BeyondTrust

Tout ce que vous devez savoir sur le PAM Just-In-Time

Pourquoi et comment l'implémenter

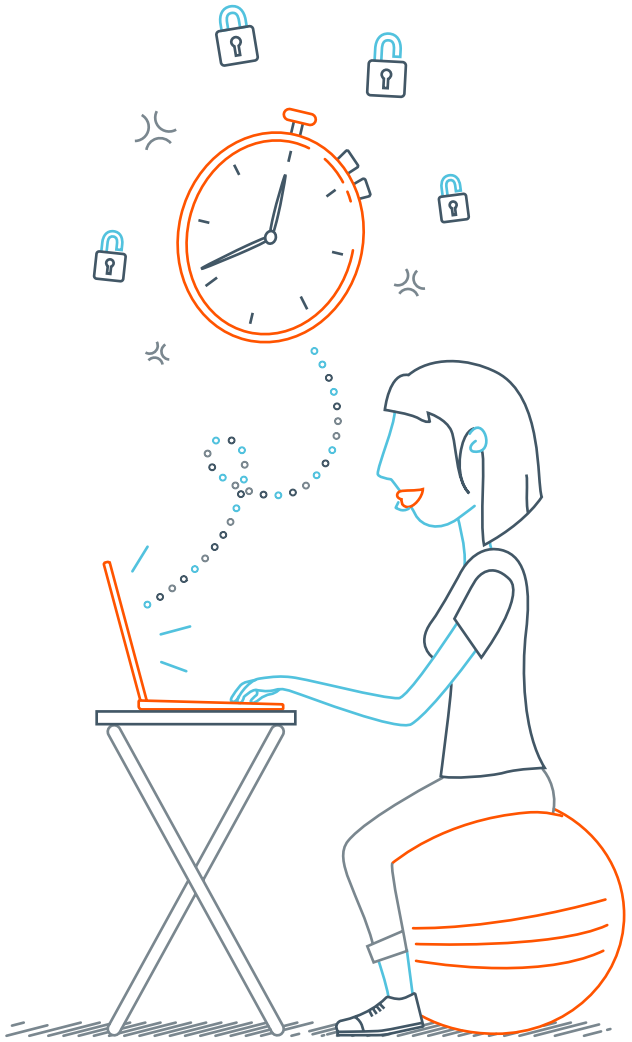
SOMMAIRE

INTRODUCTION

La durée : une composante critique de la gestion des accès

Un véritable modèle de sécurité intégrant le concept du « moindre privilège » exige que les utilisateurs, les processus, les applications et les systèmes disposent des droits et des accès nécessaires pour effectuer certaines tâches définies, et ce, pour une durée définie. Les entreprises sont de plus en plus efficaces pour appliquer l'aspect « niveau d'accès juste suffisant » à l'aide de solutions de gestion des accès privilégiés (PAM), mais elles ont largement négligé la partie « accès pendant un temps défini » et donc le risque inhérent pour les comptes d'utilisateurs privilégiés. Au cours des 40 dernières années, les comptes privilégiés « toujours actifs » (ou « always on ») ont été le mode adopté par défaut pour les accès admin et se sont multipliés dans toutes les entreprises, ce qui présente une surface de risque considérable. Un accès, des droits et des autorisations privilégiés, toujours en mode actif, sont prêts à être exercés à tout moment, pour des activités légitimes mais aussi malveillantes. Et cette surface de risque augmente rapidement avec l'expansion des environnements virtuels, cloud et DevOps, des périphériques Internet des objets (IoT), ainsi que dans des domaines émergents tels que l'automatisation de processus robotique (RPA).

Dans ce contexte, il n'est pas surprenant que l'abus et / ou la mauvaise utilisation de privilèges jouent un rôle décisif dans presque toutes les brèches de cybersécurité aujourd'hui. Avec un accès privilégié en main, un attaquant devient un insider malveillant, un scénario alarmant pour tout professionnel de l'informatique, et ce, jusqu'à la direction et au conseil d'administration. Les comptes privilégiés sont désormais vraiment partout dans votre organisation, mais les technologies de sécurité traditionnelles basées sur un périmètre donné ne peuvent protéger que les comptes privilégiés qu'au sein de ces limites. La gestion des accès privilégiés « juste à temps » (ou Just-In-Time) peut aider à réduire considérablement la surface de la menace portant sur les privilèges et à réduire les risques au sein de l'entreprise. La mise en œuvre du PAM Just-In-Time signifie que les identités ne disposent des privilèges appropriés que lorsque cela est nécessaire et pour le moins de temps possible. Ce processus peut être entièrement automatisé pour qu'il soit sans contrainte pour l'utilisateur final.



Les entreprises sont de plus en plus efficaces pour appliquer l'aspect « niveau d'accès juste suffisant » à l'aide de solutions de gestion des accès privilégiés (PAM), mais elles ont largement négligé la partie « accès pendant un temps défini » et donc le risque inhérent pour les comptes d'utilisateurs privilégiés.

Présentation du PAM JIT (Just-In-Time)

Qu'est-ce-que le PAM JIT (Just-In-Time) ?

La gestion des accès privilégiés (PAM) Just-In-Time (JIT) est une stratégie qui aligne les demandes en temps réel d'utilisation de comptes privilégiés directement avec les droits d'accès, les flux de travail et les stratégies d'accès appropriées. Les entreprises utilisent cette stratégie pour protéger les comptes privilégiés des failles causées par des accès permanents en appliquant des restrictions temporelles basées sur des paramètres comportementaux et contextuels.

Un compte privilégié est défini comme un compte auquel des privilèges et des autorisations sont accordés par rapport à un utilisateur standard. Il comprend les éléments suivants :

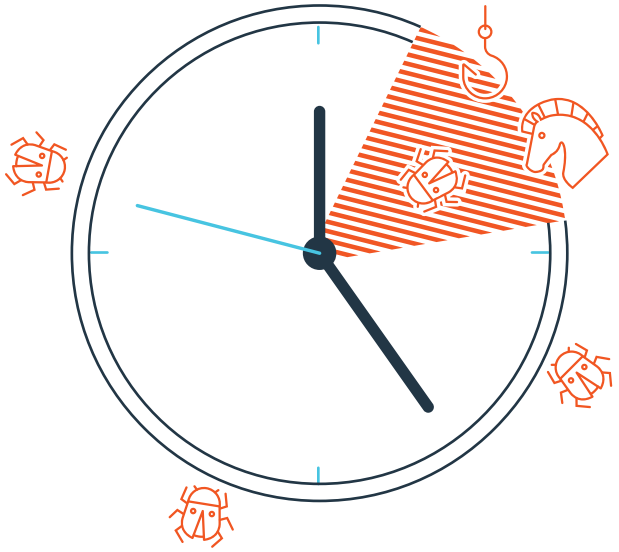
- Compte superutilisateur avec un niveau très élevé de privilèges, tels qu'administrateur (environnements Windows) ou root (environnements Unix / Linux).
- Utilisateurs privilégiés disposant de privilèges se situant entre ceux d'un compte superutilisateur et un compte utilisateur standard (également appelé compte utilisateur non privilégié ou compte avec moindre privilège).

Le PAM JIT limite fortement la durée pendant laquelle un compte possède des privilèges et des droits d'accès élevés, ce qui réduit considérablement la fenêtre de vulnérabilité pendant laquelle un acteur malveillant peut exploiter les privilèges de ce compte. Le Just-in-Time aide à appliquer le principe du moindre privilège afin de garantir que les activités privilégiées puissent être exécutées conformément aux politiques d'utilisation en place, tout en interdisant les activités privilégiées qui ne relèvent pas du bon contexte.

Lorsqu'un privilège est demandé, il doit respecter les paramètres contextuels requis avant d'être accordé. Ce privilège n'est jamais la propriété du compte. Cela atténue le risque d'utilisation abusive lorsqu'ils sont potentiellement utilisés en dehors d'un déploiement de gestion des accès privilégiés. Les comptes privilégiés ne sont plus une munition prête à être utilisée abusivement.

Considérons par exemple un compte privilégié toujours actif qui peut être « privilégié » 168 heures par semaine. En passant à une approche PAM JIT, vous pouvez réduire cet état actif de privilège de 168 heures à seulement une douzaine de minutes. Multiplier cet effet sur tous les comptes d'utilisateur privilégiés de votre organisation aura un impact véritablement considérable sur la réduction des risques.

Adopter la méthode « juste à temps » dans le cadre de votre approche de gestion des privilèges signifie que vous pouvez mettre en œuvre un véritable modèle de moindre privilège à l'échelle de l'entreprise. Et l'exposition n'est pas uniquement basée sur le temps. Les vecteurs d'attaque qui utilisent des techniques telles que le mouvement latéral sont également atténués car il n'y a pas de compte privilégié « always on » à exploiter parmi les ressources.



Les entreprises utilisent cette stratégie pour protéger les comptes privilégiés des failles causées par des accès permanents en appliquant des restrictions temporelles basées sur des paramètres comportementaux et contextuels.

AUTOMATISER LE PAM JIT (Just-In-Time)

Méthodes JIT

Une approche JIT de l'administration des privilèges oblige les organisations à établir des critères pour ces accès privilégiés Just-In-Time et à accepter que les comptes qui sont intégrés à cette politique ne soient pas disponibles en dehors du scénario bris de glace. Bien que des concepts similaires bien rodés de Just-In-Time existent dans d'autres cas d'utilisation, tels que dans le secteur industriel, appliquer ce modèle pour une solution de sécurité implique certaines considérations techniques uniques à prendre en compte au cours de son implémentation.

L'objectif d'un compte privilégié JIT est d'attribuer automatiquement les privilèges nécessaires « à la volée » en fonction d'une tâche ou d'une mission approuvée et ensuite de les retirer une fois la tâche terminée ou lorsque le créneau autorisé a expiré.

Le fait de prendre un compte utilisateur standard et d'appliquer les privilèges appropriés peut être mis en œuvre en utilisant l'une des six méthodes suivantes de JIT :

1 PRIVILÈGES JIT

Le compte dispose de privilèges, d'autorisations ou de droits supplémentaires pour effectuer une mission une fois que tous les critères sont remplis, mais uniquement pour une durée limitée. Ces droits doivent être révoqués une fois la mission terminée et il doit être certifié qu'aucun autre privilège n'a été modifié de manière inappropriée.

2 CRÉATION & SUPPRESSION DE COMPTES JIT

La création et la suppression d'un compte privilégié approprié pour répondre aux objectifs de la mission. Le compte doit pouvoir être lié à l'identité du demandeur ou du service effectuant l'opération pour le reporting et le forensics.

3 IMPERSONATION (OU EMPRUNT D'UNE IDENTITÉ) JIT

Le compte est lié à un ou plusieurs compte(s) admin préexistant(s). Lors de l'exécution d'une application ou d'une tâche spécifique, la fonction est élevée au moyen de ces identifiants. Ceci se fait souvent par automatisation ou par un script Windows "RunAs" ou *Nix SuDo. L'utilisateur ne se rend généralement pas compte qu'il utilise un compte « emprunté » pour ce type d'opérations et le processus chevauche parfois la délégation de comptes privilégiés « toujours actifs » (ou « always on »).

4 TOKÉNISATION JIT

Le token privilégié de l'application ou de la ressource est modifié avant d'être injecté dans le système d'exploitation. Cette forme de moindre privilège s'utilise sur les terminaux pour élever les privilèges et la priorité d'une application, sans élever les privilèges de l'utilisateur final.

5 APPARTENANCE À UN GROUPE JIT

L'ajout et le retrait automatiques d'un compte d'un groupe admin privilégié pour la durée de la mission. Le compte ne doit être ajouté à un groupe élevé que lorsque les critères appropriés sont réunis. L'adhésion au groupe doit être révoquée immédiatement dès la fin de la mission.

6 COMPTES ADMIN DÉSACTIVÉS JIT

Les comptes admin désactivés sont présents dans un système avec toutes les permissions, les privilèges et les droits associés à une fonction. Ils sont activés pour une mission spécifique puis désactivés une fois que les critères opérationnels sont satisfaits. Ce concept est comparable à celui des comptes admin toujours actifs, à l'exception du fait que fonctionnalité d'activation native sert à contrôler l'accès JIT.

AUTOMATISER LE PAM JUST-IN-TIME (JIT)

Déclencheurs JIT

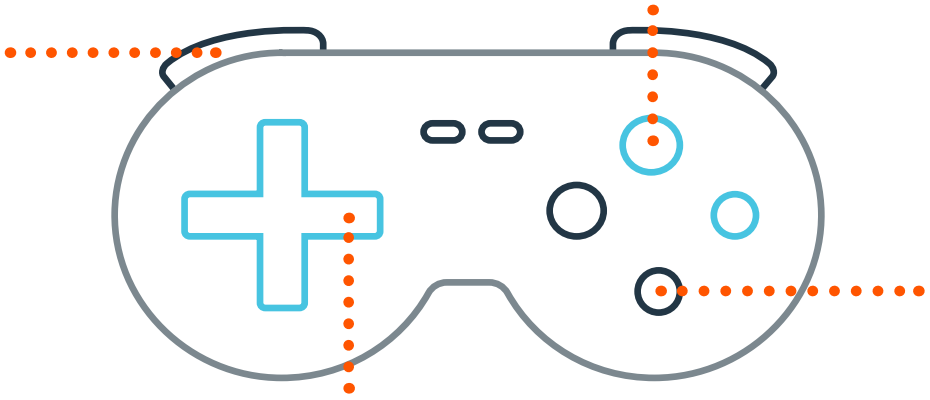
Pour que ces méthodes d'élévation des comptes privilégiés fonctionnent selon les principes de la gestion des accès privilégiés « juste à temps », les critères suivants doivent être considérés comme des déclencheurs. Ils doivent aussi tenir compte de variables comme l'heure et la date pour les fenêtres de contrôle des changements, ainsi que de critères de suspension ou de résiliation si des indicateurs de compromission sont détectés.

AUTHENTIFICATION BIFACTORIELLE (2FA) OU MULTIFACTORIELLE (MFA)

La méthode 2FA ou MFA est couramment employée pour autoriser l'accès privilégié aux comptes à privilèges toujours actifs ou JIT. Sans faire de distinction entre les deux techniques d'accès, cette méthode permet d'atténuer davantage les risques en validant que l'identité a bien un accès légitime à un compte privilégié. Ces méthodes d'authentification peuvent, toutefois, être utilisées comme déclencheur JIT pour un compte via l'une des techniques précitées.

WORKFLOW

Le concept de workflow d'approbation est généralement associé aux centres d'appels, services d'assistance et autres solutions ITSM (Information Technology Service Management). Une demande d'accès est faite et suivant un workflow d'approbation défini, l'accès est autorisé ou refusé. Quand le workflow aboutit à une approbation, il est possible d'activer un compte JIT. Celui-ci correspond généralement à l'utilisateur, l'asset, l'application, l'heure / date et à un ticket attribué dans une solution de contrôle du changement ou d'assistance technique. La surveillance des sessions privilégiées est généralement permise par les solutions PAM dans ce scénario pour vérifier que l'ensemble des actions était légitime.



ACCÈS CONTEXTUEL

L'accès contextuel se base sur des critères comme l'adresse IP source, la géolocalisation, l'appartenance à un groupe, le système d'exploitation hôte, les applications installées ou en mémoire, les vulnérabilités connues etc. Suivant la combinaison de ces critères, l'accès au compte JIT est accordé ou refusé pour satisfaire les besoins métier et atténuer les risques.

DROITS

Quand la gestion des accès privilégiés est intégrée à des solutions Identity Access Management (gestion des identités et des accès), il est possible de synchroniser les droits d'accès privilégié avec ces solutions. Ainsi, l'accès JIT peut être accordé via des solutions PAM directement, ou de façon programmée via les droits IAM. Généralement un workflow de droits IAM suppose un processus de synchronisation plus long et pas toujours en temps réel, mais il fournit un moyen de certifier les comptes selon les privilèges. Ce peut être vain si l'on relie les solutions IAM et PAM pour contrôler les accès.

Ces déclencheurs d'automatisation JIT conditionnent le fait qu'un compte puisse devenir un compte à privilège.

Règles JIT

Les deux questions à se poser sont *« quelles règles régissent l'utilisation d'un compte JIT pour un accès privilégié légitime »* et *« quelles sont les conditions à remplir pour sa révocation ? »*

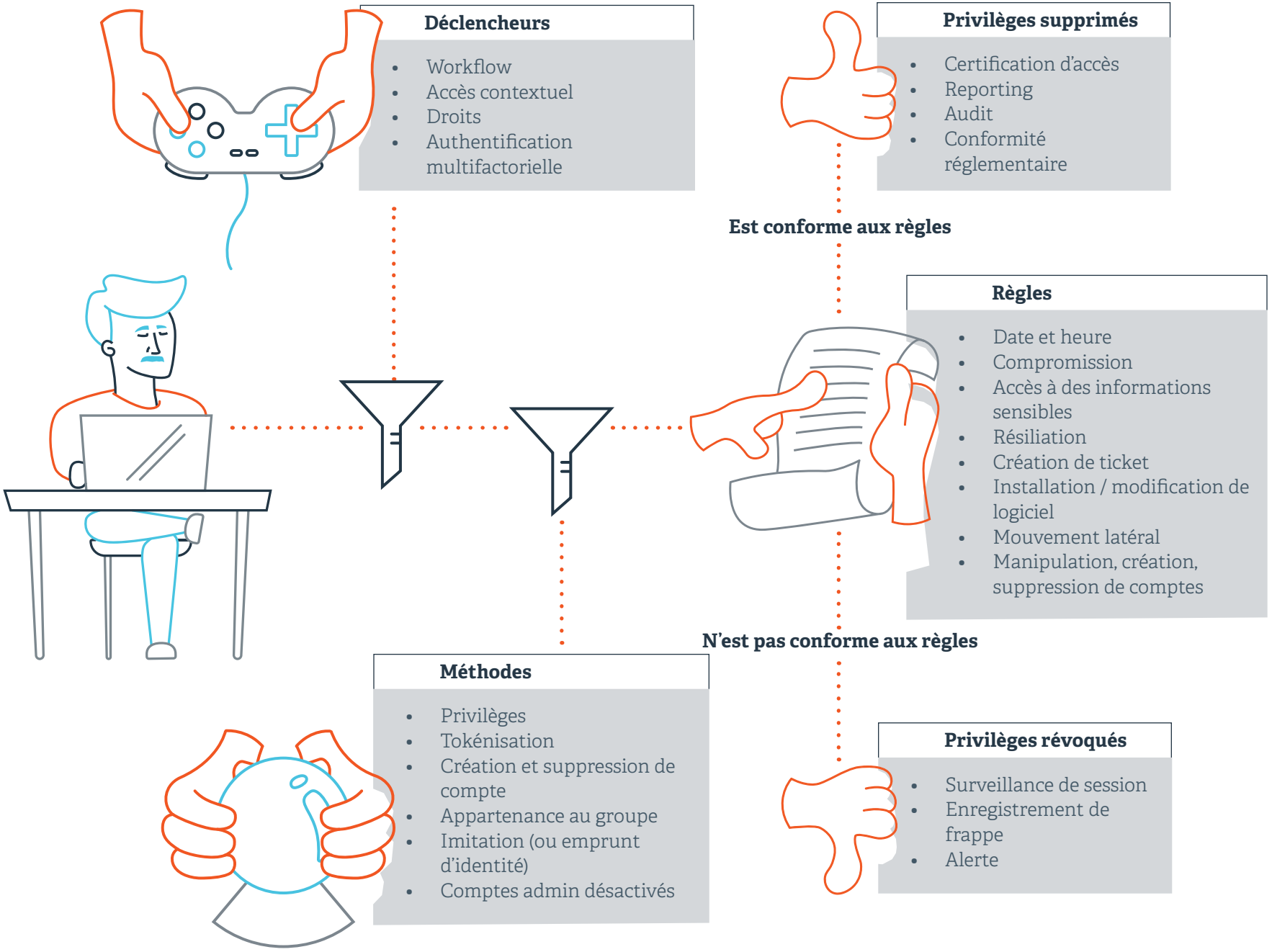
Voici quelques-unes des règles applicables :

1. **Fenêtres temporelles (date et heure) pour le contrôle de l'accès et des changements**
2. **Commandes ou applications pouvant être des indicateurs de compromission**
3. **Détection d'accès à des informations sensibles**
4. **Arrêt de la session principale**
5. **Existence de correspondances dans la solution de ticketing**
6. **Modification inappropriée de ressources, y compris installation de logiciels ou modification de fichiers**
7. **Tentatives de mouvements latéraux inappropriés**
8. **Manipulation, création ou suppression de comptes utilisateur ou de fichiers**

Cette liste n'est certes pas exhaustive mais ces éléments permettent de filtrer les critères de création ou de résiliation d'un compte JIT sur la base des déclencheurs correspondants.

AUTOMATISER LE PAM JUST-IN-TIME (JIT)

Le PAM JIT en action



Comment les solutions BeyondTrust facilitent la gestion des accès privilégiés Just-In-Time

La plateforme BeyondTrust Privileged Access Management peut vous permettre d'adopter le modèle de sécurité PAM JIT, mais aussi de renforcer la sécurité en appliquant d'autres aspects critiques de votre stratégie IAM / PAM comme la découverte et la gestion des comptes privilégiés, le moindre privilège, la gestion des identifiants, la séparation des privilèges et des tâches, l'audit des privilèges et l'analyse des menaces privilégiées.

BeyondTrust supporte le modèle « juste à temps » par la gestion centralisée des identifiants et des sessions à privilèges, l'élévation / la délégation de privilèges entre terminaux (PC, serveurs, etc.) et l'accès à distance (salariés, tiers, etc.) couplés à de nombreux déclencheurs. La plateforme BeyondTrust PAM comprend différentes solutions intégrées.

BeyondTrust supporte le modèle Just-In-Time en permettant la gestion centralisée des identifiants et des sessions à privilèges, l'élévation / la délégation de privilèges entre terminaux et l'accès à distance en tenant compte des différents déclencheurs.

Solutions BeyondTrust	Fonctions et caractéristiques supportant le PAM JIT					
Privileged Password & Session Management	**Découverte et enrôlement automatiques et continus des comptes**	**Gestion sécurisée des clés SSH**	**Gestion des mots de passe entre applications**	**Gestion des sessions privilégiées**	**Contrôle d'accès adaptatif**	**Analyse des menaces privilégiées**
Découvrez, gérez, auditez et surveillez tous les types de comptes privilégiés	Notre moteur de découverte réseau analyse, identifie et établit le profil de tous les actifs. La catégorisation dynamique permet l'enrôlement automatique dans des Smart Groups pour permettre une gestion plus efficace et des accès JIT dès que de nouveaux comptes sont détectés.	Renouvelez automatiquement les clés SSH selon un calendrier défini et appliquez des workflows avec contrôle d'accès granulaire. Il est possible d'utiliser des clés privées pour connecter en toute sécurité des utilisateurs à des systèmes Unix ou Linux via le proxy sans que la clé ne soit visible par l'utilisateur et avec enregistrement de la session à privilèges.	Eliminez les identifiants codés dans les applications via une interface API adaptable avec un nombre illimité de caches de mots de passe assurant l'évolutivité et la redondance. Ceci permet l'accès JIT aux derniers mots de passe pour n'importe quelle application.	La gestion des sessions en direct permet un véritable double contrôle et permet aux administrateurs d'enregistrer, de verrouiller et de documenter des comportements suspects sans interrompre les sessions ni ralentir la productivité, selon les activités JIT.	Evaluez le contexte « juste à temps » et facilitez les demandes d'accès en tenant compte du jour, de la date, de l'heure et de l'emplacement auxquels un utilisateur accèdera à des ressources pour déterminer sa capacité à avoir accès aux dits systèmes.	Evaluez les caractéristiques des actifs et les comportements des utilisateurs d'un jour sur l'autre et soyez informé de la portée et de la rapidité des changements détectés pour détecter des comportements suspicieux.
Endpoint Privilege Management	**Principe du moindre privilège**	**Contrôle applicatif sans contrainte pour l'utilisateur**	**Audit et reporting complets**	**Analyse des menaces privilégiées**	**Intégration avec l'écosystème de sécurité**	
Instaurez le principe du moindre privilège et supprimez les privilèges utilisateur excessifs sur les systèmes Windows, Mac, Unix, Linux et en réseau.	Elevez les privilèges d'accès aux applications pour les utilisateurs standard sur tout système d'exploitation via des contrôles granulaires basés sur des règles spécifiques, en n'octroyant que l'accès suffisant pour effectuer une tâche.	Etablissez une liste blanche, noire et grise des applications, avec un moteur de règles flexible pour instaurer des règles plus larges. Choisissez l'approbation automatique pour les utilisateurs avancés, protégés par des enregistrements complets, ou utilisez des codes « challenge-response » pour le contrôle des applications « juste à temps ».	Accélérez les investigations et simplifiez la conformité grâce à un enregistrement complet de l'activité de tous les utilisateurs.	Corrélez le comportement des utilisateurs aux données de vulnérabilités des assets et aux renseignements fournies par les meilleures solutions de sécurité tierces pour produire une image globale du risque pour l'utilisateur.	Des connecteurs intégrés aux solutions tierces, y compris aux applications helpdesk, aux scanners de gestion des vulnérabilités, aux outils SIEM etc. permettent une rentabilisation rapide des logiciels de sécurité mis en place.	

Solutions BeyondTrust		Fonctions et caractéristiques supportant le PAM JIT					
Secure Remote Access	**Accès à distance des tiers et fournisseurs**	**Contrôle des accès privilégiés**	**Surveillance des sessions**	**Réduction de la surface d'attaque**	**Intégration avec la gestion des mots de passe**	**Consoles mobiles & web**	**Audit & conformité**
Sécurisez, gérez et auditez les accès à distance privilégiés des tiers et salariés et les accès utilisés pour la prise en main à distance		Instaurez le principe du moindre privilège pour donner le bon niveau d'accès à chacun pour chaque session distante.	Contrôlez et surveillez les sessions au moyen des protocoles standard pour connexions RDP, VNC, Web et SSH.	Réduisez la surface d'attaque en consolidant le suivi, l'approbation et l'audit des comptes privilégiés « juste à temps », en un même endroit et en créant un seul chemin d'accès.	Injectez les identifiants dans les serveurs et systèmes en un clic, « juste à temps », de sorte que les utilisateurs ne voient jamais les identifiants en clair.	Utilisez des applis mobiles ou consoles web, partout, à tout moment pour réaliser vos tâches d'accès à distance.	Créez des pistes d'audit, effectuez des recherches dans les sessions et produisez des rapports en capturant les données détaillées des sessions en temps réel ou post-session et fournissez des rapports de conformité.
	Equipe technique et support	**Support par chat**	**Nombreuses plateformes supportées**	**Autorisations et rôles granulaires**	**Collaboration**	**Enregistrement des sessions et traçabilité**	**Support sur Chrome, Firefox, IE, etc.**
		Dépannez vos clients en direct depuis votre site web via Click-to-Chat, avec la possibilité d'« escalader » en temps réel, de partager l'écran et de contrôler à distance sans jamais perdre le contact avec l'utilisateur.	Dépannez les appareils Windows, Mac, Linux, iOS et Android quelque soit votre plateforme, ainsi que les terminaux utilisant RDP, Telnet, SSH et VNC.	Gérez de façon granulaire les équipes, utilisateurs, rôles et paramètres de permissions des sessions pour instaurer une posture de sécurité basée sur le moindre privilège.	Réduisez votre temps de résolution des incidents et définissez des stratégies d'« escalade » vers des ressources plus compétentes si nécesaire, tout en améliorant la satisfaction clients par la sélection de certains membres de l'équipe « juste à temps ».	Suivez les performances de l'équipe et enregistrez l'activité des sessions pour avoir toute la traçabilité nécessaire afin d'optimiser la sécurité, la conformité et la formation.	Notre console Web Rep Console HTML5 vous permet de proposer une prise en main à distance just-in-time à partir de n'importe quel navigateur, sans téléchargement.

Correspondance entre les méthodes et les déclencheurs JIT

La grille ci-dessous permet d'établir des correspondances entre les méthodes PAM JIT et les déclencheurs pour chaque solution BeyondTrust.

	Privileged Password & Session Management	Endpoint Privileged Management	Secure Remote Access
Déclencheurs			
Droits	●		●
Workflow	●	●	●
Accès contextuel	●	●	●
Multifactoriel	●	●	●
Méthodes			
Création et suppression de comptes	●		
Appartenance à un groupe	●		
Imitation ou emprunt d'identité	●	●	●
Comptes admin désactivés		●	
Tokénisation		●	

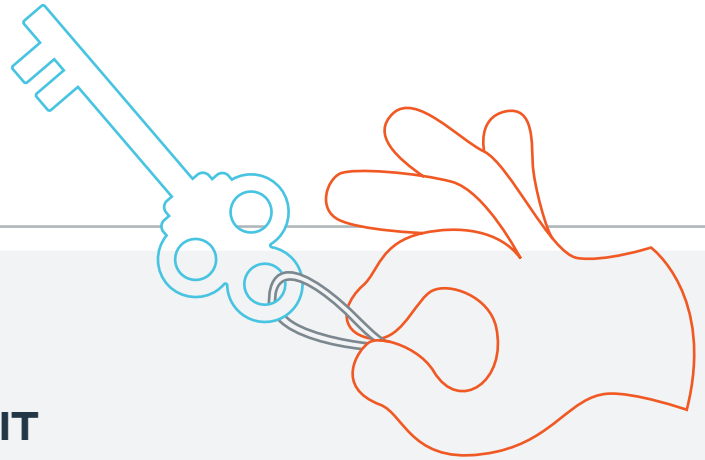
Un formidable bond en avant pour la gestion des risques IT

De nombreuses entreprises considèrent que la prochaine grande étape pour protéger leurs assets IT critiques passera par la mise en oeuvre d'une stratégie JIT parallèlement à un modèle d'accès « juste ce qu'il faut ».

La gestion des privilèges JIT devrait s'inscrire dans toute stratégie de moindre privilège. Au lieu d'activer des comptes de façon permanente une fois l'authentification faite, nous vous proposons d'exercer plus de contrôle sur les conditions d'utilisation en amenant le modèle de sécurité à refuser toute activité privilégiée jusqu'à ce que tous les critères soient remplis. Ceci induit une restriction de l'accès au compte, mais aussi des privilèges, autorisations et droits d'un compte en temps réel.

En permettant la gestion des accès privilégiés « juste à temps », avec des déclencheurs contextuels et en veillant au respect des règles en temps réel de l'utilisateur de compte privilégié, le PAM JIT apporte une réponse concrète au problème des comptes toujours actifs dans les entreprises. Plus que l'évolution naturelle de la gestion des accès privilégiés, c'est un formidable bond en avant pour la gestion des risques IT.

BeyondTrust Privileged Access Management permet de gérer les risques liés aux accès privilégiés toujours actifs présents et répartis dans des environnements IT de plus en plus hétérogènes et complexes tout en maintenant la sécurité et la productivité des utilisateurs.



Avantages du PAM JIT

1. **Le provisioning / déprovisioning de privilèges centralisé, automatisé, contextuel et limité dans le temps réduit considérablement la fenêtre de vulnérabilité pendant laquelle les privilèges pourraient être exploités**
2. **Le principe du moindre privilège induit une diminution des utilisateurs et des sessions privilégiés, ce qui renforce la sécurité mais facilite aussi les audits et la mise en conformité**
3. **L'expérience est sans incidence pour les utilisateurs, ce qui permet d'assurer une productivité optimale sans pertuber les workflows**
4. **Les comptes privilégiés toujours actifs et les vecteurs d'attaque qui les accompagnent sont éliminés**

Concepts et terminologie

Bris de glace : dans le domaine informatique, la procédure break-glass (bris de glace) consiste à révéler le mot de passe d'un compte système pour contourner les contrôles d'accès habituels en situation d'urgence quand d'autres méthodes d'accès échouent ou s'avèrent inaccessibles. La procédure break-glass confère à l'utilisateur un accès immédiat mais généralement limité dans le temps à un compte pour lequel il n'a normalement pas d'autorisation.

Gestion des accès privilégiés « juste à temps » ou PAM JIT : l'objectif de la gestion des privilèges « juste à temps » est d'assigner les privilèges nécessaires « à la volée » pour une tâche ou une mission approuvée, puis de les retirer une fois la tâche réalisée ou une fois que la fenêtre ou le contexte d'accès autorisé a expiré. La gestion des privilèges JIT permet aux entreprises de protéger les comptes privilégiés des accès toujours actifs (« always-on ») par l'application de restrictions sur la base de paramètres comportementaux et contextuels.

Moindre privilège : le principe de moindre privilège désigne le concept et la pratique de restriction des droits d'accès des utilisateurs, comptes et processus informatiques aux seules ressources absolument nécessaires pour effectuer les activités de routine autorisées. Un modèle de sécurité fondé sur le moindre privilège impose le niveau minimal de droits ou d'habilitation utilisateur lui permettant d'effectuer ses taches. Le moindre privilège s'applique également aux processus, applications, systèmes et terminaux (comme l'IoT), afin que chacun ait le juste niveau d'autorisation pour réaliser une activité autorisée.

Privilège : un privilège autorise à passer outre ou à contourner certaines restrictions de sécurité, et peut inclure des autorisations d'exécution de certaines actions, comme de mettre des systèmes à l'arrêt, de charger des pilotes, de configurer des réseaux ou systèmes, et de provisionner et configurer des comptes et des instances cloud.

Gestion des accès privilégiés ou PAM (Privileged Access Management) : parfois également appelée gestion des comptes privilégiés, gestion des identités privilégiées (Privileged Identity Management) ou encore gestion des privilèges, le PAM fait référence aux solutions et stratégies permettant de gérer et de sécuriser les comptes privilégiés et de contrôler la délégation et l'« escalade » de privilèges d'utilisateurs, d'applications, de services, de processus, de tâches etc. Les solutions PAM permettent aux entreprises de supprimer les droits admin d'utilisateurs (sur serveurs et PC) pour élever les privilèges associés à des applications ou tâches autorisées.

Compte privilégié : un compte privilégié désigne tout compte donnant un accès et des privilèges supérieurs à ceux des comptes non privilégiés (ex. comptes standard et comptes d'utilisateurs invités). Un utilisateur privilégié désigne tout utilisateur d'un accès privilégié, via un compte privilégié par exemple. Du fait de leurs droits d'accès et autorisations supérieurs, les utilisateurs et comptes privilégiés posent des risques autrement plus importants que les comptes et utilisateurs non privilégiés.

Session privilégiée : une session privilégiée est une session informatique qui implique l'exécution d'activités nécessitant des privilèges généralement supérieurs à ceux d'un utilisateur standard. Une session privilégiée est initiée par un utilisateur, un système, une application ou un service.

Gestion des sessions privilégiées ou PSM (Privileged Session Management) : la gestion des sessions privilégiées revêt la surveillance et la gestion de toutes les sessions d'utilisateurs, de systèmes, d'applications et de services induisant un accès et des autorisations supérieurs. Le PSM permet un degré supérieur de supervision et de contrôle pour mieux protéger l'environnement des menaces de l'intérieur ou d'attaques extérieures potentielles, tout en préservant les informations légales liées aux obligations réglementaires et de conformité.

Comptes utilisateur standard : les comptes utilisateur standard, également appelés comptes LUA (Least-privileged User Accounts) ou comptes non privilégiés, disposent d'un ensemble limité de privilèges. Dans un environnement où le principe du moindre privilège est appliqué, c'est le type de compte que la plupart des utilisateurs devraient utiliser dans 90 à 100% du temps. Un utilisateur standard est un utilisateur non privilégié au sein d'environnements informatiques (Windows, Mac, Linux, Unix etc.) avec des droits d'accès basiques. Ce type de compte / utilisateur a un accès limité aux ressources et paramètres, contrairement à un compte privilégié ou de superutilisateur (de type root ou admin), qui peut avoir des droits admin et d'accès privilégié bien plus importants.

Comptes superutilisateur : les comptes superutilisateur sont des comptes à privilèges très élevés généralement réservés aux employés spécialisés de l'équipe IT. Ils offrent un pouvoir sans limite ou presque pour exécuter des commandes et apporter des modifications système. Les comptes superutilisateur sont appelés « root » sous Unix / Linux et « administrateur » sous Windows. Les privilèges des comptes superutilisateur peuvent offrir un accès illimité aux fichiers, annuaires et ressources avec des privilèges maximum de lecture, d'écriture et d'exécution. Les comptes superutilisateur permettent également des changements systémiques sur un réseau, comme la création ou l'installation de fichiers ou logiciels, la modification de fichiers et de paramètres et la suppression d'utilisateurs et de données. Les superutilisateurs peuvent également accorder des droits d'accès et des autorisations à d'autres utilisateurs et les supprimer.

A propos de BeyondTrust

BeyondTrust est le leader mondial du Privileged Access Management, offrant l'approche la plus complète du marché afin de réduire les risques de failles liées à l'exploitation des privilèges. Flexible, notre plateforme permet aux organisations de sécuriser les privilèges sur les endpoints, serveurs, réseaux et environnements cloud, DevOps etc. de façon évolutive pour faire face aux menaces en constante mutation et évolution. Nos clients bénéficient ainsi de la visibilité et du contrôle dont ils ont besoin pour réduire les risques, respecter les règlementations et rendre leurs équipes plus productives. Plus de 20 000 clients dans le monde nous font confiance.

beyondtrust.com/fr

V2019_07_ENG