BeyondTrust

Stoppez les hackers dans leur élan avec les solutions de gestion des comptes et des sessions à privilèges de BeyondTrust

Conformez-vous à la directive NIS2 *avec* Privileged Access Management

TABLE DES MATIÈRES

Introduction

La directive relative à la sécurité des réseaux et de l'information (NIS), adoptée en 2016, a été la première législation européenne en matière de cybersécurité. Elle avait pour but d'établir un niveau de sécurité plus élevé et plus uniforme pour les réseaux et les systèmes d'information dans l'ensemble de l'Union européenne.

La directive a été actualisée face à l'accélération considérable de la transformation digitale et à l'évolution des vecteurs de menaces. La directive NIS2 a été officiellement adoptée en novembre 2022 et est entrée en vigueur en janvier 2023.

Elle a alors abrogé et remplacé l'ancienne version de la directive. Elle représente un pas en avant constructif dans la définition des exigences applicables aux entreprises de l'UE, pour renforcer leur cyber-résilience au cours des prochaines années. La directive NIS2 énonce également des règles claires concernant la production de rapports et les conséquences de leur non-respect.

Elle vise aussi à renforcer davantage la coopération au sein de l'UE. Il s'agit notamment de mettre en place le réseau européen des organisations de liaison en cas de crise informatique, ou « EU-CyCLONe », pour soutenir la gestion coordonnée des incidents de cybersécurité à grande échelle au niveau de l'UE.

Quels sont les changements apportés par NIS2 ?

Les principaux changements apportés par la directive NIS2 sont les suivants :

- Une plus grande variété de secteurs de l'industrie.
- Une plus grande rigueur dans la réponse aux incidents et la production de rapports sur la gestion des crises.
- Des exigences et des contrôles de sécurité renforcés.
- La sécurité de la chaîne d'approvisionnement, c'est-à-dire non seulement les entreprises elles-mêmes, mais aussi leurs prestataires et sous-traitants.
- L'intégration des meilleures pratiques de base en hygiène informatique et une formation à la cybersécurité.

De nombreuses entreprises devront réorganiser leur budgétisation afin de répondre aux exigences de cette directive dans les meilleurs délais. Le non-respect des nouvelles mesures introduites peut entraîner des pénalités pouvant atteindre 2 % du chiffre d'affaires mondial de l'entreprise concernée.

Il se peut que vous ne vous sentiez pas concerné(e) puisque votre entreprise n'est pas située dans l'UE. Sachez pourtant que la directive NIS2 s'applique à toute entreprise proposant ses services dans l'UE, indépendamment de son siège social. En outre, la directive NIS visait initialement les systèmes soutenant les infrastructures critiques nationales. La directive NIS2 a considérablement élargi l'éventail des secteurs de l'industrie qu'elle régit.

Même si aucun de ces aspects ne s'applique à votre entreprise, la directive et de nombreux autres régimes de conformité réglementaire fournissent des références utiles en ce qui concerne les meilleures pratiques pour aider toute organisation à mieux sécuriser son environnement.

Poursuivez votre lecture pour savoir comment BeyondTrust peut vous aider à aborder ce qui suit. Principales sections de la directive NIS2 :

- Gestion de la sécurité cloud (articles 33, 34 et 35)
- Gestion des comptes et des sessions à privilèges (article 44)
- Élévation des privilèges et gestion de la délégation (articles 44 et 49)
- Protection contre le ransomware (article 54)
- Sécurité du secteur des services publics (article 53)
- Sécurité de la chaîne d'approvisionnement (article 85)
- Gestion des identités (article 89)
- Rapports obligatoires sur les incidents (article 102)

Gestion de la sécurité cloud
(Directive NIS2, articles 33, 34 et 35)

Les plateformes de cloud computing telles qu'Amazon AWS, Microsoft Azure et Google Cloud Platform accordent une grande importance à la sécurisation de l'infrastructure cloud publique. Les clients sont cependant tout aussi responsables d'assurer la sécurité des applications s'exécutant dans leur infrastructure cloud.

Pour ces scénarios, les solutions **Privileged Access Management de BeyondTrust** implémentent les meilleures pratiques en matière de sécurité du cloud d'entreprise. Parmi les principales fonctionnalités de BeyondTrust dans ce domaine, nous trouvons :

- **Détection et intégration :** Répertoriez les actifs en continu dans les environnements cloud, physiques et virtuels, et intégrez-les pour les gérer.
- **Application du principe du moindre privilège :** Les privilèges « Just-in-Time » permettent d'obtenir le bon niveau d'accès sans surexposer les identifiants du système.
- **Sécurisation des accès et des « bastions hosts » :** La superposition, la surveillance et l'accès à distance sécurisé renforcent la sécurité du cloud.

Gestion des comptes et des sessions à privilèges (article 44)

L'accès reposant sur des privilèges est une nécessité. Nous devons toutefois nous assurer que l'accès aux comptes à privilèges, aux identifiants et aux secrets soit minutieusement contrôlé en mettant en place la gestion des comptes et des sessions à privilèges (PASM). Les solutions dans ce domaine, comme **Password Safe** de BeyondTrust, fournissent des mécanismes de gestion des comptes à privilèges parmi l'ensemble des systèmes d'exploitation, des applications, de l'infrastructure réseau et des appliances (y compris l'IoT).

Cela inclut :

- **Gestion des mots de passe :** Restreindre l'accès au mot de passe, à la clé ou au secret. L'application de règles de workflow pour l'archivage/extraction ainsi que de critères rigoureux pour les mots de passe.

- **Surveillance et gestion de session :** Fournir un accès géré aux systèmes sans révéler le mot de passe, enregistrer les sessions (y compris les frappes au clavier, les mouvements de la souris et les clics sur les boutons) et fournir une lecture à des fins d'audit et d'investigation.

Les hackers cibleront les comptes à privilèges bien connus dans un système pour pouvoir se déplacer latéralement dans votre environnement. Une solution de gestion des comptes et des sessions à privilèges peut stopper efficacement les pirates dans leur élan, limitant ainsi l'impact de toute activité malveillante.

Élévation des privilèges et gestion de la délégation (articles 44 et 49)

L'excès d'utilisateurs sur-privilégiés est une situation de risque courante au sein de nombreuses entreprises. Dans l'idéal, les utilisateurs devraient uniquement disposer du niveau de privilèges requis pour l'exercice de leurs fonctions. C'est ce que l'on appelle communément le principe du moindre privilège, mais la plupart des systèmes d'exploitation n'offrent pas de capacités granulaires permettant de l'appliquer. Cela signifie, par exemple, qu'un utilisateur qui doit installer Adobe Acrobat se voit attribuer tous les privilèges d'administrateur local sur son poste de travail sans qu'il y ait de délai précis pour les révoquer.

En utilisant des solutions de gestion de la délégation et de l'élévation de privilèges, telles que **Privilege Management pour Windows et Mac et Privilege Management pour Unix et Linux** de BeyondTrust, il est possible d'attribuer à l'utilisateur les privilèges spécifiques dont il a besoin, par exemple la possibilité d'installer ou d'exécuter une application spécifique dans un état privilégié, sans exposer le système à tous les risques que pose un compte à privilèges.

Ce type de capacité de contrôle fondé sur le principe du moindre privilège permet non seulement aux utilisateurs d'avoir plus d'autorisations sur leur système tout en réduisant le niveau de risque réel, mais supprime également le besoin de surveiller ce pour quoi ils utilisent des comptes à privilèges, limitant ainsi la quantité de « bruit » détectée dans le système.

En outre, la fonctionnalité d'accepter les demandes d'autorisation des utilisateurs améliore souvent la relation avec l'équipe en charge de la cybersécurité, incitant les premiers à davantage s'impliquer dans la sécurisation de l'environnement. C'est un aspect essentiel du point de vue de la sécurité.

Protection contre les ransomwares (article 54)

Les initiatives de transformation digitale, allant des déploiements et de l'utilisation étendus du cloud à l'augmentation de l'accès à distance, ont considérablement augmenté la surface d'attaque. Les pirates utilisant la technique du ransomware ont su profiter de cette faiblesse, réussissant des attaques spectaculaires qui ont perturbé des infrastructures essentielles pour des millions de personnes.

Alors que les attaques de ransomware passées (par exemple, WannaCry) avaient tendance à être non ciblées, les attaques modernes au moyen de vers qui se propagent de façon opportuniste (par exemple, Ryuk ou Trickbot) sont généralement le résultat d'actions humaines et très ciblées.

Les pirates utilisant le ransomware analysent généralement les ports pour détecter ceux qui sont ouverts et non sécurisés afin d'initier leur attaque. **Les endpoints RDP (Remote Desktop Protocol) exposés à Internet continuent d'être désignés dans les rapports sur les menaces comme étant le point d'entrée de prédilection pour le ransomware. Les pirates les utilisent pour pénétrer le système dans 50 à 80 % des attaques réussies.** Dans le même temps, d'autres technologies d'accès à distance, comme des VPN, sont également utilisées pour des cas d'usages allant bien au-delà de ce qui est sécurisé et sont souvent mal implémentées. D'autres tactiques courantes de propagation du ransomware passent par l'ingénierie sociale, par exemple des e-mails de phishing contenant des pièces jointes infectées ou des liens malveillants.

Quelle que soit la façon de les transmettre, presque tous les ransomwares nécessitent des privilèges pour s'exécuter (installer des fichiers ou des pilotes, accéder à des clés de registre, etc.), se déplacer latéralement et se propager. Les attaques par ransomware intègrent de plus en plus des techniques complexes de malware sans fichier afin de masquer la pénétration à mesure qu'elle progresse parmi les systèmes et le réseau de l'entreprise. BeyondTrust fournit une protection puissante combinant plusieurs techniques qui permet de démanteler ou d'atténuer plusieurs étapes de la chaîne d'attaque des ransomwares.

Comment les solutions BeyondTrust brisent les chaînes d'attaque à base de ransomware

- Verrouille les chemins d'accès à distance et bloque l'utilisation risquée des protocoles RDP, VNC et SSH, ainsi que des VPN.
- Évite l'exécution de ransomware en appliquant le principe du moindre privilège et en utilisant des contrôles applicatifs.
- Empêche tout code malveillant de transmettre des charges utiles de ransomware.
- Met en place une segmentation et une micro-segmentation pour isoler les actifs, les ressources et les utilisateurs et pour empêcher tout mouvement latéral sur le réseau.
- Offre une protection contre les attaques exploitant les applications et les macros de confiance.
- Stoppe une infection dans son élan pour éviter tout mouvement latéral.
- Prévient le piratage de compte en gérant tous les identifiants à privilèges.
- Applique le principe du moindre privilège, sécurise les accès à distance et offre des fonctions d'audit/gestion de session au service desk.

Sécurité du secteur des services publics (article 53)

Dans nos sociétés modernes, les services publics se caractérisent par l'importance de leurs infrastructures essentielles. Les cyberattaquants, y compris ceux agissant pour des gouvernements étrangers, peuvent infliger des dommages catastrophiques en perturbant ou en compromettant les services publics. Leurs intentions peuvent être purement politiques ou pécuniaires, en exigeant par exemple une rançon dans le cadre d'une attaque par ransomware. Dans l'ensemble, les citoyens sont très peu tolérants face à l'interruption de services publics. Certaines attaques avérées ont même visé à empoisonner les circuits d'approvisionnement en eau ou à saboter des installations nucléaires.

Les technologies opérationnelles (OT) et les systèmes de contrôle industriel (ICS), tels que ceux que l'on trouve dans les infrastructures des fournisseurs de services publics, sont de plus en plus connectés à Internet et facilement détectables, pouvant compromettre la sécurité de l'ensemble d'une infrastructure critique. Les environnements de ces infrastructures dépendent également fortement des matériels et systèmes IT existants. Certains n'ont peut-être jamais été conçus pour communiquer avec un réseau.

Privileged Remote Access de BeyondTrust contribue aussi à sécuriser les environnements OT des services publics et d'autres secteurs, tout en appliquant les principes du Zero Trust. Privileged Remote Access :

- Applique le principe du moindre privilège pour les sessions d'accès à distances.
- Traite les périphériques gérés avec le même niveau de confiance que pour ceux qui ne le sont pas, à savoir une confiance nulle.
- Fournit un accès aux applications indépendant de l'accès au réseau.
- Enregistre toutes les activités effectuées à l'aide de l'accès à distance et désactive les fonctionnalités telles que copier/coller.
- Active la sécurité par API pour protéger l'intégrité des données envoyées depuis les périphériques de l'IoT vers les systèmes de back-end.
- Active la segmentation et la micro-segmentation afin d'isoler les ressources et d'atténuer ou de contenir davantage les attaques.

Sécurité de la chaîne d'approvisionnement (article 85)

Au cours des dernières années, les attaques des chaînes d'approvisionnement, qui compromettent les logiciels ou le matériel autorisés pour infiltrer d'autres victimes, ont fait la une des journaux du monde entier. Des attaques ayant eu un impact mondial (par exemple, le piratage de SolarWinds, Kaseya) ont rapidement affecté des milliers d'entreprises, y compris de nombreuses agences gouvernementales.

En s'attaquant à un maillon faible (un employé à distance, un sous-traitant, un système mal protégé, un utilisateur sur-privilégié, une identité machine non supervisée, des ports non sécurisés ou des vulnérabilités dans un VPN), un pirate peut rapidement s'infiltrer dans une entreprise et compromettre un logiciel utilisé par des milliers de clients.

Les solutions **Privileged Access Management de BeyondTrust** offrent des fonctionnalités fondamentales pour renforcer la sécurité et contrer les attaques de la chaîne d'approvisionnement de façon efficace.

Quelques méthodes clés qu'utilisent les solutions **PAM de BeyondTrust** pour améliorer la cybersécurité de la chaîne d'approvisionnement :

- Application du principe du moindre privilège et de l'accès Just-in-Time à tous les niveaux de l'entreprise, y compris pour les accès à distance.
- Sécurisation et gestion de chaque identifiant à privilèges (mots de passe de comptes à privilèges, clés SSH, secrets DevOps, mots de passe de machines/applications, etc.).
- Gestion et surveillance de chaque session à privilèges.
- Extension des meilleures pratiques PAM au service desk.
- Mise en évidence d' informations sur la sécurité des identités pour anticiper le renforcement des défenses et bloquer les attaques en cours.

Gestion des identités
(article 89)

Il est essentiel de contrôler qui a accès à vos systèmes et applications, quel que soit le niveau de cet accès. Quelques approches essentielles en ce qui concerne l'identité des utilisateurs :

IDENTITÉ UNIQUE DANS TOUT L'ENVIRONNEMENT

Les services directory, tels que Microsoft Active Directory (AD), vous permettent de disposer d'un mécanisme fiable et solide pour proposer une authentification de base aux utilisateurs, depuis un seul endroit.
Active Directory Bridge de BeyondTrust permet aux entreprises d'étendre les fonctions de contrôle et de gestion d'AD aux systèmes Unix et Linux, éliminant ainsi le besoin d'avoir des annuaires ou des comptes locaux supplémentaires. Moins les utilisateurs ont d'identifiants et de mots de passe, plus il est probable qu'ils emploient un mot de passe complexe qu'ils n'oublieront pas ou qu'ils n'auront pas à noter quelque part.

SOURCE D'AUTHENTIFICATION UNIQUE

Les solutions de gestion des identités et des accès (IAM) vont encore plus loin en fournissant un mécanisme qui attribue de manière fiable des rôles et des responsabilités aux utilisateurs. Les fonctionnalités d'attestation et d'audit garantissent que ce qui est attribué correspond à ce qui a été provisionné.

BeyondTrust s'intègre avec des sociétés telles que SailPoint, qui offrent des fonctionnalités sophistiquées de gouvernance des identités. Vous saurez donc quelles sont les personnes dotées d'un accès et à quoi elles peuvent accéder. Ces intégrations contribuent à fournir une vision globale des identités, privilégiées ou non.

AUTHENTIFICATION MULTIFACTEUR

L'authentification peut être divisée en trois éléments basiques : quelque chose que vous savez, quelque chose que vous avez et quelque chose que vous êtes. La plupart des systèmes et des applications reposent sur quelque chose que vous connaissez, c'est-à-dire votre mot de passe. Cette approche est rarement suffisante dans le monde actuel hyperconnecté, où les utilisateurs se servent régulièrement du même mot de passe dans plusieurs endroits (en effet, même leur mot de passe professionnel est réutilisé !).

Nous constatons de plus en plus l'adoption d'un deuxième facteur d'authentification, soit quelque chose que vous avez (par exemple, une application générant des tokens sécurisés ou procurant une vérification hors bande de la possession d'un périphérique), soit quelque chose que vous êtes (à savoir, une validation biométrique via votre iris, votre empreinte digitale ou la reconnaissance de votre visage). De nombreux fournisseurs proposent ces solutions. Il est recommandé d'utiliser au moins deux facteurs (et plus encore s'il s'agit d'un accès système à privilèges et/ou particulièrement sensible).

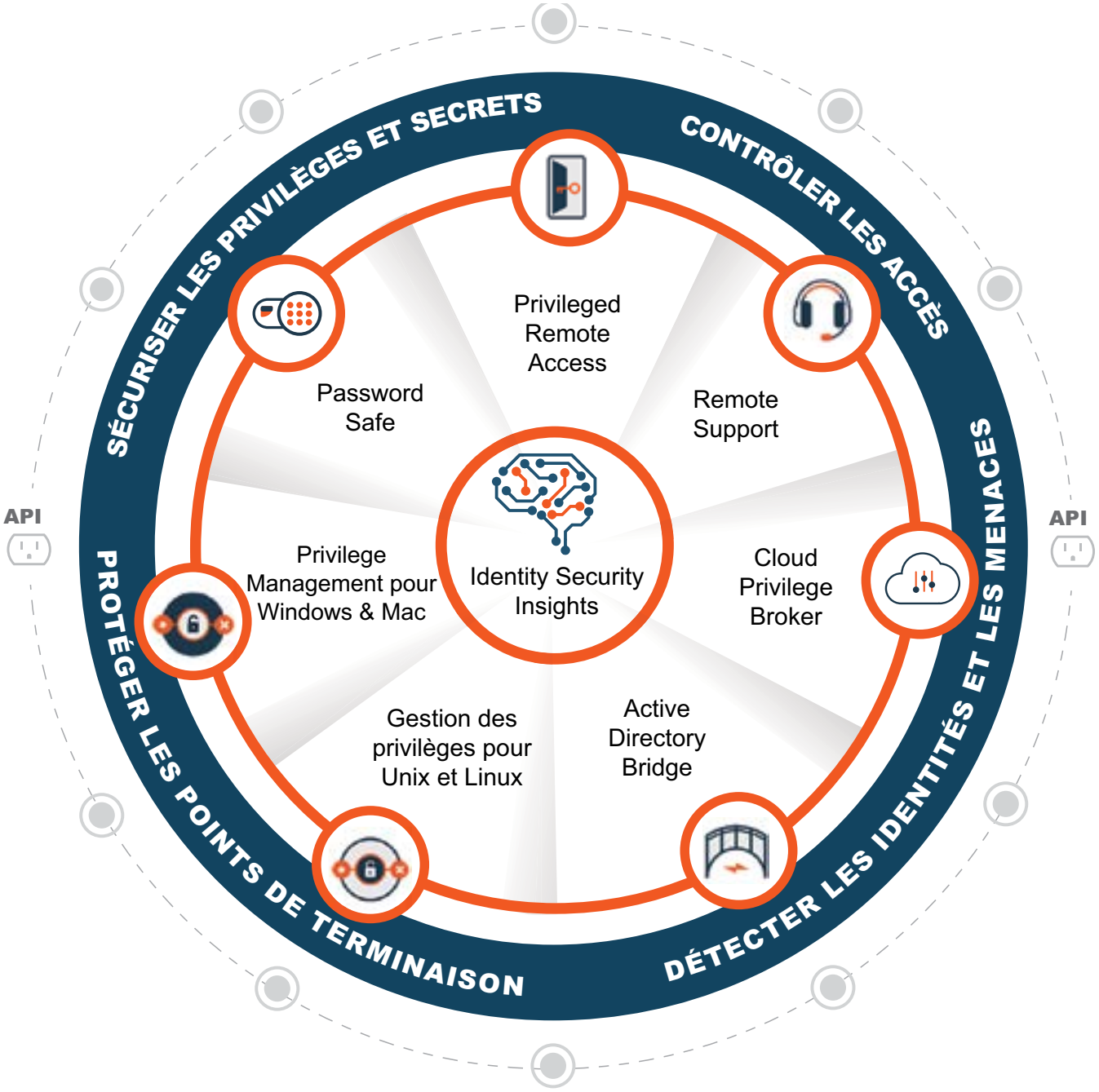
Rapports obligatoires sur les incidents (article 102)

La directive NIS2 énonce une exigence de reporting rapide et précis dans son article 102. Ces rapports sont essentiels pour évaluer l'impact d'un incident et coordonner une réponse de sorte que d'autres entités puissent se protéger.

Les produits BeyondTrust facilitent la visualisation, l'audit et le reporting des activités à privilèges et des menaces basées sur l'identité. Des produits tels que **Privileged Remote Access, Password Safe, et Remote Support** offrent de solides fonctionnalités d'audit des sessions à privilèges, tandis que nos solutions **Identity Security Insights** proposent un tableau de bord centralisé pour l'activité et les menaces basées sur l'identité.

À propos de BeyondTrust

La plateforme BeyondTrust



CLOUD | HYBRIDE | SUR SITE | OT

Password Safe: Gérez l'ensemble des mots de passe, des comptes, des identifiants, des secrets et des sessions privilégiés pour les personnes et les machines, en assurant le contrôle et la sécurité de manière globale.

Privileged Remote Access : Étendez les bonnes pratiques de gestion de sécurité des accès privilégiés au-delà du périmètre par un contrôle, une gestion et un audit granulaires de l'accès privilégié à distance.

Remote Support : Optimisez votre service support grâce à un accès sécurisé et une prise en charge pour n'importe quel appareil ou système, n'importe où dans le monde – y compris Windows, macOS, Linux, Android et iOS.

Privilege Management pour Windows/Mac : Supprimez les droits admins locaux, appliquez le principe du moindre privilège dynamiquement sur Windows et macOS, prévenez les attaques par malware et phishing, et contrôlez les applications.

Privilege Management pour Unix/Linux : Assurez la conformité, établissez le moindre privilège et le zero trust. Empêchez et minimisez les violations de sécurité – sans mettre à mal la productivité.

Active Directory Bridge : Gérez les identités et le contrôle des accès de façon rationalisée en étendant l'authentification Microsoft AD, les fonctionnalités d'authentification unique et la gestion de la configuration des stratégies de groupes aux systèmes Unix et Linux.

Identity Security Insights : Obtenez une vue centralisée des identités, des comptes et des accès privilégiés dans l'ensemble de votre parc informatique et tirez parti de recommandations concernant les menaces pour améliorer votre stratégie de sécurité des identités.

Résumé

La directive NIS2, comme de nombreuses réglementations en matière de conformité, met l'accent sur les processus et les contrôles des meilleures pratiques qui vous aident à fournir un environnement plus sûr, plus fiable et plus résilient. La plateforme Privileged Access Management de BeyondTrust est une solution intégrée qui permet de contrôler et de visualiser tous les comptes et utilisateurs à privilèges parmi toutes les plateformes de l'entreprise, **une exigence essentielle de la directive NIS2.**

Une cybersécurité solide repose avant tout sur des moyens de contrôle éprouvés. Il s'agit en particulier de contrôler l'accès à vos systèmes, de surveiller l'activité lorsque cet accès est utilisé et de fournir des données d'audit à des fins d'analyse une fois l'accès révoqué.

BeyondTrust vous permet de protéger vos identités, de bloquer les menaces et de fournir un accès dynamique pour créer et sécuriser le monde professionnel nomade actuel.

Une grande partie du travail de surveillance de nos environnements consiste à s'assurer que les utilisateurs n'abusent pas des privilèges qui leur ont été accordés. Dans ce modèle de sécurité basé sur le principe du moindre privilège, les utilisateurs reçoivent uniquement les privilèges dont ils ont absolument besoin et pour une durée strictement nécessaire. Cela se traduit par un besoin moindre de surveiller ces activités légitimes et par un nombre bien plus réduit d'événements critiques.

Pour en savoir plus sur la façon dont BeyondTrust peut vous aider à vous conformer à la directive NIS2 ou à atteindre d'autres objectifs en matière de sécurité ou de conformité, **contactez-nous dès aujourd'hui.**

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.

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**