

DONNEZ-LEUR UN ACCÈS. PAS UN VPN

BeyondTrust's Privileged Access Management permet aux professionnels de la sécurité de contrôler, de superviser et de gérer les accès des utilisateurs privilégiés à leurs systèmes stratégiques, y compris pour les fournisseurs tiers. BeyondTrust vous permet de:

- * Éliminer le point d'entrée permettant aux cybercriminels de s'immiscer dans votre environnement
- * Maintenir un contrôle granulaire des accès à votre réseau
- * Assurer, en temps réel, la surveillance et l'audit des sessions d'accès
- * Consigner les données de sécurité des sessions directement dans votre outil SIEM
- * Limiter les attaques par usurpation d'identité
- * Raccourcir les délais d'intervention en cas d'incident
- * Réaliser des investigations judiciaires efficaces
- * Remplir les missions d'audit et de mise en conformité

Le saviez-vous ?



Les cybercriminels ont généralement besoin d'à peine quelques jours ou semaines pour déterminer leur cible. S'ils parviennent à se procurer un accès VPN vers un réseau interne, ils peuvent souvent explorer ce dernier à leur guise en restant inaperçus se déplacer afin d'attendre leur objectif ultime. Les cybercriminels ciblent régulièrement les tiers qui disposent déjà de méthodes d'accès à un réseau, telles que les VPN ou RDP, en sachant que ces passerelles sont plus faciles à pirater. BeyondTrust donne aux tiers un accès aux systèmes requis sans VPN, éliminant ainsi les menaces de voir les VPN utilisés par les tiers compromis.

1 9 7 JOURS

C'est la durée moyenne nécessaire pour détecter une faille. En cas de compromission des accès d'un fournisseur, toute activité malveillante serait immédiatement bloquée dès l'expiration de la session BeyondTrust. En revanche, avec un VPN, le cybercriminel continuerait d'agir en toute liberté jusqu'à ce qu'il soit détecté.



80% des brèches débutent par la compromission d'un compte privilégié. La posture de sécurité de vos fournisseurs peut être très différente d'une entreprise à l'autre. Les cybercriminels en sont conscients et peuvent aisément identifier le tiers qui sera le plus fragile, et donc le meilleur choix, pour attaquer votre réseau.

62%

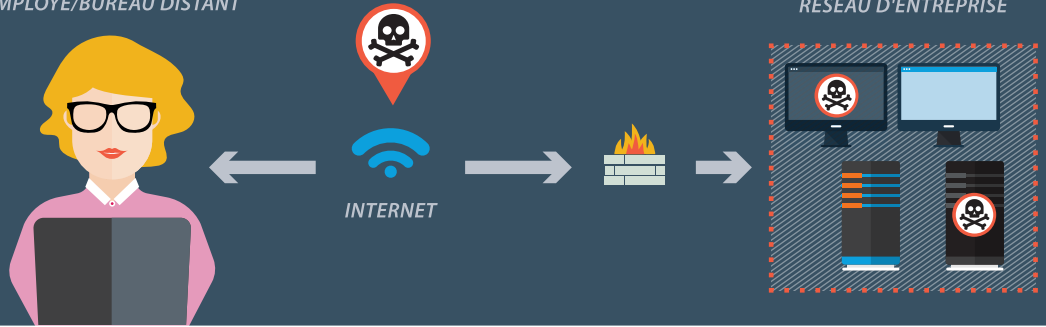
Près de 2/3 des organisations pensent que gérer les identités et les droits d'accès serait trop complexes. En moyenne, les entreprises reçoivent 1 200 demandes d'accès par mois. BeyondTrust simplifie ces opérations en permettant aux admins de centraliser la gestion, le contrôle et l'audit des accès sans perturber les procédés.

ÉLIMINER LES VPN POUR LES FOURNISSEURS

IL ÉTAIT UNE FOIS...

Le risque majeur de sécurité était l'attaque de type MtM (Man in the Middle) sur une connexion distante à votre réseau.

EMPLOYÉ/BUREAU DISTANT



Les entreprises ont commencé à mettre en œuvre des réseaux privés virtuels pour créer un tunnel crypté. Ainsi les employés itinérants et les bureaux distants, tous dignes de confiance, pouvaient accéder au réseau en éliminant les attaques MitM.

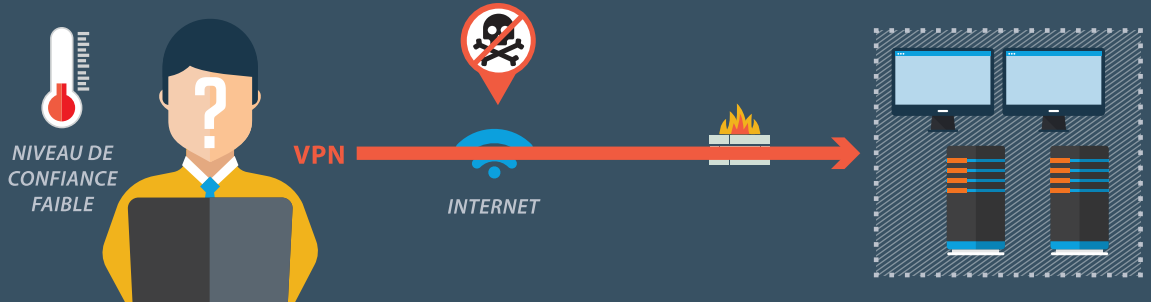
EMPLOYÉ/BUREAU DISTANT



MISSION À LA DÉRIVE !

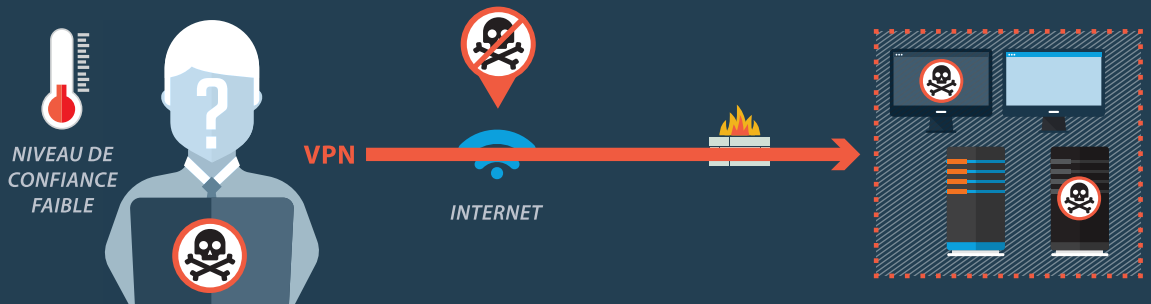
Au fur et à mesure que les tiers et les fournisseurs ont commencé à exiger des accès privilégiés à leurs réseaux, les entreprises leur octroyaient ces accès via le meilleur outil disponible, à savoir les réseaux privés virtuels.

FOURNISSEUR DISTANT



Les cybercriminels ont vite compris qu'un tiers disposant d'une connexion à un VPN était une cible parfaite pour accéder à un réseau sécurisé. Grâce à ce point d'entrée, ils disposent de l'accès et de tout le temps qu'il leur faut pour identifier et attaquer les systèmes sensibles.

FOURNISSEUR COMPROMIS



DONNEZ À VOS FOURNISSEURS DES ACCÈS SANS VPN !

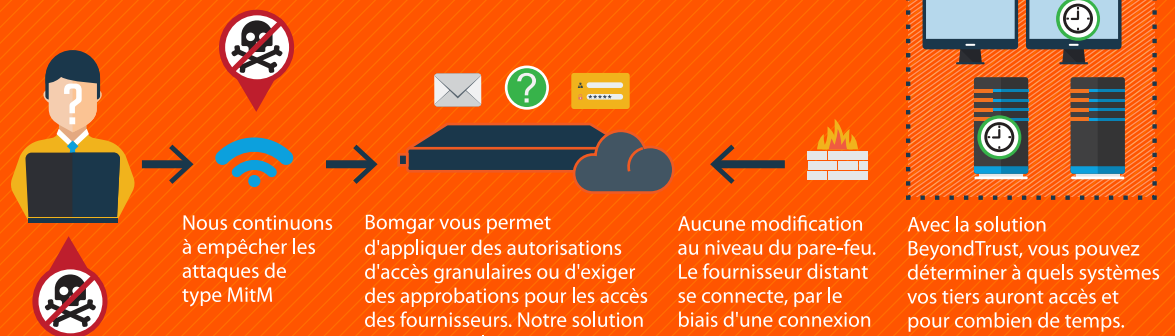
Privileged Access Management de BeyondTrust vous permet de donner des accès à votre réseau sans VPN à vos fournisseurs et sans permettre la connexion directe à vos systèmes et données critiques.

FOURNISSEUR DISTANT

INTERNET

BEYONDRUST
PRIVILEGED ACCESS MANAGEMENT -
GESTION DES ACCÈS PRIVILÉGIÉS

RÉSEAU D'ENTREPRISE



Nous continuons à empêcher les attaques de type MitM

Bomgar vous permet d'appliquer des autorisations d'accès granulaires ou d'exiger des approbations pour les accès des fournisseurs. Notre solution récupère également une piste d'audit et un enregistrement vidéo de toutes les activités des fournisseurs, avec possibilités de recherches.

Aucune modification au niveau du pare-feu. Le fournisseur distant se connecte, par le biais d'une connexion sortante uniquement, à l'appliance BeyondTrust et PAS au système cible.

Avec la solution BeyondTrust, vous pouvez déterminer à quels systèmes vos tiers auront accès et pour combien de temps. Ainsi, ils ne peuvent pas rester ni se déplacer au sein de votre réseau.