BeyondTrust

>>> Appliquer les principes du Zero Trust à la gestion des accès privilégiés (PAM)

Faire progresser le Zero Trust *grâce* à la gestion des accès privilégiés (PAM)

TABLE DES MATIÈRES

Introduction : Objectif du Zero Trust

Les principes et les architectures Zero Trust sont largement adoptés par les secteurs public et privé. Les architectures de sécurité et les défenses réseau héritées sont tout simplement inefficaces dans un monde dépendant davantage du cloud et des employés à distance. Dans le monde d'aujourd'hui, les principes Zero Trust sont devenus l'une des approches les plus efficaces pour atténuer les risques de plus en plus importants auxquels sont exposés les identités, les actifs et les ressources éminemment sensibles.

La note SP 800-207 de l'institut américain de standardisation et de technologie (NIST)[1] s'est imposée comme le référentiel du Zero Trust. Le NIST décrit cette note comme « une source définitive de concepts et principes de l'architecture Zero Trust ». La note d'origine (datant du mois d'août 2020) couvrait principalement et de façon globale les concepts du Zero Trust. Elle ne fournissait aucune base pour l'architecture et la mise en œuvre du Zero Trust à un niveau pratique.

Dans la pratique, pour mettre en place le Zero Trust, une organisation doit comprendre quelles technologies et quelles configurations peuvent être utilisées avec des principes répondant aux exigences théoriques. C'est pour combler cette lacune que le NIST a publié la note SP 1800-35[2] (de décembre 2022) sur la mise en œuvre du Zero Trust. Il existe aujourd'hui des solutions à même de répondre aux besoins théoriques et pratiques pour adopter une approche Zero Trust. Pour la technologie BeyondTrust, c'est là que ce document entre en jeu.

Ce document s'adresse aux professionnels de l'IT et de la sécurité qui souhaitent intégrer les principes du Zero Trust, tels que définis par le NIST, aux fonctionnalités réelles de gestion des accès privilégiés (PAM) et d'accès à distance sécurisés. Ces principes peuvent être mis en pratique dans les organisations publiques comme privées.

La sécurisation des identités dotées d'un accès privilégié aux systèmes, données, applications et autres ressources sensibles est une priorité. Aujourd'hui, presque toutes les attaques nécessitent un privilège pour l'exploit initial ou pour se déplacer latéralement au sein d'un réseau.

Le PAM protège les identifiants et les comptes privilégiés, applique de manière granulaire le principe du moindre privilège, surveille et gère chaque session impliquant un accès privilégié, qu'il s'agisse d'une personne, d'une machine, d'un employé ou d'un prestataire externe : **Le PAM est aussi essentiel pour mettre en place une architecture Zero Trust (ZTA) et remplir les sept principes du Zero Trust définis par le NIST dans ses publications.**

Ce document abordera :

- Les définitions et les concepts clés du Zero Trust, tels qu'énoncés par le NIST
- Les implications pour la sécurité du Zero Trust
- Les étapes pratiques de mise en place du Zero Trust avec des solutions de Privileged Access Management et de Secure Remote Access
- Comment BeyondTrust permet aux organisations d'atteindre le Zero Trust
- Ce qu'il faut considérer au moment de concevoir des architectures Zero Trust

[1] https://csrc.nist.gov/publications/detail/sp/800-207/final

[2] https://csrc.nist.gov/publications/detail/sp/1800-35/draft

Notes 800-207 et 1800-35B du NIST : Définition du Zero Trust et de l'architecture Zero Trust (ZTA)

Définition du Zero Trust

Le National Institute of Standards and Technology (NIST) définit le Zero Trust (ZT) comme « Un ensemble de paradigmes de cybersécurité en évolution, qui font passer les défenses d'un périmètre statique basé sur le réseau à un périmètre centré sur les utilisateurs, les actifs et les ressources ». Le NIST explique en outre que tous les concepts qui composent les principes du Zero Trust sont conçus pour « minimiser l'incertitude liée à l'application de décisions d'accès précises le principe du moindre privilège pour chaque demande, dans les systèmes et services d'information, face à un réseau considéré comme contesté ».

Concrètement, cela implique d'éliminer toute confiance persistante, d'effectuer une authentification en continu, de restreindre de manière granulaire l'accès au minimum nécessaire, d'appliquer des stratégies de segmentation et de microsegmentation et d'auditer en permanence l'accès. **La gestion des accès privilégiés (PAM) est une pile technologique fondamentale pour la mise en place de chacun des contrôles de sécurité essentiels au Zero Trust.**

> *« Les interactions entre les produits de la suite [de BeyondTrust] ont été brillamment et minutieusement orchestrées de sorte à maximiser notre chance d'aller aussi loin que possible dans le Zero Trust compte tenu de l'offre de produits sur le marché de la sécurité ».*
>
> *Brandon Haberfeld, Global Head of Platform Security chez Investec*

L'objectif principal du Zero Trust est de protéger les ressources de l'entreprise (en particulier, mais pas uniquement, les données). Comme indiqué dans la SP 1800-35B du NIST, cet objectif est devenu de plus en plus important pour répondre aux défis des réseaux d'aujourd'hui :

- Les réseaux sont désormais des environnements décentralisés et sans périmètre précis avec des ressources réparties entre plusieurs sites et plusieurs environnements cloud.
- Pour le bien des activités de l'entreprise, de nombreux utilisateurs ont besoin d'un accès à tout moment, sur n'importe quel appareil et peu importe où ils se trouvent.
- Les données sont stockées, transmises et traitées par programmation dans plusieurs périmètres sous le contrôle de différentes organisations pour répondre à des usages professionnels en constante évolution.
- Il n'est plus possible de simplement appliquer des contrôles d'accès au périmètre de l'environnement de l'entreprise et de supposer que tous les sujets qui s'y trouvent sont fiables.

Ainsi, la situation géographique ne peut plus être considérée comme l'élément essentiel du dispositif de sécurité de la ressource. Au lieu de cela, le modèle Zero Trust fonctionne en supposant que l'on ne peut implicitement faire confiance à aucun actif ou compte d'utilisateur uniquement en fonction de son emplacement physique, de l'emplacement du réseau ou du propriétaire de l'actif. L'authentification et l'autorisation du sujet et de l'appareil sont obligatoires avant d'établir une session avec une ressource de l'entreprise.

Définition de l'Architecture Zero Trust

La note SP 800-207 du NIST définit une architecture Zero Trust (ZTA) comme « le plan de cybersécurité d'une entreprise qui utilise des concepts Zero Trust et couvre les relations entre composants, la planification des processus et les politiques d'accès. Par conséquent, une entreprise Zero Trust est l'infrastructure réseau (physique et virtuelle) et les politiques opérationnelles mises en place dans une entreprise dans le cadre d'un plan d'architecture Zero Trust ».

Le NIST précise en outre que l'objectif principal d'une ZTA est de « protéger les données et les ressources. Elle permet un accès sécurisé et autorisé aux ressources de l'entreprise qui sont réparties entre plusieurs sites et plusieurs environnements cloud, tout en permettant à un ensemble hybride de collaborateurs et de partenaires d'accéder aux ressources à tout moment, sur n'importe quel appareil et peu importe où ils se trouvent pour le bien des activités de l'entreprise ».

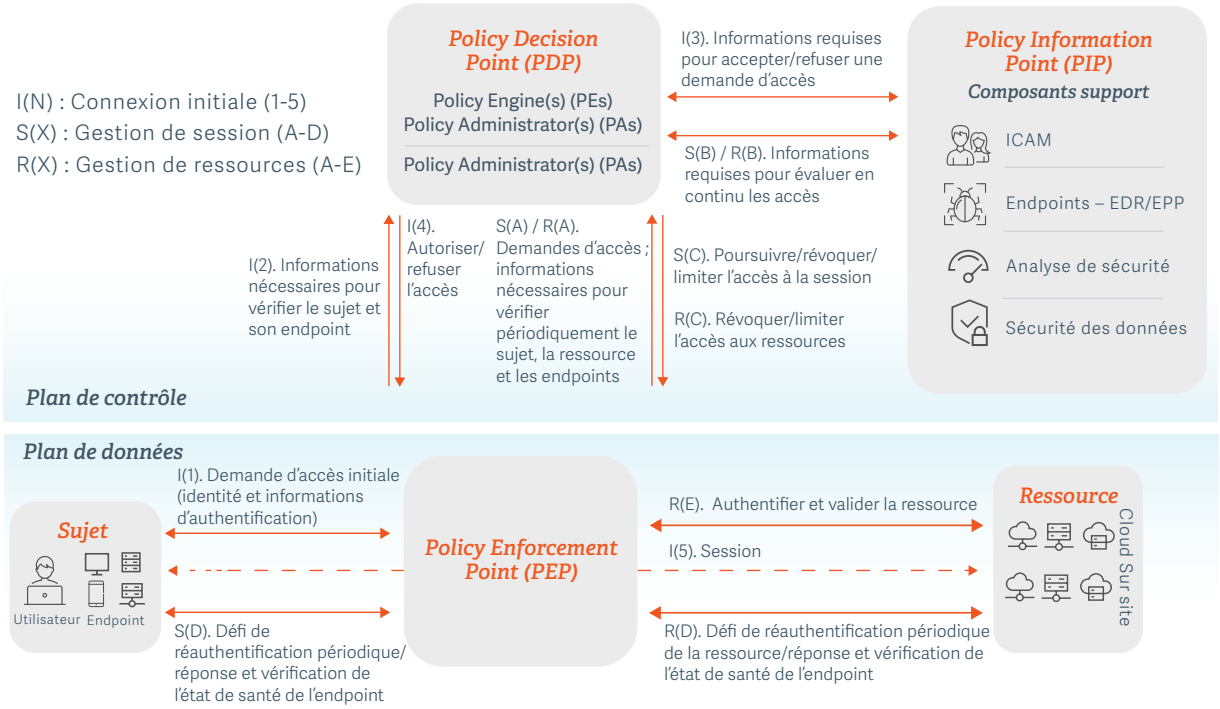
Les concepts et principes d'une architecture Zero Trust conforme à la SP 800-207 du NIST sont appliqués aux « réseaux d'entreprise composés d'appareils et de composants préétablis et qui stockent des ressources d'entreprise critiques à la fois sur site et dans le cloud ». Selon la note SP 1800-35B, la ZTA effectue en temps réel une analyse comportementale continue et une évaluation basée sur le risque de l'opération d'accès ou de la session. « Pour chaque demande d'accès, l'architecture Zero Trust (ZTA) vérifie l'identité et le rôle du demandeur, l'état de santé et les identifiants de son dispositif et éventuellement d'autres informations. Si les critères définis par la politique sont satisfaits, la ZTA crée dynamiquement une connexion sécurisée pour protéger toutes les informations transférées vers et depuis la ressource à laquelle le demandeur accéde».

Chaque demande d'accès est évaluée en vérifiant :

- Le contexte disponible au moment de l'accès, y compris l'identité et le rôle du demandeur
- L'état de santé et les identifiants du dispositif demandeur
- La sensibilité de la ressource

Architecture de référence Zero Trust

Voici un exemple de ZTA, telle que décrite dans la SP 1800-35B du NIST, appliquée à plusieurs disciplines de sécurité :



Les composants de base d'une ZTA montrés dans le diagramme d'architecture ci-dessus incluent :

- **Policy Engine (PE) :** Le PE prend la décision finale d'accorder, de refuser ou de révoquer à un sujet donné l'accès à une ressource. Le PE calcule les scores/les niveaux de confiance et détermine les décisions d'accès finales sur la base de la politique de l'entreprise et des informations fournies par les composants de support. Le PE exécute son algorithme de confiance pour évaluer chaque demande de ressource qu'il reçoit.
- **Policy Administrator (PA) :** Le PA exécute la décision du PE en envoyant des commandes au PEP pour créer ou supprimer le chemin de communication entre le sujet et la ressource. Il génère l'autorisation de session, le token d'authentification ou tout type d'identifiant nécessaire au sujet pour accéder à la ressource de l'entreprise.
- **Policy Enforcement Point (PEP) :** Le PEP protège la zone de confiance qui héberge une ou plusieurs ressources de l'entreprise. Il gère l'activation, la surveillance et éventuellement la suppression des connexions entre les sujets et les ressources de l'entreprise. Il opère selon les ordres reçus du PA.

Autres définitions importantes :

- **Policy Decision Point (PDP) :** Le PE et le PA se combinent pour constituer le PDP, qui prend la décision d'autoriser ou non l'accès d'un sujet à une ressource.
- **Policy Information Point (PIP) :** Le PIP fournit des données de télémétrie et autres pour que le PDP puisse prendre des décisions d'accès informées. Cela inclut les solutions PAM et EDR comme les solutions de réponse aux menaces d'après les identités.
- **Sujet :** Un utilisateur final, une application ou une autre entité non humaine qui demande des informations issues des ressources.
- **Passerelle :** Elle est chargée de l'activation, de la surveillance et de l'interruption de la connexion entre le sujet (utilisateur ou application) et la ressource par l'intermédiaire de l'agent, afin que toutes les activités puissent être évaluées et documentées.

Enclaves Zero Trust

La meilleure pratique de sécurité consiste à ce que les contrôles du réseau et des accès soient configurés, testés et surveillés pour que les ressources traditionnelles sur site puissent prévenir les accès inappropriés. Malheureusement, dans de nombreux environnements modernes, ces contrôles de sécurité ont été rendus moins efficaces ou ont été supprimés afin de rendre possible une variété de cas d'utilisation : des environnements de cloud hybride aux employés à distance, jusqu'aux solutions qui couvrent plusieurs emplacements et réseaux. Cela ne signifie pas que les contrôles de sécurité ont été supprimés, mais plutôt qu'un nombre suffisant d'exceptions ont été mises en œuvre pour permettre des cas d'utilisation métier supplémentaires et que les risques accrus ont été acceptés. Ce « relâchement » de l'environnement va à l'encontre du modèle Zero Trust et, dans de nombreux cas, cela se traduit par l'utilisation d'identifiants ou de secrets statiques pour que les solutions puissent interagir. De ce fait, si un emplacement se trouve compromis, l'environnement dans son ensemble se retrouve en danger.

Un nouveau périmètre doit être établi pour atteindre le Zero Trust tout en permettant ces nouveaux usages. Cela implique d'adopter une approche par zones afin de créer une enclave sécurisée. L'accès à l'enclave elle-même, ainsi qu'entre les ressources qui y résident, doit être strictement restreint.

Par conséquent, une enclave est comme un périmètre réseau au sein d'un réseau non sécurisé. La zone protégée, avec tous les contrôles de sécurité associés, est intégrée à l'intérieur.

Enclave passerelle

Un modèle d'enclave passerelle établit un périmètre segmenté granulaire avec des actifs accessibles uniquement via un chemin réseau sécurisé et surveillé. Alors que les ressources au sein de l'enclave peuvent être associées à des contrôles de sécurité assouplis pour répondre aux besoins opérationnels, elles demeurent surveillées de sorte à détecter un comportement inapproprié lorsque l'activité provient de l'extérieur de l'enclave. Considérez l'enclave comme un mini réseau de confiance au sein d'un autre réseau.

L'accès à l'enclave nécessite des contrôles de sécurité plus stricts que ce qui est mis en place via un hôte bastion classique ou des contrôles sur le routage ou les tunnels de connexion. C'est la clé pour parvenir à une segmentation.

Voici d'autres conditions nécessaires au fonctionnement du Zero Trust au sein d'une enclave :

- Une ressource externe centralise la politique et l'administration pour tous les accès.
- L'accès est déterminé par un moteur logique qui traite la règle et les attributs pour accorder ou limiter l'accès.
- L'accès est entièrement documenté, de l'autorisation jusqu'à la gestion et l'enregistrement complets de la session.
- Les sessions font l'objet d'un contrôle de l'activité comportementale, depuis leur lancement jusqu'à tout mouvement latéral requis pour réaliser une tâche. Une activité inappropriée peut être traitée en temps réel.
- L'accès n'est pas absolu et doit se caractériser par des processus comme le just-in-time, y compris pour les connexions éphémères, et par une intégration dans un système de gestion informatique et d'autres solutions de gestion du changement.
- Aucune session ni aucun trafic ne peuvent accéder à l'enclave, à moins d'un traitement via le plan de contrôle. En d'autres termes, tout mouvement latéral dans l'enclave doit être refusé en utilisant des contrôles réseau et de sécurité des accès traditionnels. L'enclave doit fonctionner comme un segment sécurisé du réseau, entièrement verrouillée et n'offrant aucune porte dérobée.

Le succès de ce modèle passe par un équilibre entre tous ces impératifs. Les utilisateurs et les applications autorisés doivent lancer une session qui peut être vérifiée et connectée à l'enclave passerelle. Il faut un contrôle de session, une injection d'identifiants et un principe du moindre privilège pour surmonter les problèmes de sécurité et de conformité que rencontre une organisation et être fidèle aux objectifs du Zero Trust.

Enclaves de ressources

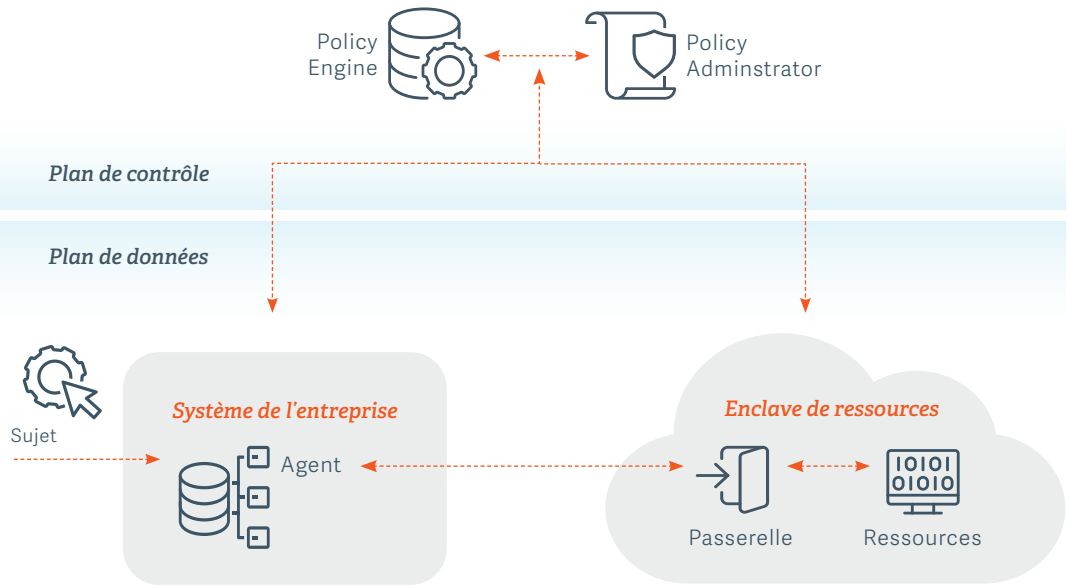
L'enclave de ressources est une variante d'une zone réseau ou VLAN. Elle consiste en un ensemble de ressources ou actifs (applications, systèmes d'exploitation, dispositifs réseau, bases de données, etc.) avec un périmètre renforcé autour de tous les actifs. Le périmètre, au lieu d'être une zone réseau étendue, est isolé et ne s'applique qu'aux actifs critiques situés dans l'enclave de ressources pour un objectif donné. Une enclave de ressources est essentiellement une zone réseau sécurisée totalement segmentée avec un accès externe limité. Tout type d'accès doit passer par une passerelle correspondant à la description d'une enclave passerelle. En résumé, une enclave passerelle définit le chemin d'accès sécurisé et l'enclave de ressources définit les ressources qu'elle contient.

Il y aura potentiellement dans chaque organisation des dizaines, voire des centaines, d'enclaves de ressources sécurisées par des listes de contrôle d'accès traditionnelles et un durcissement des conditions d'accès au réseau. Cela revient à étendre le concept de micro-segmentation à des configurations uniques afin de satisfaire aux besoins opérationnels ou technologiques. Une enclave de ressources est adaptable aux systèmes hérités, et l'architecture doit être compatible avec la notion de Zero Trust, de façon native ou en utilisant une approche d'enclave passerelle.

Par conséquent, les ressources au sein de l'enclave s'appuient sur des modèles classiques de contrôle de la sécurité et ne préviennent pas nécessairement les menaces dans l'enclave elle-même (par ex. des mouvements latéraux inappropriés) sauf si la connexion est totalement surveillée. Par exemple, les menaces liées aux mouvements latéraux ne sont atténuées qu'entre les sujets et d'une enclave de ressources à une autre.

En principe, toutes les sessions et connexions doivent être applicables, que l'utilisateur ou l'application soit au bureau ou non. Ce paradigme peut aider une architecture Zero Trust (ZTA) à jouer un rôle central pour surmonter les défis d'un réseau hérité lorsqu'un vaste périmètre réseau n'est plus utilisé à des fins de sécurité.

Considérons ce diagramme simplifié de l'architecture Zero Trust d'une passerelle d'enclave sécurisée conforme aux recommandations du NIST :



Dans un pur environnement Zero Trust, l'enclave passerelle et l'enclave de ressources peuvent exister sur un actif unique et, par conséquent, l'application est restreinte de manière adéquate. Bien que ce soit le but, ce n'est pas réalisable pour de nombreuses organisations adoptant le Zero Trust pour la première fois. Le concept d'enclave peut être étendu ou rétréci en fonction des ressources et actifs mis en œuvre dans le cadre d'un projet Zero Trust.

La gestion des accès privilégiés (PAM) est essentielle au Zero Trust

La notion de gestion des accès privilégiés (PAM) englobe toutes les stratégies et technologies de cybersécurité permettant d'exercer un contrôle sur les accès et autorisations des utilisateurs, comptes, processus et systèmes bénéficiant de droits accrus (« privilégiés ») dans un environnement IT donné. Les usages vont de l'application du moindre privilège à la gestion des comptes/identifiants privilégiés, en passant par la sécurisation de tous les accès à distance privilégiés, etc. Le PAM est un contrôle de sécurité fondamental qui s'inscrit dans le cadre plus large de la gestion des identités et des accès.

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

Curtis Jack, Manager of Technical Engineering chez Oxford Properties Group

Consultez l'étude de cas

Aujourd'hui, les entreprises et les administrations sont confrontées au défi de sécuriser beaucoup plus de comptes privilégiés et de prendre en charge des réseaux distants, hybrides et décentralisés beaucoup plus importants que par le passé – nombre d'entre eux ne sont même pas considérés comme des comptes privilégiés traditionnels exploités par des administrateurs ou des propriétaires de systèmes.

Nous faisons face à un volume d'outils, d'utilisateurs et de machines nécessitant un accès privilégié plus important que jamais. Les ressources et les comptes privilégiés peuvent être provisionnés à grande échelle dans plusieurs environnements cloud. Cependant, même les ressources éphémères peuvent créer une surface de risque et doivent être prises en compte de manière appropriée par des contrôles de sécurité.

De plus en plus, les ressources qui nécessitent une authentification, des privilèges et des accès peuvent se trouver hors du périmètre des politiques de l'entreprise. Cela peut inclure d'autres ressources ou identités, comptes et processus non approuvés. C'est à partir de toutes ses contraintes pratiques qu'est né le concept de plan de données, qu'il est important de gérer.

Une architecture Zero Trust (ZTA) répond aux défis modernes de sécurité des accès privilégiés. Une ZTA impose aux collaborateurs et partenaires à distance un accès granulaire, sécurisé et autorisé à proximité des ressources, qu'elles soient situées sur site ou dans le cloud, conformément à la politique d'accès définie par une organisation.

Grâce à la granularité de la gestion des accès privilégiés, le Zero Trust est à même de garantir que tous les accès sont gérés et documentés pour un comportement approprié, indépendamment de la taille et de la conception de l'enclave considérée. Aujourd'hui, c'est là un défi particulièrement important à relever pour que les organisations puissent répondre à leurs obligations légales et aux critères des cyber assurances.

Comment le Privileged Access Management (PAM) de BeyondTrust met en place une ZTA

Comme prévu par le NIST (SP 800-207), un modèle de sécurité Zero Trust élimine la confiance continue et applique l'authentification, le principe du moindre privilège et le contrôle d'accès adaptatif. Cette stratégie assure aussi la segmentation et la micro-segmentation pour un accès sécurisé. Une approche Zero Trust se rapporte à disposer constamment d'une visibilité et d'un contrôle sur qui fait quoi dans votre réseau. Ce sont là des capacités essentielles que fournissent les solutions modernes de gestion des accès privilégiés (PAM), comme celle de BeyondTrust.

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

Brandon Haberfeld, Global Head of Platform Security chez Investec.

Consultez l'étude de cas

Les solutions **Privileged Access Management de BeyondTrust** permettent une mise en œuvre intelligente et pratique du modèle de sécurité Zero Trust du NIST sans perturber les processus métier. Nos solutions éliminent la confiance persistante en garantissant que l'ensemble des autorisations et accès privilégiés sont audités en permanence. Le principe du moindre privilège est provisionné par le just-in-time et révoqué immédiatement après l'achèvement d'une tâche, un changement de contexte ou l'expiration d'un certain délai.

Avec BeyondTrust, vous pouvez commencer par les cas d'utilisation PAM les plus urgents pour votre organisation, puis traiter de manière transparente les cas d'utilisation restant au fil du temps. Chaque cas d'utilisation, une fois résolu, fournira plus de contrôle et de responsabilité pour les comptes, les actifs, les utilisateurs, les systèmes et les activités dans votre environnement de privilèges, tout en éliminant et atténuant plusieurs vecteurs de menace. De plus, BeyondTrust fournit des contrôles de sécurité centralisés des accès privilégiés couvrant votre environnement hétérogène : sur site, cloud/multicloud (AWS, Azure, etc.), Windows, macOS, Unix, Linux, etc. Aucun autre fournisseur n'offre un contrôle aussi approfondi et étendu des accès privilégiés.

Plus vous traitez de cas d'utilisation, plus les synergies du PAM apparaissent et plus vous aurez d'impact sur la réduction des risques pour l'entreprise, sur les activités opérationnelles et sur la réalisation des objectifs Zero Trust.

De façon générale, le PAM de BeyondTrust fournit les fonctionnalités suivantes dans les environnements sur site et dans le cloud :

- Il recense, intègre et répertorie l'ensemble des identités, comptes et actifs privilégiés.
- Il impose un accès variable et une authentification continue afin de s'assurer que tous les appareils, utilisateurs, comptes et identités ont une forte confiance dans l'identité qu'ils revendiquent, c'est-à-dire qu'ils sont bien ce qu'ils disent être, au-delà de la simple authentification positive.
- Il concède juste assez d'accès et de droits privilégiés en appliquant le principe du moindre privilège, y compris l'accès just-in-time, à toutes les sessions, endpoints et applications.
- Il permet aux prestataires externes, collaborateurs et centres de services d'accéder aux sessions et applications de confiance par un accès à distance sécurisé et à moindre privilège.
- Il met en place une segmentation et une micro-segmentation pour isoler les actifs et les utilisateurs et pour empêcher tout mouvement latéral sur le réseau.

- Il surveille et gère chaque session privilégiée, offrant visibilité et contrôle en continu sur qui fait quoi et pourquoi, de sorte que tout comportement suspect puisse déclencher une révocation immédiate des autorisations et de l'accès.
- Il étend l'authentification Microsoft® Active Directory, les fonctionnalités d'authentification unique et la gestion de la configuration de la règle de groupe aux systèmes Unix et Linux, simplifiant ainsi la gestion sécurisée des identités et la mise en œuvre du Zero Trust à l'échelle de l'entreprise, quels que soient le système d'exploitation ou l'application.

Tableau : Comment le PAM de BeyondTrust est intégré à l'Architecture Zero Trust du NIST

		Concepts de base de la ZTA du NIST			
		Policy Engine (PE)	**Policy Administrator (PA)**	**Policy Enforcement Point (PEP)**	**Passerelle**
Solutions BeyondTrust	**Password Safe**	Situé au niveau des capacités de gestion régissant la gestion des secrets et des modèles d'accès basés sur les rôles et les attributs définis par l'administrateur de politique. Le policy engine de Password Safe de BeyondTrust décide de la disponibilité d'un accès à partir d'un grand nombre de critères et surveille les accès privilégiés, même s'ils sont éphémères.	Il crée, met à jour et gère la politique pour les utilisateurs finaux et les identités machines afin d'accorder les accès et d'automatiser les sessions privilégiées. L'accès à l'enclave de la ressource est octroyé par le Policy Administrator et peut être géré via la console BeyondInsight de BeyondTrust.		La passerelle est mise en place en utilisant : 1. une appliance BeyondTrust en tant que Worker Node lors de l'installation complète de Password Safe sur site, qu'il y ait ou non un accès à Internet. 2. (de préférence) un Resource Broker lors de l'utilisation de Password Safe pour gérer des actifs sur site. La passerelle répond à une demande d'accès privilégié à une session ou à une application depuis un Policy Engine approuvé. C'est un aspect essentiel du Zero Trust, car l'utilisateur ne se voit jamais accorder un accès direct à une ressource, comme c'est le cas lorsqu'il utilise un protocole natif du système d'exploitation. Toute la connectivité est gérée et surveillée par l'agent et seule l'activité de session (écran, terminal ou page Web) est divulguée au sujet demandeur.

	Concepts de base de la ZTA du NIST			
	Policy Engine (PE)	**Policy Administrator (PA)**	**Policy Enforcement Point (PEP)**	**Passerelle**
Privileged Remote Access	Situé au niveau des capacités de gestion régissant l'accès à distance et des modèles d'accès basés sur les rôles et les attributs définis par le Policy Administrator. Secure Remote Access de BeyondTrust peut gérer les ressources et les utilisateurs dans n'importe quelle zone du réseau, quel qu'en soit le périmètre, tant que l'accès à Internet est disponible.	Il crée, met à jour et gère la politique pour les utilisateurs finaux, il autorise l'accès et il automatise l'accès à distance aux applications. C'est la base du Zero Trust. L'accès à la ressource ou à l'application est octroyé par le Policy Administrator et il peut être géré via la console Secure Remote Access de BeyondTrust.	Mise en place par un Jump Client. Il répond à une demande d'accès à distance à une session ou à une application à partir d'un Policy Engine de confiance ou d'un proxy intermédiaire appelé Jump Point. Un utilisateur ne se voit jamais accorder un accès direct à une ressource, comme c'est le cas lorsqu'il utilise un protocole natif du système d'exploitation. Toute la connectivité est gérée et surveillée, et seule l'activité de la session (écran, terminal ou page Web) est communiquée à l'utilisateur qui en	
Gestion des privilèges pour Windows/Mac et Unix/Linux	Le Policy Engine est situé au niveau des capacités de gestion du moteur des règles, politiques et connexions régissant l'accès aux endpoints au moindre privilège, ainsi qu'au niveau des modèles d'accès basés sur les rôles et les attributs définis par le Policy Administrator.	Le Web Policy Administrator crée, met à jour et gère la politique pour les utilisateurs finaux, il autorise l'accès et il automatise l'accès aux applications. C'est la base du Zero Trust. L'accès à la ressource ou à l'application est octroyé par le Policy Administrator et il peut être géré via l'interface de gestion des privilèges de BeyondTrust pour Windows et Mac (en cas de déploiement via le cloud).	Le Policy Enforcement Point est le client à moindre privilège installé sur les endpoints Windows, macOs, Unix et Linux. Pour Windows et macOS, il lance les applications privilégiées et effectue le contrôle des applications sur les endpoints pour le compte de l'utilisateur ou de l'application. La fonction du Policy Enforcement Point compare la demande d'exécution de l'application à la politique définie et lance (ou bloque) l'application avec les privilèges appropriés, sans utiliser réellement les identifiants privilégiés. Cette fonctionnalité est fondamentale pour le Zero Trust, car l'application ou l'utilisateur ne reçoit jamais d'identifiants administratifs, mais peut exécuter une application avec des privilèges. Pour Unix/Linux, il initie des ordres à partir de l'hôte au nom de l'utilisateur ou de l'application, sans que l'utilisateur final ne se connecte réellement.Il restitue les résultats de manière transparente à l'utilisateur final.	

Privileged Password Management

La transformation digitale ouvre la voie à la prolifération des comptes et des accès privilégiés

Les organisations font désormais face à une explosion du nombre de comptes privilégiés à gérer (utilisateurs humains, applications, machines, etc.). Ces comptes privilégiés sont nécessaires à des technologies sur site, dans le cloud, aux environnements hybrides et à de nombreuses solutions SaaS, IaaS et PaaS qui assurent l'efficacité d'une entreprise moderne.

Les identifiants privilégiés et autres secrets doivent être gérés à l'aide d'un modèle capable de prendre en charge votre environnement moderne. L'accès aux mots de passe et aux secrets doit tenir compte des identités des utilisateurs humains et machines, que ce soit sur site ou dans le cloud, ou qu'elles fassent l'objet d'une licence octroyée par un sous-traitant, un prestataire ou un fournisseur de solutions.

Permettre un accès et un contrôle des privilèges sécurisés et adaptatifs grâce à la gestion des mots de passe privilégiés

La gestion des mots de passe privilégiés (également appelée gestion des comptes et des sessions privilégiés) offre un moyen optimal d'architecturer un accès aux ressources sensibles, ce qui la rend parfaitement adaptée aux défis actuels. Pour cela, il faut utiliser un modèle utilisant une passerelle d'enclave Zero Trust comme décrit plus haut.

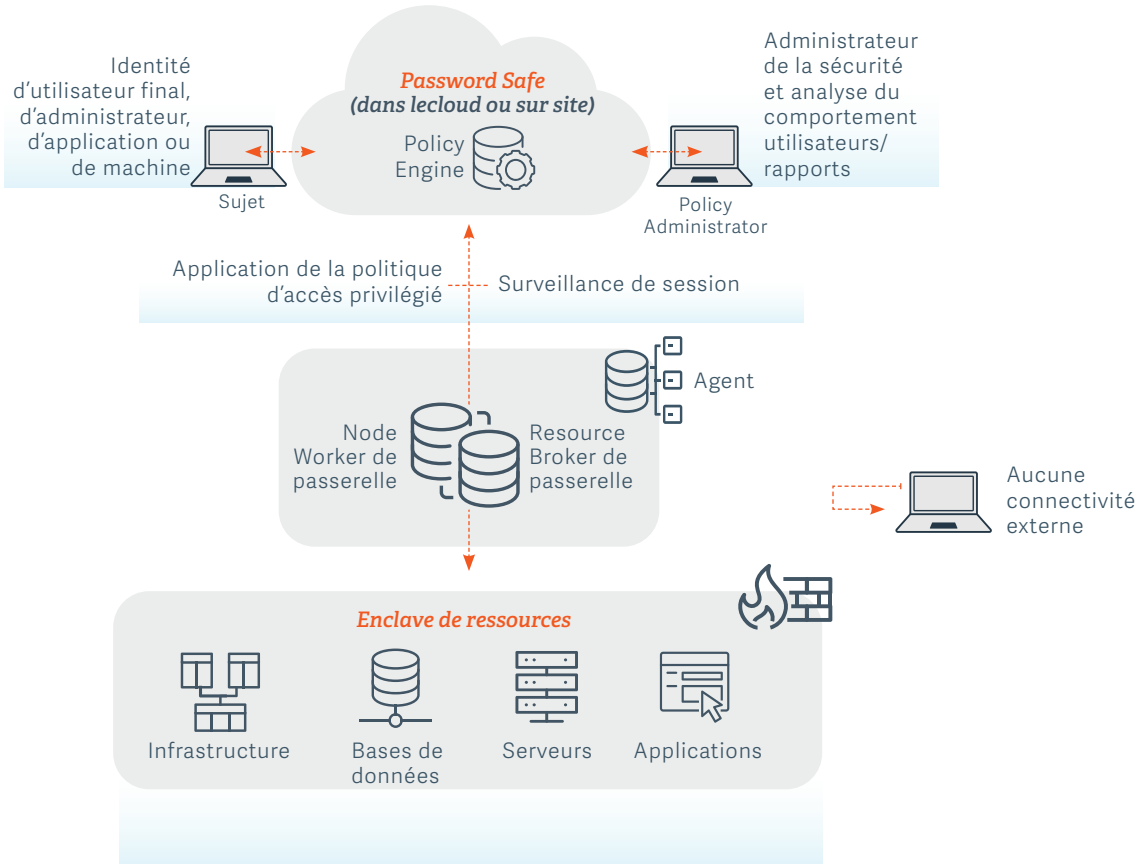
Password Safe, la solution de gestion des mots de passe privilégiés de BeyondTrust, garantit que vos ressources sont gérées et protégées contre les abus de connexion potentiellement inappropriés, et que toutes les ressources contenues dans une enclave sont exécutées dans le cadre d'un modèle Zero Trust. Cela signifie qu'il ne sera fait confiance à aucune identité d'utilisateur final ou machine pour une session privilégiée directe, sauf si l'accès peut avoir lieu par l'intermédiaire d'une passerelle. L'activité de toutes les sessions est intégralement surveillée. Cela vaut pour tout endroit où se trouve une enclave de ressources, quel qu'en soit le périmètre.

Password Safe est particulièrement utile pour le Zero Trust:

- Stockage sécurisé et récupération des mots de passe, d'identifiants et d'autres secrets pour autoriser les accès à des identités d'utilisateurs humains et machines.
- Renouvellement automatique des mots de passe d'accès à des ressources, en fonction de processus ou d'un calendrier, ou à la demande et la mise à disposition d'une API disposant de nombreuses fonctionnalités permettant d'autres automatisations.
- Enregistrement des mots de passe et des secrets passés pour accéder aux sauvegardes, aux instantanés de machines virtuelles et aux environnements de reprise d'activité après sinistre.
- Gestion complète des sessions, avec leur surveillance, enregistrement, lecture et analyse, à la fois en temps réel et depuis une perspective historique à des fins d'audit de conformité, d'analyse et de formation.
- Autorisation d'accès uniquement via une technologie de passerelle sécurisée permettant d'empêcher ou surveiller tout mouvement latéral sur le réseau, de négocier des accès via des composants distincts, de détailler et d'imposer une politique d'accès appropriée.
- Utilisation de l'architecture de gestion des mots de passe privilégiés pour les environnements existants, avec une distribution minimale.

Avec la conception détaillée dans ce document, tous les usages de Password Safe de BeyondTrust peuvent suivre le principe du moindre privilège et just-in-time, être intégrés à des solutions de gestion informatique, et permettre d'obtenir les avantages d'une enclave Zero Trust déployée à des fins d'administration et d'accès.

Architecture Password Safe pour un modèle d'enclave Zero Trust



Dans le diagramme ci-dessus, le système de l'entreprise est la console Password Safe ou l'API REST qui fournit une aide pour l'automatisation et les comptes non humains. Il convient également de noter que le rôle de l'agent est étroitement associé au policy engine. Son rôle est de communiquer au sujet les mots de passe ou les secrets depuis un emplacement de stockage chiffré et d'effectuer des contrôles et une rotation des ressources gérées existantes. Il s'agit notamment d'accéder à l'historique des mots de passe et des secrets et de gérer les décisions du policy engine, y compris la durée de l'accès.

Toute mise en œuvre partielle de ce modèle est susceptible d'améliorer la gestion des mots de passe privilégiés dans le cadre d'un périmètre défini par logiciel. Cette architecture offre une bien meilleure protection que de permettre des accès sans restriction à toute ressource en utilisant des identifiants statiques, surtout si le mot de passe et les secrets sont à facteur unique et réutilisés en raison des limites des solutions existantes.

Accès à distance sécurisé

Les risques liés à l'accès à distance sont nombreux dans un environnement de travail hybride

La meilleure pratique de sécurité consiste à ce que les protocoles natifs d'accès à distance soient désactivés pour tout périphérique informatique fourni par l'entreprise. Malheureusement, dans de nombreux environnements (en particulier en ce qui concerne les employés à distance), ce contrôle de sécurité n'a pas été mis en place et les appareils à distance peuvent accéder aux ressources de l'entreprise en utilisant des voies d'accès à distance insuffisamment sécurisées.

La logique de la mise en place de protocoles tels que RDP, SSH et VNC est une source de discorde entre les équipes informatiques et celles chargées de la sécurité de l'information. L'un des arguments est le besoin de disposer d'une technologie d'accès à distance à faible coût conçue pour être prise en charge dès le début par le système d'exploitation. C'est un argument que font généralement valoir les services informatiques en raison soit d'un manque d'expérience en matière de sécurité, soit de contraintes budgétaires. Les équipes chargées de la sécurité et de la conformité, quant à elles, se méfient des vulnérabilités inhérentes aux protocoles natifs, des exploits possibles et de l'absence d'audit et de routage sécurisé du réseau.

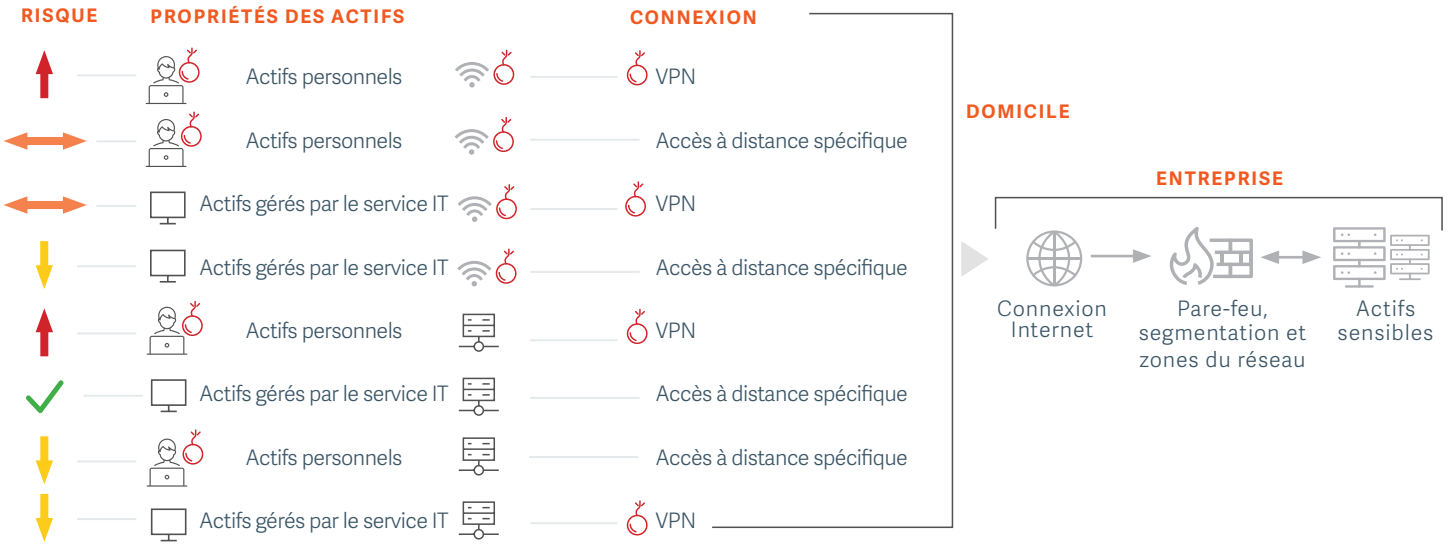
Il existe certainement un juste équilibre entre ces approches. Les utilisateurs autorisés doivent pouvoir lancer une session d'accès à distance sécurisée à n'importe quel appareil, à tout moment et quel que soit le protocole. En outre, il convient d'utiliser le contrôle des sessions, l'injection d'identifiants et le principe du moindre privilège pour surmonter les problèmes de sécurité et de conformité que rencontre une organisation. Ces fonctionnalités doivent être opérantes, que le collaborateur soit au bureau ou à distance. C'estest particulièrement vrai si la session à distance est seulement là pour permettre l'utilisation d'une application, au lieu d'être une session à distance à partir d'un endpoint.

Comment un utilisateur peut-il exploiter une application sans avoir besoin d'un VPN et répondre aux principes du Zero Trust ? Un accès à distance sécurisé compatible Zero Trust peut résoudre ce problème pour les applications et surmonter les difficultés inhérentes au routage de protocole traditionnel.

Comment une architecture Zero Trust peut surmonter les difficultés inhérentes aux protocoles natifs d'accès à distance

Une ZTA peut jouer un rôle central pour surmonter les difficultés inhérentes aux protocoles natifs d'accès à distance. Un système d'accès à distance Zero Trust peut s'adapter à pratiquement tous les environnements et permettre un flux de travail just-in-time (JIT) et avec Zero Standing Privileges (ZSP), ce qui signifie qu'aucun compte ne dispose de privilège permanent.

Le diagramme ci-dessous illustre les risques du travail à distance dans un environnement décentralisé et sans périmètre. Il illustre les différentes combinaisons d'actifs, de connectivité, de technologie d'accès à distance et de points de vulnérabilité aux attaques. En outre, avec une connexion normale, les applications peuvent fonctionner à distance ou à l'aide d'une session à distance. Pour sécuriser toutes les activités, la connexion elle-même doit être sécurisée et tous les accès doivent être fournis uniquement via une technologie d'accès à distance sécurisée.



Dans le graphique ci-dessus, chaque symbole de menace représente un risque.

- Trois menaces : inacceptable, risque critique
- Deux menaces : niveau moyen de risque acceptable
- Une menace : risque faible en cas d'accès à distance
- Zéro menace : meilleure configuration pour une connexion à distance acceptable

Notez que l'utilisation d'un appareil personnel avec un client utilisant un VPN fourni par l'entreprise représente toujours un risque critique, que la connexion soit filaire ou non. En effet, l'appareil n'est pas géré et l'organisation n'a aucun contrôle sur la façon dont il est utilisé, mis à jour ou exploité, y compris sur les autres logiciels qui peuvent être installés ce qui inclut les logiciels malveillants.

Dans cet environnement décentralisé, des menaces existent lors de l'accès à des ressources internes sensibles à partir des configurations suivantes :

1. Équipement personnel (BYOD) non géré, sans patch, multi-utilisateur, en fin de vie ou exposé au phishing ou aux logiciels malveillants. En outre, les utilisateurs BYOD sont généralement leurs propres administrateurs locaux, ce qui amplifie le risque.

2. Réseaux domestiques non sécurisés utilisant le WiFi où la connexion est potentiellement non sécurisée, a un mot de passe faible, est complètement libre ou peut permettre une interception (man-in-the-middle attack) en raison d'un SSID commun ou d'un mauvais cryptage. En outre, d'autres appareils peuvent compromettre le réseau sans fil ou surveiller les communications. Cela comprend les comptes privilégiés hors du périmètre des politiques de l'entreprise utilisés par les réseaux domestiques accédant aux solutions SaaS grand public.

3. La technologie VPN, qui utilise généralement le split tunneling et ne devrait jamais être installée sur des appareils personnels, pourrait compromettre les communications et ouvrir la porte à des mouvements latéraux via les failles du réseau domestique. Étant donné que la technologie VPN ne fonctionne qu'au niveau de la couche réseau, elle n'est pas en mesure de surveiller les sessions ou les applications à distance. En règle générale, les utilisateurs à distance n'ont besoin, pour un programme ou une session spécifique, que d'un accès à l'application (c'est-à-dire à la couche applicative).

Gérer les risques liés à l'accès à distance avec le Zero Trust

Pour atténuer les menaces, une combinaison de Zero Trust, d'appareils gérés par les services IT, de gouvernance IT et de gestion des accès privilégiés peut réussir là où la technologie traditionnelle seule peut présenter un risque inacceptable.

- **Gestion par les services IT** – Contrôles de sécurité gérés pour l'évaluation des risques, y compris les disciplines de base pour la gestion des vulnérabilités et des correctifs.
- **Connexion** – Minimiser les risques réseau avec une connexion filaire au lieu d'une connexion sans fil inconnue.
- **Gestion des accès privilégiés** – Les sessions d'accès à distance sont initiées au niveau de la couche applicative selon le rôle, y compris le brouillage des identifiants. Cela élimine le besoin de trafic au niveau de la couche réseau par application et par utilisateur. L'élévation des privilèges est strictement contrôlée localement et sur l'ensemble du réseau, ce qui élimine également les identifiants administratifs locaux et les droits admin des utilisateurs finaux.
- **Gouvernance** – Documentation de toutes les activités privilégiées à des fins de conformité, y compris le comportement des utilisateurs d'accès à distance.
- **Zero Trust** – Mise en œuvre de contrôles stricts et d'une architecture de gestion basée sur le cloud pour toutes les sessions d'accès à distance respectant le Zero Trust. Ainsi, le Zero Trust, allié au principe du moindre privilège s'applique à toutes les sessions, quelles que soient leur origine ou leur destination. Cela garantit la possibilité d'atténuer pleinement les risques en n'exposant jamais les privilèges racines ou les privilèges administratifs hors périmètre étendu ou à l'utilisateur final.

Cette combinaison de technologies et de stratégies fonctionne car non seulement vous sécurisez le périphérique source, mais vous minimisez également les risques réseau :

- en utilisant une connexion filaire
- en contrôlant strictement l'accès à distance
- en n'effectuant aucun routage de protocole comme SSH
- en enregistrant toutes les activités de session à des fins de conformité et d'analyse comportementale

Enfin, le fait d'appliquer le Zero Trust allié au principe du moindre privilège garantit que les risques peuvent être entièrement atténués en n'exposant jamais des privilèges root ou administratifs hors du périmètre. Les VPN seuls ne peuvent le faire sans avoir recours à des solutions de gestion des privilèges.

Étendez les contrôles PAM et Zero Trust au-delà du périmètre avec le Privileged Remote Access de BeyondTrust

Les VPN ne peuvent pas gérer efficacement les risques à l'intérieur d'un périmètre ou d'une enclave définis. Pour que le Zero Trust soit efficace, il faut que le réseau et l'environnement soient sécurisés avant qu'une ZTA puisse être mise en place.

Privileged Remote Access de BeyondTrust est conçu pour gérer les sessions et, avec quelques ajustements, peut incorporer un modèle Zero Trust. La solution étend les meilleures pratiques de gestion des accès privilégiés au-delà de votre périmètre. Privileged Remote Access permet aux organisations d'appliquer le principe du moindre privilège et de solides contrôles d'audit à tous les accès à distance demandés par des collaborateurs, des prestataires externes et des centres de services. Les utilisateurs peuvent accéder rapidement et en toute sécurité à n'importe quel système distant, sur n'importe quelle plateforme et à tout moment. Ils peuvent également tirer parti du coffre-fort de mots de passe intégré pour découvrir, intégrer et gérer les identifiants privilégiées. Ainsi, Privileged Remote Access de BeyondTrust fournit des contrôles granulaires de type « moindre privilège » qui seraient, dans la pratique, inimaginables avec des VPN et de nombreuses autres technologies d'accès à distance couramment utilisées.

Lorsque des protocoles ou outils natifs sont nécessaires, BeyondTrust offre également des fonctionnalités de gestion d'accès à l'infrastructure via notre solution Privileged Remote Access. Cette fonctionnalité combine des flux de travail natifs, des principes Zero Trust (tels que le Just-in-Time et l'absence de privilège permanent) et une piste d'audit complète.

Pour les spécialistes des technologies, comme les développeurs et les ingénieurs cloud ops, l'utilisation de VPN s'est avérée un mal nécessaire – les environnements disparates nécessitant même parfois plusieurs VPN. Bien que les VPN soient cryptés et généralement sécurisés, ils permettent un accès plus large que ce qui est généralement nécessaire. De plus, du point de vue des activités quotidiennes, l'utilisateur doit se rappeler quel VPN doit être utilisé pour chaque appareil et il doit connaître les identifiants propres à ce système.

Grâce à Privileged Remote Access, l'utilisateur peut n'utiliser qu'une seule console, utiliser ses outils natifs (à savoir SQL, SSH et RDP) et injecter des identifiants à partir d'un coffre-fort sécurisé ; en outre, une piste d'audit complète (et consolidée) sera générée pour chaque session. Cette méthodologie donne aux utilisateurs le flux de travail souhaité pour la gestion de l'ensemble de l'infrastructure et offre à l'organisation la sécurité et l'étanchéité nécessaires lors d'un audit.

Le Zero Trust de Privileged Remote Access est particulièrement utile pour les finalités suivantes :

- Appliquer le principe du moindre privilège et des contrôles d'audit solides à tous les accès à distance pour les collaborateurs, sous-traitants, prestataires externes et le personnel des centres de services.
- Gérer et injecter automatiquement des identifiants dans les sessions et applications à distance de sorte que l'utilisateur final ne les voie jamais ou n'en ait jamais connaissance lors d'une utilisation à bon escient (possibilité de l'intégrer à Password Safe de BeyondTrust pour une gestion plus étendue des informations d'authentification privilégiées).
- Sécuriser l'accès à l'infrastructure par un Jump Server sécurisé avec authentification multi facteurs, autorisation adaptative, et surveillance des sessions pour les consoles d'administrateur. Cela s'applique également aux accès qui traversent des zones réseau de confiance.

- Fournir un accès à des pages Web, telles que le portail Azure ou Microsoft 365, via un navigateur Chromium verrouillé et intégré.
- Mettre en place des frontières entre les systèmes de développement, de test et de production conformément aux meilleures pratiques SecDevOps.
- Fournir une micro-segmentation au niveau des applications de sorte à empêcher les utilisateurs d'exploiter des applications et autres ressources auxquelles ils ne sont pas autorisés à accéder.

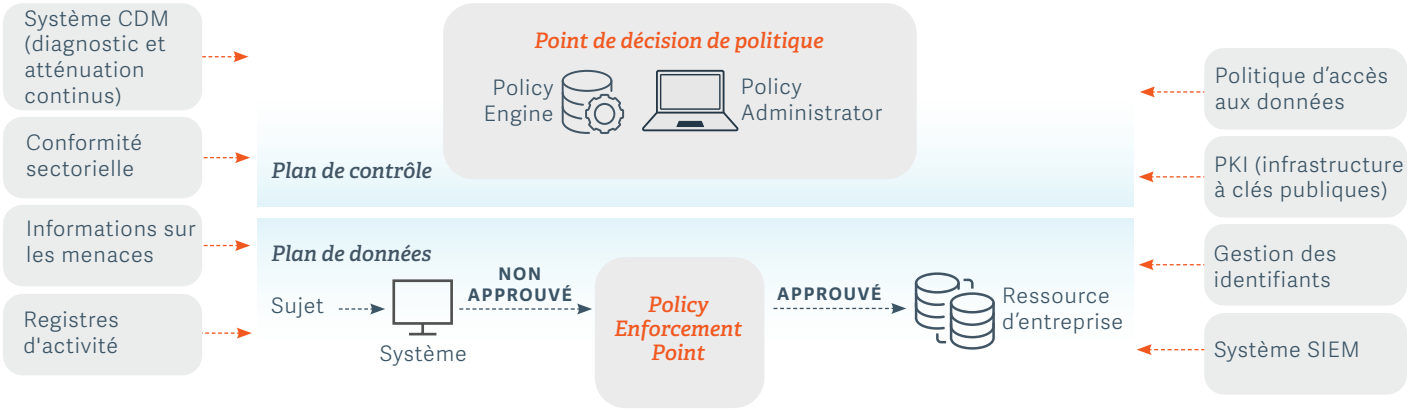
Privileged Remote Access offre les avantages suivants par rapport au VPN seul.

Comparaison des fonctionnalités de Privileged Remote Access de BeyondTrust avec celles d'un VPN classique :

VPN contre Privileged Remote Access de BeyondTrust

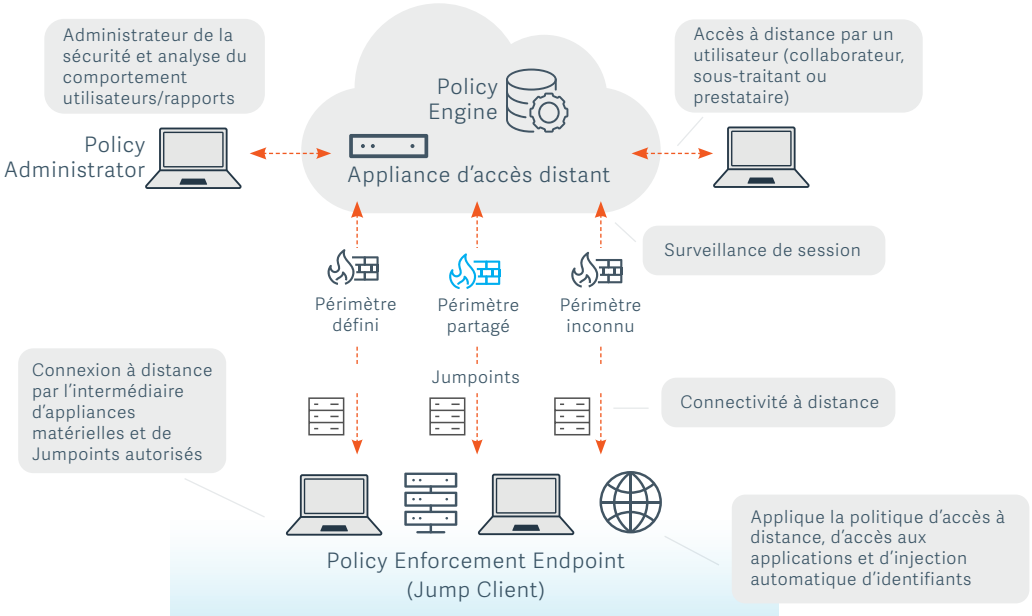
Fonctionnalité	VPN	BeyondTrust
Accès à distance	•	•
Connexion sécurisée	•	•
Accès à la couche réseau (tunnel par protocole)	•	•
Trafic crypté	•	•
Virtualisation de la couche application		•
Poste de travail à distance		•
Accès au protocole du poste de travail à distance par proxy		•
Accès VNC par proxy		•
Accès SSH par proxy		•
Surveillance de session d'application		•
Enregistrement de session d'application		•
Accès Just-in-Time		•
Architecture Zero Trust		•
Intégration de la gestion des accès privilégiés (PAM)		•
Sécurisation des équipements personnels		•
Intégration aux solutions ITSM		•
Gestion des mots de passe et stockage des identifiants		•
Déploiement dans le cloud ou sur site (appliance matérielle ou virtuelle)		•
Accès sans agent		•
Grande compatibilité avec les différents systèmes d'exploitation et plateformes		•
Prévention des mouvements latéraux		•
Piste d'audit et rapports de session		•

Considérons ensuite ce diagramme simplifié de l'architecture d'un accès à distance Zero Trust conforme aux recommandations du NIST :



Avec cette configuration, toutes les sessions à distance doivent respecter les principe du moindre privilège et l'accès just-in-time, s'intégrer aux solutions de gestion informatique et suivre une architecture Zero Trust de sorte que la politique et l'administration respectent les meilleures pratiques reconnues en matière de sécurité.

Voici comment cela fonctionne au quotidien avec un principe Zero Trust et Privileged Remote Access de BeyondTrust :



Pas d'accès direct des utilisateurs à distance à un actif.
Application de la politique Zero Trust par l'intermédiaire d'un policy engine, d'un routage réseau et d'accès à distance spécifiques pour les clients.

Toute mise en œuvre partielle de ce modèle peut constituer une amélioration de la sécurité IT dans le cadre d'un périmètre défini par logiciel. Cette architecture offre une sécurité beaucoup plus importante que la configuration dans laquelle vous autoriseriez dans votre environnement un ordinateur personnel utilisant un accès VPN pour exécuter des tâches administratives.

Endpoint Privilege Management

Les utilisateurs de Windows et macOS disposent de trop de privilèges

Pour la quasi-totalitédes organisations, le moyen le plus simple de contrôler les parcs d'endpoints Windows et macOS consiste à mettre en œuvre le principe de moindre privilège en retirant aux utilisateurs finaux leurs droits administrateurs locaux permanents. Malheureusement, de nombreuses organisations n'ont appliqué ce contrôle de sécurité clé que partiellement ou imparfaitement, ce qui les rend vulnérables aux cyberattaques de toutes sortes.

Pour mettre en place efficacement le principe du moindre privilège, l'organisation doit trouver une solution qui permet de concilier harmonieusement les deux objectifs suivants.

- **Productivité :** De nombreuses tâches que les utilisateurs finaux doivent effectuer quotidiennement nécessitent des droits admin, notamment pour installer des applications ou modifier des paramètres système. Si leurs droits admin leur sont retirés sans solution de remplacement, leur productivité peut s'en trouver fortement entravée.
- **Sécurité :** L'organisation doit supprimer tous les droits admin locaux, exercer un contrôle des applications censées être installées ou exécutées par différents groupes d'utilisateurs finaux et limiter les tâches que les utilisateurs finaux peuvent exécuter sur leurs endpoints, afin de réduire l'exposition aux menaces.

Ces objectifs soulignent l'importance d'une architecture Zero Trust pour la gestion des privilèges sur les endpoints, en particulier compte tenu de la flexibilité de l'environnement de travail hybride. Adopter la bonne solution de gestion des privilèges sur les endpoints dans le cadre d'une architecture Zero Trust permet de s'adapter aux environnements de travail au bureau et à domicile et de combler l'écart souvent constaté entre la gestion des privilèges et des applications, tout en assurant une bonne gestion des authentifications.

Mettre en place une ZTA avec Privilege Management pour Windows & Mac de BeyondTrust

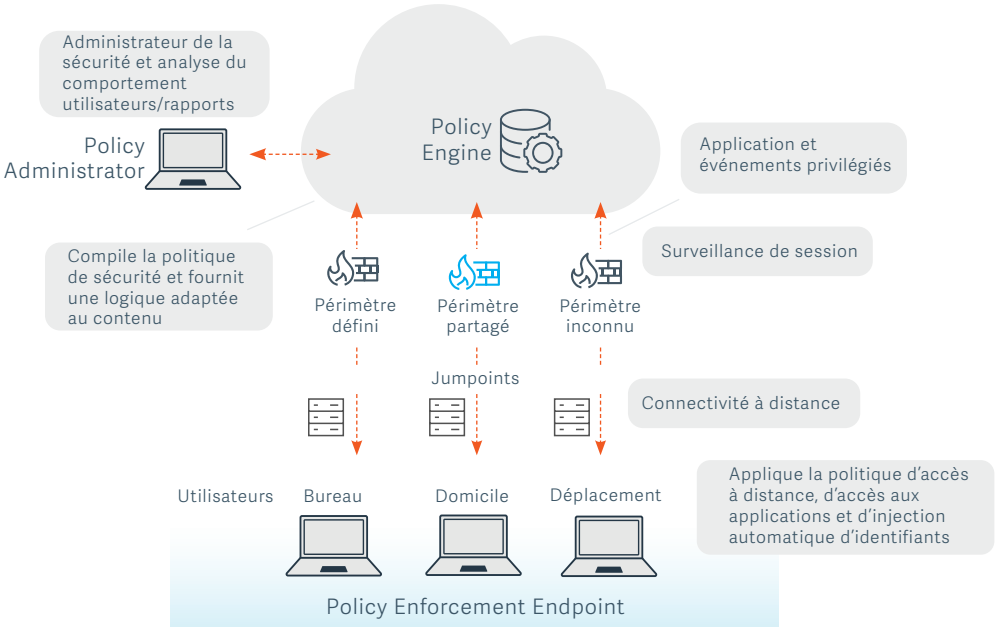
Privilege Management pour Windows & Mac de BeyondTrust atteint de façon élégante les deux objectifs fixés pour toute solution efficace de gestion des privilèges sur les endpoints. Il supprime les droits admin excessifs et applique un contrôle moderne des applications, tout en élevant de façon dynamique les droits des utilisateurs finaux de sorte qu'ils disposent de l'accès nécessaire au moment où ils en ont besoin, sans entraver leur productivité.

Privilege Management pour Windows & Mac est particulièrement utile pour les finalités suivantes :

- Mettre en place la sécurité Zero Trust en supprimant les droits admin excessifs et en éliminant les privilèges persistants.
- Appliquer un contrôle granulaire des applications et imposer le principe du moindre privilège pour l'ensemble des applications, navigateurs Web, systèmes et autres ressources en donnant aux utilisateurs l'accès nécessaire et suffisant au moment où ils en ont besoin.
- Bloquer les attaques qui tirent parti d'applications approuvées, telles qu'Office, Adobe et les navigateurs Web, en appliquant des contrôles de sécurité intégrés selon le contexte.
- Réduire considérablement l'exposition aux cyberattaques et protéger contre les attaques des logiciels malveillants, ransomwares et de phishing.
- Fournir une piste d'audit unique de toutes les activités des utilisateurs avec des tableaux de bord sous forme de graphiques et des rapports.

Privilege Management pour Windows & Mac, ainsi que Privilege Management pour Unix & Linux (traité dans la section suivante) et **Active Directory Bridge**, constituent ensemble la solution Endpoint Privilege Management de BeyondTrust. Cette solution combine la gestion du moindre privilège et le contrôle des applications de sorte à réduire au minimum la surface d'attaque des endpoints et d'éliminer les mouvements latéraux indésirables sur la totalité de votre environnement hétérogène.

Considérez ce diagramme de Privilege Management pour Windows & Mac conforme à la ZTA du NIST :



Aucun privilège administrateur approuvé pour les utilisateurs, local comme à distance. Les applications sont approuvées pour l'élévation ou bloquées pour l'exécution.

Si vous envisagez de restructurer, de redéployer ou de moderniser votre modèle de sécurité des endpoints, vous pouvez atteindre le Zero Trust pour l'élévation des privilèges, le principe du moindre privilège et le contrôle des applications en tirant parti de ce paradigme. Ce modèle répond à toutes les exigences du Zero Trust et permet à la gestion des privilèges sur les endpoints d'étendre ses fonctions à d'autres modèles de sécurité, tels que l'accès Just-In-Time.

Du point de vue de l'architecture, l'enclave entière est située à l'endpoint et représente la base idéale pour toute architecture Zero Trust et toute approche de segmentation.

Le risque relatif aux privilèges Unix et Linux met en péril les données et les actifs sensibles

Les administrateurs Unix et Linux n'utilisent physiquement que rarement, voire jamais, le clavier associé directement à leur actif, si tant est qu'un clavier y soit connecté. C'est presque toujours le cas lorsque vous travaillez dans le cloud.

L'administration, et même l'accès root, sont octroyés à la personne physique. Cette personne utilise une technologie d'accès à distance et des protocoles tels que SSH pour effectuer une tâche. Si l'administration sous Unix et Linux est principalement effectuée à distance, une question se pose : d'où provient cette administration à distance ? Est-ce sur site et au sein d'un réseau approuvé, ou l'utilisateur travaille-t-il à distance, par exemple de son bureau chez lui, voire de son canapé ? Si vous considérez chaque session d'accès à distance comme une forme d'accès à distance privilégié, puisque l'accès est en fait octroyé par quelqu'un qui opère à distance, le clavier et la souris sont alors bien loin du périphérique informatique réel.

Aujourd'hui, les réseaux non sécurisés d'utilisateurs travaillant à domicile, ou depuis n'importe quel endroit, forment une extension de nos périmètres informatiques. Par conséquent, nous sommes exposés à de nouveaux vecteurs d'attaque et à de potentielles difficultés de conformité réglementaire qui doivent être résolues. Pour l'administration sous Unix et Linux, cela représente un risque inacceptable. En effet, les données et applications les plus sensibles d'une entreprise classique résident généralement sur ces plateformes essentielles.

Toute connexion dépend d'identifiants sécurisées qui suivent le modèle du moindre privilège, de l'accès Just-In-Time et de l'authentification à usage unique.

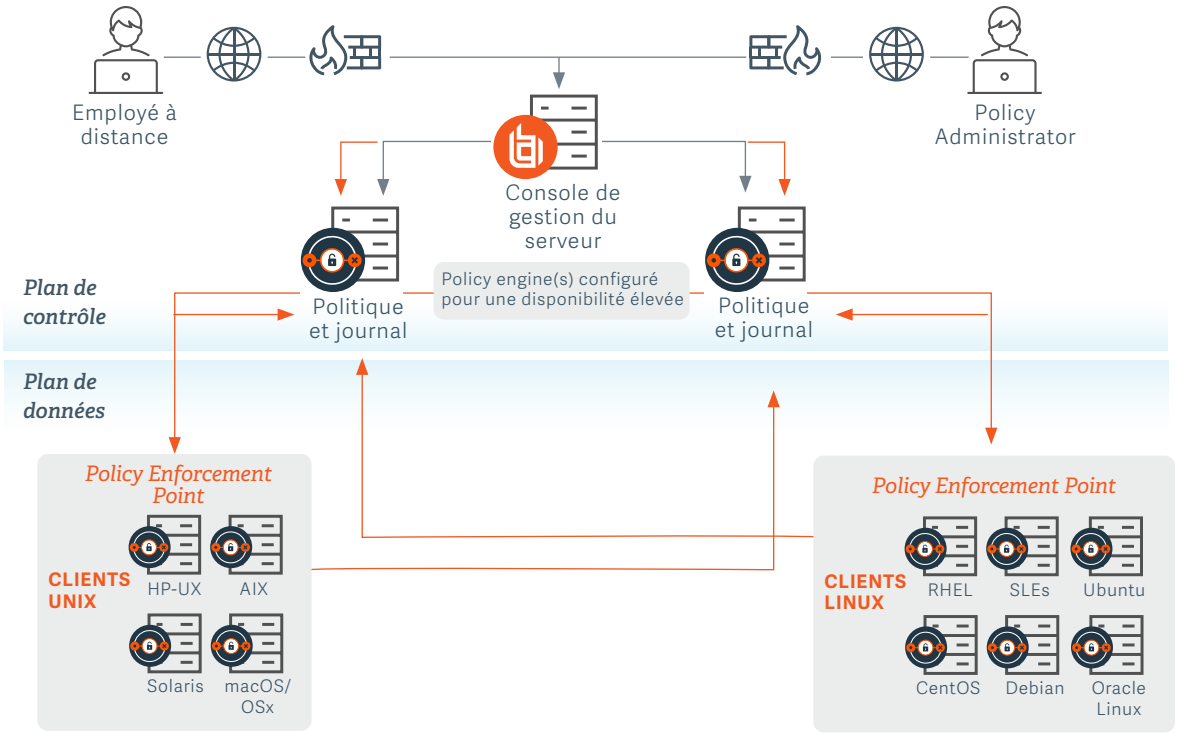
Mettre en place une ZTA pour votre parc de serveurs avec Privilege Management pour Unix & Linux de BeyondTrust

Privilege Management pour Unix & Linux de BeyondTrust permet aux organisations de contrôler de manière granulaire les accès privilégiés, d'assurer la conformité et de réduire considérablement les cyberrisques. Le produit peut appliquer des facteurs tels que l'heure, le jour, l'emplacement et le statut de vulnérabilité de l'application ou de l'actif, afin d'améliorer la prise de décision relative à l'élévation de privilèges. Les fonctionnalités du produit vont bien au-delà de la commande « sudo » (se substituer à l'utilisateur pour faire) : administration centralisée, gestion et surveillance des sessions, vérification de l'intégrité des fichiers et améliorations importantes de la productivité.

Privilege Management pour Unix & Linux est particulièrement utile pour les finalités suivantes :

- Supprimer les droits admin et mettre en place le principe du moindre privilège sur l'ensemble des endpoints Unix/Linux.
- Permettre aux utilisateurs d'accéder de façon sécurisée à des commandes spécifiques et à des sessions à distance sans avoir à utiliser un compte root ou administrateur.
- Passer à un état ZSP (sans privilège permanent) par l'élévation dynamique et le just-in-time des privilèges pour les processus, les applications, etc., mais pas pour les utilisateurs finaux.
- Mettre en place la séparation des tâches et des privilèges pour limiter les privilèges associés à un compte ou processus donné.

Considérez ce diagramme de Privilege Management pour Unix & Linux conforme à la ZTA du NIST :



Des contrôles de sécurité Zero Trust sans faille pour Windows, Unix & Linux grâce à AD Bridge

Active Directory (AD) Bridge de BeyondTrust, qui fait partie de la solution Endpoint Privilege Management, joue un rôle important dans la prise en charge et la simplification d'une stratégie Zero Trust pour les machines Unix/Linux, tout en aidant les organisations à se conformer à d'autres obligations réglementaires.

AD Bridge centralise l'authentification pour les environnements Unix et Linux en étendant l'authentification Kerberos et l'authentification unique de Microsoft AD. Les utilisateurs utilisent leurs identifiants AD pour accéder aux systèmes Unix & Linux de façon transparente.

Les organisations peuvent obtenir des politiques et des contrôles cohérents pour l'ensemble de leurs activités en étendant les outils natifs de gestion des politiques de groupe de sorte à inclure les paramètres Unix et Linux. Les utilisateurs passent d'un poste de travail à une machine distante ou d'un système à l'autre, sans qu'il soit nécessaire d'entrer à nouveau les identifiants. L'exploitation de la stratégie de groupe Microsoft sur des plateformes non Windows permet également une gestion centralisée de la configuration, réduisant ainsi les risques et la complexité liés à la gestion d'un environnement hétérogène.

Historiquement, les administrateurs de la sécurité ont eu du mal à convertir, appliquer, imposer et auditer les politiques du NIST et d'autres organismes dans l'ensemble de l'entreprise. AD Bridge facilite la cartographie automatique des paramètres du NIST et leur application aux machines, qu'elles soient sur site ou dans le cloud. Les paramètres du NIST peuvent être imposés par des objectifs de politique de groupe Active Directory. Ainsi, s'il y a une tentative de modification de ces paramètres, même via le compte root, ceux-ci seront immédiatement réinstallés et cela déclenchera une alerte indiquant une violation de politique. Cette alerte pourra être transmise à votre solution de gestion des informations et des événements de sécurité, telle qu'Elasticsearch, qui est intégrée de façon native à AD Bridge.

Privilege Management pour AD Bridge est particulièrement utile pour les finalités suivantes :

- Fournir un ensemble d'outils unique et familier pour gérer les systèmes Windows et Unix/Linux
- Centraliser la gestion des politiques de groupe
- Fournir des audits détaillés aux équipes Audit et Conformité
- Étendre l'authentification unique (SSO), le partage de fichiers et le contrôle d'accès à d'autres systèmes que Windows.

Considérations relatives à la conception du Zero Trust

« Dette technique » et systèmes existants

Les applications, l'infrastructure et les systèmes d'exploitation existants ne sont très certainement pas adaptés au Zero Trust. Ils ignorent le concept du moindre privilège, sont peu adaptés au contrôle des applications et manquent de modèles d'élévation des privilèges ou de modèles d'authentification qui permettraient d'effectuer des modifications dynamiques découlant d'une utilisation contextuelle. Le concept de télétravail leur est inconnu, de même que les architectures réseau modernes, sans parler du cloud. Leur fonctionnement repose sur une connexion réseau directe et les capacités de surveillance des sessions ou des mouvements latéraux leur font défaut. En fait, leur sécurité dépend probablement fortement du réseau.

Reconcevoir, recoder et redéployer des applications internes peut être coûteux et perturber les activités. Seul un sérieux impératif professionnel peut justifier le recours à ce genre de projets. Il n'est pas toujours possible d'ajouter des contrôles de sécurité aux applications existantes pour les rendre totalement fiables. Il est probable que vos applications existantes ne sont pas équipées pour prendre en charge les modèles de connexion d'une telle spécification et qu'elles ne sont pas codées de façon à fonctionner dans un modèle d'enclave de ressources tel que spécifié par le NIST.

Par conséquent, en fonction de l'architecture de votre application tierce personnalisée ou existante, envisagez d'utiliser :

- Le Zero Trust avec la gestion des mots de passe privilégiés comme mécanisme pour toute session gérée, lorsque la connexion doit être surveillée et gérée.
- Le Zero Trust avec la gestion des privilèges sur les endpoints comme mécanisme d'élévation de privilèges des employés à distance, d'accès au moindre privilège et de contrôle des applications.

- Le Zero Trust avec la gestion des accès privilégiés comme mécanisme d'authentification des employés à distance, l'accès au moindre privilège et la surveillance des sessions.
- Le Zero Trust avec un accès à distance sécurisé comme mécanisme de connexion des employés à distance.

Cette approche vous permettra de mettre en œuvre des contrôles Zero Trust et d'améliorer votre posture de sécurité sans avoir à reconcevoir les systèmes en place.

Toute mise en place du Zero Trust nécessite une approche par couche ou par enveloppe pour être compatible avec les systèmes existants. Cependant une pure approche Zero Trust suppose d'appliquer tous ces concepts à l'ensemble des ressources, où qu'elles se trouvent. Toutefois, vous pouvez :

- Consigner l'activité des sessions à distance, enregistrer les sessions d'écran interactif et surveiller les événements pour rechercher les comportements potentiellement malveillants. Il s'agit d'une mise en place partielle de Zero Trust avec Secure Remote Access qui pourra être suffisante dans certains environnements pour atténuer les risques. C'est un aspect important lorsqu'une seule session à distance peut interagir avec plusieurs systèmes en arrière-plan qui ne sont pas gérés, ce qui est particulièrement intéressant pour un acteur malveillant.
- Consigner les activités privilégiées, capturer les lancements de processus et surveiller les événements pour rechercher des comportements potentiellement malveillants. Il s'agit d'une mise en place partielle du Zero Trust avec Privileged Access Management qui pourra être suffisante dans certains environnements pour atténuer les risques d'accès aux applications à distance.
- Consigner les activités à l'écran, capturer les lancements de processus, compter les frappes au clavier et surveiller les journaux de logs pour rechercher les comportements potentiellement malveillants. Il s'agit d'une mise en place partielle du Zero Trust avec Privileged Access Management. En conjonction avec des listes de contrôle d'accès bien définies, cela est suffisant pour gérer, surveiller et atténuer les risques d'accès à distance à vos actifs Unix et Linux à partir de pratiquement n'importe quel emplacement source.

Technologies peer-to-peer

Si vous pensez que votre organisation n'utilise pas de technologie de mise en réseau peer-to-peer (P2P), il se peut que vous n'ayez pas conscience des paramètres par défaut dans Windows 10. En 2015, Windows 10 a introduit une technologie peer-to-peer pour partager les mises à jour de Windows entre systèmes homologues afin d'économiser de la bande passante. Bien que certaines organisations désactivent cette possibilité, d'autres ne savent peut-être pas qu'elle existe.

Cela représente un risque de mouvement latéral privilégié entre les systèmes. Même si aucune vulnérabilité ou attaque malveillante n'a tiré parti de cette lacune, cela génère des communications qui violent le modèle Zero Trust de la même manière qu'un serveur de messagerie doit communiquer avec le client de messagerie de chaque utilisateur final. Il ne doit y avoir aucun mouvement latéral non autorisé, même à l'intérieur d'un micropérimètre donné.

De plus, si les employés à distance utilisent des protocoles comme ZigBee ou une autre technologie de réseau maillé pour l'IdO, vous vous apercevrez qu'ils fonctionnent en violation du Zero Trust. Ils ont besoin de communications peer-to-peer pour fonctionner et leur modèle de confiance repose entièrement sur des clés ou des mots de passe, sans modèle dynamique pour l'authentification des modifications.

Compte tenu de tout cela, il convient de prendre en compte les éléments suivants :

1. Créer une enclave de ressources pour toute l'installation n'est pas faisable. Les enclaves de ressources doivent être bien définies et aussi petites que possible. Elles nécessitent des communications peer-to-peer pour fonctionner et le modèle de confiance repose strictement sur des clés ou des mots de passe, sans modèle dynamique pour l'authentification à des fins d'accès via une passerelle. Elles peuvent être gérées en utilisant un gestionnaire de mots de passe privilégiés mais pas dans une architecture Zero Trust.

Par conséquent, si vous décidez d'adopter le Zero Trust et Privileged Password Management, il vous faudra renforcer la protection de vos ressources pour rendre possible un modèle d'enclave et refuser toute communication réseau inappropriée avec quoi que ce soit au sein de cette enclave définie.

Même s'il existera des exceptions pour les communications au sein de l'enclave elle-même, dans le concept, le périmètre se limitera à l'ensemble de ressources. Une gestion des accès privilégiés au moyen d'une passerelle devrait être le moyen d'autoriser tout accès externe.

2. Si vous décidez d'adopter le Zero Trust et Privileged Password Management, il vous faudra renforcer la protection de votre modèle de sécurité des endpoints pour refuser toute communication réseau inappropriée sur le même sous-réseau que la source ou la destination. Bien qu'il puisse y avoir des exceptions pour les périphériques tels que les imprimantes locales, dans le concept le périmètre s'arrête au périphérique lui-même, il est défini par des applications et des privilèges.L'accès à distance ne contrôle que la connexion point à point.

3. Vérifiez si votre environnement Unix et Linux utilise des technologies similaires, dispose de technologies peer-to-peer ou de réseau maillé activées, même pour la gestion de la politique ou du réseau. Celles-ci présentent une énorme pierre d'achoppement pour adopter tout système d'accès à distance de confiance.Le mouvement latéral sera toujours intrinsèquement présent sous une forme ou une autre.

Faites équipe avec BeyondTrust pour votre mission Zero Trust

Des organisations des secteurs public et privé du monde entier s'associent à BeyondTrust pour mettre en place des principes et des architectures de sécurité Zero Trust.

Ressources supplémentaires

ÉTUDE DE CAS Le cheminement d'Investec vers le Zero Trust : de la théorie à la pratique

ÉTUDE DE CAS Comment Oxford Properties Group a mis en place une architecture Zero Trust avec BeyondTrust

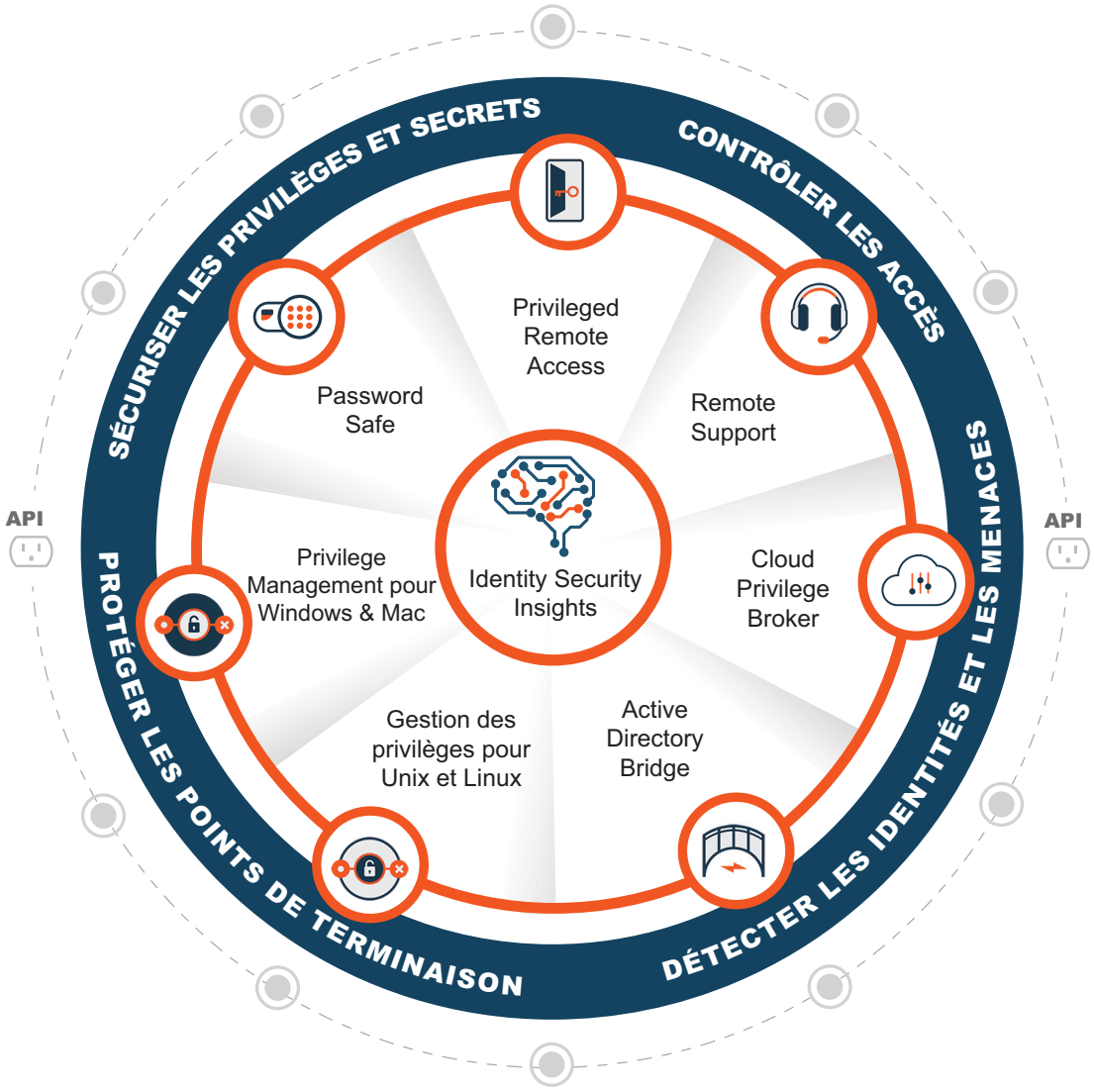
LIVRE BLANC Correspondance entre les fonctionnalités de BeyondTrust et les principes de Zero Trust du NIST (SP 800-207)

Cet article explore en détail les 7 principes du Zero Trust et montre comment BeyondTrust peut vous aider à les appliquer. Le document associe également de façon détaillée chaque usage du PAM de BeyondTrust aux principes du Zero Trust.

Si vous souhaitez discuter de votre projet Zero Trust avec BeyondTrust, n'hésitez pas à nous contacter.

À propos de BeyondTrust

La plateforme BeyondTrust



À PROPOS DE BEYONDTRUST

BeyondTrust est le leader mondial de la sécurité intelligente de l'identité et de l'accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique afin de renforcer et de sécuriser l'environnement de travail hybride. Nos produits intégrés et notre plate-forme offrent la solution de gestion des accès privilégiés (PAM) la plus avancée du secteur, permettant aux organisations de réduire rapidement leur surface d'attaque dans les environnements traditionnels, cloud et hybrides. Nos produits intégrés et notre plate-forme offrent la solution de gestion des accès privilégiés (PAM) la plus avancée du secteur, permettant aux organisations de réduire rapidement leur surface d'attaque dans les environnements traditionnels, cloud et hybrides.

Avec un héritage d'innovation et un engagement ferme envers les clients, les solutions BeyondTrust sont simples à déployer, à gérer et à adapter à l'évolution des entreprises. 20 000 clients, dont 75 des 100 premières entreprises du classement Fortune et un réseau mondial de partenaires nous font confiance.

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