin d'exécuter seulement des tâches ou commandes spécifiques.

Audit et conformité
Fournissez les détails d'audit aux équipes chargées de la conformité et gérez de manière centralisée les politiques de groupe.

Sécurité Unix/ Linux améliorée
Étendez l'authentification unique (SSO), le partage de fichiers, les politiques de sécurité et le contrôle d'accès à d'autres systèmes que Windows.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

« Commencer avec AD Bridge a fait toute la différence pour accélérer l'exécution de notre stratégie Zero Trust chez Investec »

Brandon Haberfeld, Global Head of Platform Security, **Investec**

6

Obtenez une visibilité et des informations sur les menaces pour toutes les identités afin d'atténuer les risques de manière proactive

Deux tendances expliquent en grande partie pourquoi les organisations peinent à se protéger elles-mêmes. La première est que la taille des parcs numériques et des surfaces d'attaque augmente, alors que leur visibilité sur les menaces diminue. La seconde est le développement exponentiel des identités humaines et machines ainsi que la prolifération de nouveaux chemins d'accès vers des systèmes et des données critiques qui a affaibli la visibilité de la plupart des équipes de sécurité sur les menaces et les autres dangers.

De nos jours, la plupart des organisations utilisent plus d'une dizaine de systèmes pour gérer les identités et les droits d'accès, ce qui accentue d'autant plus la complexité et étend la surface d'attaque. En outre, une grande proportion de ces systèmes de gestion des identités et des accès/de gouvernance et d'administration des identités sont eux-mêmes des cibles de choix pour les cyberattaquants.

Lorsque le système de gestion des identités devient lui-même compromis, infiltrer l'environnement à grande échelle devient un jeu d'enfant pour un attaquant.

D'autre part, les professionnels IT et de la sécurité sont déjà surchargés de données liées aux vulnérabilités et aux menaces. Malheureusement, les menaces persistantes avancées (APT) passent souvent inaperçues. En effet, les solutions traditionnelles d'analyse de la sécurité ne sont pas en mesure de mettre en corrélation des données liées aux identités d'origines diverses (par exemple, comptes privilégiés, utilisateurs, ressources, droits d'accès au cloud, etc.) pour détecter les risques masqués. Des événements en apparence isolés sont considérés comme des exceptions, filtrés ou perdus dans une multitude de données. L'intrus peut ainsi continuer à pénétrer le réseau, le préjudice gagnant en ampleur. Il a déjà été constaté que les attaques reposant sur l'IA sont plus insaisissables et difficiles à repérer.

Il manque aux organisations une vue centralisée sur les identités, les comptes et les accès à privilèges dans l'ensemble de leur parc informatique. Généralement, une visibilité plus fragmentée et cloisonnée se traduit par :

- Risque accru que des solutions ne s'intègrent ou ne communiquent pas bien entre elles, ce qui génère des temps d'arrêt, des failles de sécurité et de la frustration.
- Charge administrative toujours plus élevée.
- Orchestration retardée de la réponse aux menaces.
- Incapacité partielle ou totale à satisfaire les auditeurs ou à répondre aux demandes d'investigation en temps opportun.
- Risques de sécurité pour l'infrastructure des identités elle-même.

Comment les équipes en charge de la sécurité et des opérations IT sont-elles en mesure de déterminer l'origine des menaces, de les hiérarchiser et de rapidement atténuer les risques ?

Objectif

Une vue globale et intelligente sur l'ensemble des identités et des accès dans votre parc sur site et multicloud afin d'obtenir une vision plus claire des risques. Profitez de la capacité à identifier les nouveaux vecteurs d'attaque précédemment indétectables dans un environnement cloisonné. Favorisez l'hygiène des identités avec des recommandations exploitables avant qu'elles ne deviennent une menace. Détectez les menaces liées à l'identité et réagissez de façon proactive. Accélérez les enquêtes sur les menaces pour en tirer plus rapidement des conclusions. Comprenez les chaînes d'attaque complexes, les vecteurs d'attaque et le rayon d'action des identités et des comptes compromis. Soyez au fait des renseignements nécessaires pour organiser la réponse optimale à une menace ou à une violation.

Solution

Identity Security Insights de BeyondTrust tire parti de puissantes fonctionnalités du PAM, CIEM et ITDR pour fournir des renseignements exhaustifs sur les menaces liées à l'identité. Cela offre aux équipes IT et de sécurité une visibilité totale sur l'ensemble des identités, des privilèges et des accès, permettant ainsi d'observer leur impact réel sur votre stratégie de sécurité.

Identity Security Insights apporte à la gamme BeyondTrust des niveaux révolutionnaires de renseignements sur les identités et les menaces et rend tous les produits et solutions connectées de BeyondTrust nettement plus performants et puissants.

Obtenez des analyses pertinentes et exploitables dont vos équipes peuvent tirer profit pour immédiatement améliorer votre stratégie de sécurité et éliminer les backdoors ainsi que les points faibles potentiellement dangereux.

Identity Security Insights se combine avec d'autres solutions BeyondTrust et sources de données tierces (y compris Okta, Ping Identity et Microsoft Entra ID / Azure Active Directory) pour exploiter les données corrélées des utilisateurs, des comptes et des privilèges, tout en offrant de puissantes fonctionnalités de détection et de réponse aux menaces liées à l'identité. Appliquez des recommandations guidées, basées sur des renseignements globaux concernant les menaces liées à l'identité, classées par ordre d'importance, afin de garantir un accès à moindre privilège. Aucune autre solution n'offre une vue aussi complète des vulnérabilités basées sur les privilèges et les identités, tout en identifiant les privilèges qui révèlent des chemins d'attaque et des backdoors vers des ressources sensibles.

Les trois principaux cas d'usages

Visibilité unifiée et multiplateforme
Bénéficiez d'une vue globale des identités et des accès sur l'ensemble de votre parc sur site et multicloud, et identifiez des vecteurs d'attaque auparavant invisibles.

Hygiène de sécurité proactive de l'identité
Identifiez les comptes/utilisateurs surprivilégiés et les contrôles de sécurité inefficaces. Tirez parti de recommandations exploitables pour dimensionner correctement les privilèges et atténuer les autres problèmes potentiels avant qu'ils ne deviennent une menace.

Détection des menaces liées à l'identité
Ciblez les anomalies, notamment les événements impliquant plusieurs identités et comptes, et accélérez les enquêtes sur les menaces.

Pour obtenir une checklist complète des fonctionnalités, veuillez vous reporter à l'Annexe 2 : Feuille d'analyse du PAM Buyer's Guide

« Ce que j'apprécie le plus concernant Identity Security Insights est de voir mon Okta. [BeyondTrust] est également le seul en mesure d'accéder à ce genre d'informations pour tous mes employés et mes serveurs.
À part les solutions BeyondTrust, je n'ai pas d'autre outil collectant ce genre d'informations locales. [BeyondTrust] peut me montrer beaucoup de choses que personne d'autre ne peut me montrer. »

Chris Dailey, Manager of Information Security,
Benjamin Moore

En suivant correctement les étapes précédentes, vous répondrez à la plupart de vos besoins PAM, éliminerez ou atténuerez de nombreux vecteurs d'attaque à privilèges, et réduirez fortement votre exposition aux menaces.

Presque chaque technologie émergente ayant la capacité de transformer l'IT s'accompagne de défis pour la sécurité, par exemple la façon de gérer les identités ou les modèles et les privilèges d'authentification. Ces défis présentent les types de failles que les attaquants avisés recherchent et exploitent.

Bien qu'il y ait de nombreux cas d'usages en périphérie que les solutions BeyondTrust peuvent prendre en charge et qui ne sont pas couverts dans ce document, penchons-nous brièvement sur plusieurs aspects importants ayant émergé au cours des dernières années qui présentent des défis uniques.

Gestion de la sécurité des accès et des identités spécialisée et analyses de faisabilité pour le PAM

Dans cette section, découvrez comment BeyondTrust vous aide à relever les défis suivants :

- Sécurité DevOps
- Sécurité pour l'OT (technologie opérationnelle) et les endpoints non traditionnels
- Sécurité de l'automatisation des processus robotiques (RPA)
- Qualification pour cyberassurance
- Mise en place du Zero Trust

DevOps

La plupart des organisations ont adopté de nos jours des pratiques de DevOps. Pourtant, la sécurité est souvent une réflexion après coup, voire une victime, de la vitesse et des outils (souvent en open source) utilisés dans les environnements DevOps.

Bien que le DevOps parvienne à condenser les cycles de développement grâce à l'automatisation et exploite les capacités d'adaptation du cloud, l'inconvénient est qu'il peut également « automatiser l'insécurité », générant des failles d'ampleur sur le plan de la sécurité, de la conformité et des opérations.

Certaines failles courantes liées au DevOps incluent :

- Code non sécurisé, mots de passe codés en dur et autres expositions de privilèges.
- Scripts ou vulnérabilités dans les outils CI/CD, tels qu'Ansible, Chef ou Puppet, pourraient déployer des malwares ou saboter du code.
- Provisionnement excessif de privilèges dans tout le paysage DevOps.
- Partage de secrets.
- Vulnérabilités, mauvaises configurations et autres faiblesses dans les conteneurs.

Bien qu'il soit évident que la sécurité doit être intégrée au DevOps, comment y parvenir sans affecter la vitesse et l'agilité ?

Les solutions BeyondTrust réduisent les risques liés au DevOps et aux CI/CD en renforçant la visibilité et le contrôle sur les secrets et les API, les privilèges admins et les configurations système.

En unifiant ces fonctionnalités dans les cas d'usages sur site, virtuels, dans le cloud ou DevOps, les services IT peuvent atteindre leurs objectifs d'agilité sans recourir à des processus fastidieux.

Les fonctionnalités PAM de BeyondTrust pour la sécurisation des environnements DevOps et CI/CD :

- Inventaires et intégrations automatiques de l'ensemble des workflows automatisés et des ressources DevOps afin d'améliorer la visibilité et le support aux fins d'audit et de conformité.
- Recherche, sécurise et gère de façon centralisée l'utilisation de mots de passe, de secrets, de clés et de certificats codés en dur. Cela inclut un accès développeur au code source, aux outils ou aux applications DevOps, aux scripts, aux serveurs de test et aux versions de production, éliminant ainsi un vecteur d'attaque fréquemment exploité par les cyberattaquants.
- Mise en place du principe de moindre privilège, accordant uniquement les autorisations requises et seulement pour la période nécessaire. Cela permet de générer de façon appropriée des machines et des images, ainsi que de procéder à des opérations de déploiement, de configuration et de remédiation en ce qui concerne les problèmes de production dans les machines et les images.
- Contrôle des applications pour garantir l'utilisation des bons outils et dans le bon contexte, limitant ainsi les risques de mouvements latéraux en cas d'accès d'un cyberattaquant.
- Mise en place des limites entre les systèmes de développement, de test et de production.
- Gestion et audit de toutes les sessions privilégiées, offrant la visibilité si vitale pour les équipes de sécurité, ainsi qu'un support aux fins d'audit et de conformité.

Fonctionnant de concert, les solutions BeyondTrust vous offrent une couverture PAM complète dans votre environnement DevOps, permettant à vos équipes de maintenir la sécurité tout en conservant une agilité de développement optimale.

Technologie opérationnelle, IoT et endpoints non traditionnels

L'Internet des objets (IoT) est devenu la norme dans les entreprises. D'autres endpoints non traditionnels sont également omniprésents aujourd'hui dans la plupart des organisations.

Ces endpoints manquent souvent de fonctionnalités de sécurité de base, disposent souvent d'identifiants par défaut et codés en dur ou intégrés, peuvent comporter un firmware difficile à corriger ou à mettre à jour et sont associés à de nombreux autres risques. Fréquemment, ces dispositifs et ces systèmes n'ont pas été conçus dans le but d'être connectés au réseau d'entreprise. Les systèmes ICS (systèmes de contrôle industriels) et SCADA (acquisition et contrôle des données), qui étaient traditionnellement « hermétiques » pour protéger leurs fonctions critiques tout en garantissant la sécurité des communautés environnantes et de l'environnement, sont de plus en plus connectés et exposés. En outre, de nombreux fournisseurs d'ICS utilisent désormais des technologies IT standard au sein de leurs solutions, les rendant plus vulnérables aux attaques.

Les outils existants n'ont généralement pas la capacité de découvrir, d'intégrer et de gérer en toute sécurité divers types de dispositifs et leur accès, et encore moins à grande échelle. Cela se traduit par des vulnérabilités dangereuses pour la sécurité disséminées dans les environnements OT et IT. Mirai et d'autres botnets, qui ont entraîné des perturbations massives et paralysé certaines entreprises, ne sont qu'un aperçu de ce qui peut résulter de failles dans la sécurité des dispositifs IoT. La compromission de systèmes OT peut endommager de façon catastrophique l'infrastructure et mettre en danger de nombreuses vies humaines.

Comment les organisations peuvent-elles prendre en compte et sécuriser de manière cohérente une quantité toujours croissante d'endpoints non traditionnels, notamment les dispositifs de l'IoT et de l'IoT industriel (IIoT), SCADA, ICS et même les périphériques réseau classiques, tels que les routeurs, les commutateurs et les pare-feu ?

BeyondTrust fut la première entreprise à commercialiser une solution PAM offrant des fonctionnalités de contrôle granulaire et d'audit de l'activité des utilisateurs privilégiés sur les dispositifs réseau, IoT et OT (ICS, SCADA, etc.). BeyondTrust vous permet d'étendre les meilleures pratiques du PAM ainsi que les principes de sécurité Zero Trust vers les systèmes OT et les endpoints non traditionnels.

Les fonctionnalités PAM de BeyondTrust pour améliorer la sécurité de l'OT :

- Détection et intégration de tous les dispositifs pour la gestion.
- Mise en place des meilleures pratiques en matière de gestion des identifiants, telles que l'élimination des identifiants intégrés/codés en dur et la sécurisation des identifiants dans un coffre-fort inviolable et centralisé.
- Suppression des droits admins et application du moindre privilège à granularité fine pour tous les endpoints et tous les accès.
- Sécurisation des accès à distance (pour les employés, fournisseurs, vers/entre les systèmes, etc.) grâce à une solution robuste sans VPN qui se superpose également à l'authentification MFA.
- Activation de la segmentation et de la microsegmentation afin d'isoler les réseaux et les ressources.
- Suivi et enregistrement des sessions afin de fournir une piste d'audit complète de l'activité des utilisateurs.
- Analyse du comportement pour détecter les activités suspectes d'utilisateurs.
- Prise en charge de n'importe quel appareil SSH ou Telnet.
- Compatibilité avec le modèle Purdue et le Zero Trust.

En outre, BeyondTrust vous permet de mettre en œuvre nos technologies dans n'importe quel ordre, ce qui est souvent nécessaire pour les environnements OT.

« La majorité des systèmes auxquels nous accédons ne sont pas des systèmes IT traditionnels. Ce sont des systèmes de contrôle, comme des ascenseurs intelligents, des systèmes de surveillance et des unités de CVC, dans lesquels il n'est pas possible d'installer des logiciels antivirus. Nous avons bien conscience que la gestion des accès à privilèges est l'un des principes les plus importants d'un programme de cybersécurité moderne et un élément essentiel de toute architecture Zero Trust ainsi que de tout cadre solide de sécurité BYOD ».

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

Automatisation des processus robotiques

L'automatisation des processus robotiques (RPA) est une méthode émergente évoluant rapidement visant à utiliser des logiciels robots pour éliminer les tâches banales et routinières qui épuiseraient autrement les ressources IT.

Les contrôles natifs de sécurité RPA sont cependant souvent inadaptés. Par exemple, les ensembles d'outils RPA disposent généralement de droits excessifs, et intègrent ou codent en dur les identifiants afin d'établir rapidement des connexions pour l'automatisation.

BeyondTrust est en mesure d'étendre les bonnes pratiques de gestion des accès à privilèges (PAM) à votre implémentation RPA.

Les fonctionnalités PAM de BeyondTrust pour améliorer la sécurité en matière de RPA :

- Analyse, identification, catégorisation dynamique intégration automatique et profilage de tous les éléments pouvant être inclus dans un workflow RPA et les ressources associées.
- Mise en place des meilleures pratiques pour la gestion des mots de passe, notamment en éliminant les identifiants RPA intégrés ou codés en dur, tout en protégeant l'organisation des exploits automatisés via une API étendue et compatible RPA.
- Assurance que les mots de passe puissent être automatiquement réinitialisés après l'utilisation du RPA pour assurer la sécurité du workflow.
- Application du principe de moindre privilège et un contrôle granulaire dans l'ensemble des processus, ensembles d'outils et workflows RPA.
- Restriction l'accès aux seules applications autorisées.
- Prise en charge et intégration d'un grand nombre d'outils RPA (Blue Prism, UiPath, Pega, etc.).

Qualification pour cyberassurance

Au cours des dernières années, les cyberassureurs ont durci les critères d'admission, augmenté les primes d'assurance et ont même annulé la couverture pour de nombreuses organisations. Cela est dû en grande partie à une augmentation sans précèdent des cyberattaques coûteuses et des paiements de rançons.

Les compagnies de cyberassurances et les assureurs reconnaissent que les contrôles de gestion des accès à privilèges assurent une sécurité fondamentale pour chaque organisation, préviennent de nombreuses cyberattaques et minimisent considérablement les dommages causés par toute violation potentielle.

Privileged Access Management de BeyondTrust peut vous aider à réunir les conditions pour bénéficier d'une cyberassurance et des meilleures primes, tout en réduisant de façon drastique votre exposition aux cyberrisques.

Les solutions PAM offrent des fonctionnalités indispensables, notamment l'application du principe de moindre privilège, la gestion des identifiants et des comptes privilégiés et la sécurisation des accès distants : des critères communs qui déterminent l'approbation d'une police de cyberassurance.

BeyondTrust peut vous aider à répondre aux exigences en matière de sécurité requis pour prétendre à une police de cyberassurance :

- Supprime les droits admins locaux sur les ordinateurs portables et de bureau des utilisateurs et applique le principe du moindre privilège.
- S'assure que tous les comptes humains ou non (y compris les comptes de service) respectent en permanence le principe du moindre privilège.
- Protège, contrôle et audite l'accès à distance des employés et des fournisseurs, en garantissant également que les identifiants utilisés pour l'accès à distance soient gérés et sécurisés.
- Met en place l'authentification MFA pour renforcer la sécurité des accès à distance.
- Fournit une protection mixte pour bloquer ou atténuer les attaques par ransomware.

EN SAVOIR PLUS

Répondre aux exigences de la cyberassurance et profiter des meilleures primes avec BeyondTrust :

Téléchargez : Cybersecurity Insurance Checklist
Visitez : Centre des ressources pédagogiques et des solutions pour la cyberassurance

Protection mixte contre le ransomware par BeyondTrust :
Visitez : Centre des ressources pédagogiques et des solutions pour la protection contre le ransomware

Zero Trust

Le besoin du Zero Trust s'est accentué au cours des dernières années face à l'augmentation de la décentralisation IT, du télétravail et à l'érosion du périmètre réseau.

Les principes et les architectures du Zero Trust visent à éliminer l'approbation persistante, à appliquer l'authentification continue, le principe du moindre privilège et le contrôle d'accès adaptatif. Ils permettent de mettre en place une segmentation et une microsegmentation pour garantir des accès sécurisés. Un objectif clé du Zero Trust est d'avoir en permanence une visibilité sur qui fait quoi et pour quel motif, ainsi que vous offrir l'assurance de contrôler ou limiter toute menace visant le réseau.

Les solutions BeyondTrust permettent une mise en œuvre intelligente et pratique du modèle de sécurité Zero Trust du NIST **sans perturber les processus métiers quotidiens.**

Les solutions BeyondTrust contribuent à la mise en œuvre des sept principes fondamentaux du Zero Trust du NIST en s'efforçant continuellement d'identifier et de sécuriser chaque utilisateur (humain, non humain, employé, fournisseur), ressource et session privilégiés dans l'ensemble de votre environnement numérique. Contrôlez le qui, le quoi, le quand, le pourquoi et le où en ce qui concerne les accès. Mettez en œuvre des contrôles de sécurité Zero Trust pour réduire votre exposition aux attaques, minimiser les périodes sujettes aux menaces et améliorer votre protection contre les ransomwares, les malwares, les menaces persistantes avancées et internes, et bien plus encore.

Fonctionnalités BeyondTrust pour faire progresser le Zero Trust :

- Découvre, dresse l'inventaire et regroupe intelligemment toutes les ressources privilégiées pour éliminer les angles morts, mettre en lumière le shadow IT et contrôler les points d'accès.
- Applique continuellement des contrôles d'accès adaptatifs et Just-In-Time en fonction du contexte.
- Gère et applique les pratiques exemplaires de sécurité des identifiants pour l'ensemble des mots de passe privilégiés, des secrets et des clés de comptes.
- Applique des contrôles du moindre privilège pour dimensionner l'accès de chaque identité et compte - humain, application, machine, employé, fournisseur, etc.
- Implémente une segmentation et une micro-segmentation pour isoler divers actifs, ressources et utilisateurs pour restreindre les mouvements latéraux.
- Sécurise les accès distants avec des fonctionnalités adaptatives et granulaires du privilège allant bien au-delà des VPN, RDP et autres technologies classiques d'accès distant.
- Sécurise les accès à tous les plans de contrôle (cloud, virtuel, DevOps) et aux applications sensibles.
- Gère, surveille et audite chaque session privilégiée.
- Simplifie la gestion sécurisée des identités et l'implémentation du Zero Trust à l'échelle de l'entreprise en étendant les fonctionnalités d'authentification Microsoft Active Directory (AD), de SSO et de gestion de la configuration des stratégies de groupe aux environnements Unix/Linux.

EN SAVOIR PLUS

Pour en savoir plus sur la façon dont BeyondTrust aborde le Zero Trust :

Apprenez à associer les principes Zero Trust du NIST et les fonctionnalités existantes des produits de gestion des accès à privilèges (PAM) et des accès à distance sécurisés. Découvrez les étapes et les architectures de mise en œuvre.

Téléchargez : Faire progresser le Zero Trust grâce à la gestion des accès à privilèges (PAM)

Découvrez comment les solutions BeyondTrust respectent et s'alignent sur les sept principes fondamentaux du modèle Zero Trust du NIST, comment les cas d'usages communs du PAM le respectent également, et plus encore.

Téléchargez : Correspondance entre les fonctionnalités de BeyondTrust et les principes de Zero Trust du NIST (SP 800-207)

Lisez les témoignages de nos clients sur leurs implémentations réussies :

Regardez : Le chemin d'Investec vers le Zero Trust : de la théorie à la pratique

Regardez : Oxford Properties Group - Créer une stratégie de cybersécurité de Zero Trust pour plusieurs sites

Visitez : Centre des ressources pédagogiques et des solutions pour rendre le Zero Trust opérationnel

« Les interactions entre les produits de la suite [de BeyondTrust] ont été brillamment et minutieusement orchestrées de sorte à maximiser notre chance d'aller aussi loin que possible dans le Zero Trust compte tenu de l'offre de produits sur le marché de la sécurité. »

Brandon Haberfeld, Global Head of Platform Security,
Investec

Pour quels motifs choisir un fournisseur unique pour obtenir d'une gestion complète des accès à privilèges ?

Nous croyons que ce qui nous rend différents dans le marché PAM est l'étendue et la profondeur de notre offre de solutions, la facilité d'utilisation de nos produits, la diversité des intégrations tierces disponibles, notre parcours de plusieurs décennies de leadership et d'innovation éprouvés, ainsi que nos équipes.

La différence BeyondTrust

Différenciateur 1 : Étendue, profondeur et flexibilité de notre solution PAM

BeyondTrust offre ce que les experts du marché considèrent comme la variété la plus complète de solutions de gestion des accès à privilèges disponibles. BeyondTrust se démarque en raison de l'étendue et de la profondeur inégalées des cas d'usages PAM couverts, du caractère exhaustif de nos solutions, de notre vision, de nos innovations technologiques et de notre plateforme de gestion centralisée.

Nous avons pensé à tout—Windows, macOS, Unix, Linux, cloud, sur site, humains (employés ou fournisseurs) et machines.

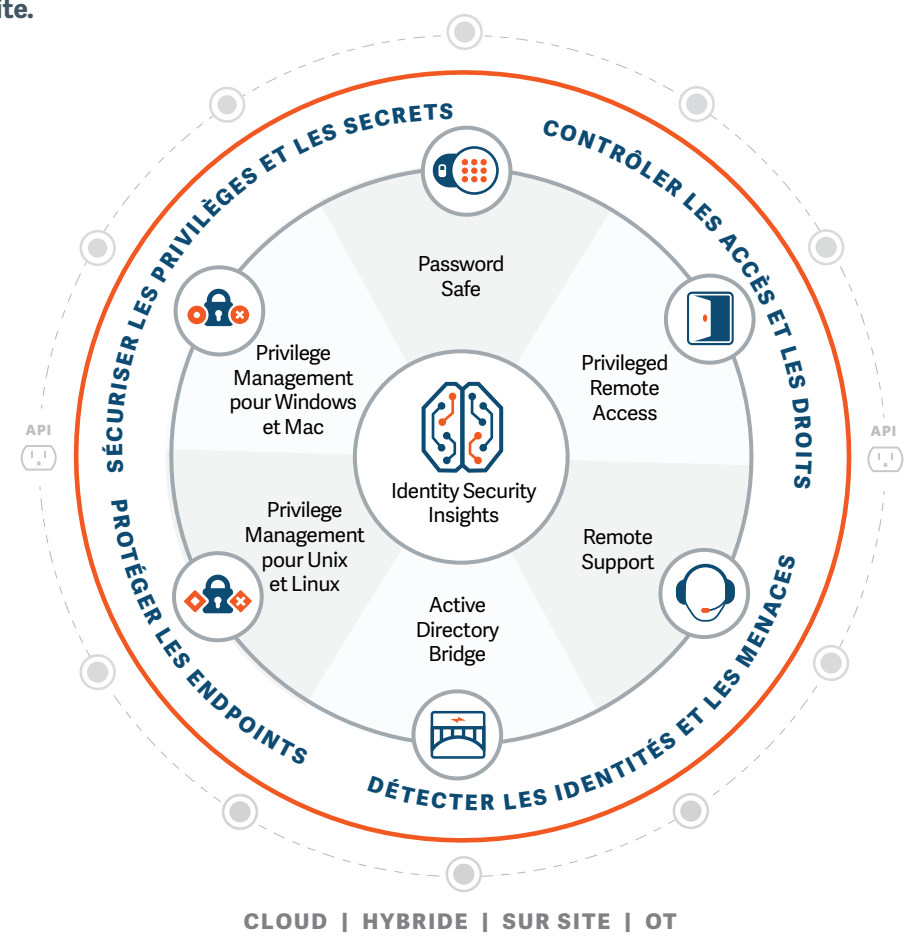
BeyondTrust combine de façon unique trois disciplines - PAM, CIEM et ITDR - pour aider les organisations à renforcer de manière globale leur sécurité des identités et à prendre en compte chaque niveau de privilèges.

À la différence des autres fournisseurs PAM, BeyondTrust ne vous oblige pas à gérer les accès à privilèges « à notre façon ». La plateforme évolutive de BeyondTrust vous permet de déployer un ensemble complet de fonctionnalités PAM en une fois, ou de les mettre en place au fil du temps à votre propre rythme. Vous pouvez commencer par un coffre-fort à mots de passe (Password Safe), mais vous n'êtes pas obligé de le faire. Vous pouvez vous lancer tout aussi simplement avec Privileged Remote Access, AD Bridge, ou Privilege Management pour Windows et macOS ou pour Unix et Linux.

Nous vous offrons aussi le choix du modèle de déploiement qui répond le mieux à vos besoins : appliances dans le cloud, virtuelles ou sur site.

Aucun autre fournisseur PAM n'offre autant d'options de déploiement.

Quel que soit le produit ou le modèle de déploiement choisi, vous commencerez immédiatement à réduire les risques et à améliorer l'administration.



Différenciateur 2 :
Une expérience utilisateur intelligente améliore la productivité et permet de tirer parti des fonctionnalités plus rapidement

Nous faisons en sorte que le PAM fonctionne mieux et plus facilement. BeyondTrust y parvient en se concentrant sur l'expérience utilisateur et sur des fonctionnalités optimisant la productivité qui font la joie de nos clients et leur permettent de gagner rapidement en sécurité et en efficacité opérationnelle.

BeyondTrust s'engage également à fournir une accessibilité numérique, et nous prenons des mesures proactives pour garantir que nos produits adhèrent aux normes des Web Content Accessibility Guidelines (WCAG) 2.0 level AA, une conformité garantie en vertu d'audits tiers et de formations en interne.

Une expérience utilisateur intelligente favorise la facilité d'utilisation et une sécurité de qualité

Chaque trimestre, parallèlement à l'enquête sur notre taux de recommandation (NPS), notre équipe chargée de l'expérience utilisateur recueille des scores d'utilisabilité standardisés pour nos produits. Ces scores sont collectés au moyen d'une version modifiée du questionnaire post-test sur l'utilisabilité du système (PSSUQ), un outil d'évaluation qui a prouvé son efficacité continue des centaines de fois dans des publications scientifiques très respectées, sur une période de 35 ans.

Nos enquêtes ont démontré que nos produits BeyondTrust offrent une utilisabilité de premier plan, et nous aident à continuer de les améliorer.

Nous concevons nos produits en respectant les trois principes suivants menant à une expérience utilisateur de qualité :

Supprime les difficultés
Moins il rencontre de difficultés, plus l'utilisateur est susceptible d'adopter le produit et de l'utiliser efficacement. Nous comprenons qu'il est dans la nature humaine que les personnes (à savoir les utilisateurs) préfèrent éviter les difficultés. Il est important d'appliquer de bonnes pratiques en matière de sécurité !

Minimise les erreurs humaines
L'erreur humaine demeure l'une des causes principales des incidents de sécurité IT, particulièrement dans le cloud. Si l'expérience d'utilisation du produit ou du service est conçue comme il se doit, elle élimine le risque d'erreur. En revanche, si l'expérience est confuse ou n'informe pas clairement l'utilisateur, il est plus probable que celui-ci commette une erreur ou passe à côté de quelque chose de crucial.

Améliore la vitesse
Plus l'expérience d'utilisation est bonne, plus il est probable que les informations importantes, critiques ou urgentes soient remarquées rapidement. Cela signifie que l'utilisateur passe moins de temps à chercher des renseignements.

Nous utilisons nos propres produits et tirons des enseignements de leur utilisation en interne, ainsi que des commentaires externes, afin d'améliorer continuellement l'expérience utilisateur.

Des fonctionnalités uniques pour constater plus rapidement les bénéfices et optimiser la productivité

L'un des avantages du PAM, s'il est utilisé correctement, qui surprend bon nombre de nos utilisateurs est le suivant :

- Améliore la productivité des admins utilisant nos outils
- Sécurise la productivité des utilisateurs, notamment parmi les tiers-mainteneurs
- Renforce l'efficacité opérationnelle à tous les échelons de l'entreprise

Par exemple, le démarrage d'une session privilégiée avec BeyondTrust est plus rapide et plus simple qu'avec les outils concurrents, et garantit la mise en place des contrôles de sécurité et d'audit les plus robustes.

Privilege Management pour Unix et Linux procure non seulement une sécurité et un contrôle d'audit bien supérieurs à ceux de sudo et d'autres outils, mais offre également de puissantes fonctionnalités de gestion centralisée qui rendent son utilisation bien plus facile, en particulier à grande échelle.

Privilege Management pour Windows et Mac procure des modèles QuickStart qui permettent aux organisations d'appliquer des contrôles du moindre privilège en quelques minutes ou quelques heures, et non en plusieurs semaines ou mois.

Password Safe permet aux organisations de détecter automatiquement, d'intégrer et d'appliquer les meilleures pratiques de sécurité parmi tous les types de comptes et d'identifiants à privilèges (mots de passe, clés, secrets, etc.) grâce aux Smart Rules, notre mécanisme d'automatisation leader sur le marché.

Nous n'exigeons pas non plus de services professionnels pour les mises à jour et n'annulons pas un accord de support si ceux-ci ne sont pas utilisés.

« La sécurité doit être fluide, faire partie du flux normal. Elle ne doit pas arrêter un utilisateur dans son travail. Pour que la sécurité demeure, elle doit être conçue efficacement, à défaut de quoi vous risqueriez d'introduire davantage de risques par inadvertance. »

Angela Duggan, VP of User Experience,
BeyondTrust

EN SAVOIR PLUS

BeyondTrust et l'expérience utilisateur :

Blog : Comment tirer parti de l'expérience utilisateur pour défragmenter votre solution de sécurité

Blog : Une expérience utilisateur de qualité conduit à une sécurité de même calibre

Blog : L'engagement de BeyondTrust envers l'accessibilité numérique

Différenciateur 3 : Innovateurs en matière de sécurité, nous révolutionnons le PAM et la sécurité des identités

BeyondTrust est reconnu par les analystes en tant que leader du PAM, non seulement en raison de l'excellence de nos produits et de l'exhaustivité de nos solutions, mais aussi pour nos innovations. Nous pensons mériter cette reconnaissance. BeyondTrust a un parcours de plusieurs décennies marquées par les innovations et a fait figure de pionnier en ce qui concerne de nombreuses fonctionnalités PAM indispensables qui en sont l'essence même aujourd'hui. **Nous ne nous arrêterons pas là.**

Nos solutions de sécurisation de l'accès à distance pour les employés et les fournisseurs ont été lancées des années avant celles de la concurrence. Cela s'explique probablement par le fait que nous avons soutenu le télétravail et le travail hybride au profit de nos employés bien avant que cela ne devienne courant.

D'autres fournisseurs essaient toujours de nous rattraper alors que nous continuons de rendre nos fonctionnalités d'accès à distance sécurisé encore plus robustes et faciles à utiliser.

Pour certaines des innovations de BeyondTrust, dont beaucoup sont brevetées :

- Nous avons été les premiers à proposer une solution basée sur le principe du moindre privilège pour Microsoft Windows.
- Nous avons été les premiers à proposer une solution basée sur le principe du moindre privilège pour Apple macOS.
- Nous avons lancé la première solution de gestion des privilèges pour endpoints. Cette dernière intègre un mécanisme intelligent antipiratage capable de protéger notre logiciel et nos paramètres de configuration basés sur le principe du moindre privilège contre une modification par des processus dotés de droits accrus, tout en permettant à la solution d'être administrée par de véritables administrateurs système.
- Nous avons été les premiers à intégrer une solution d'accès à distance qui propage véritablement les meilleures pratiques en matière de PAM et de sécurisation des accès aux fournisseurs et aux employés travaillant à distance.

BeyondTrust a fait figure de pionnier en introduisant pour la première fois sur le marché de nombreuses innovations majeures pour la gestion des accès à privilèges sous Unix/Linux, notamment :

- Technologie d'audit et de contrôle avancés (ACA) qui inspecte les activités au sein des scripts, contrôle les accès aux dossiers et aux fichiers (y compris au niveau root), et bloque les programmes compromis et malveillants.
- Services de noms de registres (Registry Name Services) qui fournissent des fonctions de reprise en séquence et d'équilibrage de charge automatisées, une gestion centralisée basée sur des rôles ainsi que la possibilité de créer des groupes de clients partageant une configuration ou une stratégie en fonction du rôle ou de l'organisation de l'entreprise.
- Contrôle de l'intégrité des fichiers qui s'assure que les « choses » dont vous autorisez l'élévation de droits, et les processus effectuant l'élévation, n'ont pas été compromis.

BeyondTrust est le premier (et le seul) fournisseur de produits à combiner le PAM traditionnel avec la gestion des droits relatifs à l'infrastructure cloud (CIEM) et des fonctions de détection et de réponse aux menaces liées à l'identité (ITDR). Ces fonctionnalités permettent d'atteindre une visibilité holistique, ainsi que des capacités de prévention, de détection et de remédiation dans un monde informatique hybride et de travail nomade.

Nous proposons aussi la première solution PAM à offrir une gestion des identifiants de niveau entreprise associant la gestion des secrets DevOps dans un outil unique, sans frais supplémentaires pour les clients.

Aujourd'hui, BeyondTrust continue d'ouvrir la voie grâce à notre vision et à notre roadmap ambitieuses.

Nous cherchons à répondre de façon proactive aux besoins émergents et futurs de nos clients en lançant notre solution révolutionnaire Identity Security Insights, ainsi qu'en améliorant nos solutions existantes. Cette volonté leur permet de demeurer en permanence les meilleures de leur catégorie en termes de fonctionnalités, de capacités et d'utilisabilité.

Différenciateur 4 : Intégrations et interopérabilité

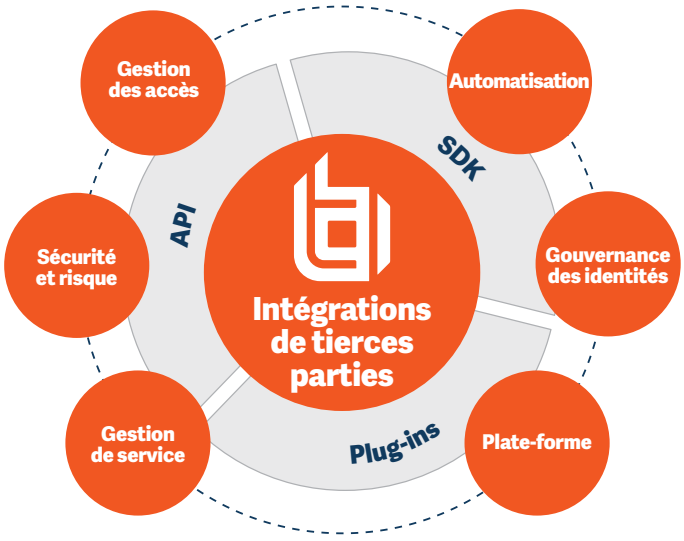
Les solutions et les plateformes de BeyondTrust sont conçues judicieusement pour rendre les intégrations avec des outils tiers importants aussi harmonieuses et complémentaires que possible. Nous savons pertinemment que vous n'avez pas besoin d'une autre solution de sécurité cloisonnée.

BeyondTrust vous dote d'une compréhension complète de l'environnement moderne des menaces en prenant en compte à la fois les risques externes et internes. Nos solutions intègrent des données pertinentes concernant la sécurité - y compris les exploits, les activités à privilèges risquées, les systèmes et applications vulnérables, les exigences de conformité et les atténuations - pour aider nos clients à prendre des décisions en étant mieux informés pour assurer leur protection. Les solutions BeyondTrust recueillent aussi des informations importantes qui peuvent être partagées avec vos autres outils et systèmes IT et de sécurité.

Intégration de l'écosystème

Exemple d'intégrations BeyondTrust avec des technologies tierces

Vous pouvez en savoir plus sur notre fructueux écosystème de partenaires technologiques en visitant notre page Alliances technologiques.



Différenciateur 5 : Leader reconnu par les analystes et plébiscité par les clients dans le secteur du PAM

Que pensent les meilleurs analystes au sujet de Privileged Access Management ?

BeyondTrust a été reconnu comme leader en matière de gestion des accès à privilèges et de gestion des identités privilégiées dans les rapports d'analystes indépendants les plus récents de Gartner, Forrester Research et KuppingerCole.

2023 Gartner® Magic Quadrant™ for Privileged Access Management
2023 KuppingerCole Leadership Compass: Privileged Access Management
The Forrester Wave™: Privileged Identity Management, T4 2020

20 000 clients dans plus de 100 pays choisissent BeyondTrust.

Année après année, les meilleurs analystes du marché nous considèrent comme un leader du PAM. Mais le fait d'être reconnus par nos clients nous rend encore plus fiers.

BeyondTrust a eu l'honneur d'être distingué en tant que le choix des clients dans l'étude Gartner Peer Insights pour le Privileged Access Management pour la deuxième année consécutive. En outre, BeyondTrust a été désigné comme le choix des clients 2023 dans l'étude Gartner® Peer Insights™ pour le Remote Desktop Software.

Vous pouvez consulter ce que nos clients pensent de nous sur la plateforme Gartner Peer Insights, où nous avons recueilli plus de 450 scores à cinq étoiles de leur part.

Différenciateur 6 : Expérience avérée et présence mondiale de BeyondTrust

Plus de 20 000 clients font confiance aux solutions BeyondTrust, qui sont soutenues par nos plus de 1 500 employés répartis dans plus de 20 pays et par un vaste réseau mondial de partenaires.

Nous comprenons que chaque client a des besoins et des exigences uniques. Avec plus de 1 000 partenaires partout dans le monde, nous disposons du réseau et de l'expertise nécessaire pour fournir des solutions sur mesure répondant à ces besoins. Nous cherchons proactivement à conclure des partenariats avec des organisations dotées des capacités, de l'expertise et du savoir-faire appropriés pour nous offrir à nos clients les solutions et l'expérience qu'ils attendent, et plus encore.

Avec des milliers de déploiements réussis dans divers cas d'usages et industries satisfaisant aux exigences réglementaires en matière de sécurité et de conformité dans le monde entier, BeyondTrust dispose de l'équipe la plus efficace pour vous aider à atteindre vos objectifs en matière de PAM et de sécurisation des identités.

75 %
du Fortune 100

95 %
taux de fidélisation

55
Taux de recommandation leader sur le marché

95 %
de clients satisfaits de l'expérience utilisateur

« Le soutien dont nous avons bénéficié a été phénoménal, tant au niveau du support technique que de leur engagement envers notre succès. J'aurais lancé ce projet bien plus tôt si j'avais su à quel point c'était si simple avec BeyondTrust. »

Chris Stucker, Associate IAM Director,
University of Utah

Différenciateur 7 : Nos équipes

C'est un fait, nous sommes recommandés par les analystes et les clients. Mais nous le sommes aussi par nos employés, qui sont à la base de la réussite de notre entreprise, jour après jour.

Notre environnement de travail fait en sorte que nos employés célèbrent et recommandent continuellement BeyondTrust. Chaque année, nous sommes reconnus comme étant une entreprise où les employés s'épanouissent le mieux. Fortune Magazine et Great Place to Work nous classent au 22e rang des meilleurs environnements de travail dans le secteur technologique (grandes entreprises).

97 %

des employés BeyondTrust indiquent leur satisfaction d'y travailler

/

57 %

des employés dans une entreprise américaine typique

SOURCE
Great Places to Work®,
Étude mondiale sur l'engagement des employés

Reconnaissances récentes de BeyondTrust en tant que lieu de travail où la culture d'entreprise et l'expérience des employés sont exceptionnelles

Inc. Magazine Best Workplaces 2022
Fortune Magazine Best Workplaces in Technology™ 2022
Fortune Magazine Best Workplaces for Women™ 2022
Fortune Magazine Best Workplaces for Parents™ 2022
Great Place to Work Best Workplaces™ in Tech UK 2022
Nova Scotia's Top Employer 2022, par Mediacorp Canada Inc.

Maintenir un environnement de travail sain, productif et épanouissant est la pierre angulaire de notre succès. Cela se reflète dans les produits de haute qualité que nous commercialisons, nos innovations continues et la satisfaction de nos clients, comme le prouvent des enquêtes, des évaluations sur des sites tiers et plus encore.

Soyons honnêtes—Le PAM et la sécurisation des identités sont parfois difficiles.

Votre environnement et vos priorités évoluent probablement. En ce qui concerne les entreprises du secteur numérique, il n'y a jamais un moment dans la journée où le cyberrisque n'est pas présent et où les pirates ne sont pas en train d'affûter leurs armes.

BeyondTrust est votre partenaire de confiance.

Nos équipes sont prêtes à vous aider à comprendre cet environnement et à vous montrer comment atteindre au mieux vos objectifs.

Étapes suivantes de votre parcours vers le PAM et la sécurisation des identités

Ce document a défini les fonctionnalités requises pour une solution complète de gestion des accès à privilèges. Cette solution va bien au-delà du PAM traditionnel pour intégrer la gestion des droits relatifs à l'infrastructure cloud (CIEM) et les fonctionnalités de détection et de réponse aux menaces liées à l'identité (ITDR). Ces fonctionnalités sont nécessaires à la survie dans un monde où les niveaux de privilèges, les accès distants et les attaques sophistiquées et véloces, telles celles tirant parti de l'IA, prolifèrent.

BeyondTrust sera à vos côtés en tant que conseiller de confiance dans votre parcours vers le PAM. Nous disposons de l'expérience et de l'expertise qui vous aident à comprendre comment les solutions et fonctionnalités du PAM peuvent répondre aux besoins de votre entreprise.

Nous vous présentons deux modèles dans l'annexe de ce document. Le premier peut vous aider à effectuer une analyse interne en ce qui concerne l'adoption du PAM. Il vous servira à procéder à un alignement au sein de votre organisation, ainsi qu'avec votre fournisseur PAM. Procéder ainsi peut contribuer à accélérer les approbations internes d'un projet PAM et à vous mettre sur la bonne voie. Le second vous aidera à évaluer les fournisseurs PAM, y compris BeyondTrust, en comparant différentes fonctionnalités importantes de gestion des accès à privilèges.

Pourquoi devriez-vous devenir partenaire de BeyondTrust ?

BeyondTrust offre une valeur inestimable aux clients grâce à notre ensemble de solutions intégrées. **Le résultat ?** Une réduction des coûts, de la complexité et des failles résultant de l'utilisation d'outils compartimentés.

- BeyondTrust est le seul fournisseur à répondre aux besoins de tous les cas d'usages du Privileged Access Management. Notre solution exhaustive comprend des fonctionnalités importantes qu'aucun autre fournisseur ne propose.
  Nos fonctionnalités nouvelle génération étendent votre champ de vision sur les chemins qu'empruntent les menaces à base de privilèges et aux chaînes d'attaques basées sur l'identité, au-delà de ce que d'autres solutions peuvent fournir.
- L'étendue de nos solutions et la flexibilité de nos offres vous permettent d'appréhender les scénarios de menaces actuels tout en vous préparant aux éventualités de demain.
- Vous pouvez choisir le modèle de déploiement qui répond le mieux à vos besoins – notamment des appliances dans le cloud, virtuelles ou sur site. Aucun autre fournisseur PAM ne vous offre autant de choix.
- BeyondTrust maximise votre ROI pour la sécurité, car nous faisons de vos besoins une priorité et ne facturons pas de frais supplémentaires pour des fonctionnalités que nous considérons comme essentielles.
- Nous habilitons et soutenons nos équipes de sorte que nous puissions réussir tous ensemble.

Atteignez vos objectifs en matière de sécurité avec BeyondTrust

Prévenir les violations

- Réduire la surface d'attaque
- Éviter les attaques de ransomware
- Protéger les accès à privilèges et supprimer les droits admins
- Éliminer les privilèges excessifs
- Sécuriser les applications critiques et mettre en place un contrôle applicatif

Gagner en efficacité

- Simplifier les workflows IT
- Automatiser les tâches à privilèges
- Intégrer dans l'écosystème existant
- Tirer parti des investissements existants

Atteindre la conformité

- Appliquer le principe du moindre privilège
- Répondre aux exigences réglementaires, du Zero Trust et de la protection des données
- Accorder des autorisations granulaires
- Suivre et enregistrer toutes les activités à privilèges
- Tirer parti d'une piste d'audit centralisée

Optimiser et protéger l'activité

- Obtenir une visibilité sur tous les accès distants et à privilèges
- Éliminer les VPN pour les utilisateurs privilégiés
- Implémenter des contrôles d'accès Just-in-Time
- Activer des fonctions de diagnostic et de dépannage pour le service support

BeyondTrust

BeyondTrust est le leader mondial de la gestion intelligente des identités et de la sécurisation des accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique. Nous sommes à la pointe de l'innovation en matière de sécurisation des identités et bénéficions de la confiance de 20 000 clients, dont 75 font partie du classement Fortune 100, ainsi que d'un écosystème mondial de partenaires.

Pour en savoir plus, rendez-vous sur www.beyondtrust.com/fr

Annexe 1 : Modèle de fiche de travail pour une analyse de faisabilité du PAM

Quelles métriques essayons-nous d'améliorer/changer pour ce projet ? (quantifier la réussite)	
Pourquoi cherchons-nous à atteindre ce résultat maintenant et pas antérieurement ?	
À quelle stratégie commerciale plus globale cette initiative est-elle liée ? (sécurité, conformité, cyberassurance, Zero Trust, excellence opérationnelle, etc.)	
Quels sont les KPI de gestion que ce projet soutient ?	
Quelle unité commerciale sera chargée de piloter ce programme/projet ?	
Comment ce danger pour la sécurité est-il évalué en ce qui concerne le niveau de risque opérationnel ? (négligeable, faible, moyen, élevé, grave, très grave)	
Comment ce risque de sécurité est-il évalué s'agissant de la probabilité qu'il se manifeste ? (très improbable, peu probable, probable, très probable, presque certain, certain)	
Quel est le résultat commercial spécifique/mesurable que le changement apportera ?	
Coût de l'inaction – Que perdons-nous si nous ne réagissons pas face à ce problème ? (mesurer le risque et l'impact)	
Comment cette initiative est-elle financée ?	
Quelles solutions sont envisagées ?	
Quel processus de gouvernance décisionnelle ce projet adoptera-t-il ?	
Description des « pressions indiscutables »/du calendrier des mesures ?	
Risques associés à ce projet ? (internes, externes)	
Quelles métriques essayons-nous d'améliorer/changer pour ce projet ? (quantifier la réussite)	

Annexe 2 : Votre PAM Buyer's Guide faisabilité du PAM

Fonctionnalités supérieures de gestion des identités, des comptes et des identifiants à privilèges	BeyondTrust	Fournisseur A	Fournisseur B
Effectue une détection et un profilage complets du réseau et du cloud avec une intégration automatisée des identités et des comptes privilégiés de tous types - y compris les comptes admins partagés, d'utilisateur, d'application et de service ; les clés SSH, les comptes de base de données ; les identités et les comptes cloud (Entra ID / Azure AD, etc.) ; les comptes de réseaux sociaux ; les comptes machines ; les secrets DevOps ; les clés d'API et les identifiants d'automatisation des processus robotisés (RPA). Cela inclut aussi les identités et les comptes de fournisseurs.	✔		
Indique où et comment les mots de passe privilégiés sont utilisés, révélant les angles morts et les mauvaises pratiques en matière de sécurité, notamment les mots de passe par défaut, partagés et/ou intégrés, l'utilisation du même compte admin pour plusieurs comptes de service, la réutilisation de clés SSH sur plusieurs serveurs, etc.).	✔		
Gère et audite l'accès aux applications métiers des employés, avec des dossiers sécurisés et un plug-in de navigateur qui indique automatiquement les noms d'utilisateur et les mots de passe.	✔		
Gère les identifiants sur chaque plateforme (Windows, Unix, Linux, Cloud, sur site, etc.), répertoire, périphérique matériel, application, service/daemon, pare-feu, routeur, etc.	✔		
Centralise, sécurise et chiffre tous les identifiants à privilèges dans une banque ou un coffre-fort inviolable. Idéalement, la solution prend en charge les algorithmes de chiffrement standard de l'industrie, tels que AES 256.	✔		
Crée dynamiquement des ensembles d'autorisations selon les données récupérées lors des analyses.	✔		
Met en place des appels d'API pour éliminer les identifiants intégrés ou codés en dur dans les fichiers, applications, scripts et autres codes.	✔		
Automatise la rotation des mots de passe, des clés SSH et d'autres secrets selon un calendrier défini, notamment après chaque utilisation pour les comptes les plus sensibles ou pour ceux confrontés à une compromission ou à un risque de sécurité accrus.	✔		
Applique votre politique de gestion des mots de passe privilégiés, y compris la complexité, le caractère unique (différents mots de passe pour chaque ressource, compte, etc.), l'expiration, la rotation, l'injection et l'extraction des mots de passe, y compris l'élimination de ceux par défaut et d'autres règles.	✔		
Automatise les workflows tout au long du cycle de vie de la gestion des mots de passe.	✔		
Procure un contrôle d'accès granulaire.	✔		
Offre une meilleure sécurité pour l'authentification SSO et ne divulgue jamais le mot de passe à l'utilisateur final.	✔		
Effectue une surveillance et une gestion rigoureuses des sessions pour garantir un « audit propre » de toutes les activités privilégiées et pour mettre en pause ou bloquer immédiatement les sessions suspectes jusqu'à ce que leur légitimité soit déterminée.	✔		
N'exige aucun outil tiers supplémentaire ni Java pour la gestion de session, utilise à la place des outils natifs (MSTSC, PuTTY).	✔		
Permet l'application d'un véritable principe du moindre privilège en tirant parti d'un modèle de sécurité « just-enough » (rien que le nécessaire) et « just-in-time » (uniquement pour la période requise).	✔		
Tire parti des normes de l'industrie, comme SAML et RADIUS, pour une intégration avec toute solution d'authentification MFA.	✔		
Offre des options « bris de glace » pour extraire un mot de passe en cas d'urgence.	✔		
Met à profit un entrepôt de données et une analyse des menaces dans l'ensemble du paysage des privilèges.	✔		
Fournit une solution unifiée et complète pour gérer les identités humaines (utilisateurs privilégiés) et non humaines (application, machine, compte de service, etc.) qui inclut la surveillance/gestion des sessions, sans nécessiter des interfaces multiples/différentes ou une facturation distincte pour chacune d'elles.	✔		
Rend possible une automatisation des tâches privilégiées pour réduire le risque posé par l'automatisation des tâches répétitives à plusieurs étapes.	✔		
Procure des fonctionnalités de reporting et d'analyse étendues à l'équipe SOC et une visibilité aux managers sur la gestion des identifiants à privilèges.	✔		
Instaure une prise en charge des audits et de la conformité de niveau entreprise en procurant des pistes d'audit claires et distinctes pour toutes les activités impliquant des identifiants sous gestion.	✔		

Principales fonctionnalités de Privileged Remote Access

	BeyondTrust	Fournisseur A	Fournisseur B
Applique le principe du moindre privilège en accordant aux utilisateurs autorisés un accès « just-enough » pour réaliser des activités « just-in-time » pour les sessions distantes.	✔		
Contrôle et surveille les sessions au moyen de protocoles standard pour les connexions RDP, VNC, http/s et SSH.	✔		
Permet un accès granulaire à des systèmes spécifiques, ce qui améliore la sécurité et élimine les accès « all-or-nothing » (tout ou rien).	✔		
Offre à l'utilisateur la possibilité d'injecter des identifiants directement dans la session d'accès, celui-ci n'ayant jamais besoin de connaître ou de voir l'identifiant (y compris pour les comptes dont l'authentification MFA est activée durant une session d'accès en Jump Web).	✔		
Crée une piste d'audit pour fournir une visibilité sur l'activité des fournisseurs sur votre réseau et respecter les exigences de conformité en contrôlant les chemins d'accès aux réseaux IT utilisés par les fournisseurs.	✔		
Gère les accès à privilèges à l'infrastructure et aux ressources de l'entreprise qui utilisent des consoles de gestion basées sur le Web, y compris des serveurs IaaS, des environnements d'hyperviseur et des interfaces de configuration Web pour l'infrastructure réseau principale.	✔		
Rend possible des intégrations harmonieuses et prêtes à l'emploi avec ITSM, SIEM, SCIM et Password Management, ainsi qu'avec d'autres solutions logicielles d'entreprise classiques.	✔		
Permet la MFA ainsi que d'autres méthodes d'authentification alternatives telles que TouchID ou FaceID.	✔		
Tire parti des normes du marché, comme SAML et RADIUS, pour une intégration avec tout outil d'authentification MFA.	✔		

Principales fonctionnalités de gestion des privilèges pour Windows et macOS

	BeyondTrust	Fournisseur A	Fournisseur B
Met en œuvre un véritable principe du moindre privilège en supprimant les droits administratifs locaux existants pour les utilisateurs de serveur et de postes de travail, le tout en permettant une élévation des privilèges dynamique et Just-in-Time des privilèges pour des applications et des tâches spécifiques.	✔		
Applique un contrôle applicatif puissant, permettant de décider quelles applications les utilisateurs peuvent installer ou exécuter, avec la flexibilité de définir des règles générales ou granulaires au moyen d'un processus opérationnel peu gourmand en ressources.	✔		
Met en place des restrictions basées sur des règles lors de l'installation d'un logiciel, de l'utilisation et de changements de la configuration du système d'exploitation.	✔		
Définit des règles via Active Directory Group Policy et Web Services avec la prise en charge de systèmes hermétiques et de ressources hors domaine.	✔		
Élimine les installations de logiciels non autorisés, les mesures de contournement ou les failles pouvant mener à un exploit.	✔		
Produit des rapports sur le comportement des utilisateurs privilégiés, notamment les applications installées ou exécutées, les modifications du système et de la configuration, ainsi que celles apportées aux fichiers de données ou de règles critiques.	✔		
Fournit une piste d'audit unique et irréprochable pour toutes les activités d'utilisateurs qui simplifie l'atteinte de la conformité et rationalise les investigations forensiques.	✔		
Simplifie les opérations en éliminant la nécessité pour les utilisateurs finaux d'avoir deux comptes.	✔		
Permet un contrôle granulaire des accès et des autorisations des API, étendant le principe du moindre privilège aux comptes d'API.	✔		
Fournit une technique permettant d'utiliser de véritables privilèges de domaine ou locaux lorsque nécessaire.	✔		
Centralise la gestion, les règles, le reporting et l'analyse dans une seule solution rationalisée.	✔		
S'intègre à la sécurisation des identités, à l'ITSM, au SIEM et à d'autres outils de gestion des privilèges afin d'améliorer et d'intégrer la pile technologique de sécurité existante, en améliorant les flux de travail et en permettant une compréhension plus complète des risques.	✔		

Principales fonctions de gestion des privilèges pour Unix et Linux	BeyondTrust	Fournisseur A	Fournisseur B
Applique le principe du moindre privilège et élimine l'utilisation au niveau root sans affecter la productivité des utilisateurs.	✔		
Met en place une administration Just-in-Time (JIT) avec la capacité d'affecter des privilèges dynamiques aux comptes et aux ressources, tout en veillant à ce que les identités disposent uniquement des privilèges appropriés, pour la durée et au moment requis.	✔		
Exécute des fonctions de contrôle et d'audit granulaires des applications, des commandes, des fichiers et des scripts, en offrant une protection contre les menaces malveillantes et les erreurs involontaires.	✔		
Enregistre et indexe toutes les sessions pour une détection rapide durant les audits.	✔		
Applique de façon adaptative un enregistrement complet de la frappe clavier pour les sessions les plus sensibles.	✔		
Fournit une vue claire et une piste d'audit « propre » sur qui fait quoi et où.	✔		
Consolide les logs d'audit et centralise le reporting pour tous les domaines de serveurs.	✔		
Prend en charge un module d'authentification enfichable pour permettre l'utilisation de systèmes d'authentification standard.	✔		
Met à disposition un langage de règles puissant et flexible afin d'offrir un chemin de migration en abandonnant sudo.	✔		
Provisionne et déprovisionne les privilèges en toute transparence, assurant la conformité et la satisfaction.	✔		
Inclut une fonction de surveillance de l'intégrité des fichiers pour les protéger les fichiers ainsi que les programmes critiques contre une altération.	✔		
Procure une API REST pour faciliter l'intégration avec des produits tiers.	✔		
Permet une prise en charge étendue de nombreuses plateformes Unix et Linux.	✔		
Intègre l'ensemble des règles, rôles et données de log via une console basée sur le Web.	✔		
Met à profit un entrepôt de données et une analyse des menaces dans l'ensemble du paysage des privilèges.	✔		
S'intègre à la sécurisation des identités, à l'ITSM, au SIEM et à d'autres outils de gestion des privilèges afin d'améliorer et d'intégrer la pile technologique de sécurité existante, en améliorant les flux de travail et en permettant une compréhension plus complète des risques.	✔		

Principales fonctionnalités d'Active Directory Bridge	BeyondTrust	Fournisseur A	Fournisseur B
Offre un mécanisme d'authentification SSO pour toute application d'entreprise prenant en charge Kerberos ou LDAP.	✔		
Met à disposition un ensemble d'outils unique et familier pour la gestion des systèmes Windows et Unix/Linux (par exemple : utilisateurs et ordinateurs Active Directory ou ADUC).	✔		
Permet aux utilisateurs d'utiliser leurs identifiants Active Directory pour accéder aux environnements Unix et Linux, consolidant divers annuaires de fichiers de mots de passe, NIS et LDAP dans Active Directory, et supprimant le besoin de gérer les comptes d'utilisateurs séparément.	✔		
S'intègre avec les services Linux et Unix via PAM et Kerberos (Samba, NFS, Apache, etc).	✔		
Ajoute des systèmes Linux et Unix au réseau sans devoir modifier le schéma Active Directory.	✔		
Fournit un framework pluggable avec une interface similaire à la console de gestion Microsoft dans Linux.	✔		
Prend en charge une grande variété de plateformes Unix et Linux, y compris CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, SUSE, RedHat, Solaris, Ubuntu et des architectures telles que x86_64, SPARC, PPC, PPCLE et s390.	✔		
Assure la conformité avec SOX, PCI, HIPAA et d'autres réglementations.	✔		
Tire parti des normes du marché, comme SAML et RADIUS, pour une intégration avec tout outil d'authentification MFA.	✔		

Principales fonctionnalités de visibilité sur la sécurité des identités et de renseignements sur les menaces	BeyondTrust	Fournisseur A	Fournisseur B
Fournit une vision centralisée et holistique des identités et des accès pour l'ensemble de votre parc multicloud et sur site.	✔		
Procure une représentation claire et simple à comprendre des comptes, des privilèges et des accès associés à chaque identité.	✔		
Identifie les privilèges problématiques et les droits multicloud et vous aide à les redimensionner.	✔		
Repère les mauvaises configurations potentielles en matière de sécurité et vous aide à en atténuer les risques de façon proactive.	✔		
Identifie les comptes surprivilégiés et ceux dont les privilèges présentent des risques élevés, les comptes inactifs ou orphelins, les identités partiellement révoquées et d'autres problèmes de sécurité.	✔		
Détecte les activités suspectes et vous alerte, y compris les événements impliquant plusieurs identités et comptes.	✔		
Met en évidence les risques liés à l'identité et leur donne un sens, y compris le rayon d'action potentiel de chaque compte et de chaque identité, ce qui vous permet de prendre des mesures décisives.	✔		
Met en corrélation les données de bas niveau provenant d'une variété de solutions tierces pour révéler les utilisateurs et les ressources à haut risque et identifier les menaces critiques.	✔		
S'intègre avec d'autres solutions pour déverrouiller les fonctionnalités de détection et de réponse aux menaces liées à l'identité (ITDR), permettant une orchestration rapide des réponses pour la sécurité afin de bloquer ou d'atténuer les menaces.	✔		
Produit des rapports sur la conformité, le benchmarking, l'analyse des menaces, les scénarios envisageant toutes les éventualités et plus encore.	✔		