



GUIDE: GESTION DES PRIVILEGES SUR LES ENDPOINTS

Apprenez-en davantage sur le moindre privilège et découvrez les bénéfices pour les entreprises



SYNOPSIS

Dans ce livre blanc, vous approfondirez vos connaissances sur ce qu'est la gestion des privilèges sur les endpoints et en quoi une approche efficace permet de renforcer la sécurité d'une entreprise au regard de la cybercriminalité croissante.

Nous évoquerons les origines du concept du « moindre privilège », les bénéfices du contrôle des applications dans le paysage actuel des cybermenaces et comment la gestion des privilèges sur les endpoints permet de lutter contre ces menaces sans nuire à la productivité des utilisateurs.

SOMMAIRE

1 Comprendre le paysage de la cybersécurité	3
2 Le concept du « moindre privilège »	5
3 Qu'est-ce que la gestion des privilèges sur les endpoints (EPM) ?	7
4 Exploitation de EPM à partir du Cloud (SaaS)	11
5 Présentation de la solution Endpoint Privilege Management de BeyondTrust	12
6 Bénéfices supplémentaires de la gestion des privilèges sur les endpoints	14
7 Comment déployer ce type de solutions ?	15
8 Synthèse	16
9 Prochaines étapes & ressources	16

1 Comprendre le paysage de la cybersécurité

Pour mieux comprendre le rôle de la gestion des privilèges sur les endpoints dans le contexte actuel, il convient d'abord de comprendre le climat de cybersécurité dans lequel nous évoluons. Mais avant d'entrer dans les détails de cette technologie et de ses bénéfices, examinons quelques-unes des études les plus récentes de façon à dresser un portrait juste et objectif du paysage en 2019 et au-delà.

McAfee Labs

Dans son [rapport sur les menaces](#), daté de décembre 2018, McAfee Labs a identifié 63 millions de nouveaux échantillons de malwares - un record.¹ Le nombre total d'échantillons dans la base de données a ainsi dépassé la barre des 837 millions.

Raj Samani, Chief Scientist chez McAfee, explique que « les agresseurs continuent de tirer profit des fonctionnalités bénignes et dynamiques des technologies de plateformes comme PowerShell, de l'imprudence constante des victimes de phishing, et du laxisme tout aussi fréquent des entreprises qui peinent à corriger les vulnérabilités en installant les patchs et mises à jour de sécurité disponibles ».

Dans son rapport sur les menaces, McAfee explore les secteurs les plus vulnérables aux cyberattaques. Tandis que le nombre des incidents rapportés est en recul de 12%, ceux concernant le secteur public ont progressé de 150% depuis le précédent trimestre et ceux visant la finance de 64%.

Autre information de ce rapport : la progression tout au long de 2018 d'un nouveau malware JavaScript qui ne montre aucun signe de ralentissement. Dans le monde, les malwares mobiles ont progressé de 46% l'an dernier, atteignant 24 millions d'échantillons, et les échantillons de ransomware ont progressé de 45% pour dépasser les 18 millions.⁵ Il est évident que le cybercrime s'intensifie avec des assaillants qui emploient de nouvelles méthodes de compromissions difficiles à détecter. Quand on considère que 80% des compromissions de sécurité impliquent des identifiants privilégiés,⁶ il n'est plus possible d'ignorer les dangers associés aux droits admin.



« La croissance de 100 milliards de dollars du cybercrime s'explique par l'adoption de nouvelles technologies par les cybercriminels, la facilité de perpétrer des cybercrimes, y compris la multiplication des centres de cybercrime, et la sophistication financière croissante des meilleurs cybercriminels. »

[ECONOMIC IMPACT OF CYBERCRIME – NO SLOWING DOWN, MCAFEE, FEB. 2018](#)

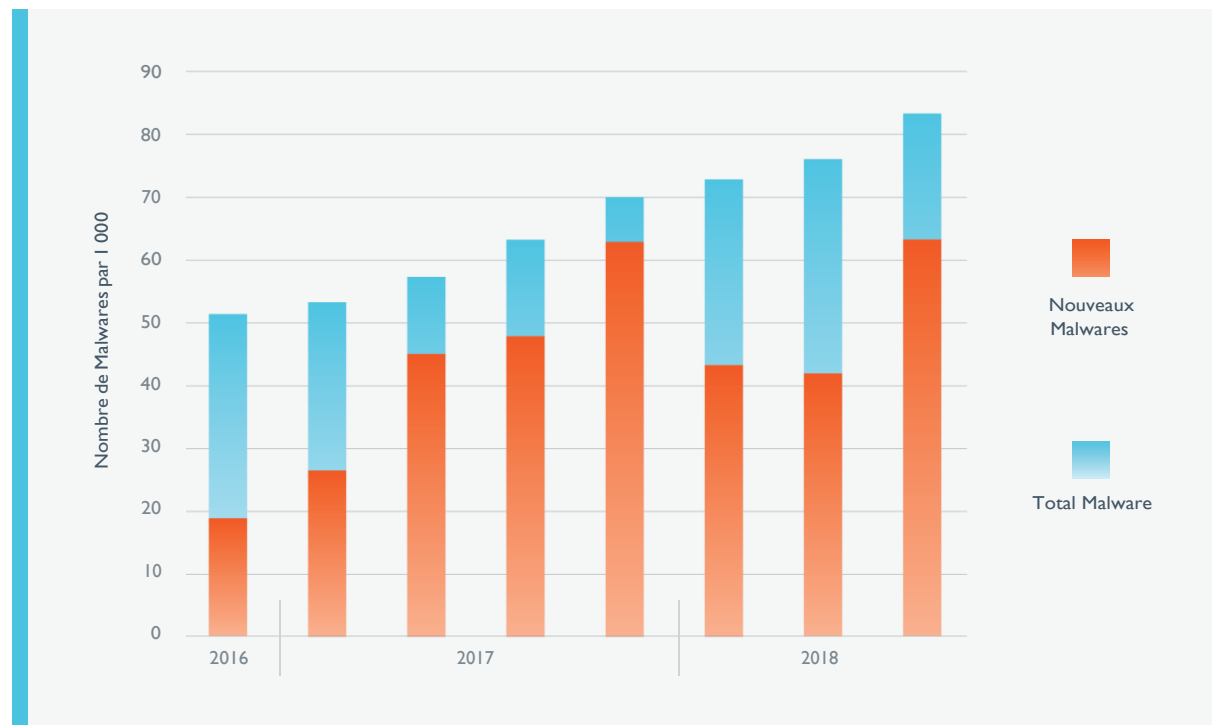


Figure 1: Statistiques des Malwares 2016-2018 (McAfee Labs Threat Report Dec. 2018)

2

Le concept
du « moindre
privilège »

Pour déterminer l'efficacité des solutions de gestion des privilèges sur les endpoints dans la lutte contre les cyberattaques, nous devons d'abord envisager le principe de sécurité sous-jacent du « moindre privilège ».

Disposer de droits admin locaux confère à un utilisateur les privilèges dont il a besoin pour lancer la plupart sinon toutes les fonctions à partir du système d'exploitation d'un ordinateur. Ces privilèges permettent notamment d'installer des pilotes logiciels et matériels, de changer les paramètres système et d'installer des mises à jour système. Les utilisateurs peuvent aussi créer des comptes utilisateur et changer leurs mots de passe. Les très nombreuses entreprises qui attribuent des droits admin locaux pour faciliter le support IT s'exposent à des risques élevés de compromission de sécurité.

Approche courante de gestion des comptes utilisateur privilégiés, le modèle du « moindre privilège » consiste à attribuer aux utilisateurs et aux programmes le juste niveau de permission pour effectuer des tâches spécifiques.

« Les entreprises devraient appliquer le principe du « moindre privilège » aux accès admin locaux. La grande majorité des utilisateurs n'a pas besoin d'un accès admin local dans l'OS Windows moderne. Quand une application ou un service requiert un privilège administrateur, l'utilisateur doit se connecter comme un utilisateur standard, puis élever les privilèges selon la règle en vigueur. »

[REDUCE ACCESS TO WINDOWS LOCAL ADMINISTRATOR WITH ENDPOINT](#)

[PRIVILEGE MANAGEMENT, OCTOBER 20, 2017](#)

Le concept du « moindre privilège » n'est pas un phénomène récent. Il date d'octobre 1974, quand Jerome H. Saltzer et Michael D. Schroeder ont publié un article intitulé '[The Protection of Information in Computer Systems](#).' Cet article explore la mécanique de protection d'informations enregistrées sur un ordinateur contre les tentatives d'utilisation ou de modification non autorisées et, ce faisant, il souligne le plus ancien principe de « moindre privilège » :

« Chaque programme et chaque utilisateur du système devraient fonctionner avec le niveau minimum de privilèges nécessaires pour faire son travail. Ce principe limite essentiellement les dommages pouvant résulter d'un accident ou d'une erreur. Il réduit également au minimum le nombre d'interactions potentielles des programmes privilégiés pour réaliser l'opération, de sorte que les usages accidentels, indésirables ou impropres des privilèges risquent moins de se produire. »

Même si l'approche du « moindre privilège » date d'il y a plus de 40 ans, elle demeure une mesure de sécurité fondamentale pour les entreprises qui cherchent à se protéger de l'intensification des attaques malveillantes. Il s'agit essentiellement de retirer les droits admin locaux aux utilisateurs.

Le « moindre privilège » est encore plus efficace lorsqu'il est combiné avec le concept de liste blanche des applications. Il s'agit d'établir un index des applications logicielles autorisées à être présentes et actives sur un système informatique. L'objectif est de protéger les ordinateurs et les réseaux des applications potentiellement dangereuses.

Une solution efficace établira des règles en fonctions des types d'applications autorisées, empêchant ainsi automatiquement l'exécution des applications non approuvées. L'intégration de ces deux approches aboutit à la gestion des privilèges sur les terminaux.

Les méthodes permettant d'obtenir le moins de privilèges possible ont quelque peu évolué depuis la création du concept, car les utilisateurs cherchent des moyens de mettre en place les meilleures pratiques, de rendre le déploiement plus simple et d'offrir un délai de rentabilité rapide.

Ainsi, il est désormais possible de prendre des mesures importantes en faveur d'un environnement à moindre privilège grâce à des solutions basées sur le logiciel-service (SaaS), qui offrent tous les avantages susmentionnés du cloud sous forme d'abonnement. Ce point sera abordé plus en détail dans la prochaine section.

3 Qu'est-ce que la gestion des privilèges sur les endpoints ?

Les endpoints sont des dispositifs auxquels les utilisateurs se connectent - des ordinateurs Windows ou Mac, fixes ou portables, et des serveurs - et où l'on exécute des applications. Les technologies de gestion des privilèges sur ces terminaux permettent aux entreprises de contrôler quelles actions peuvent ou ne peuvent pas être exécutées par un endpoint donné.

Dans de nombreuses entreprises, tous les utilisateurs ou une partie d'entre eux ont des droits admin complets, qui leur permettent d'exécuter des applications inconnues. Ainsi les malwares peuvent tourner avec des privilèges élevés, les contrôles de sécurité peuvent être contournés et il est possible d'installer et d'exécuter des logiciels sans contrôle ni visibilité.

Les entreprises ont tendance à attribuer des droits admin locaux à tous leurs salariés pour faciliter la gestion du support IT et des pertes de productivité. Ce faisant, elles exposent leurs données confidentielles à plus de risques, notamment de vol par des hackers.

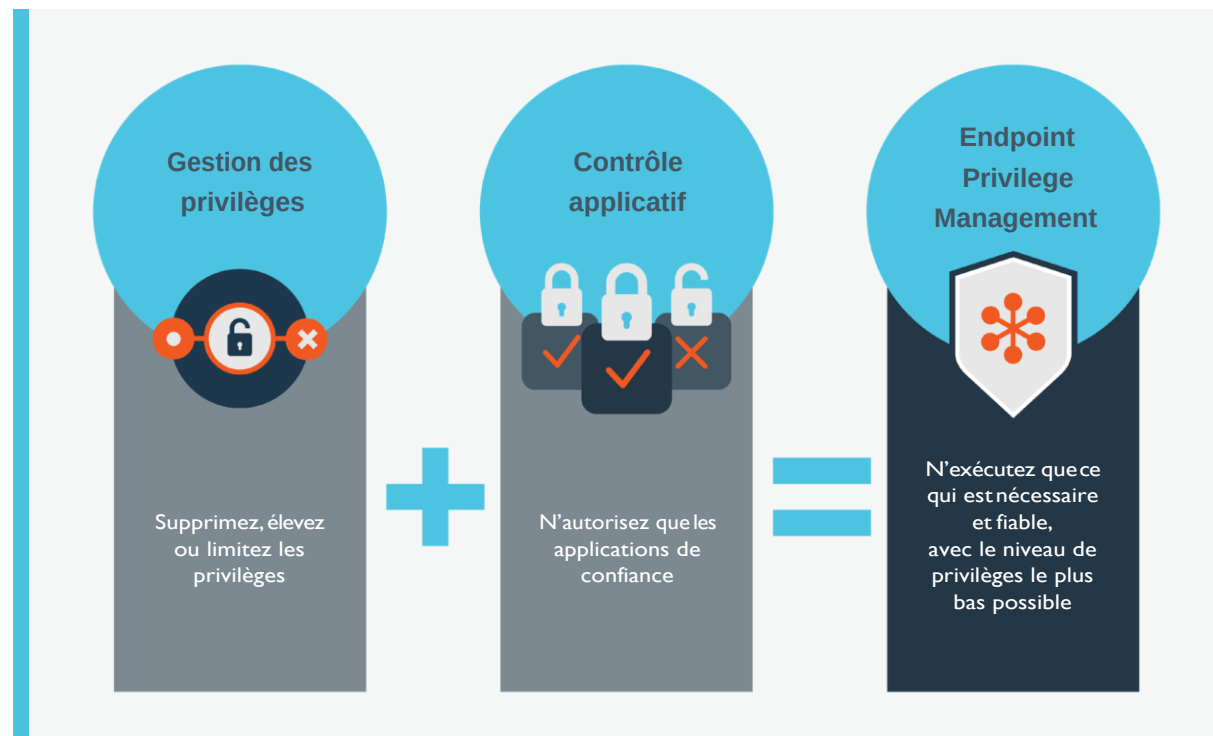


Figure 2: Le combo gagnant : gestion des privilèges et contrôle applicatif

Dans son livre blanc, l'analyste Lori Robinson de Gartner définit clairement la gestion des privilèges sur les terminaux comme la combinaison de la gestion des privilèges et du contrôle applicatif :

« Les technologies Endpoint Privilege Management (EPM) combinent le contrôle applicatif et la gestion de privilèges pour faire en sorte que seules les applications de confiance tournent avec des privilèges aussi restreints que possible. Avec l'EPM, les entreprises peuvent supprimer l'accès admin local avec un impact minime sur les utilisateurs. »

« Grâce à l'élévation à la demande des privilèges, le Endpoint Protection Management fournit automatiquement aux utilisateurs les privilèges nécessaires pour exécuter les applications de confiance et effectuer les tâches autorisées. Des fonctions en libre-service, de workflow et d'auto-élévation assurent une protection supplémentaire et offrent aux utilisateurs l'accès à des opérations non encore approuvées. »

Selon Gartner, la gestion des privilèges sur les endpoints « utilise la gestion des privilèges et le contrôle applicatif pour déterminer si l'application est exécutable et si oui, sous quelles conditions de privilèges. »

La gestion des privilèges sur les endpoints consiste à offrir un accès suffisant à vos salariés pour qu'ils demeurent productifs, sans leur concéder des droits admin complets sur vos systèmes IT.

L'accès est autorisé au niveau de l'application et non de l'utilisateur. Ainsi, les salariés n'obtiennent pas d'autorisation pour plus, et encore moins pour moins que le minimum nécessaire pour la tâche à accomplir.

Utiliser la gestion des privilèges sur les endpoints pour lutter contre les menaces

Le contrôle applicatif et le « moindre privilège » sont une combinaison efficace dans la prévention des malwares.

Dans sa parution [Architecting Privileged Access Management for Cyber Defense](#), l'analyste de Gartner Homan Farahmand note que « le paysage des menaces liées aux accès privilégiés, en se développant, accentue le risque de cyberattaques avec de lourdes conséquences à la clé. Les professionnels techniques doivent concevoir les fonctionnalités de contrôle des accès privilégiés de sorte à ce qu'elles permettent de se défendre contre les scénarios d'exploitation et résister à des attaques persistantes avancées. »

Lori Robinson de Gartner explique que « en cas d'abus ou de compromission de l'accès admin local, les conséquences peuvent être un affaiblissement de la sécurité, la perte de données, des coûts de support élevés et une piètre expérience utilisateur... Les utilisateurs avec des droits admin locaux complets ont le contrôle total du terminal, y compris :

- | Installer ou exécuter des processus ou applications non autorisés
- | Installer des malwares exploitant l'accès privilégié (intentionnellement ou non)
- | Désactiver les paramètres système et de sécurité
- | Appliquer les changements de système de fichiers
- | Changer la configuration standard du poste de travail »

Et si les droits admin locaux ne sont pas aussi puissants que les privilèges de domaine ou de serveur, ils ne peuvent être ignorés pour autant. Il est en effet possible d'exploiter des droits admin locaux pour obtenir l'accès à des contrôles réseau supplémentaires (comme l'accès au domaine ou à l'application).



« Les accès excessifs des salariés sont l'un des risques non contrôlés qui se développent le plus simplement parce que les entreprises ignorent par où commencer. »

ROBERT HERJAVEC, CEO ET FONDATEUR DE HERJAVEC GROUP

L'édition la plus récente du Microsoft Vulnerabilities Report révèle, qu'au cours des cinq dernières années, 81% de toutes les vulnérabilités Microsoft critiques découvertes auraient pu être évitées par le retrait des droits admin

Identifier la bonne solution et la mettre en place

La gestion des privilèges sur les endpoints ou Endpoint Privilege Management est vitale pour la sécurité d'une entreprise mais perçue depuis toujours comme difficile à déployer avec, si l'on n'y prend pas garde, un plus gros volume d'appels du support IT au gré des difficultés d'accès aux documents ou applications.

Robinson de Gartner souligne que « réduire l'accès aux droits admin locaux est l'une des meilleures options pour améliorer la sécurité Windows. Toutefois, il n'est pas simple de concilier les restrictions d'accès avec l'expérience utilisateur. »

Des fonctionnalités de gestion des exceptions s'imposent pour maintenir la productivité des utilisateurs, même dans le contexte d'un compte utilisateur standard.

Une méthode populaire pour gérer les demandes nouvelles et inconnues est de fournir une simple « invite » de code. L'utilisateur doit demander au support IT un code d'authentification pour poursuivre. C'est la garantie d'une couche de sécurité supplémentaire, le professionnel IT étant capable de déterminer si l'action présente un niveau de risque ou si elle peut être mise sur liste blanche à l'avenir.

« Les technologies de gestion des privilèges sur les terminaux peuvent servir à élever, gérer et contrôler l'accès des utilisateurs. La solution la plus légère pour la gestion des privilèges Windows est la solution native User Account Control (UAC), mais il lui manque la finesse des contrôles et fonctionnalités de reporting des autres solutions EPM sur le marché. » DR. JESSICA BARKER, CO-CEO OF CYGENTA & PRÉSIDENTE DE CLUBCISO

4 Exploitation de EPM à partir du Cloud (SaaS)

Le déploiement de la gestion des privilèges sur les endpoints à partir du cloud permet aux clients d'éliminer plus facilement les privilèges inutiles et de stopper les attaques malveillantes en appliquant le principe du moindre privilège sur leurs systèmes Windows et Mac.

Une solution EPM en mode SaaS compétente peut offrir la même disponibilité, sécurité, accès et évolutivité qu'une offre on-prem, tout en supprimant les frais généraux de gestion de l'infrastructure.

Pour les entreprises qui cherchent à réduire les risques liés aux accès privilégiés sans ajouter de charges administratives et financières à leur organisation, les solutions SaaS se caractérisent par un déploiement rapide et rendent la gestion des accès privilégiés plus simple et plus rentable. Une offre SaaS est disponible sous forme d'abonnement, ce qui permet aux clients de ne payer que ce dont ils ont besoin et de le faire évoluer en fonction de leur activité.

Dans l'étude susmentionnée, lorsque nous avons demandé si une solution SaaS pour l'EPM serait une perspective intéressante, 58 % du panel a répondu par l'affirmative, tandis que 33 % a déclaré que cela ne ferait aucune différence.

Parmi les six principales raisons invoquées pour expliquer les avantages d'une solution SaaS EPM, nous trouvons :

- | Simplicité de gestion
- | Meilleure évolutivité et grande flexibilité
- | Amélioration de l'expérience client
- | Amélioration de la productivité/efficacité
- | Réduction de la charge de travail du personnel informatique
- | Solution mise à jour plus régulièrement



Si le principe du moindre privilège est appliqué correctement et que l'utilisateur n'a pas besoin des privilèges admin pour son travail quotidien alors l'attaquant devra faire beaucoup plus d'efforts pour faire escalader les privilèges et se déplacer latéralement vers d'autres machines.

PAULA JANUSZKIEWICZ, CYBERSECURITY EXPERT

5

**Présentation
de la solution
Endpoint
Privilege
Management de
BeyondTrust**

Avec [Endpoint Privilege Management](#), vous pouvez éliminer les privilèges superflus et élever les droits des systèmes Windows, Mac, Unix, Linux et en réseau sans ralentir la productivité.

Nous associons le meilleur de la gestion de privilèges et du contrôle applicatif, facilitant le retrait des droits admin pour plus de conformité, de sécurité et d'efficacité. La solution se déploie en quelques heures, s'appuie sur plus de 20 critères de validation pour élever les applications en toute sécurité et flexibilité, et évolue aisément pour répondre aux besoins des entreprises les plus importantes et complexes. Un moteur de règles puissant et des fonctions de traitement des exceptions aident à réduire l'impact sur les utilisateurs et les équipes IT.

Voici six des caractéristiques de notre solution Endpoint Privilege Management :

1. Instauration du moindre privilège

Elevez les privilèges d'accès aux applications pour les utilisateurs standard sous Windows ou MacOS via des contrôles granulaires basés sur des règles définies, afin de réduire la surface d'attaque en n'octroyant que l'accès nécessaire pour effectuer une tâche donnée.

2. Contrôle transparent des applications

Instaurez une liste blanche d'applications de confiance avec un moteur de règles flexible pour définir des règles, choisir l'approbation automatique pour les utilisateurs avancés, protégés par des pistes d'audit complètes, ou utilisez des codes « challenge – réponse ».

3. Gestion applicative basée sur les vulnérabilités

Utilisez les données de vulnérabilités des applications fournies par BeyondTrust Enterprise Vulnerability Management pour bénéficier de renseignements en temps réel sur le risque des applications visées pour l'élévation des privilèges.

4. Audit et reporting

Etablissez une traçabilité infalsifiable de l'activité de tous les utilisateurs, accélérez les opérations post-mortem et simplifiez la mise en conformité grâce à un reporting complet.

5. Analyse des menaces privilégiées

Corrélez le comportement des utilisateurs avec les données de vulnérabilités des ressources et les informations de sécurité issues des meilleures solutions de sécurité afin de fournir une vision complète et globale des risques pour les utilisateurs finaux.

6. Intégrations de l'écosystème de sécurité

Des connecteurs intégrés aux solutions tierces, y compris aux logiciels de support technique, aux scanners de vulnérabilités, aux SIEM, etc. permettent une rentabilisation rapide des investissements dans la sécurité.

Ceci n'est pas une liste exhaustive, mais Endpoint Privilege Management permet de lutter contre les vecteurs d'attaque suivants :

- | Installation de spyware et adware
- | Accès aux données appartenant à d'autres utilisateurs
- | Remplacement des fichiers d'OS et d'autres programmes par un cheval de Troie
- | Désactivation/désinstallation d'anti-virus
- | Création et modification des comptes utilisateur
- | Réinitialisation des mots de passe locaux
- | Bascule de la machine en mode non-bootable
- | Exposition de réseaux entiers à des malwares, virus et attaques par déni de service (DOS)
- | Corruption ou manipulation de données
- | Changements de configuration de tout un système
- | Fuite de données sensibles
- | Désactivation de fonctions/produits de sécurité

L'installation d'une solution complète de gestion des privilèges sur les endpoints permet non seulement de réduire les menaces précédemment citées, mais aussi de renforcer la productivité.

6 Bénéfices supplémentaires de la gestion des privilèges sur les endpoints

Les principaux avantages de la gestion des privilèges sur les terminaux sont l'atténuation des menaces internes et externes, l'aide à la mise en conformité et la nette amélioration de l'efficacité opérationnelle.

Mais le déploiement de BeyondTrust Endpoint Privilege Management apporte aussi d'autres bénéfices.

1. Visibilité accrue sur les privilèges

Si elle est efficace, la solution veillera à ce que vous ayez suffisamment de visibilité et de contrôle sur les activités de votre entreprise. Vous saurez quelles sont les applications utilisées et installées, quelles tâches et applications ont besoin de privilèges et combien d'utilisateurs disposent de droits admin locaux. Les fonctionnalités de reporting favorisent la visibilité et les audits. Des tableaux de bord et rapports complets permettent d'avoir accès à un niveau de détail poussé si nécessaire.

2. Gestion des systèmes / applications vieillissants

Les logiciels et applications obsolètes créent des vulnérabilités et sont visés par les hackers, surtout quand ils nécessitent des droits admin. Selon le rapport Remediation Gap de Kenna Security, la plupart des entreprises attendent 100 à 120 jours pour corriger les vulnérabilités et beaucoup ne les corrigent même pas. La solution Endpoint Privilege Management de BeyondTrust vous permet de créer des listes blanches pour gérer les applications de confiance et bloquer les versions datées ou non autorisées des logiciels.

3. Travailleurs distants

Les télétravailleurs ou salariés itinérants ont généralement besoin de flexibilité pour modifier les paramètres, installer des logiciels et mettre à jour des applications en toutes circonstances. Etablir des règles de flexibilité basse, moyenne ou élevée vous permet d'accorder les privilèges en fonction du rôle, et d'assurer ainsi productivité et sécurité.

4. Accès des tiers

Le fait d'accorder des droits admin à des utilisateurs externes pose un risque de sécurité. Une solution efficace de gestion des privilèges sur les terminaux permet aux tierces parties de faire ce qu'elles ont besoin de faire uniquement (sur les seuls serveurs concernés) au moyen d'applications et de processus autorisés, pendant un intervalle donné, sur un emplacement validé.

7

**Comment
déployer ce
type de
solutions ?**

Cela prend généralement des mois pour déployer une solution de gestion des privilèges sur les endpoints. Et c'est une tâche laborieuse que de configurer la solution selon les besoins spécifiques d'une entreprise. Or en s'appuyant sur des années d'expérience en termes de scénarios de déploiement, BeyondTrust a créé des modèles prêts instantanément et adaptés à la majorité des besoins des entreprises.

Ainsi vous pouvez rendre Endpoint Privilege Management opérationnel en une nuit pour réaliser rapidement des gains de sécurité, puis affiner les paramétrages au fil du temps. Cette base de référence vous permet de renforcer la sécurité sans nuire à la productivité des utilisateurs. Aucune autre solution n'offre ce niveau de confort, de flexibilité ni cette rapidité de déploiement.

La règle Quick Start permet aux entreprises d'appliquer trois modèles selon les besoins de flexibilité du rôle :

Flexibilité basse (stagiaires, intérimaires, sous-traitants)

Les utilisateurs sont invités à entrer un code PIN généré informatiquement. Ainsi un professionnel IT compétent peut vérifier toute installation de logiciel ou modification apportée au système afin de déterminer le niveau de risque en amont.

Flexibilité moyenne (front-office, ventes)

L'authentification est requise, si bien que les utilisateurs doivent indiquer leurs identifiants pour installer des applications. Ceci permet d'ajouter une couche de sécurité supplémentaire entre des installations potentiellement dangereuses et votre réseau.

Flexibilité élevée (ingénierie, IT, QA)

Ceci est le modèle le plus flexible puisque les utilisateurs sont invités à indiquer une raison professionnelle valable avant de pouvoir installer des applications ou modifier le système. Pour faire leur travail, il leur faut un tel accès.

BeyondTrust collecte des données précises sur le comportement des utilisateurs, avec une analyse des tendances pour identifier les applications qui ont besoin de privilèges plus élevés, lesquelles s'exécutent depuis le profil de l'utilisateur et lesquelles sont installées. Ces données servent ensuite à créer des modèles personnalisés et donc adaptés à votre entreprise, à mesure que vous affinez votre déploiement. Ainsi, vous élevez seulement les applications dont chaque utilisateur a besoin, de sorte que seules les applications de confiance puissent être exécutées.

8 Synthèse

Nous espérons que ce livre blanc vous aura apporté un éclairage efficace et pertinent sur la gestion des privilèges sur les terminaux, mais aussi sur ses avantages à court et long termes pour les entreprises de toutes les tailles. Si l'expression est en elle-même relativement récente, le concept est dans l'air depuis un moment, ce qui en fait une méthode largement testée et validée.

En combinant gestion des privilèges et contrôle applicatif, notre solution Endpoint Privilege Management aide les entreprises à réduire le risque d'une compromission de sécurité, sans nuire à la productivité. Si vous souhaitez en savoir plus sur la façon dont BeyondTrust peut vous aider à gérer et contrôler vos comptes privilégiés, inscrivez-vous pour bénéficier d'une démo gratuite.

9 Prochaines étapes & ressources

En traitant les droits d'admins non gérés, vous pouvez rapidement assurer la sécurité des endpoints tout en éliminant les failles de sécurité et en respectant les exigences de conformité, sans entraver la productivité des utilisateurs.

Contactez BeyondTrust dès aujourd'hui pour programmer une démonstration de Endpoint Privilege Management et consulter ces ressources supplémentaires.

Livre Blanc

| [Microsoft Vulnerabilities Report 2020](#)

Case Study

| [How the University of Derby Secure their Endpoints with BeyondTrust](#)

Vidéo

| [A Two-Minute Overview of our Endpoint Privilege Management Solution](#)

Fiches Produits

| [Privilege Management for Windows & Mac](#)

| [Privilege Management for Unix & Linux](#)

À PROPOS DE LA GESTION DES PRIVILÈGES SUR LES ENDPOINTS

[Endpoint Privilege Management](#) de BeyondTrust élève les privilèges au rang d'applications connues qui les requièrent, contrôle l'utilisation des applications, enregistre et génère des rapports sur les activités des comptes privilégiés.

Grâce au contrôle granulaire des applications, aux multiples options de déploiement et à la fonction unique de démarrage rapide, il n'a jamais été aussi simple d'obtenir le moins de privilèges possible sans nuire à la productivité des utilisateurs.

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/fr