Guide de l'acheteur pour une gestion complète des accès privilégiés (PAM)

BeyondTrust

TABLE DES MATIÈRES

01 **COMMENT UTILISER CE GUIDE DE L'ACHETEUR** 3

02 **LA GESTION COMPLETE DES PRIVILEGES EN SEPT ETAPES** 5

01: Intensifier la responsabilité et le contrôle des mots de passe à privilèges..... 6

02: Instauration du moindre privilège et contrôle des applications pour Windows et Mac... 9

03: Accès à distance sécurisé des fournisseurs et employés..... 11

04: Implémentation du principe de moindre privilège et audit des accès des environnements de serveurs Unix et Linux..... 13

05: De meilleures décisions de privilèges fondées sur le risque au niveau de l'utilisateur, de l'actif et de l'application..... 15

06: Unification et centralisation de la gestion des privilèges, des règles, du reporting et de l'analyse des menaces..... 16

07: Intégration d'Unix, Linux et macOS à Windows..... 18

PAM pour les cas d'usage émergeants..... 20

03 **CE QUI DISTINGUE BEYONDTRUST** 23

Differenciateur N°1 : Richesse, profondeur et flexibilité de notre plateforme PAM..... 23

Differenciateur N°2 : Précurseur de la sécurité – Révolutionne le PAM..... 24

Differenciateur N°3 : Intégrations et interopérabilité avec les solutions de tiers pour mieux rentabiliser les investissements de sécurité..... 25

Differenciateur N°4 : Leader PAM reconnu..... 26

Differenciateur N°5 : Grande expérience et présence mondiale..... 27

04 **PROCHAINES ETAPES DE VOTRE PARCOURS PAM** 27

05 **ANNEXE : MODELE DE GUIDE DE L'ACHETEUR DE SOLUTIONS PAM** 30

COMMENT UTILISER CE GUIDE

Les privilèges sont partout : dans les systèmes d'exploitation, les systèmes de fichiers, les applications, les bases de données, les hyperviseurs, les plateformes de gestion cloud, les outils DevOps, les processus d'automatisation robotisée, etc. Les cybercriminels se tiennent à l'affût des privilèges/accès privilégiés car c'est le moyen d'accéder rapidement aux cibles les plus sensibles d'une entreprise. Une fois qu'ils détiennent des identifiants privilégiés et qu'ils ont obtenu les droits d'accès, les vecteurs de menace ou malwares se muent en menaces internes.

La surface d'attaque s'agrandit

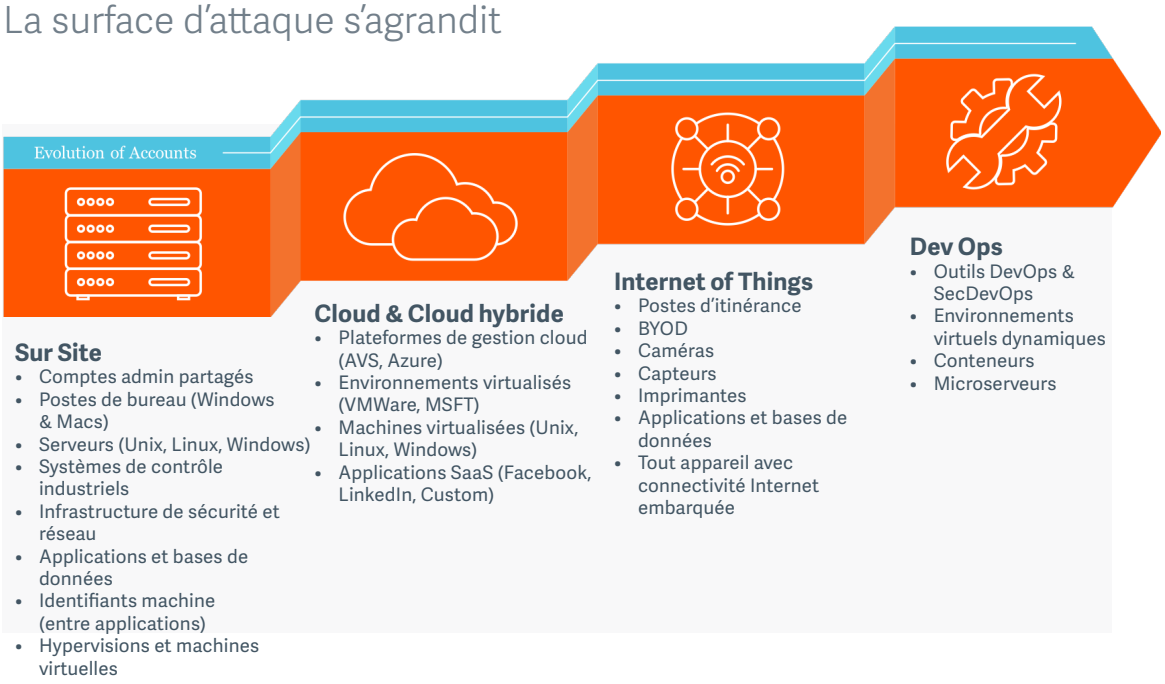

FIGURE 1: La dissolution du périmètre traditionnel augmente nettement la surface d'attaque des privilèges et la complexité des menaces

Le contrôle, la surveillance, les audits des privilèges et des accès privilégiés, pour les salariés, les fournisseurs, les systèmes, les applications, l'IoT et tout ce qui touche à votre environnement IT, sont absolument nécessaires pour se protéger des vecteurs de menace internes et externes et répondre aux mesures de conformité sans cesse plus nombreuses.

Mais par où commencer ? Est-ce qu'Unix est particulièrement risqué ? Et les identifiants privilégiés ? Qu'en est-il des machines des utilisateurs ? Et ensuite, comment savoir quels aspects traiter en priorité ?

C'est ce que vous apprendrez en lisant ce Guide de l'acheteur d'une solution PAM : par où commencer votre projet PAM (privileged access management), comment évoluer vers une meilleure sécurité et quels résultats en attendre. Nous allons commencer par les bases du PAM qui permettent d'atténuer la majorité des risques. Puis nous aborderons d'autres scénarios d'utilisation majeurs pour finir par des scénarios inédits.

Pour avoir accompagné plusieurs milliers de déploiements de clients, il apparaît que la plupart suivent une stratégie relativement commune mais, dans tous les cas, vos choix PAM seront fondés sur une appréciation des risques dans votre entreprise. En choisissant les bons fournisseurs et partenaires, votre approche de gestion des accès privilégiés devra toutefois être fluide.

Problèmes liés aux privilèges des environnements sans gestion du PAM	→ Objectifs visés du PAM
Processus manuels de gestion des mots de passe à privilèges y compris dans des tableurs ou des coffres physiques	Gestion automatisée des mots de passe et des sessions pour tous les comptes à privilèges
La plupart des utilisateurs ont un accès administrateur sur leurs machines	Instauration du principe de moindre privilège fondé sur des règles, sur tous les systèmes et les machines de l'entreprise
Manque d'audit et de contrôle des comptes root et des comptes à privilèges	Contrôle total et responsabilité des utilisateurs à privilèges sur tous les systèmes, afin d'éliminer les accès root ou les méthodes de type sudo
Aucune surveillance de session, ni enregistrement de l'utilisation faite des privilèges	Enregistrement automatique de la frappe/vidéo/par-dessus l'épaule
Accès du personnel interne et de tiers non contrôlés ou sur le mode « tout ou rien »	Un contrôle granulaire et flexible limite l'accès à distance des fournisseurs et salariés autorisés aux seules ressources dont ils ont effectivement besoin
Pas de réelle visibilité sur les menaces ni sur la manière de les gérer	Analyse intégrée des menaces pour affiner la prise de décision
Infrastructure des services d'annuaires désorganisée et chaotique, avec coexistence d'identifiants multiples et des règles incohérentes entre Windows, Unix, Linux, etc.	Authentification unique SSO (single sign on) auprès de systèmes hétérogènes s'appuyant sur une infrastructure commune
Incohérences entre la gestion des identités privilégiées et non privilégiées	Gestion transparente des identités privilégiées et non privilégiées pour une couverture à 100%
Productivité ralentie et de très nombreux tickets de demande de support	Les utilisateurs sont autorisés à faire ce qu'ils doivent. Baisse du nombre de demandes d'assistance du fait des moindres risques pour la sécurité
RISQUES TRES ELEVES POUR LA SECURITE	**FORTE REDUCTION DES RISQUES POUR LA SECURITE**

FIGURE 2: Perfectionner les contrôles PAM se traduit par une amélioration de la sécurité, des conditions d'audit et des opérations en général. Plus vous viserez des objectifs ambitieux, plus vous réduirez les risques, ainsi que la surface d'attaque, et meilleure sera votre gestion de la sécurité.

En faisant évoluer vos capacités de PAM, vous allez réduire la surface d'attaque, combler les failles de sécurité, améliorer vos capacités de réponse et faciliter votre mise en conformité. Vous dissuaderez également de nombreux attaquants opportunistes cherchant à exploiter les cibles les plus vulnérables.

La prochaine section de ce livre blanc expose une approche en sept étapes pour une gestion plus efficace des accès privilégiés.

LA GESTION COMPLETE DES PRIVILEGES EN SEPT ETAPES

Cette section du livre blanc présente sept aspects centraux de la gestion des accès privilégiés et détaille les fonctionnalités primordiales pour chacun.

Une fois réalisé, chacun de ces aspects vous confère plus de contrôle sur les comptes, actifs, utilisateurs, systèmes et activités au sein de votre environnement privilégié, tout en éliminant et en atténuant les effets de nombreux vecteurs de menaces. Vous pouvez choisir de tous les réaliser d'un coup ou de procéder de façon progressive étape par étape. Plus vous combinerez d'aspects, plus vous profiterez de synergies PAM avec à la clé une forte réduction des risques et des améliorations opérationnelles pour votre entreprise.

Tout au long de votre démarche de sélection et de déploiement d'une solution de gestion des accès à privilèges, gardez ces exigences en tête pour mieux convaincre de la valeur du programme au plus haut de la hiérarchie :

- **Coût total de possession :** les gains de temps réalisés (par le remplacement de processus manuels par l'automatisation) vous permettent-ils de redéployer des ressources au profit d'autres initiatives ?
- **Délai de rentabilisation :** dans quel délai pensez-vous renforcer les contrôles de sécurité et réduire les risques ? Dans combien de temps aurez-vous tenu vos objectifs grâce à la solution ?
- **Intégrations :** la solution s'intègre-t-elle bien au reste de votre écosystème de sécurité (IAM, SIEM, service d'assistance, analytique) ? Vous permet-elle de prendre de meilleures décisions en fonction du risque ? Si elle fonctionne bien uniquement de façon ponctuelle/autonome, ce n'est probablement pas une solution qui s'inscrira dans le long terme. D'un autre côté, si la solution offre des synergies combinées avec vos autres solutions de sécurité, elle vous aidera sûrement à mieux rentabiliser vos autres investissements.
- **Longévité :** le fournisseur de la solution va-t-il accompagner votre développement ou même favoriser votre croissance via ses fonctions de sécurité ? Le fournisseur a-t-il les ressources pour faire évoluer ses capacités et la richesse de ses fonctionnalités pour s'adapter aux scénarios PAM de demain ?

01

Intensifier la responsabilité et le contrôle des mots de passe à privilèges

Le point de départ logique afin de mieux contrôler les privilèges consiste à accroître la responsabilité vis-à-vis des identifiants privilégiés. Selon Forrester Research, des identifiants privilégiés sont impliqués dans 80% des compromissions de données.

Les administrateurs se partagent fréquemment les mêmes mots de passe, ce qui rend quasi impossible l'obtention d'une piste d'audit claire. De nombreux systèmes, applications et terminaux (IoT, etc.) comportent des mots de passe embarqués ou codés en dur, ouvrant la voie à des usages abusifs. Des mots de passes sont également nécessaires pour les accès inter-applications et pour les applications vers les bases de données. Et de nouveaux identifiants privilégiés viennent s'ajouter avec les instances cloud/virtuelles éphémères. Et la liste se poursuit.

Les mesures de gestion manuelle des mots de passe (découverte, rotation, instauration des meilleures pratiques de sécurité) sont connues pour manquer de fiabilité, elles sont complexes et chronophages et difficiles à déployer à grande échelle. Et certaines de ces meilleures pratiques, comme l'élimination et la centralisation de certains types de mots de passe embarqués, sont quasi impossibles sans outils d'entreprise.

Comment garantir la sécurité et la responsabilité à l'échelle des différents types d'identifiants privilégiés sans ralentir la productivité des administrateurs ni d'autres workflows ou processus ?

Objectif : disposer d'une solution complète et automatisée capable de découvrir les très nombreux comptes/types d'identifiants privilégiés (humains et non-humains) dans votre environnement, de placer ces comptes/identifiants sous gestion et de démontrer aux auditeurs qu'ils sont correctement gérés. Une telle solution élimine d'emblée certains vecteurs d'attaque privilégiée et en atténue d'autres, de façon à réduire nettement l'exposition de l'entreprise aux risques de sécurité. Cela induit une solution de gestion des mots de passe et identifiants privilégiés capable d'automatiser chaque phase du cycle de vie des mots de passe d'après vos règles de sécurité.

Principales fonctionnalités de gestion des identifiants privilégiés

- ☐ **Analyse complète du réseau, découverte et profilage** avec auto-intégration des comptes à privilèges de tous types (comptes admin partagés, utilisateur, application, comptes de service, clés SSH, comptes de base de données, comptes cloud et de réseaux sociaux, identifiants machine, DevOps, RPA, y compris des tiers/fournisseurs).
- ☐ **Mise en lumière d'où et comment les mots de passe à privilèges sont utilisés,** révélant les angles morts et les mauvaises pratiques (mots de passe par défaut, partagés et/ou embarqués, utilisation du même compte Admin pour plusieurs comptes de service, réutilisation des clés SSH sur plusieurs serveurs, etc.).
- ☐ **Gestion des identifiants sur toutes les plateformes** (Windows, Unix, Linux, Cloud, sur site, etc.), des annuaires, périphériques, applications, services/démons, pare-feu, routeurs, etc.
- ☐ **Centralisation, sécurisation et chiffrement de tous les identifiants privilégiés** dans un coffre-fort inviolable. (Idéalement, la solution prend en charge les algorithmes de chiffrement standard comme AES 256.)
- ☐ **Attribution dynamique de permissions** d'après les données d'analyse.
- ☐ **Implémentation d'appels d'API** pour éliminer les identifiants embarqués/codés en dur dans les fichiers, applications, scripts et autre type de code.
- ☐ **Rotation automatisée des mots de passe, clés SSH et autres secrets** selon un calendrier défini et après chaque utilisation des comptes les plus sensibles ou pour les comptes ayant un fort risque d'exposition/de compromission.
- ☐ **Application de votre politique de gestion des mots de passe à privilèges,** comprenant la complexité des mots de passe, l'unicité (mots de passe différents pour chaque actif, compte, etc.), l'expiration, la rotation, check in/check out, l'élimination des mots de passe par défaut, etc.
- ☐ **Automatisation des workflows** sur tout le cycle de vie de gestion des mots de passe.
- ☐ **Contrôle d'accès granulaire.**
- ☐ **Authentification unique (SSO)** sans ne jamais révéler le mot de passe à l'utilisateur.
- ☐ **Surveillance et gestion rigoureuses de session** pour établir un audit clair de toute l'activité privilégiée et mettre immédiatement en pause ou interrompre les sessions suspectes jusqu'à validation de leur légitimité.
- ☐ **Aucun recours à des outil tiers** ou à du Java pour la gestion de session, mais des outils natifs (MSTSC, PuTTY).
- ☐ **Instauration du principe de moindre privilège** via un modèle de sécurité avec accès tout juste suffisant et juste à temps.
- ☐ **Interface moderne centralisée** (HTML5) pour simplifier l'adoption et l'administration.
- ☐ **Utilisation des protocoles standards,** comme SAML et RADIUS, pour s'intégrer à n'importe quelle solution d'authentification multi-facteurs (MFA).
- ☐ **Propose une option bris de glace** de consultation des mots de passe.
- ☐ **Stockage intégré des données** et analyse des menaces pour l'ensemble des privilèges
- ☐ **Une seule solution complète et unifiée** pour gérer les identités humaines (utilisateurs à privilèges) et non-humaines (application, machine, compte de service, etc.), avec surveillance/gestion de session incluses, sans autre interface, ni frais supplémentaires.
- ☐ **Options de déploiement flexibles :** appliances matérielles, appliances virtuelles, ou logiciels

Autres considérations : quelle est l'importance de l'évolutivité ? Avez-vous quelques centaines d'identifiants privilégiés ou bien plusieurs milliers ? Il existe une poignée de solutions de PAM capables de prendre en charge des dizaines voire des centaines de milliers d'identifiants privilégiés. Rares sont celles qui peuvent également gérer de très grands nombres de clés SSH. Aussi s'il est important pour vous (et à raison) de surveiller et gérer toutes les sessions privilégiées, sachez que quelques fournisseurs d'élite sont en capacité de surveiller/gérer des centaines de milliers de sessions concurrentes. Et seul BeyondTrust propose l'ensemble de ces fonctionnalités et répond aux besoins de montée en charge des entreprises dans tout type d'environnement.

Autre considération : quelle est votre position par rapport à la complexité de la sécurité, au chevauchement de solutions et aux redondances entre les solutions de différents fournisseurs ? En moyenne, les entreprises utilisent quatre méthodes différentes de gestion des identifiants privilégiés. Comme le faisait remarquer Gartner dans son Magic Quadrant consacré aux solutions PAM, de nombreux fournisseurs proposent des composants distincts de gestion des identifiants privilégiés, chacun avec sa propre console de gestion. Bien sûr, il existe des fournisseurs de niche qui proposent des fonctionnalités autonomes de gestion des clés SSH ou de gestion des mots de passe des applications ou de gestion des secrets. Seul BeyondTrust propose une solution aussi complète et évolutive pour gérer, surveiller et auditer tous les types d'identifiants privilégiés de façon centralisée et unifiée. Certains grands éditeurs vous contraignent à acquérir jusqu'à six solutions différentes !

Solution : Password Safe de BeyondTrust unifie la gestion des mots de passe et des sessions privilégiés, permettant la découverte en toute sécurité, la gestion, les audits et la surveillance de tout identifiant privilégié (humain, applicatif, machine, etc.), et réduisant de ce fait le risque d'utilisation abusive des identifiants privilégiés en plus de favoriser la mise en conformité. La solution offre des performances inédites d'analyse et de reporting des menaces (comme la corrélation entre le comportement anormal d'un utilisateur à privilèges et les données de tiers pour déterminer le degré de sévérité de la menace).

02

Instauration du moindre privilège et contrôle des applications pour Windows et Mac

Une fois que les identifiants et comptes à privilèges sont systématiquement découverts, intégrés et gérés, l'étape suivante consiste à instaurer le moindre privilège sur les machines des utilisateurs en supprimant les droits locaux d'administration. Si vous avez des serveurs Windows, vous procéderez de même pour les accès privilégiés en définissant les droits des comptes de vos différents comptes d'administrateur (réseau, Microsoft Exchange, Active Directory, base de données, développeurs, service d'assistance, personnel informatique / utilisateurs à privilèges, etc.).

> 77% des 192 vulnérabilités critiques Microsoft signalées en 2019 auraient pu être éliminées en supprimant les droits locaux admins des utilisateurs.
>
> **MICROSOFT VULNERABILITIES REPORT 2020, BEYONDTRUST**

Une approche de moindre privilège fait en sorte que les utilisateurs n'obtiennent d'autorisations que pour les systèmes, applications et données dont ils ont besoin pour leur rôle. Plutôt que d'activer des privilèges en permanence, avec le risque d'utilisation abusive, les privilèges ne sont élevés qu'au cas par cas. En partant de la configuration par défaut d'un utilisateur standard et en n'élevant ses privilèges qu'au besoin, vous réduisez nettement la surface d'attaques, vous limitez la progression latérale et vous diminuez les risques d'infection et de propagation des menaces, du phishing et des ransomwares. Des contrôles et audits stricts des accès admin contribuent également à la protection de vos actifs les plus sensibles.

Cela coûte cher, en temps et en argent, d'utiliser des outils ad hoc natifs, développés en interne, pour activer ou restreindre les privilèges utilisateur. Et alors que par défaut les utilisateurs ne devraient pas bénéficier de privilèges admin ou super utilisateur locaux, certaines applications exigent des privilèges rehaussés pour s'exécuter.

Comment les organisations IT réduisent-elles le risque lié aux privilèges excessifs des utilisateurs sans pénaliser la productivité ni surcharger le service d'assistance par des demandes de privilèges et permissions ?

Objectif : pouvoir éliminer efficacement les droits locaux admins des systèmes Windows et macOS, contrôler et auditer les accès à privilèges aux serveurs et systèmes sensibles et appliquer un contrôle granulaire aux applications. Ceci suppose des solutions de gestion des privilèges des terminaux qui suppriment les privilèges des utilisateurs et procèdent d'une technologie à base de règles pour élever les privilèges des applications, sans élever ceux des utilisateurs.

Principales fonctionnalités liées au moindre privilège sur Windows & Mac

- ☐ **Privilèges standard par défaut pour tous les utilisateurs de PC et serveurs,** avec la possibilité d'élever des privilèges pour certaines applications et tâches spécifiques sans nécessiter d'identifiants à privilèges.
- ☐ **Puissantes couches de contrôle des applications** pour les listes blanches des applications de confiance avec des règles larges ou granulaires au choix.
- ☐ **Restrictions** d'installation et d'utilisation de logiciels, et de changements de configuration de l'OS.
- ☐ **Annulation de la nécessité pour les utilisateurs de posséder deux comptes.**
- ☐ **Choix dynamique du moindre privilège** fondé sur le risque de vulnérabilité de l'application en temps réel.
- ☐ **Conformité automatique des applications aux règles** d'après les règles de l'actif ; recours aux règles intelligentes pour alerter et regrouper les dispositifs et les événements.
- ☐ **Surveillance des sessions, capture des écrans et enregistrement de la frappe** lors des accès privilégiés.
- ☐ **Audit et reporting des changements apportés** aux fichiers, règles, systèmes, applications et données critiques, de façon à éliminer les installations non autorisées de logiciels, les contournements ou failles pouvant être exploitées.
- ☐ **Technique** permettant d'utiliser les privilèges locaux ou de domaine au besoin.
- ☐ **Instauration du principe de moindre privilège** via un modèle de sécurité avec accès juste suffisant et juste à temps.
- ☐ **Piste d'audit irréprochable** de l'activité de tous les utilisateurs pour accélérer les investigations et simplifier la conformité.
- ☐ **Centralisation de l'administration, des règles, du reporting et de l'analytique.**
- ☐ **Intégration d'autres modules de gestion des privilèges** pour une gestion complète des accès à privilèges.
- ☐ **Stockage intégré des données** et analyse des menaces pour l'ensemble des privilèges.
- ☐ **Analyse du comportement des utilisateurs** par la collecte, le stockage, l'indexation des journaux de frappe, des enregistrements de sessions et des autres événements privilégiés.
- ☐ **Définition des règles** via Active Directory Group Policy, Web Services ou McAfee ePO y compris pour les systèmes isolés et les actifs hors domaine.

Autres considérations : dans quelle mesure le délai de rentabilisation de la solution est-il important pour vous ? Certaines solutions appellent une coordination complexe de services alors que d'autres permettent de réduire les risques et les tickets de demande d'assistance en quelques semaines seulement.

Autre considération : avez-vous un parc de serveurs Unix/Linux ou des terminaux non traditionnels raccordés à votre réseau ? De nombreux fournisseurs proposant le moindre privilège pour Windows ne le font pas pour Unix, Linux et macOS, sans parler des terminaux non traditionnels. Ne préféreriez-vous pas une solution unifiée capable d'instaurer le moindre privilège et d'appliquer les meilleures pratiques de contrôle des applications à tous vos terminaux, Windows, Unix, Linux, Mac, ICS, SCADA, IoT, périphériques réseau, etc. ? BeyondTrust est le seul à pourvoir à l'ensemble de ces besoins.

Solution: La gestion des privilèges de BeyondTrust pour Windows et Mac (partie de l'offre Endpoint Privilege Management de BeyondTrust) instaure l'accès selon le principe du moindre privilège et facilite la conformité des PC et serveurs Microsoft Windows physiques et virtuels et des postes macOS, tout en demeurant totalement invisible et transparente pour l'utilisateur. La solution promet un ROI solide en comblant les failles de sécurité, en améliorant l'efficacité opérationnelle par la diminution des tickets d'assistance portant sur la sécurité et en accélérant la tenue des objectifs de conformité. De plus, la solution se déploie plus rapidement que celles des concurrents, avec des fonctionnalités plus fines et un délai de valorisation plus court.

03

Accès à distance sécurisé des fournisseurs et employés

Les accès à distance sont les maillons faibles de la plupart des entreprises et les cybercriminels le savent. Les administrateurs IT, salariés et fournisseurs tiers ont besoin d'un accès privilégié ou de la possibilité d'élever les privilèges pour faire leur travail correctement. Souvent, les entreprises manquent de visibilité sur ce que font les fournisseurs qui se connectent à leur réseau. Les VPN offrent un accès bien trop large. La plupart des autres solutions d'accès à distance comme les VPN présentent les mêmes inconvénients :

- Absence de paramètres de sécurité granulaires
- Incapacité à produire un audit complet
- Manque de prise en charge de multiples systèmes d'exploitation et cas d'usage

> 69 % des sondés admettent qu'ils ont manifestement ou possiblement subi une compromission de données du fait d'un accès fournisseur au cours de l'année passée.
>
> **RAPPORT 2019 SUR LES MENACES LIEES AUX ACCES PRIVILEGIES, BEYONDTRUST**

Ce sont des inconvénients majeurs. Et compte tenu de l'ampleur du problème, on comprend l'urgence. Comme l'a montré le rapport 2019 des menaces liées aux accès privilégiés de BeyondTrust, 182 fournisseurs en moyenne se connectent aux systèmes/ressources d'une entreprise au cours d'une semaine. Vu le nombre élevé des terminaux d'accès à distance, du peu de visibilité et des audits et contrôles de sécurité insuffisants, ce n'est qu'une question de temps avant que l'accès à distance d'un employé ou fournisseur soit compromis.

Comment les organisations peuvent-elles mieux surveiller l'accès aux utilisateurs à privilèges sans pénaliser l'agilité ?

Objectif : remplacez l'accès à distance « tout ou rien » des fournisseurs par l'accès granulaire basé sur le rôle à des systèmes spécifiques et à des paramètres de session prédéfinis. Les fournisseurs et utilisateurs interne ont accès à des systèmes et applications spécifiques, pendant une durée donnée. Les administrateurs approuvent ou rejettent les demandes d'accès quel que soit l'appareil utilisé et où qu'ils se trouvent, toutes plateformes confondues.

Principales fonctionnalités pour les accès à distance privilégiés

- ☐ **Instauration du principe de moindre privilège** en octroyant aux utilisateurs autorisés un accès tout juste suffisant pour leurs activités juste à temps dans le cadre de sessions à distance.
- ☐ **Contrôle et surveillance des sessions** utilisant les protocoles standard des connexions RDP, VNC, HTTP/S et SSH.
- ☐ **Accès granulaire** à des systèmes spécifiques, de façon à renforcer la sécurité et à éliminer l'accès « tout ou rien ».
- ☐ **Possibilité d'injection des identifiants** directement dans la session d'accès ; l'utilisateur n'a jamais besoin de voir ni de connaître l'identifiant. (y compris pour les comptes avec authentification MFA lors d'une session Web Jump Access).
- ☐ **Création d'une piste d'audit** de visibilité de l'activité des fournisseurs sur le réseau, facilitant la conformité par le contrôle des chemins d'accès aux réseaux IT empruntés par les fournisseurs.
- ☐ **Gestion efficace des accès privilégiés aux actifs de votre entreprise** qui dépendent de consoles d'administration web, y compris les serveurs IaaS, les environnements d'hyperviseur et les interfaces de configuration web pour vos infrastructures réseaux.
- ☐ **Intégration des outils existants** comme SIEM, Change Management, SCIM et Password Management.
- ☐ **Intégrations instantanées et transparentes** avec ITSM, SIEM et SCIM et autres solutions logicielles d'entreprise courantes.
- ☐ **Authentification TouchID/FaceID** auprès de la console mobile d'accès à distance privilégié.
- ☐ **Utilisation des standards de l'industrie,** comme SAML et RADIUS, pour s'intégrer à n'importe quelle solution d'authentification multi-facteurs (MFA).

Solution: Privileged Remote Access de BeyondTrust permet aux professionnels de la sécurité et de l'IT de mieux contrôler, gérer et auditer les accès privilégiés aux systèmes critiques des salariés, sous-traitants et tiers autorisés, sans VPN. Privileged Remote Access peut aider votre entreprise à protéger ses données sensibles et à se conformer à ses obligations légales (PCI, HIPAA, ISO, RGPD, etc.). Vous pouvez déployer la solution Privileged Remote Access sur site via une appliance physique ou virtuelle durcie ou sur un cloud sécurisé. La solution dispose d'un coffre-fort de gestion des identifiants privilégiés avec des fonctionnalités de découverte, gestion, rotation, audit et surveillance des comptes à privilèges, des comptes de domaine ou locaux admins partagés au compte admin personnel d'un utilisateur, jusqu'aux clés SSH, comptes cloud et de réseaux sociaux. La solution vault SaaS cloud-ready peut gérer plus de 5.000 identifiants Windows et en stocker jusqu'à 10.000.

BeyondTrust est le seul fournisseur PAM à proposer des fonctionnalités matures et testées favorisant l'extension des bonnes pratiques des accès à privilèges aux fournisseurs, sous-traitant et télétravailleurs. Nos principaux concurrents commencent dans ce domaine.

04

Implémentation du principe de moindre privilège et audit des accès des environnements de serveurs Unix et Linux

Les applications stratégiques, critiques ou 1-Tiers sur serveurs Unix et Linux attirent les cybercriminels. Les identifiants des utilisateurs à privilèges de ces ressources peuvent également donner accès aux données e-commerce, aux systèmes ERP avec les données des salariés, aux informations client et aux données financières sensibles.

Pour qu'ils puissent faire leur travail, les administrateurs IT ont besoin de mots de passe root, d'un statut de super utilisateur ou d'autres privilèges élevés. Malheureusement, cette pratique expose à des risques de sécurité importants du fait de l'utilisation abusive, indirecte, accidentelle ou délibérée de ces identifiants privilégiés.

Des outils ad hoc natifs et open source peuvent suffire. Cependant dans les environnements serveurs de complexité modeste, utiliser ces outils « gratuits » peut revenir cher à plusieurs égards. Voici quelques-uns des inconvénients possiblement dangereux ou onéreux de sudo et d'autres outils basiques :

- Déficiences inquiétantes en termes de visibilité, d'investigation et d'audit : manque de surveillance de l'intégrité des fichiers, de protection des fichiers journaux ou de possibilité d'enregistrer les sessions et la frappe clavier en prévision d'audits
- Graves failles de sécurité : ces outils ne tiennent pas compte de l'activité au sein des scripts et des applications de tiers, ouvrant la voie à des applications non approuvées. Les outils OS natifs ne permettent pas de déléguer des autorisations sans révéler les mots de passe.
- Complexité administrative et manque d'évolutivité : il faut généralement gérer les règles sur chaque serveur quand on utilise sudo ou d'autres outils basiques
- Manque de support d'entreprise
- Chemin de migration inefficace depuis sudo, le cas échéant

D'autres outils, dont sudo, font qu'il est quasiment impossible de maintenir les bonnes pratiques de sécurité et de conformité sauf dans les environnements IT les plus simples. Or les risques de contrôles inadaptés des accès à privilèges dans vos environnements Unix/Linux sont de loin trop importants.

Objectif : visibilité et contrôle de toutes les activités privilégiées sur les systèmes Unix et Linux. Instauration systématique du principe de moindre privilège, délégation efficace des privilèges Unix et Linux et autorisation sans révéler les mots de passe des comptes root ou autres. La possibilité d'abandonner sudo, ou de le compléter avec des fonctionnalités d'entreprise venant combler les déficiences de sécurité et d'audit, et de simplifier l'administration en limitant le risque d'erreur.

Principales fonctionnalités de gestion des privilèges des serveurs pour Unix & Linux

- ☐ **Instauration du moindre privilège** sans utiliser le compte Root.
- ☐ **Administration 'juste-à-temps' (JIT)**, avec attribution de privilèges dynamiques aux comptes et actifs de sorte que les identités n'aient accès qu'aux privilèges nécessaires pendant une durée déterminée.
- ☐ **Contrôle granulaire et audit** des applications, commandes, fichiers et scripts.
- ☐ **Enregistrement et indexation** de toutes les sessions pour accélérer la découverte en cas d'audit.
- ☐ **Enregistrement adaptatif de la frappe** pour les sessions les plus sensibles.
- ☐ **Totale visibilité** avec piste d'audit claire de l'activité de chacun.
- ☐ **Consolidation des journaux d'audit** et reporting centralisé à l'échelle de tous les domaines de serveurs.
- ☐ **Module d'authentification enfichable** afin de pouvoir utiliser des systèmes d'authentification standard.
- ☐ **Langage de règle puissant et flexible** pour faciliter la migration depuis sudo.
- ☐ **Provisioning/déprovisioning transparents des privilèges**, pour faciliter la mise en conformité.
- ☐ **Surveillance de l'intégrité des fichiers** pour empêcher toute falsification des fichiers et binaires critiques.
- ☐ **API REST** pour faciliter l'intégration des produits de tiers.
- ☐ **Support** de nombreuses plateformes Unix et Linux.
- ☐ **Console web pour l'intégration de toutes les règles, des rôles et données des fichiers journaux.**
- ☐ **Stockage intégré des données** et analyse des menaces pour l'ensemble des privilèges

Autres considérations : Avez-vous aussi des serveurs et des terminaux Windows ? Préféreriez-vous un fournisseur et une plateforme PAM uniques pour tous vos terminaux ou acceptez-vous plusieurs fournisseurs et consoles pour différents OS. Est-ce également important d'appliquer l'authentification unique (single-sign-on) à votre infrastructure hétérogène et d'unifier la gestion des règles pour Unix, Linux, macOS et Windows ? Si vous recherchez une meilleure couverture PAM et une moindre complexité, seule une poignée de fournisseurs peut satisfaire vos besoins.

Solution : La gestion des privilèges de BeyondTrust pour Unix & Linux (partie de l'offre Endpoint Privilege Management de BeyondTrust) est la meilleure solution de sécurité des accès privilégiés Unix/Linux. La solution vous permet de contrôler les privilèges des comptes root Unix/Linux avec analytique et reporting centralisés et enregistrement de la frappe. Elle aide à réduire les risques et à se mettre en conformité plus rapidement qu'avec des outils natifs et sudo. Par sa gestion juste-à-temps des privilèges (éliminant les accès privilégiés persistants), elle réduit la durée de possession de privilèges élevés et des droits d'accès pour réduire la fenêtre de vulnérabilité et d'exploitation des privilèges de comptes par des criminels. Cette solution PAM Unix/Linux est la plus puissante de l'industrie, avec un faible coût total de possession (TCO) par rapport aux offres concurrentes du fait de sa gestion centralisée des comptes à privilèges qui permet de tenir les objectifs de sécurité et d'audit plus rapidement. Privilege Management for Unix & Linux permet de stimuler la sécurité, la responsabilité et la productivité des utilisateurs et des administrateurs de serveurs, sans les risques associés à sudo Open Source.

05

De meilleures décisions de privilèges fondées sur le risque au niveau de l'utilisateur, de l'actif et de l'application

Une fois les identifiants privilégiés sous gestion, avec des utilisateurs qui ont le strict niveau de privilèges nécessaire pour faire leur travail, il devient possible d'utiliser les données des vulnérabilités en temps réel pour prendre de meilleures décisions d'élévation des privilèges. Par exemple, si une application comporte une vulnérabilité, devez-vous l'autoriser à avoir accès pour une opération hautement sensible ? La réponse dépend de facteurs contextuels propres à votre environnement. Vous devez vérifier ces trois points au préalable :

1. Savoir où se situe la vulnérabilité
2. Comprendre l'évolution du niveau de risque selon les actifs avec lesquels l'application vulnérable interagit, et quels privilèges elle élève, et comment vous évaluez ces scénarios de risque
3. Pouvoir orchestrer une réponse en temps réel en cohérence avec vos règles et votre appétence pour le risque

Mais comment faire à une très grande échelle comme c'est le cas dans la plupart des entreprises ?

Objectif : l'intégration transparente de fonctionnalités automatisées d'élévation/délégation de privilèges avec des données sur les vulnérabilités, les risques et les menaces pour prendre des décisions d'accès privilégiés plus intelligentes.

Principales fonctionnalités d'aide à l'élévation/la délégation de privilèges sur la base de risques en temps réel

- ☐ **Evaluation des niveaux de menace en temps réel** pour l'utilisateur, l'actif sollicité et l'application exécutée.
- ☐ **Exécution d'actions pour les applications et les processus** selon les règles définies (ex. autoriser l'élévation des privilèges, supprimer les permissions administratives ou empêcher une application de s'exécuter).
- ☐ **Révélation de risques émergents** par l'identification et le reporting des types d'activités pouvant être à risque.
- ☐ **Activation de workflows avancés d'élévation/délégation de privilèges** pour pouvoir prendre des mesures correctives d'élimination proactive des menaces potentielles, comme la fin d'une session ou l'intensification de consignation, audit et examen de la session privilégiée.

Solution : Endpoint Privilege Management de BeyondTrust (qui comprend les produits Privilege Management for Windows & Mac et Privilege Management for Unix & Linux) et BeyondInsight fonctionnent ensemble pour analyser automatiquement les applications en cours d'exécution à la recherche de vulnérabilités (déclenchement d'alertes, réduction des privilèges des applications ou blocage du lancement d'après les règles). La plateforme BeyondInsight de gestion des accès privilégiés est la plus complète et innovante de l'industrie. Vos administrateurs obtiennent une vue complète des vulnérabilités et des privilèges qui donnent potentiellement accès à votre environnement ainsi que des privilèges d'accès à vos actifs sensibles. En centralisant l'intelligence des risques et des menaces, BeyondInsight aide à instaurer une approche « universelle » de gestion des privilèges.

06

Unification et centralisation de la gestion des privilèges, des règles, du reporting et de l'analyse des menaces

Chacun sait que les professionnels IT et de la sécurité sont noyés sous les informations relatives aux privilèges, aux vulnérabilités et aux attaques. Malheureusement, des menaces persistantes avancées (APT) demeurent souvent indétectées car les solutions traditionnelles d'analyse de la sécurité sont incapables de corréler des données diverses pour révéler les risques cachés. Des événements apparemment isolés sont traités comme des exceptions, filtrés ou perdus dans la masse des données. L'intrus continue de s'infiltrer sur le réseau et de faire des dégâts.

Généralement, plus vous avez d'outils, chacun avec ses interfaces administratives et son code spécifique, plus vous risquez :

- Des risques accrus de mauvaise intégration ou mauvaise communication de vos solutions entre elles, avec à la clé des temps d'arrêt, des failles de sécurité et de la frustration
- Des courbes d'apprentissage plus abruptes pour vos administrateurs
- Une charge administrative plus forte et persistante
- Une orchestration différée vis-à-vis des menaces

Comment les équipes de sécurité et des opérations IT savent d'où les menaces proviennent, comment les prioriser et comment atténuer rapidement les risques ?

Objectif : une vue holistique du risque avec analyse avancée des menaces permettant aux professionnels IT et de sécurité d'identifier rapidement les cas de compromission de données, sophistiqués comme typiques. Ceci permet aussi d'identifier les utilisateurs et actifs à haut risque en corrélant les données de privilèges de bas niveau, des vulnérabilités et des menaces de plusieurs solutions de tiers.

Capacités de Gestion et d'Analyse des Menaces

- ☐ **Regroupe, évalue et rend compte des actifs** par plage IP, convention de nommage, OS, domaine, applications, fonction métier, Active Directory, etc.
- ☐ **Permet l'orchestration rapide de la réponse de sécurité** pour bloquer ou atténuer les menaces.
- ☐ **Autorise les importations d'Active Directory** ou la personnalisation des permissions.
- ☐ **Corrèle les données de bas niveau** de multiples solutions tierces pour révéler les menaces critiques.
- ☐ **Corrèle l'activité système** avec une base de données de malwares actualisée en permanence.
- ☐ **Rend compte de la conformité**, des bancs d'essai, de l'analyse des menaces, des scénarios hypothétiques, des besoins en ressources, etc.
- ☐ **Présente, trie et filtre les données historiques** selon plusieurs perspectives. Localise les actifs réseau (locaux et distants), web, mobiles, cloud et virtuels, ainsi que les comptes à privilèges.
- ☐ **Etablit les profils IP, DNS, OS**, d'adresses Mac, des utilisateurs, des comptes, de l'âge des mots de passe, des ports, des services, des logiciels, des processus, des équipements et des fichiers journaux d'événements, etc.
- ☐ **Propose des workflows, systèmes de ticket et notifications** pour coordonner les équipes IT et de sécurité.
- ☐ **Partage les données** avec de grandes solutions SIEM, GRC, NMS, et d'assistance.

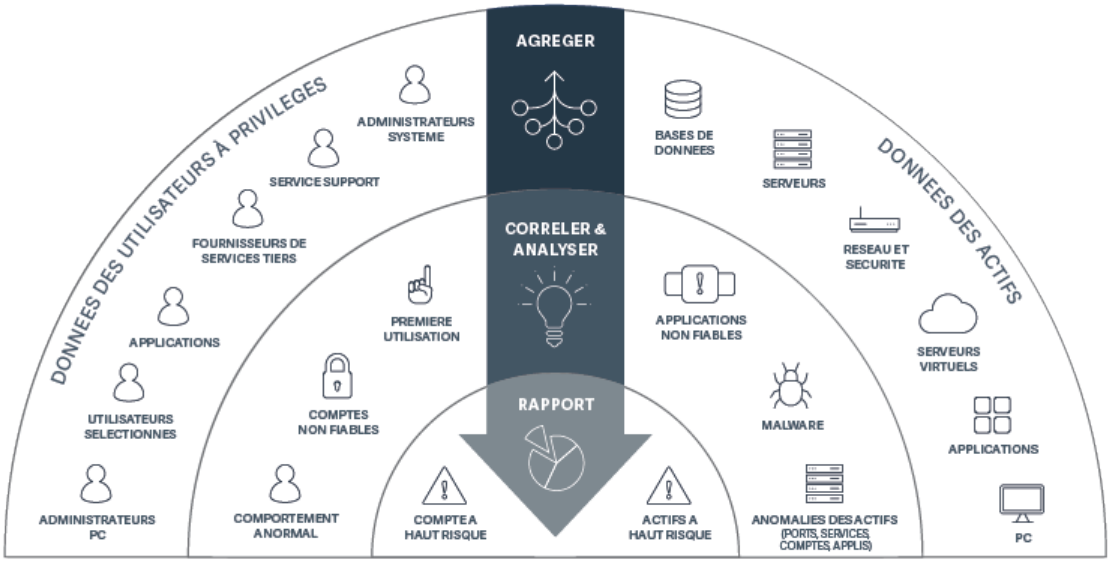

FIGURE 3: Gestion et analyse intégrées des menaces pour les privilèges et les vulnérabilités externes

Solution : Les solutions BeyondTrust de gestion des accès privilégiés sont unifiées et centralisées via notre plateforme BeyondInsight, pour une gestion et un contrôle des règles également centralisés. BeyondInsight propose des fonctionnalités intégrées de découverte d'actifs, profilage, regroupement intelligent, analyse des menaces, reporting et des connecteurs avec des systèmes tiers. BeyondInsight confère aux équipes IT et de sécurité une vue contextuelle unique sur les risques liés aux privilèges.

07

Intégration d'Unix, Linux et macOS à Windows

Une fois que vous contrôlez mieux les accès privilégiés des environnements Unix et Linux, l'étape logique suivante consiste à réunir ces systèmes sous un cadre commun de gestion, de règles et d'authentification unique. Les systèmes Unix, Linux et MacOS sont traditionnellement gérés comme des systèmes autonomes, chacun dans son silo avec ses propres utilisateurs, groupes, règles de contrôle d'accès, fichiers de configuration et mots de passe à mémoriser. Devoir gérer un environnement hétérogène composé de ces silos, en plus de l'environnement Microsoft, induit un manque de cohérence d'administration pour l'IT, une complexité superflue pour les utilisateurs et des risques pour l'entreprise.

Comment les organisations IT s'y prennent-elles pour gérer les règles à l'échelle de plusieurs plateformes et proposer une expérience utilisateur rationalisée avec moins d'erreurs et de délais d'administration ?

Objectif : l'authentification centralisée des environnements Windows, Unix, Linux et macOS pour réduire les risques et la complexité de gestion d'un environnement hétérogène. Gains d'efficacité grâce à une diminution du nombre d'identifiants (et donc des appels en cas d'oubli) et du nombre de systèmes différents, de configurations et de règles à gérer. Ceci suppose de déployer une solution Active Directory Bridging.

Principales fonctionnalités d'Active Directory Bridge

- **Authentification unique** auprès de toute application supportant Kerberos ou LDAP.
- **Utilisation des mêmes outils** pour gérer les systèmes Windows et Unix/Linux (ex. utilisateurs et ordinateurs Active Directory, ADUC).
- **Possibilité pour les utilisateurs d'utiliser leurs identifiants Active Directory** pour l'accès à Unix, Linux et macOS, par la consolidation de fichiers de mots de passe, référentiels NIS et LDAP dans Active Directory, ce qui empêche de devoir gérer les comptes utilisateur séparément.
- **N'exige pas de modifications de schéma Active Directory pour l'ajout** de systèmes Linux, Unix ou macOS au réseau.
- **Fournit un framework enfichable** avec une interface comparable à Microsoft Management Console sur Linux ou macOS (la prise en charge de l'application Apple Workgroup Manager permet une gestion et un contrôle plus transparents des paramètres système macOS).
- **Prise en charge d'un large éventail de plateformes Unix, Linux et MacOS**, y compris CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, Suse, RedHat, Solaris, Ubuntu, et d'autres.
- **Facilite la mise en conformité avec SOX, PCI, HIPAA** et d'autres réglementations.
- **Fonctionnement au sein d'une famille de solutions de gestion des accès privilégiés.**

Solution : AD Bridge de BeyondTrust (partie de l'offre Endpoint Privilege Management de BeyondTrust) étend l'authentification Kerberos de Microsoft Active Directory, l'authentification unique et la gestion de configuration de Group Policy aux systèmes Unix, Linux et Mac pour gagner en efficacité, faciliter la conformité et réduire les risques. En centralisant la gestion des identifiants et des configurations et en mobilisant l'infrastructure Windows Active Directory, AD Bridge de BeyondTrust accélère la réalisation de vos objectifs de sécurité et d'audit, tout en dopant la productivité des utilisateurs et des administrateurs de serveurs

PAM pour les cas d'usage émergeants

En respectant ces étapes, vous répondrez à la plupart de vos besoins PAM, vous éliminerez ou atténuerez de nombreux vecteurs de menaces privilégiées et vous réduirez grandement votre surface d'attaque.

Quasiment toutes les nouvelles technologies de transformation de l'IT s'accompagnent de défis pour la sécurité, liés notamment à la gestion des modèles d'identité et d'authentification et aux privilèges. C'est le genre de faille qui séduisent particulièrement les criminels.

La plateforme PAM de BeyondTrust est conçue de façon à s'adapter en toute flexibilité à vos besoins changeants et futurs. Et si les solutions BeyondTrust peuvent couvrir bien plus de scénarios que ceux cités ici, voici trois aspects importants ayant émergé ces dernières années, chacun avec des enjeux spécifiques.

DevOps

La plupart des entreprises ont déjà adopté les pratiques DevOps. Pourtant, les aspects de sécurité des outils, souvent Open Source et utilisés dans les environnements DevOps, sont souvent négligés.

Les cycles de développement DevOps, condensés par l'automatisation, et qui s'étendent fréquemment à l'échelle du cloud, créent aussi un inconvénient : « l'automatisation de l'insécurité », avec à la clé des failles massives de sécurité, de conformité et opérationnelles. Voici quelques-uns des risques DevOps courants :

- Code mal sécurisé, mots de passe codés en dur et autres expositions de privilèges
- Scripts ou vulnérabilités dans les outils CI/CD, comme Ansible, Chef ou Puppet, qui pourraient déployer des malwares ou des programmes de sabotage
- Provisioning excessif de privilèges dans tout le périmètre DevOps
- Partage de secrets
- Vulnérabilités, erreurs de configuration et autres faiblesses des conteneurs

Comment donc inclure les exigences de sécurité à DevOps sans nuire à la rapidité et à l'agilité ?

Solution : Les solutions BeyondTrust PAM réduisent les risques sur toute la chaîne d'approvisionnement IT par une visibilité et un contrôle accru des secrets, privilèges admin et des vulnérabilités et configurations système. En unifiant ces fonctionnalités pour les scénarios sur site, virtuels, cloud et DevOps, les entreprises IT pourront tenir leurs objectifs d'agilité sans processus laborieux. DevOps Secrets Safe de BeyondTrust permet une gestion centralisée et sécurisée, un audit des secrets et autres identifiants privilégiés utilisés par les applications, des outils et autres identités non-humaines. C'est la garantie de gains d'agilité tout en contrôlant les identifiants et autres secrets de la chaîne d'outils CI/ CD, y compris les mots de passe, clés, certificats, applications et autres processus automatisés. EndPoint Privilege Management de BeyondTrust instaure le principe de moindre privilège et de contrôle des applications dans tout l'environnement. Ensemble, les solutions BeyondTrust assurent une couverture PAM totale de votre environnement DevOps :

- Inventaire de tous les actifs DevOps.
- Détection, protection et gestion centralisée de tous les mots de passe codés en dur et des secrets partagés (y compris accès développeur au code source, outils DevOps, scripts, serveurs de test, de builds et de productions)
- Instauration du moindre privilège, n'autorisant que les permissions strictement nécessaires aux bonnes machines et images, et déploiement, configuration et correction des problèmes de production des machines et images
- Etablissement de frontières entre les systèmes de dev, de test et de production
- Réunion de toutes les fonctions sur une plateforme de gestion unique

Terminaux non traditionnels (IoT / IIoT, ICS, SCADA, et périphériques réseau)

L'IoT s'est généralisé dans les entreprises. D'autres terminaux non traditionnels se multiplient également dans les entreprises. Ces terminaux manquent souvent de fonctions de sécurité de base, ils ont souvent des identifiants embarqués, par défaut ou codés en dur, ils peuvent inclure des firmwares difficiles à corriger ou actualiser et induire de nombreux autres risques.

Le plus souvent, ces terminaux n'ont pas été conçus avec l'intention de les connecter au réseau de l'entreprise. Les systèmes de contrôles industriels (ICS, Industrial control systems) et SCADA (supervisory control and data acquisition), le plus souvent isolés pour protéger leurs fonctions stratégiques et pour garantir la sécurité des populations avoisinantes et de l'environnement, sont de plus en plus connectés et exposés. De plus, de nombreux fournisseurs ICS utilisent désormais des technologies IT standard au sein de leurs solutions, ce qui les rend plus accessibles aux attaques.

Les outils préexistants n'étaient généralement pas capables de découvrir, intégrer et gérer la sécurité de ces différents types de terminaux, encore moins à grande échelle. D'où la multiplication des expositions de sécurité dans tout l'environnement IT. Mirai et d'autres botnets, à l'origine de nombreuses perturbations ayant paralysé des entreprises, ne sont que la partie visible des compromissions de sécurité des dispositifs IoT. Des terminaux ICS et SCADA ainsi compromis pourraient endommager de façon catastrophique l'infrastructure et mettre en péril de nombreuses vies.

Comment les entreprises peuvent-elles s'y prendre pour sécuriser, à très grande échelle, le nombre croissant des terminaux non-traditionnels, des dispositifs IoT / et IoT industriel (IIoT), des terminaux SCADA et ICS, et même des simples périphériques réseau (routeurs, commutateurs, pare-feu) ?

BeyondTrust fut le premier à commercialiser une solution PAM avec contrôle granulaire des commandes et audit de l'activité des utilisateurs à privilèges sur les périphériques réseau, IoT, ICS et SCADA, venant s'ajouter à la plateforme BeyondTrust de gestion des accès privilégiés pour assurer la couverture de tous les terminaux. Avec la suite PAM intégrée de BeyondTrust, vous pouvez étendre les meilleures pratiques PAM à ces terminaux non traditionnels. Notre plateforme :

- Découvre l'ensemble des terminaux à gérer et les intègre
- Applique les meilleures pratiques de gestion des mots de passe, à savoir éliminer les identifiants embarqués/codés en dur et protéger les identifiants dans un coffre inviolable et centralisé
- Applique le contrôle granulaire du principe de moindre privilège, permettant de contrôler quelles commandes les utilisateurs peuvent exécuter
- Surveille et enregistre les sessions pour produire une piste d'audit complète de l'activité des utilisateurs
- Analyse les comportements pour détecter toute activité suspecte
- Prend en charge n'importe quel terminal SSH ou Telnet

Automatisation robotisée des processus

L'automatisation robotisée des processus ou RPA (Robotic process automation) est une méthode qui évolue rapidement, qui consiste à utiliser des robots logiciels pour éliminer les tâches laborieuses de routine qui viendraient sinon peser sur d'autres ressources IT. Mais les contrôles de sécurité RPA sont souvent inadaptés. Les outils RPA disposent souvent de droits excessifs avec des identifiants embarqués ou codés en dur permettant d'établir des connexions d'automatisation.

BeyondTrust sait étendre les meilleures pratiques PAM à votre déploiement RPA. Par exemple, la plateforme PAM de BeyondTrust intégrant DevOps Secrets Safe et Endpoint Privilege Management :

- Analyse, identifie, profile, catégorise dynamiquement et auto-intègre tous les actifs pouvant être inclus dans un workflow RPA et les ressources sous-jacentes
- Applique les meilleures pratiques de gestion des mots de passe, y compris l'élimination des identifiants RPA codés en dur ou embarqués, et protège l'entreprise du risque d'être exploitée de façon automatisée via une API compatible RPA
- Veille à la réinitialisation automatique des mots de passe après utilisation RPA pour assurer la sécurité du workflow
- Instaure le moindre privilège et le contrôle granulaire à l'échelle des processus RPA, des outils et des workflows
- Restreint l'accès aux seules applications autorisées

CE QUI DISTINGUE BEYONDTRUST

Pourquoi choisir un seul fournisseur pour tous les besoins de gestion des accès privilégiés ? Ce qui nous distingue sur le marché PAM, c'est la richesse et la profondeur de notre offre de solutions, la diversité des intégrations de tiers disponibles et notre position de leader et de précurseur depuis plusieurs décennies. Seul BeyondTrust propose une approche universelle de gestion des privilèges capable de protéger chaque utilisateur, chaque session et chaque terminal à l'échelle de tout l'environnement privilégié.

DIFFERENCIATEUR N°1 :

Richesse, profondeur et flexibilité de notre plateforme PAM

Selon les experts, BeyondTrust propose l'éventail le plus complet des solutions de gestion des accès privilégiés actuellement disponible. Dans son édition 2018 du Magic Quadrant consacré à la gestion des accès à privilèges, Gartner a nommé BeyondTrust comme étant le leader du marché du PAM, toutes catégories de solutions confondues.

Partant de l'instauration du principe de moindre privilège sur les systèmes Windows, Mac, Unix et Linux ; la gestion automatisée des mots de passe et des sessions ; la protection des accès distants des salariés et des tiers et l'intégration des systèmes Unix, Linux et macOS avec Microsoft Active Directory ; l'audit de l'activité des utilisateurs et des administrateurs, BeyondTrust unifie toutes ces fonctionnalités au sein d'une même plateforme intégrée, qui offre une gestion centralisée des règles et une interface de reporting.

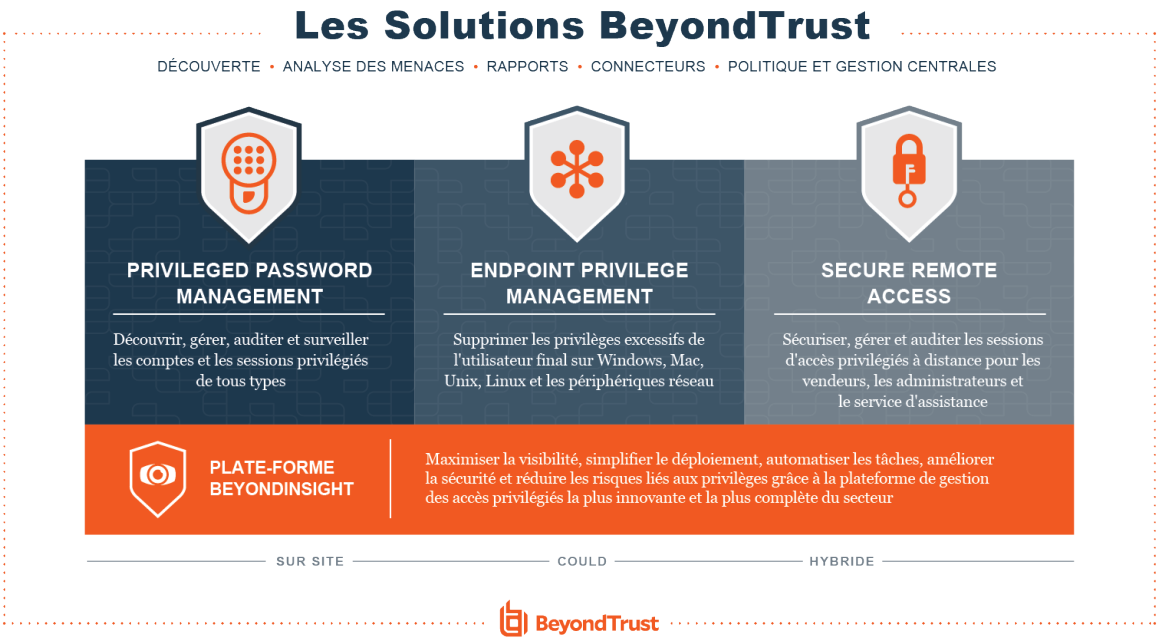

FIGURE 4: Les solutions BeyondTrust

La plateforme de gestion centralisée évolutive de BeyondTrust vous permet de déployer des fonctionnalités PAM complètes ou de progresser à votre rythme.

DIFFERENCIATEUR N°2 :

Précurseur de la sécurité – Révolutionne le PAM

BeyondTrust est un leader du PAM reconnu par les analystes, pour l'excellence de nos produits et l'exhaustivité de nos solutions, mais aussi pour notre capacité d'innovation. Nous pensons mériter cette reconnaissance. Voilà plusieurs décennies que BeyondTrust innove et propose des fonctionnalités inédites qui ont façonné l'univers PAM. Et nous ne comptons pas nous arrêter là.

Voici quelques innovations PAM de BeyondTrust, dont beaucoup sont brevetées :

- Première solution de moindre privilège pour Microsoft Windows
- Première solution de moindre privilège pour Apple macOS
- Première solution de gestion des privilèges des terminaux avec mécanisme intelligent inviolable capable de protéger les paramètres et le logiciel de moindre privilège de toute modification de processus élevés, tout en permettant à de vrais administrateurs système d'administrer la solution
- Première solution à intégrer une sécurité robuste des accès à distance permettant d'étendre les meilleures pratiques PAM aux fournisseurs et aux télétravailleurs
- Première plateforme intégrée couvrant l'ensemble des scénarios PAM communs aux grandes plateformes (Windows, macOS, Unix, Linux)
- Première solution PAM avec contrôle granulaire des commandes et audit de l'activité des utilisateurs à privilèges sur les périphériques réseau et terminaux IoT, ICS et SCADA, assurant la couverture de tous les terminaux
- Premier à commercialiser de nombreuses innovations de gestion des accès privilégiés Unix/Linux, dont :
  - » la technologie Advanced audit and control (ACA), d'audit des activités dans les scripts, de contrôle de l'accès aux fichiers et dossiers (même pour root) et de blocage des fichiers binaires malveillants et falsifiés
  - » Registry Name Services, avec basculement et équilibrage de charge automatiques et centralisés, gestion centralisée fondée sur le rôle et possibilité de regrouper des clients ayant en commun une configuration ou une règle d'après le rôle ou la division
  - » Surveillance de l'intégrité des fichiers, qui garantit que ce que vous autorisez à élever et les processus qui opèrent l'élévation ne sont pas compromis
- Première plateforme PAM disponible sur AWS Marketplace, sur Microsoft Azure Marketplace et sur Google Cloud
- Première solution PAM adaptée aux déploiements par des fournisseurs de services gérés ou MSP (Managed Service Provider), sur site ou dans le cloud

Pour de nombreuses fonctionnalités (accès à distance, Unix/Linux, etc.), nos concurrents les plus proches n'en sont encore qu'aux débuts, sans aucune comparaison avec la richesse et la profondeur de nos offres.

Et BeyondTrust poursuit sa révolution du marché PAM, avec la vision et la feuille de route les plus larges. Nous tentons toujours de répondre aux besoins futurs de nos clients en améliorant nos solutions, en termes de fonctions, de capacités et de facilité d'utilisation, tout en veillant à ce que notre plateforme couvre la plupart des scénarios PAM.

DIFFERENCIATEUR Nº3 :

Intégrations et interopérabilité avec les solutions de tiers pour mieux rentabiliser les investissements de sécurité

L'architecture des solutions et de la plateforme BeyondTrust est conçue pour favoriser l'intégration transparente et synergique des principaux outils tiers. Nous savons que la dernière chose dont vous avez besoin c'est d'une autre solution de sécurité silotée.

BeyondTrust vous permet d'avoir une compréhension holistique de l'ensemble des menaces actuelles liées aux risques internes et externes. Nos solutions incluent les données de sécurité pertinentes, exploits existants, activité privilégiée risquée, systèmes et applications vulnérables, exigences de conformité, atténuation des risques, etc., de façon à aider nos clients à prendre de meilleures décisions de sécurité.

La plateforme BeyondTrust peut intégrer les pares-feux de nouvelle génération (Palo Alto Networks, etc.) et des outils SIEM pour corréler les risques et aider à prendre de meilleures décisions. BeyondTrust propose également l'intégration de nombreuses solutions de gestion des accès et des identités (Okta, Onelogin, Savyint, etc.) et de gouvernance d'identité (Sailpoint, etc.). Par exemple, notre intégration System for Crossdomain Identity Management (SCIM) avec SailPoint permet de gérer efficacement l'accès des utilisateurs à privilègeset non privilégiés et d'utiliser l'authentification unique SSO. Les organisations IT obtiennent une visibilité totale sur les rôles assignés et les accès utilisateur, mais aussi sur l'ensemble des utilisateurs et les changements de rôles.

Nos intégrations de différentes plateformes d'assistance (ServiceNow, Cherwell Software, etc.) aident à renforcer la sécurité et à améliorer la productivité des services d'assistance IT.

Nous sommes également fiers d'être reconnus pour la deuxième année consécutive (2018 & 2017) par McAfee comme leur partenaire Security Innovation Alliance (SIA) de l'année, parmi 150 partenaires SIA. Nous avons fait certifier les intégrations Password Safe et Endpoint Privilege Management de BeyondTrust avec les solutions McAfee de sorte que les entreprises puissent mieux contrôler les risques et éliminer les menaces.

Intégrations à l'échelle de l'écosystème

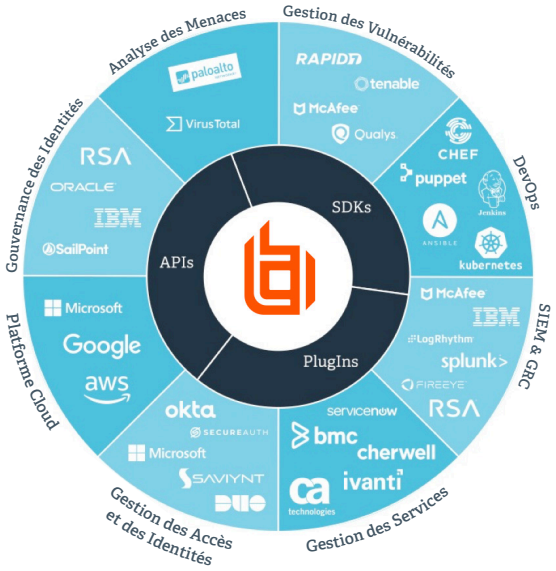

FIGURE 5: Echantillon des intégrations BeyondTrust aux technologie de tiers

Plus d'informations sur ce sujet sur notre page Partenaires.

DIFFERENCIATEUR N°4 :

Leader PAM reconnu

Qu'est-ce que les meilleurs analystes ont à dire au sujet de la gestion PAM ? BeyondTrust a été reconnu Leader de la gestion PAM (Privileged Access Management) à l'occasion des récentes études indépendantes de Gartner, Forrester Research et KuppingerCole. BeyondTrust se distingue par la richesse des scénarios PAM couverts, l'exhaustivité de notre solution, notre vision et notre capacité d'innovation technologique, et notre plateforme de gestion centralisée. Nous vous invitons à lire vous-même ces rapports :

- Gartner Magic Quadrant for Privileged Access Management
- The Forrester Wave™: Privileged Identity Management, 4ème trimestre 2018
- KuppingerCole Leadership Compass for Privileged Access Management

Gartner peerinsights customers' choice™

Nous avons également été distingués par le choix des clients de Gartner Peer Insights pour la gestion des accès privilégiés. Plus de 200 évaluations vérifiées de clients de BeyondTrust sont disponibles ici sur le site Gartner Peer Insights.

DIFFERENCIATEUR N°5 :

Grande expérience et présence mondiale

Plus de 20.000 clients dans plus de 80 pays font confiance aux solutions de BeyondTrust, soutenues par nos quelque 800 salariés dans une vingtaine de pays et notre vaste réseau mondial de partenaires. Avec plusieurs milliers de déploiements à son actif dans différents secteurs d'industrie et pour de nombreux scénarios de sécurité et de conformité réglementaire partout dans le monde, BeyondTrust dispose de la meilleure équipe pour vous aider à concrétiser vos objectifs PAM.

PROCHAINES ETAPES DE VOTRE PARCOURS PAM

Nous avons vu quelles fonctionnalités définissent une solution complète de gestion des accès privilégiés.

Pourquoi devenir partenaire de BeyondTrust ?

- Seul fournisseur PAM disposant d'une véritable plateforme unifiée, BeyondTrust apporte une formidable valeur ajoutée à ses clients, depuis la gestion et règles centralisées, au reporting intégré et à l'analyse des menaces. Résultat ? Des coûts et une complexité réduits et une meilleure couverture qu'avec des outils en silo.
- BeyondTrust est le seul fournisseur PAM à couvrir l'ensemble des scénarios PAM. Notre solution PAM complète inclut des fonctionnalités inexistantes chez nos concurrents, comme la fonctionnalité Privileged Remote Access intégrée pour les salariés et fournisseurs, et la surveillance de l'intégrité des fichiers. Une solution aussi complète réduit le niveau de complexité et accélère la rentabilisation.
- La richesse de nos solutions et la flexibilité de notre plateforme font que nous savons gérer les actuels scénarios de menace et nous préparer aux perspectives futures.
- Aucun fournisseur PAM n'offre autant de choix de déploiement : sur site, cloud privé ou SaaS.
- Comme nous vous donnons la priorité et que nous ne majorons pas le prix des fonctionnalités essentielles, BeyondTrust vous aide à optimiser votre ROI en toute sécurité.
- Because we put you first and *don't price gouge for capabilities that we believe are essential*, BeyondTrust maximizes your security ROI.

Synthèse des principales fonctionnalités PAM et avantages de BeyondTrust

- **Découvre, intègre et gère les identifiants privilégiés en toute sécurité**, pour les comptes humains et non-humains des différents environnements IT.
- **Gère et surveille toutes les sessions privilégiées** (y compris pause et/ou interruption des sessions suspectes en temps réel), et audite et rend compte de toutes les activités privilégiées, y compris liées aux accès de fournisseurs tiers.

- **Contrôle l'élévation et la délégation de privilèges, et instaure le moindre privilège** sur tous les terminaux (Windows, Mac, Unix, Linux), ICS, SCADA et périphériques réseau, etc. BeyondTrust vous permet d'élever le niveau d'accès aux applications, sans élever les droits de l'utilisateur.
- **Instaure l'accès juste à temps :** vérification que les comptes à privilèges ne sont pas toujours en état actif, de façon à réduire la fenêtre de menace.
- **Couvre le plus large éventail de scénarios d'accès à distance sécurisé.** Depuis l'extension des meilleures pratiques PAM et de la sécurisation des accès à distance des fournisseurs et des télétravailleurs jusqu'à la fourniture de solutions de support à distance sans pareil utilisées par les services support et les services de gestion IT, aucun autre fournisseur de sécurité IT ne traite la sécurité des accès à distance aussi globalement que BeyondTrust.
- **Authentifie les utilisateurs d'environnements hétérogènes** par l'extension de l'authentification AD Kerberos et de l'authentification unique à toutes les plateformes (Windows, macOS, Unix, Linux, etc.).
- **Permet de mieux guider les décisions liées aux privilèges en tenant compte du statut de vulnérabilité en temps réel :** technologie brevetée d'analyse automatique des applications en cours d'exécution pour mieux informer les équipes IT et de sécurité en vue d'appliquer la quarantaine, de réduire les privilèges des applications ou d'empêcher le lancement d'une application.
- **Offre un reporting complet avec analyse des menaces :** les fonctionnalités analytiques et de reporting réunies dans un même tableau de bord permettent aux équipes d'avoir l'information et les vues dont elles ont besoin pour bien gérer le risque lié aux utilisateurs, aux applications et aux actifs et justifier de la conformité.
- **Permet l'intégration étroite des technologies de tiers :** avec à la clé des synergies de gestion des risques, une meilleure visibilité, un contexte plus éclairant et de meilleures performances opérationnelles.

Principaux avantages des solutions PAM de BeyondTrust

- Atténuent les menaces externes (malwares, hackers, etc.) et internes
- Etablissent les responsabilités par la surveillance et l'enregistrement des sessions, l'enregistrement de frappe et l'audit en temps réel
- Protègent tout votre environnement IT, infrastructures sur site, cloud, hybrides et DevOps
- Permettent des décisions éclairées de gestion des risques IT à partir de données issues d'outils d'intelligence contextuelle de la sécurité, y compris les informations de privilèges des actifs, utilisateurs et comptes
- Favorisent la réussite des audits, le respect des obligations gouvernementales et de l'industrie et la production des rapports
- Réunissent les conditions de sécurité et de productivité des équipes et des partenaires
- Facilitent l'adoption de nouvelles technologies et initiatives métier

A PROPOS DE BEYONDTRUST

BeyondTrust est le leader mondial de la gestion des accès privilégiés (PAM), permettant aux organisations de sécuriser et de gérer l'ensemble de leur univers de privilèges. Nos produits et notre plateforme intégrés offrent la solution PAM la plus avancée du secteur, permettant aux entreprises de réduire rapidement leur surface d'attaque dans des environnements traditionnels, cloud et hybrides.

L'approche BeyondTrust Universal Privilege Management sécurise et protège les privilèges sur les mots de passe, les endpoints et les accès, donnant aux organisations la visibilité et le contrôle dont elles ont besoin pour réduire les risques, se mettre en conformité et augmenter leur productivité. Nos produits permettent d'attribuer le juste niveau de privilèges juste pour le temps requis, créant ainsi une expérience sans friction pour les utilisateurs et contribuant ainsi à plus de productivité.
Héritant de nombreuses années d'innovation et ayant fait leurs preuves auprès de clients partout dans le monde, les solutions BeyondTrust sont faciles à déployer, à gérer et à adapter à mesure que les entreprises évoluent. 20 000 clients, dont 70% du Fortune 500, et un réseau mondial de partenaires nous font confiance.

beyondtrust.com

ANNEXE : MODELE DE GUIDE DE L'ACHETEUR DE SOLUTIONS PAM

Principales fonctionnalités de gestion des identifiants privilégiés	BeyondTrust	Fournisseur A	Fournisseur B
Analyse complète du réseau, découverte et profilage avec auto-intégration des comptes à privilèges de tous types (comptes partagés admin, utilisateur, application et de service, clés SSH, comptes de base de données, comptes cloud et de réseaux sociaux, identifiants machine, DevOps, RPA, y compris des tiers/fournisseurs).	✓		
Information sur où et comment les mots de passe à privilèges sont utilisés, révélant les angles morts et les mauvaises pratiques (mots de passe par défaut, partagés et/ou embarqués, utilisation du même compte Admin pour plusieurs comptes de service, réutilisation des clés SSH sur plusieurs serveurs, etc.).	✓		
Gestion des identifiants sur toutes les plateformes (Windows, Unix, Linux, Cloud, sur site, etc.), annuaires, périphériques, applications, services/démons, pare-feu, routeurs, etc.	✓		
Centralisation, sécurisation et chiffrement de tous les identifiants privilégiés dans un coffre-fort/vault inviolable. (Idéalement, la solution prend en charge les algorithmes de chiffrement standard comme AES 256.)	✓		
Attribution dynamique de permissions d'après les données d'analyse.	✓		
Appels API pour éliminer les identifiants embarqués/codés en dur dans les fichiers, applications, scripts et autre type de code.	✓		
Rotation automatisée des mots de passe, clés SSH et autres secrets selon un calendrier défini, après chaque utilisation des comptes les plus sensibles ou pour les comptes ayant un fort risque d'exposition/de compromission.	✓		
Instauration de vos règles de gestion des mots de passe à privilèges, tel que la complexité des mots de passe, unicité (mots de passe différents pour chaque actif, compte, etc.), expiration, rotation, check in/check out, élimination des mots de passe par défaut, etc.	✓		

Suite à la page suivante...

Principales fonctionnalités de gestion des identifiants privilégiés	BeyondTrust	Fournisseur A	Fournisseur B
Automatisation des workflows sur tout le cycle de vie de gestion des mots de passe.	✓		
Contrôle d'accès granulaire.	✓		
Authentification unique (SSO) sans jamais révéler le mot de passe à l'utilisateur.	✓		
Surveillance et gestion rigoureuses de session pour établir un audit clair de toute l'activité privilégiée et mettre immédiatement en pause ou interrompre les sessions suspectes jusqu'à validation de leur légitimité.	✓		
Aucun outil de tiers nécessaire ni recours à Java pour la gestion de session, mais des outils natifs (MSTSC, PuTTY).	✓		
Instauration du principe de moindre privilège via un modèle de sécurité avec accès tout juste suffisant et juste à temps.	✓		
Interface moderne centralisée (HTML5) pour simplifier l'adoption et l'administration par les utilisateurs.	✓		
Intégration basée sur les standards, comme SAML et RADIUS, de n'importe quelle solution MFA. Utilisation des standards de l'industrie, comme SAML et RADIUS, pour s'intégrer à n'importe quelle solution d'authentification multi-facteurs (MFA).	✓		
Options break-glass (bris de glace) de consultation des mots de passe.	✓		
Stockage intégré des données et analyse des menaces pour l'ensemble des privilèges	✓		
Une seule solution complète et unifiée pour gérer les identités humaines (utilisateurs à privilèges) et non-humaines (application, machine, compte de service, etc.), avec surveillance/gestion de session incluses, sans autre interface ni frais supplémentaires.	✓		
Options de déploiement flexibles : appliances matérielles, appliances virtuelles, ou logiciels.	✓		

Principales fonctionnalités liées au moindre privilège sur Windows & Mac	BeyondTrust	Fournisseur A	Fournisseur B
Privilèges standard par défaut pour tous les utilisateurs de PC et serveurs, avec la possibilité d'élever des privilèges pour certaines applications et tâches spécifiques sans nécessiter d'identifiants à privilèges.	✓		
Puissantes couches de contrôle des applications pour les listes blanches des applications de confiance avec des règles larges ou granulaires au choix.	✓		
Restrictions d'installation et d'utilisation de logiciels, et de changements de configuration de l'OS.	✓		
Annulation de la nécessité pour les utilisateurs **de posséder deux comptes**	✓		
Décision de moindre privilège pour les applications fondée sur le risque de vulnérabilité de l'application en temps réel.	✓		
Conformité automatique des applications aux règles d'après les règles de l'actif ; recours aux règles intelligentes pour alerter et regrouper les dispositifs et les événements.	✓		
Surveillance des sessions, capture des écrans et enregistrement de la frappe lors des accès privilégiés.	✓		
Audit et reporting des changements apportés aux fichiers, règles, systèmes, applications et données critiques, de façon à éliminer les installations non autorisées de logiciels, les contournements ou failles pouvant être exploitées.	✓		
Technique permettant d'utiliser les vrais privilèges locaux ou de domaine au besoin.	✓		
Instauration du principe de moindre privilège via un modèle de sécurité avec accès tout juste suffisant et juste à temps.	✓		
Piste d'audit irréprochable de l'activité de tous les utilisateurs pour accélérer les investigations et simplifier la conformité.	✓		
Gestion, règles, reporting et analytique centralisés.	✓		
Intégration d'autres modules de gestion des privilèges pour une gestion complète des accès à privilèges.	✓		

Continued on next page...

Principales fonctionnalités liées au moindre privilège sur Windows & Mac	BeyondTrust	Fournisseur A	Fournisseur B
Stockage intégré des données et analyse des menaces pour l'ensemble des privilèges	✓		
Analyse du comportement des utilisateurs par la collecte, le stockage en toute sécurité et l'indexation des journaux de frappe, enregistrements de sessions et autres événements privilégiés.	✓		
Définition des règles via Active Directory Group Policy, Web Services ou McAfee ePO y compris aux actifs hors domaine.	✓		

Fonctionnalités pour les accès à distance privilégiés	BeyondTrust	Fournisseur A	Fournisseur B
Instauration du principe de moindre privilège en octroyant aux utilisateurs autorisés un accès tout juste suffisant pour leurs activités juste à temps dans le cadre de sessions à distance.	✓		
Contrôle et surveillance des sessions au moyen des protocoles standard des connexions RDP, VNC, HTTP/S et SSH.	✓		
Accès granulaire à des systèmes spécifiques, de façon à renforcer la sécurité et à éliminer l'accès « tout ou rien ».	✓		
Possibilité d'injection des identifiants directement dans la session d'accès; l'utilisateur n'a jamais besoin de voir ni de connaître l'identifiant. (y compris pour les comptes avec authentification MFA lors d'une session Web Jump Access).	✓		
Création d'une piste d'audit de visibilité de l'activité des fournisseurs sur le réseau, facilitant la conformité par le contrôle des chemins d'accès aux réseaux IT empruntés.	✓		
Gestion efficace des accès privilégiés aux actifs de votre entreprise qui dépendent de consoles d'administration web, y compris les serveurs IaaS, les environnements d'hyperviseur et les interfaces de configuration web pour vos infrastructures réseaux.	✓		
Intégration des outils existants comme SIEM, Change Management, SCIM et Password Management.	✓		

Suite à la page suivante...

Fonctionnalités pour les accès à distance privilégiés	BeyondTrust	Fournisseur A	Fournisseur B
Intégrations instantanées et transparentes avec ITSM, SIEM et SCIM et autres solutions logicielles d'entreprise courantes.	✓		
Authentification TouchID/FaceID auprès de la console mobile d'accès à distance privilégié.	✓		
Intégration basée sur les standards, comme SAML et RADIUS, de n'importe quel outil MFA.	✓		

Principales fonctionnalités de gestion des privilèges des serveurs pour Unix & Linux	BeyondTrust	Fournisseur A	Fournisseur B
Instauration du moindre privilège sans utiliser le compte Root.	✓		
Administration juste à temps (JIT), avec attribution de privilèges dynamiques aux comptes et actifs de sorte que les identités n'aient accès qu'aux privilèges nécessaires pendant une durée déterminée.	✓		
Contrôle granulaire et audit des applications, commandes, fichiers et scripts.	✓		
Enregistrement et indexation de toutes les sessions pour accélérer la découverte en cas d'audit.	✓		
Enregistrement adaptatif de la frappe pour les sessions les plus sensibles.	✓		
Totale visibilité avec piste d'audit de l'activité de chacun.	✓		
Consolidation des journaux d'audit et reporting centralisé à l'échelle de tous les domaines de serveurs.	✓		
Module d'authentification enfichable afin de pouvoir utiliser des systèmes d'authentification standard.	✓		

Suite à la page suivante...

Principales fonctionnalités de gestion des privilèges des serveurs pour Unix & Linux	BeyondTrust	Fournisseur A	Fournisseur B
Langage de règle puissant et flexible pour faciliter la migration depuis sudo.	✓		
Provisioning/déprovisioning transparents des privilèges, pour faciliter la mise en conformité.	✓		
Surveillance de l'intégrité des fichiers pour empêcher toute falsification des fichiers et binaires critiques.	✓		
API REST pour faciliter l'intégration des produits de tiers.	✓		
Support de nombreuses plateformes Unix et Linux.	✓		
Console web pour l'intégration de toutes les règles, des rôles et données des fichiers journaux.	✓		
Stockage intégré des données et analyse des menaces pour l'ensemble des privilèges	✓		

Principales fonctionnalités d'aide à l'élévation/la délégation de privilèges sur la base de risques en temps réel	BeyondTrust	Fournisseur A	Fournisseur B
Evaluation des niveaux de menace en temps réel pour l'utilisateur, l'actif sollicité et l'application exécutée.	✓		
Exécution d'actions pour les applications et les processus selon les règles définies (ex. autoriser l'escalade des privilèges, supprimer les permissions administratives ou empêcher une application de s'exécuter).	✓		
Révélation de risques émergents par l'identification et le reporting des types d'activités pouvant être à risque.	✓		
Activation de workflows avancés d'élévation/délégation de privilèges pour pouvoir prendre des mesures correctives d'élimination proactive des menaces potentielles, comme la fin d'une session ou l'intensification de consignation, audit et examen de la session privilégiée.	✓		

Principales fonctionnalités de gestion et d'analyse des menaces	BeyondTrust	Fournisseur A	Fournisseur B
Regroupe, évalue et rend compte des actifs par plage IP, convention de nommage, OS, domaine, applications, fonction métier, Active Directory, etc.	✓		
Permet l'orchestration rapide de la réponse de sécurité pour bloquer ou atténuer les menaces.	✓		
Autorise les importations d'Active Directory ou la personnalisation des permissions.	✓		
Corrèle les données de bas niveau de multiples solutions tierces pour révéler les menaces critiques.	✓		
Corrèle l'activité système avec une base de données de malwares actualisée en permanence.	✓		
Rend compte de la conformité, des bancs d'essai, de l'analyse des menaces, des scénarios hypothétiques, des besoins en ressources, etc.	✓		
Présente, trie et filtre les données historiques selon plusieurs perspectives.	✓		
Localise les actifs réseau (locaux et distants), web, mobiles, cloud et virtuels, ainsi que les comptes à privilèges.	✓		
Etablit les profils IP, DNS, OS, d'adresses Mac, des utilisateurs, des comptes, de l'âge des mots de passe, des ports, des services, des logiciels, des processus, des équipements et des fichiers journaux d'événements, etc.	✓		
Propose des workflows, systèmes de ticket et notifications pour coordonner les équipes IT et de sécurité.	✓		
Partage les données avec de grandes solutions SIEM, GRC, NMS, et d'assistance.	✓		

Principales fonctionnalités d'Active Directory Bridge	BeyondTrust	Fournisseur A	Fournisseur B
Authentification unique auprès de toute application supportant Kerberos ou LDAP.	✓		
Utilisation des mêmes outils pour gérer les systèmes Windows et Unix/Linux (ex. utilisateurs et ordinateurs Active Directory, ADUC).	✓		
Possibilité pour les utilisateurs d'utiliser leurs identifiants Active Directory pour l'accès à Unix, Linux et macOS, par la consolidation de fichiers de mots de passe, référentiels NIS et LDAP dans Active Directory, ce qui empêche de devoir gérer les comptes utilisateur séparément.	✓		
N'exige pas de modifications de schéma Active Directory pour l'ajout de systèmes Linux, Unix ou macOS au réseau.	✓		
Fournit un framework enfichable avec une interface comparable à Microsoft Management Console sur Linux ou macOS (la prise en charge de l'application Apple Workgroup Manager permet une gestion et un contrôle plus transparents des paramètres système macOS).	✓		
Prise en charge d'un large éventail de plateformes Unix, Linux et MacOS, y compris CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, Suse, RedHat, Solaris, Ubuntu, et d'autres.	✓		
Facilite la mise en conformité avec SOX, PCI, HIPAA et d'autres réglementations.	✓		
Fonctionnement au sein d'une famille de solutions de gestion des accès privilégiés.	✓		