BeyondTrust

Renforcez Vos Effectifs Distants En Toute Sécurité

Maintenez La Productivité Des Télétravailleurs Sans Risque Pour La Sécurité

INTRODUCTION

Les services IT sont sous pression comme jamais pour maintenir la productivité d'effectifs en télétravail qui n'ont jamais été aussi nombreux que depuis quelques semaines.

Comme beaucoup d'équipes IT en sont à faire des heures supplémentaires au service des télétravailleurs, la priorité n'est peut-être pas au maintien des pratiques de sécurité et de la conformité, alors même que les **cybercriminels sont à l'affût d'opportunités** pour tirer profit des circonstances.

Si la gestion d'équipes distantes fait normalement partie des pratiques courantes, des **considérations urgentes et inédites** viennent peser sur les entreprises et leurs salariés en cette crise du coronavirus.

Les agresseurs sont volontiers opportunistes. **Les hackers visent les entreprises avec de grandes surfaces d'attaque en raison de politiques de sécurité obsolètes ou au moindre signe de relâchement des mesures de sécurité en période de crise.**

Les plus gros poissons ne sont pas les seuls visés. **Les PME et les administrations publiques locales, comme les écoles, sont particulièrement victimes de malwares et de ransomwares depuis quelques années.**

SOMMAIRE

IMPACT DU COVID-19

Quels sont les défis les plus urgents en matière de sécurité pour les effectifs en télétravail?

De nombreuses entreprises ont dû basculer en télétravail dans un laps de temps très court. Certaines ont pu équiper leurs salariés avec des machines correctement configurées et protégées, mais ce ne sont pas les plus nombreuses.

Voici quelques pratiques de télétravail qui créent des risques :

Pratiques Génératrices de Risques

- Relâchement des règles BYOD (bring your own device)
- Utilisation personnelle de PC portables professionnels, pour l'école à la maison par exemple
- Utilisation d'outils d'accès à distance mal protégés ou datés pour se connecter au réseau
- Utilisation de VPN « always-on » pour les connexions de tous les utilisateurs, même si certains n'ont besoin que d'applications et de données basées dans le cloud
- Ouverture d'e-mails malicieux, plus nombreux en cette période de pandémie
- Téléchargement de logiciel possiblement malveillant, avec le risque de propager un malware dans votre environnement de l'entreprise

Le Gartner a récemment mené une étude, « Solving the Challenges of Modern Remote Access »,* pour éclairer les responsables des risques et de la sécurité sur les problématiques liées à la montée en charge rapide des accès à distance à grande échelle. Cette étude conclut que **la plupart des entreprises n'ont la capacité et les licences que pour un petit nombre d'utilisateurs et qu'elles ne sont pas préparées à basculer l'ensemble de leurs effectifs en télétravail** sur des périodes aussi longues que celle imposée par le COVID-19. De plus, les entreprises n'ont généralement pas la bande passante suffisante pour que tous puissent opérer à distance simultanément.

Gartner, « Solving the Challenges of Modern Remote Access », Rob Smith, Steve Riley, Nathan Hill, Jeremy D'Hoinne, 25 mars 2020

Certaines pratiques d'hygiène de la cybersécurité, correctement gérées en temps normal, peuvent exposer l'entreprise à des risques :

- Partage d'appareil
- Connexions Internet sans fil mal sécurisées
- Réutilisation ou partage de mots de passe
- Ouverture d'e-mail contenant un ransomware
- Téléchargement de logiciel possible vecteur de malware
- Conservation des mots de passe dans des endroits mal protégés ou sur des feuilles volantes

Comment les entreprises peuvent-elles fournir des outils sûrs de télétravail pour maintenir la continuité de l'activité et éviter de tomber dans le piège de cyberattaques?

SUPPORT IT

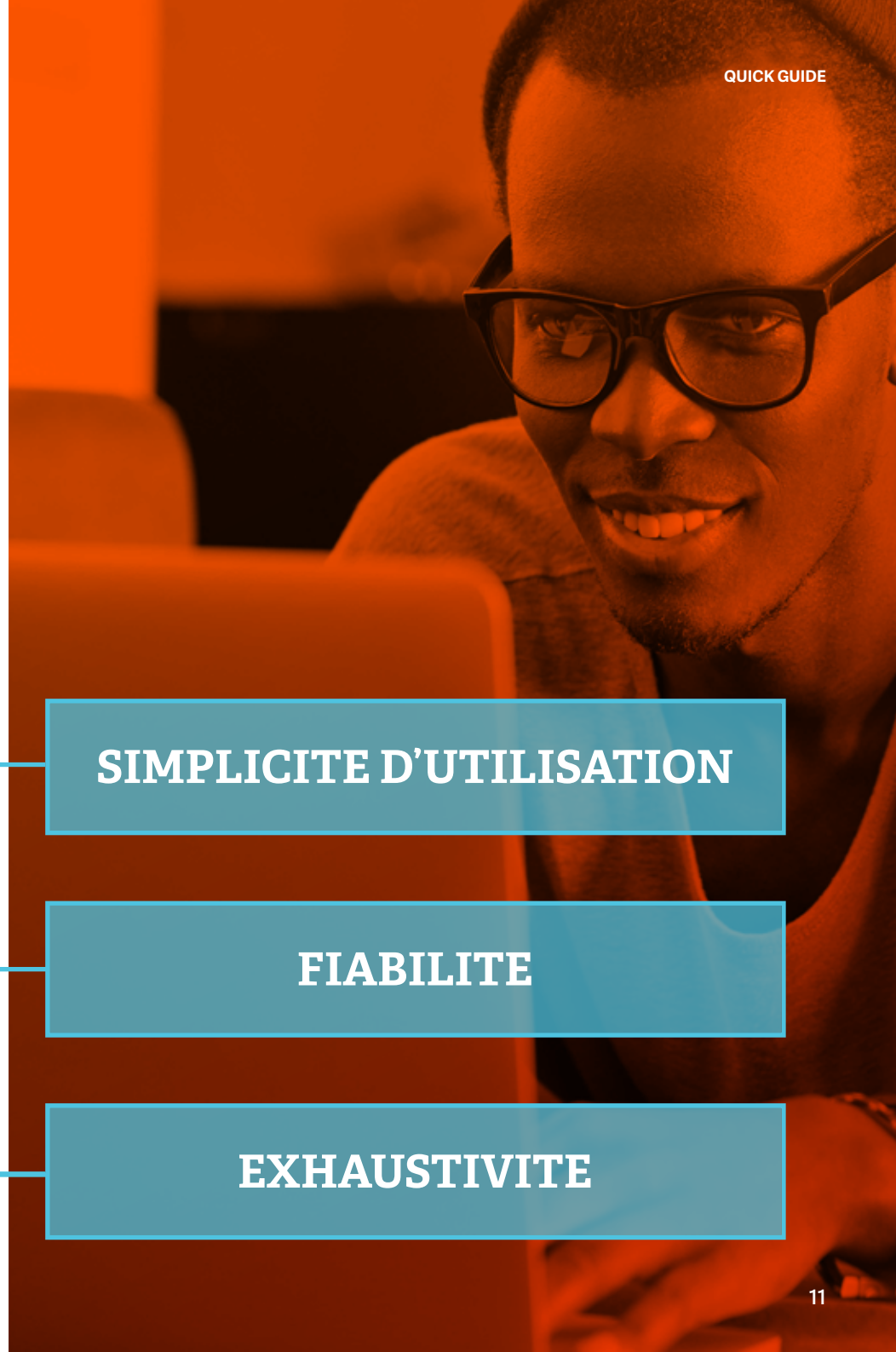
Les services sont-ils bien équipés pour gérer cette activité croissante?

INTENSIFICATION DES PRESSIONS SUR LE SUPPORT IT

Le télétravail obligatoire fait peser d'énormes pressions sur l'infrastructure IT et les systèmes. Les employés du support IT se retrouvent à devoir aider les télétravailleurs alors qu'ils sont eux-mêmes en télétravail.

Les outils de support efficaces ont un impact direct sur la fluidité du télétravail. Mais ces solutions doivent pouvoir monter en charge et s'adapter à des exigences de sécurité strictes tout en facilitant la productivité des techniciens.

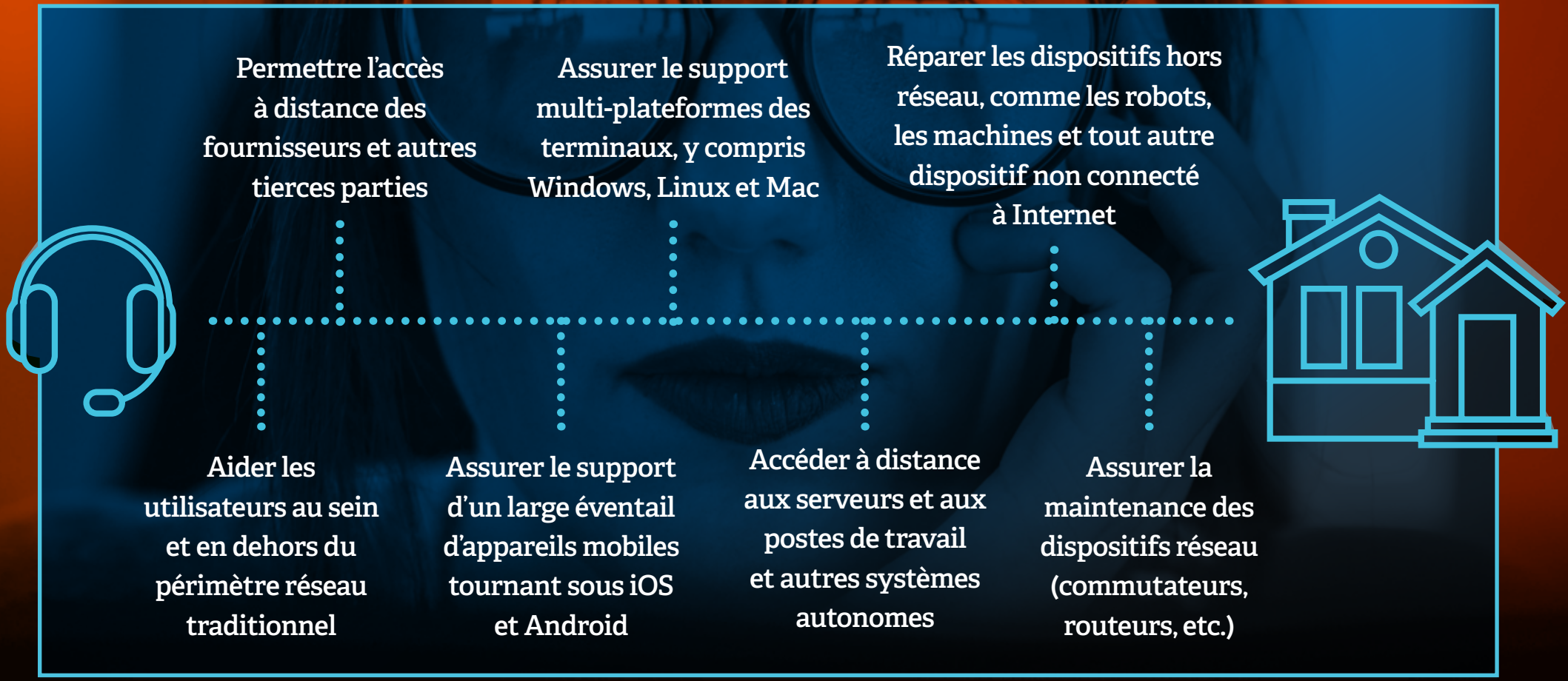
De plus, la solution doit réunir les critères suivants:



- **SIMPLICITE D'UTILISATION**
- **FIABILITE**
- **EXHAUSTIVITE**

SCENARIOS ENVISAGEABLES

Les entreprises ont besoin d'une solution sûre de support à distance capable de couvrir un large éventail de scénarios et qui améliore globalement l'expérience d'assistance d'une façon efficace et sûre. Voici quelques-uns des scénarios les plus courants :



En ces temps compliqués, il est primordial de choisir le bon logiciel de support à distance pour maintenir la productivité et la sécurité du support IT.

ASSUREZ LE SUPPORT DE TOUT DISPOSITIF OU SYSTÈME PARTOUT DANS LE MONDE

BeyondTrust Remote Support

Assurez la prise en main à distance, fiable et sûre, des salariés présents ou non sur votre réseau. Vous pourrez voir leur écran, discuter par chat, élever les privilèges et avoir accès à la caméra de leur smartphone pour dépanner leurs périphériques. Une seule solution assure le support des systèmes Windows, Mac, Linux, iOS, Android et des périphériques réseau.

La solution Remote Support de BeyondTrust est conçue pour améliorer le fonctionnement de votre support IT. Notre solution couvre le plus large éventail de scénarios d'utilisation avec les meilleures garanties de sécurité des accès à distance.
La solution Remote Support de BeyondTrust est la seule certifiée FIPS 140-2 Level 2.

Connectez-vous sur votre réseau local ou externe et apportez votre support aux différents systèmes, toutes plateformes confondues, tout en bénéficiant de puissantes synergies d'intégration.

VPN

Qui est présent sur votre réseau et pour quoi faire?

LES INCONVENIENTS DES CONNEXIONS VPN

Toutes les entreprises ou presque doivent permettre les accès à distance. Les salariés doivent pouvoir se connecter aux systèmes depuis l'extérieur, de l'autre côté du pare-feu. Mais de par sa nature, l'accès à distance expose à des risques de cybersécurité. Pour établir des connexions à distance pour leurs salariés, les entreprises utilisent souvent une forme de VPN (Virtual Private Network). Les VPN fonctionnent bien quand les télétravailleurs utilisent chez eux des PC portables du bureau. Mais s'ils se connectent à partir d'un PC portable ou d'un terminal personnel, ou s'il s'agit de fournisseurs ou sous-traitants amenés à se connecter à vos systèmes, la gestion de la sécurité des VPN peut s'avérer plus complexe.

Risques liés à la sécurité des VPN

- Les VPN donnent accès au réseau au-delà du strict nécessaire
- Les VPN ne sont pas simples à gérer avec le risque d'un accès trop large ou d'accès laissés ouverts après la suppression ou le retrait d'hôtes
- Les VPN fonctionnent en mode « tout ou rien », délivrant une autorisation d'accès totale, sans granularité

COMMENT ENCADRER LES RISQUES LIES AUX VPN

Les hackers prennent parfois des jours, voir des semaines, avant de trouver ce qu'ils recherchent. Dès que des criminels obtiennent un accès VPN entre un système et un réseau interne, ils restent souvent indétectés et utilisent des techniques d'infiltration jusqu'à toucher au but. Ils ciblent de préférence les télétravailleurs ou les fournisseurs externes qui utilisent leurs systèmes personnels avec accès VPN, sachant que ce sera plus facile à compromettre.

182

Nombre moyen de fournisseurs tiers* dont les équipes IT déclarent avoir un accès à leur réseau interne au moins une fois par semaine.

Beaucoup disposent de privilèges excessifs avec un accès trop large pour leur rôle.

**BeyondTrust, "Privileged Access Threat Report 2019"*

BeyondTrust Privileged Remote Access

BeyondTrust Privileged Remote Access permet la gestion sécurisée des sessions, avec la possibilité d'un accès proxy par RDP, SSH ou hôte Windows/Unix/Linux, sans passer par un VPN. L'attribution dynamique de privilèges juste à temps via Adaptive Workflow Control permet aux entreprises de verrouiller l'accès aux ressources en fonction du jour, de la date, de l'heure et de la position géographique. Par exemple, si vous savez que des télétravailleurs vont se connecter à partir de systèmes en particulier, vous pouvez n'autoriser les accès que depuis certaines adresses ou zones géographiques. Vous pouvez aussi imposer des règles de contrôle des conditions d'accessibilité des comptes et programmer des alertes en cas de violation des règles.

En combinant BeyondTrust Privileged Remote Access et vos VPN d'entreprise, vous pourrez réduire la surface d'attaque et stimuler la productivité **en procédant comme suit:**

1. Instaurer le principe de moindre privilège en accordant uniquement le bon niveau d'accès à chacun
2. Permettre la responsabilité individuelle des comptes partagés
3. Définir quels terminaux sont accessibles et quand inscrire des applications en liste blanche ou noire
4. Supprimer l'obligation administrative de configurer et installer des VPN pour les fournisseurs et télétravailleurs qui utilisent leurs systèmes personnels
5. Contrôler et surveiller les sessions via un agent sécurisé ou au moyen des protocoles standard pour connexions RDP, VNC, Web et SSH

AUTRES CONSIDERATIONS

Performance des VPN

La plupart des installations de VPN, même utilisées conjointement avec des systèmes configurés par l'entreprise, ne sont pas prévues pour toute une entreprise en télétravail. En autorisant certains utilisateurs, comme des fournisseurs ou des télétravailleurs qui utilisent leurs propres systèmes personnels, à se connecter via Privileged Remote Access, vous pourrez réduire la pression sur votre VPN et accroître le niveau de performance.

Outre le risque d'introduire des problèmes de sécurité dans l'environnement, les mouvements en masse vers des VPN peuvent induire de sérieux ralentissements de performance.

Risques que posent les VPN à grande échelle

- Les technologies VPN sont généralement difficiles à monter en charge rapidement si bien que quand un grand nombre de personnes souhaitent se connecter soudainement, la solution peut rencontrer des difficultés à fonctionner de façon acceptable
- Les VPN dépendent beaucoup de la largeur de bande passante disponible au domicile de l'utilisateur et de celle dont l'application a besoin
- Les VPN ne sont généralement pas configurés pour permettre l'accès à l'ensemble des ressources disponibles lorsque la personne se connecte sur un réseau officiel au sein des bureaux

ACCES A DISTANCE SIMPLIFIE

Depuis tout terminal fourni par l'entreprise ou appartenant à l'utilisateur

UNE VOIE SIMPLE POUR LES UTILISATEURS

BeyondTrust Privileged Remote Access

Les employés qui ont laissé leur poste de bureau ou leur PC portable au bureau peuvent utiliser BeyondTrust Privileged Remote Access pour se connecter en toute sécurité au poste de travail qu'ils utilisent habituellement. Ils peuvent le faire depuis un PC lambda ou une tablette via un navigateur web.

De nombreux télétravailleurs utiliseront le PC portable fourni par leur entreprise, mais les autres pourront **utiliser n'importe lequel des équipements suivants pour se connecter à votre réseau:**

BeyondTrust aide les télétravailleurs à avoir accès aux ressources dont ils ont besoin pour demeurer productifs, via les machines de leur employeur ou leurs systèmes personnels.

- Salariés utilisant leurs machines personnelles
- Fournisseurs ou sous-traitants utilisant les systèmes de l'entreprise ou des PC portables personnels

Si ceux qui utilisent des systèmes fournis par l'entreprise peuvent être considérés comme étant de confiance, les autres télétravailleurs posent un risque de sécurité majeur pour l'entreprise s'ils se connectent à son VPN. Pour les hackers, ces configurations sont propices à l'infiltration de votre réseau et à l'établissement d'une présence persistante.

Dans tous ces scénarios, **BeyondTrust permet aux équipes IT de:**

- **Accorder un accès à distance granulaire fondé sur le rôle avec authentification multifactorielle**
- **Proposer un chemin d'accès simple et sécurisé aux ressources réseau, y compris à un ordinateur laissé au travail, via une console web HTML5 sans aucune configuration spéciale requise**
- **Provisionner et déprovisionner les privilèges utilisateurs des télétravailleurs qui se connectent à votre système**

CYBER-HYGIENE

Les mots de passe sont comme les bactéries, mieux vaut ne pas les partager

LE ROLE DE LA GESTION DES MOTS DE PASSE

Outre le fait qu'il faille se laver les mains pour éviter de s'échanger des germes de coronavirus, les télétravailleurs doivent aussi éviter de se partager des mots de passe. Les mots de passe mal gérés ou contrôlés constituent un risque de sécurité majeur pour les entreprises. Comme les utilisateurs ont trop de mots de passe, ils en viennent à se les partager, à les réutiliser ou à les conserver sans réelles mesures de sécurité. Ces pratiques rendent les systèmes vulnérables aux attaques.

Lorsque des salariés peinent à se rappeler les mots de passe, ils tendent à:

Lorsque vous envisagez une solution d'accès à distance, pensez à l'intégration d'un coffre-fort

De Mauvaises Habitudes en Matière de Mots de Passe qui Créent des Risques

- Noter leurs mots de passe
- Oublier leurs mots de passe
- Choisir des mots de passe très simples et faciles à compromettre ou réutiliser d'anciens mots de passe

PROTECTION DES IDENTIFIANTS PRIVILEGIES

BeyondTrust Vault

Fournie avec Privileged Remote Access et Remote Support, BeyondTrust Vault est une solution cloud simple et rapide qui unifie la gestion des sessions et le vaulting d'identifiants pour les utilisateurs privilégiés internes et tiers.

BeyondTrust Password Safe

BeyondTrust Password Safe combine gestion des mots de passe et des sessions privilégiés de façon à découvrir, gérer et auditer toute l'activité des identifiants privilégiés. Password Safe facilite le contrôle des comptes utilisateur privilégiés, des applications, des clés SSH, des comptes admin cloud, des comptes RPA, etc. avec une piste d'audit interrogeable à des fins d'investigation de conformité (audit).

Gagnez en flexibilité pour mieux protéger et contrôler la gestion des identifiants privilégiés et la surveillance de session avec des modèles qui s'adaptent à vos besoins métiers spécifiques.

ENDPOINT PRIVILEGE MANAGEMENT

Protégez les terminaux distants des attaques et malwares

En plus de perturber les workflows et processus habituels des utilisateurs, le basculement brutal au télétravail à grande échelle a sérieusement mis à mal les processus et règles de sécurité. De nombreuses entreprises sont mal préparées pour supporter tous leurs effectifs en télétravail, pourtant il le faut bien pour assurer la continuité de l'activité.

Ceux qui doivent se mettre soudainement au télétravail, pour la première fois pour beaucoup, risquent de rencontrer les difficultés suivantes :

- **Différences par rapport à l'environnement de travail normal**
- **Déconnexion du réseau sécurisé habituel**
- **Exposition au risque de menaces externes et internes**
- **Nécessité d'utiliser de nouvelles technologies pour rester connecté et productif**

Ils attendent beaucoup du support IT. Et s'ils n'obtiennent pas satisfaction ou qu'ils cherchent eux-mêmes des solutions, ils risquent d'installer des outils et des applications et d'exposer toute l'entreprise à des risques de sécurité.

Soit les utilisateurs **n'ont aucun droit admin** et ils ne peuvent rien faire, soit ils **ont tous les droits admin** et un pouvoir excessif.

MAINTIEN DE LA SECURITE ET DE LA PRODUCTIVITE

Avec l'intensification des cyberattaques visant les télétravailleurs, il faut absolument que les entreprises sécurisent les machines des utilisateurs et qu'elles empêchent l'introduction de malwares et ransomwares dans leur environnement.

Les solutions BeyondTrust Endpoint Privilege Management instaurent le principe du moindre privilège sur tous les postes de travail et serveurs, de sorte que chaque utilisateur ait le niveau exact d'accès privilégié, tout en bloquant l'introduction de malwares et ransomwares sur le réseau de l'entreprise. Ainsi, les utilisateurs peuvent effectuer leurs activités courantes, comme installer et mettre à jour les applications autorisées, les imprimantes, caméras, etc. sans disposer pour autant de droits admin excessifs et sans risquer de submerger le support IT.

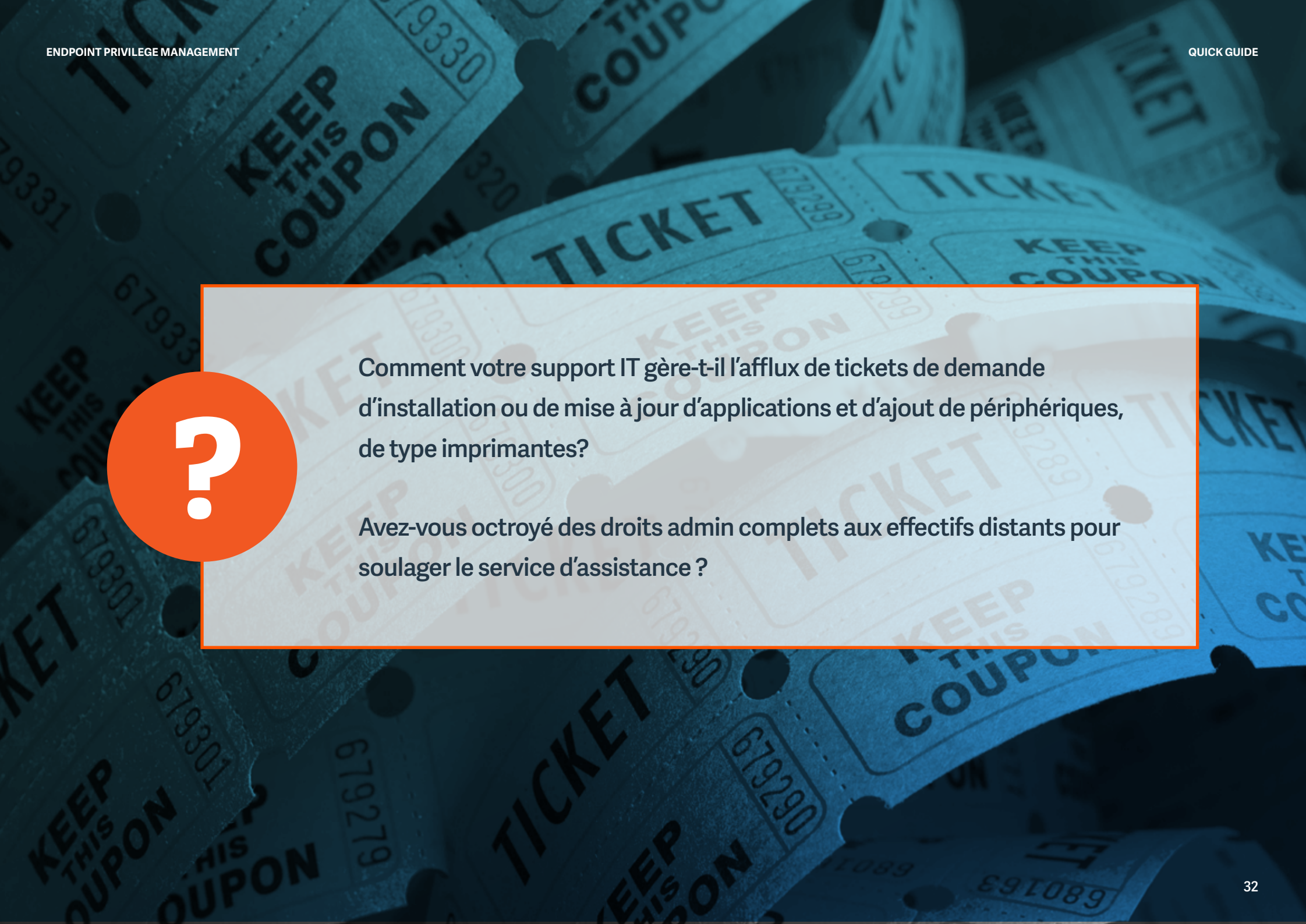
Pour bloquer les attaques que les logiciels antivirus laissent passer, supprimez les droits admin, instaurez le principe du moindre privilège, autorisez l'élévation de privilèges et sécurisez les applis par la protection totale des applications.

Avec Endpoint Privilege Management, les entreprises peuvent déployer rapidement des règles pour l'ensemble des utilisateurs ou pour des groupes d'utilisateurs. Nos règles QuickStart fondées sur les données de plusieurs milliers de déploiements permettent aux administrateurs IT de déployer des modèles flexibles et de les faire appliquer rapidement.

Notre expérience des déploiements de plus de 50 millions de terminaux dans différents secteurs d'industrie nous a permis de créer une approche éprouvée, avec des délais parmi les plus courts.

> "Les clients les plus importants ont mesuré une **réduction de 75%** du nombre de tickets de demande d'assistance après avoir supprimé les droits admin."
>
> *- Sami Laiho, Microsoft MVP*
> *Hacker Ethique**

*BeyondTrust, "Microsoft Vulnerabilities Report 2020"



Comment votre support IT gère-t-il l'afflux de tickets de demande d'installation ou de mise à jour d'applications et d'ajout de périphériques, de type imprimantes?

Avez-vous octroyé des droits admin complets aux effectifs distants pour soulager le service d'assistance ?

COMMENT SOULAGER LE SUPPORT IT?

BeyondTrust Privilege Management for Windows & Mac

Éliminez les privilèges superflus et rehaussez les droits des utilisateurs sous Windows et Mac 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.

Voici les avantages offerts:

- Réduction du nombre de tickets de demande d'assistance en permettant aux utilisateurs d'installer et d'exécuter les applications pré-approuvées, selon des règles prêtes à l'emploi
- Droits ponctuels d'installation des seules applications approuvées/considérées sûres
- Intégration de ServiceNow et d'autres outils ITSM pour automatiser l'envoi d'un ticket, afin le support IT puisse décider de façon éclairée de donner suite ou non à la demande d'un utilisateur de lancer une application, une installation, un script ou une tâche
- Résolution rapide d'un problème pour l'ensemble des utilisateurs, via l'actualisation globale des règles
- Autorisation des utilisateurs à installer eux-mêmes les imprimantes et autres équipements autorisés/validés.

?

Comment faire en sorte que les utilisateurs ne puissent pas introduire des malwares et ransomwares dans votre environnement ?

BeyondTrust Privilege Management pour Windows et Mac réduit la surface d'attaque de **plusieurs façons:**

1. Instauration du moindre privilège sur l'ensemble des postes et des serveurs, de façon à maintenir la sécurité, la productivité et l'efficacité opérationnelle
2. Blocage en temps réel des attaques impliquant des applis de confiance, des scripts malveillants et des pièces jointes aux e-mails
3. Utilisation d'une liste blanche automatisée avec gestion fine des exceptions pour contrôler ce que les utilisateurs peuvent ou non installer et exécuter
4. Elaboration/Mise en place d'une piste de contrôle de toute l'activité des utilisateurs pour les besoins d'investigations et de conformité
5. Corrélation entre le comportement des utilisateurs et les données liées à la vulnérabilité des ressources, afin d'évaluer le risque pour l'utilisateur final à l'aide d'analyses avancées des menaces

C'EST MAINTENANT

Equipez dès aujourd'hui vos salariés en télétravail

SIMPLICITE DE DEPLOIEMENT POUR ETRE OPERATIONNEL RAPIDEMENT

Il existe plusieurs options de déploiement des solutions BeyondTrust, notamment sous forme d'appliances virtuelles et SaaS, afin d'être opérationnel rapidement. Avec les solutions Secure Remote Access de BeyondTrust, il n'est pas nécessaire de télécharger un agent, les utilisateurs se connectent via une console web depuis n'importe quel navigateur. Quant à Endpoint Privilege Management (EPM), les agents sont déployés rapidement sur les terminaux, et les règles appliquées, sans interruption pour les utilisateurs.

L'administration simplifiée doublée de workflows rationalisés ou automatisés soulagent également vos équipes IT. Voici les avantages qu'il y a à utiliser les solutions BeyondTrust:

AVANTAGES

Chemins d'accès consolidés	Suivi d'accès	Applis mobiles	Piste d'audit	Règles QuickStart (EPM)
Faire transiter toutes les connexions via un chemin d'accès unique, contribue à réduire la surface d'attaque tout en établissant une liste unique des terminaux autorisés pour chaque utilisateur.	Définir les préférences pour être alerté lorsqu'un prestataire/ utilisateur privilégié accède à votre réseau/ vos systèmes, ou lorsqu'une session est initiée par un accès à distance	Les administrateurs peuvent utiliser leurs appareils mobiles pour approuver les demandes et surveiller les accès où qu'ils se trouvent	Enregistrement de toutes les sessions pour satisfaire les exigences de conformité et faciliter les investigations et obligations de reporting	Maintien de la sécurité, de la productivité et de l'efficacité des opérations IT par l'instauration du moindre privilège sur l'ensemble des postes de travail de l'environnement

BeyondTrust permet aux entreprises d'appliquer le principe de moindre privilège et des contrôles d'audit robustes à l'ensemble des accès à distance des salariés, fournisseurs et support IT. Les utilisateurs peuvent **accéder rapidement et en toute sécurité à tout système distant, sur n'importe quelle plateforme, où qu'elle soit**, et le coffre-fort de mots de passe intégré peut leur permettre de découvrir, intégrer et gérer des identifiants privilégiés.

Obtenez une totale visibilité et le contrôle des accès à distance internes et externes, sécurisez la connectivité aux actifs gérés et créez une piste d'audit inviolable de façon à simplifier votre mise en conformité.

Vous pouvez aussi empêcher les utilisateurs de télécharger des logiciels malveillants et d'ouvrir les pièces jointes dangereuses des e-mails de phishing pour protéger votre environnement.

Le tout en réduisant l'afflux de tickets de demande de support avec la garantie de respecter les obligations de conformité.

Notre approche vous offre la capacité de donner le bon niveau d'accès au bon moment, en toute transparence pour l'utilisateur.

BeyondTrust

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. 20 000 clients, dont 70% du Fortune 500, et un réseau mondial de partenaires nous font confiance.

Pour en savoir plus : beyondtrust.com

V2020_05_FRE