Rapport 2023 sur les risques liés aux VPN

Cybersecurity INSIDERS

Synthèse

Historiquement, les réseaux privés virtuels (VPN) ont permis des accès à distance de base. La dissémination géographique croissante des collaborateurs et l'adoption des technologies cloud remettent en question la connectivité de base proposée par les VPN.Alors que les menaces évoluent rapidement, les VPN ne peuvent pas fournir l'accès sécurisé et segmenté que les entreprises appellent de leurs vœux. Au contraire, les VPN offrent souvent un accès complet au réseau de l'entreprise, ce qui accentue les risques de cyberattaques quand des acteurs malveillants disposent d'un accès par le biais d'identifiants de connexion. En outre, les VPN interconnectent plusieurs sites, offrent un accès à des tiers, prennent en charge des appareils non gérés et permettent aux dispositifs IoT de se connecter. Cependant, ces divers cas d'utilisation poussent les VPN au-delà de leurs objectifs initiaux, créant souvent des failles de sécurité dans un contexte de menaces de plus en plus complexes et versatiles.

Ce rapport, basé sur une enquête menée auprès de 382 professionnels de l'informatique et experts en cybersécurité, explore de nombreux défis en matière de sécurité et d'expérience utilisateur. Le rapport 2023 sur les risques du VPN pointe la complexité de la gestion actuelle des VPN, les problématiques d'expérience utilisateur, la vulnérabilité face aux diverses cyberattaques et le potentiel de ces attaques à nuire à la posture de sécurité générale des entreprises.Le rapport se penche également sur des modèles de sécurité plus robustes, avec le Zero Trust émergeant en tant que levier pertinent pour sécuriser et accélérer la transformation numérique.

LES TEMPS FORTS DE L'ENQUÊTE SONT LES SUIVANTS :

Vulnérabilités des VPN et impacts sur la cybersécurité : malgré leur rôle essentiel, les VPN génèrent des risques de sécurité, 88 % des entreprises se disant légèrement à extrêmement préoccupées par l'idée que les VPN puissent mettre en péril la sécurité de leur environnement. En outre, 45 % des entreprises confirment avoir subi au moins une attaque exploitant des vulnérabilités liées aux des VPN au cours des 12 derniers mois, tandis qu'une sur trois a été victime d'attaques par ransomware liées aux VPN. La menace croissante des hackers exploitant les vulnérabilités des VPN rend urgent le renforcement de la sécurité des architectures VPN actuelles.

Synthèse

Utilisation des VPN et expérience utilisateur : les VPN répondent à différentes utilisations, 84 % des personnes interrogées déclarant que l'accès à distance des collaborateurs constitue leur application principale. Toutefois, les utilisateurs font état d'une expérience moins qu'optimale : la majorité d'entre eux ne sont pas satisfaits de l'expérience que leur offre leur VPN (72 %), soulignant ainsi la nécessité de disposer de solutions d'accès à distance plus conviviales et plus fiables au sein des environnements digitaux.

Vecteurs d'attaque : une entreprise sur deux a été confrontée à des attaques liées au VPN au cours de l'année écoulée. Les vecteurs d'attaque liés au VPN doivent faire l'objet d'une attention particulière en raison du rôle critique qu'ils jouent dans l'opérationnel et les communications des entreprises. En outre, les utilisateurs tiers, tels que les sous-traitants et les fournisseurs, constituent des passerelles potentielles pour un accès malveillant aux réseaux, ce qui complique davantage la tâche des équipes de sécurité. Dans le cadre de l'enquête, 9 personnes interrogées sur 10 se disent préoccupées par le fait que des tiers puissent servir de passerelle pour accéder à leurs réseaux via un accès VPN.

Adopter le Zero Trust : la transition vers un modèle Zero Trust est une priorité pour une majorité d'entreprises. Environ 9 répondants sur 10 se disent intéressés par le Zero Trust, et plus d'un quart (27 %) ont déjà mis en œuvre le Zero Trust. 37 % des répondants prévoient de remplacer leur VPN par des solutions d'accès réseau Zero Trust (ZTNA).

Nous remercions Zscaler pour sa contribution à cette enquête sur les risques liés aux VPN. L'expertise de l'entreprise en matière de solutions Zero Trust et d'accès sécurisé a considérablement enrichi nos conclusions.

Nous sommes convaincus que les enseignements de ce rapport constitueront une ressource précieuse pour les professionnels de l'informatique et de la cybersécurité dans leur démarche vers une sécurité Zero Trust.

Cordialement,

Holger Schulze

Holger Schulze
CEO et fondateur
Cybersecurity Insiders

Cybersecurity
INSIDERS

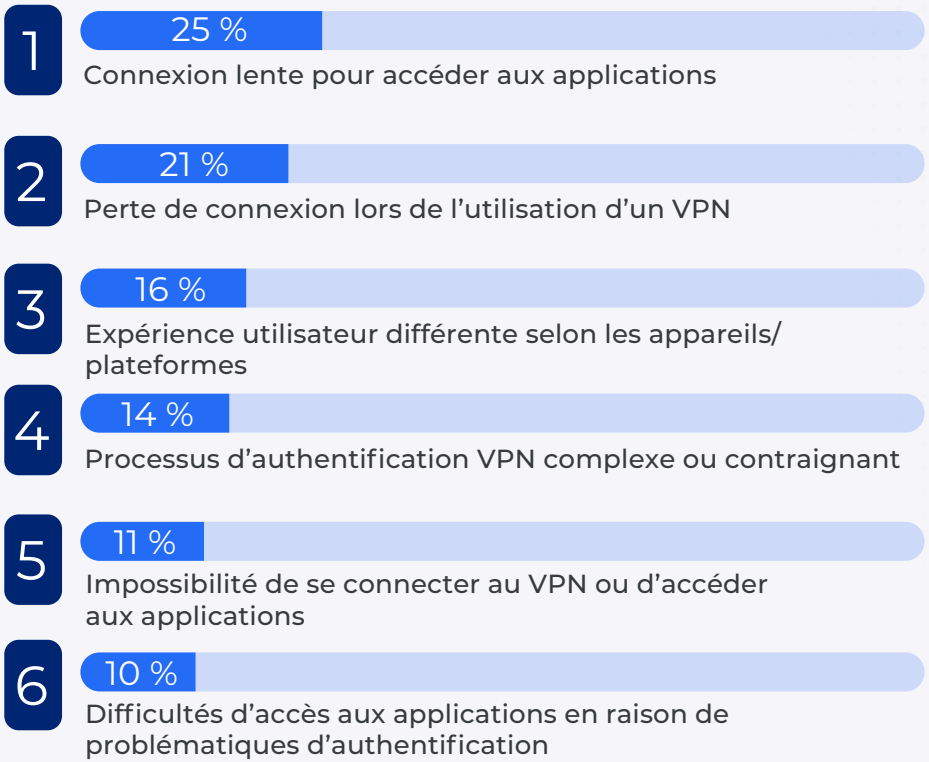
VPN : les utilisateurs sont à la peine

Parmi les problèmes liés au VPN, la lenteur des accès aux applications via le VPN est celui le plus courant, signalé par 25 % des personnes interrogées. Parmi les autres carences notables, citons les interruptions de connexion lors de l'utilisation du VPN (21 %) et une expérience utilisateur qui varie entre les différents appareils/plateformes (16 %).

Au vu de ces résultats, il est évident que l'amélioration de l'expérience utilisateur des accès à distance devrait constituer une priorité pour de nombreuses entreprises.Un accès fluide et fiable ne favorise pas seulement la productivité, mais peut également renforcer la sécurité en encourageant le respect des politiques de sécurité.

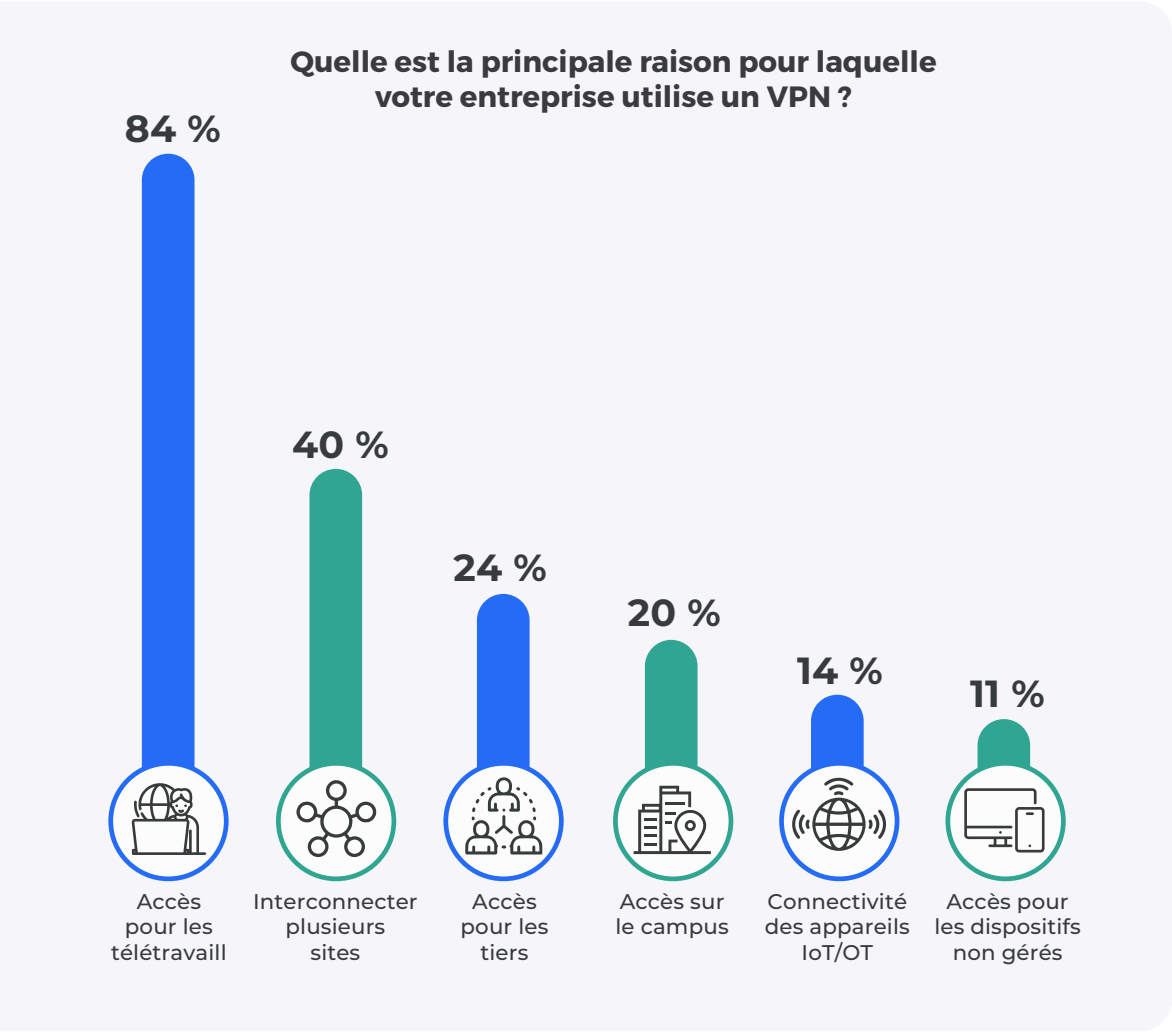
Les axes améliorations peuvent être divers : optimisation des performances du réseau, connexions moins lentes et plus stables, simplification du processus d'authentification VPN ou encore une même expérience utilisateur, quelle que soit la plateforme utilisée. Des mécanismes de support solides doivent également être mis en place pour aider les utilisateurs à résoudre les difficultés qu'ils peuvent rencontrer lorsqu'ils utilisent un VPN.

Quelle est la doléance la plus fréquente formulée par vos utilisateurs lorsqu'ils accèdent à des applications via un VPN ?



Autres 3 %

Principal cas d’utilisation du VPN : accès à distance pour les collaborateurs



Autres 3 %

Les VPN permettent depuis longtemps de connecter les collaborateurs distants au réseau de l’entreprise pour permettre différents cas d'utilisation tels que le télétravail et des connexions avec des tiers.

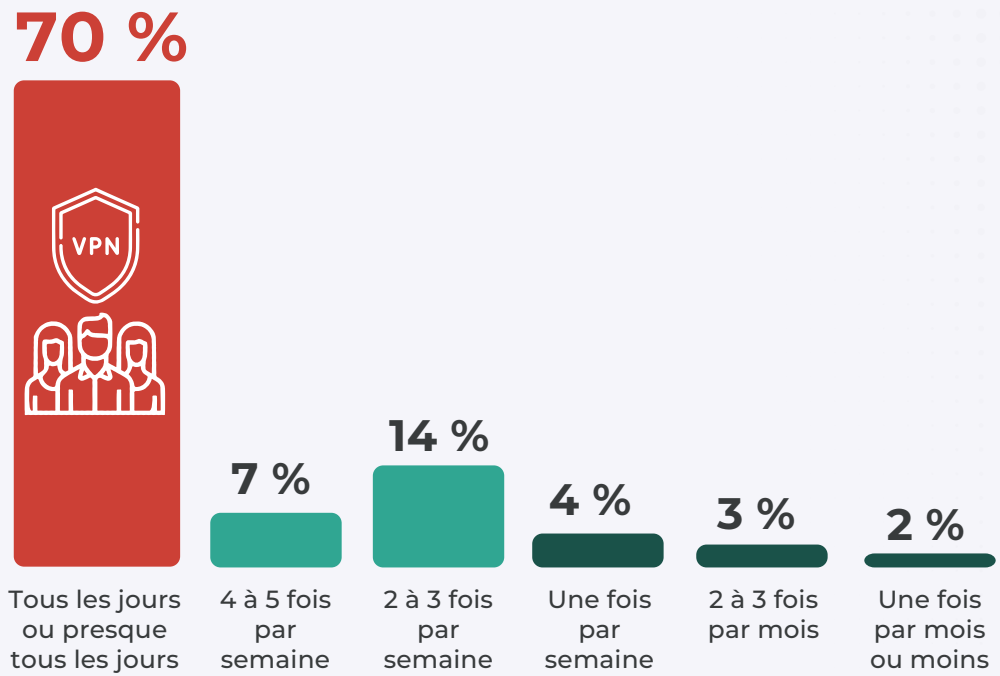
Dans la plupart des entreprises (84 %), l’objectif principal des VPN est d'offrir un accès aux collaborateurs distants. Cet objectif fait écho à la tendance du télétravail qui a considérablement évolué au cours des récentes années. Il est toutefois intéressant de noter que seuls 11 % des entreprises font appel au VPN pour piloter l’accès des appareils non gérés, ce qui met en évidence une vulnérabilité que les entreprises ne prennent peut-être pas entièrement en compte.

Une forte dépendance à l'égard du VPN

Un nombre important d'utilisateurs finaux (70 %) utilisent les VPN quotidiennement ou presque, ce qui témoigne d'une forte dépendance à l'égard des VPN dans les tâches quotidiennes. Si l'on ajoute les personnes qui utilisent les VPN 4 à 5 fois par semaine, 77 % des personnes interrogées utilisent pratiquement tous les jours un VPN dans le cadre de leur travail. Il est intéressant de noter qu'aucune des personnes interrogées n'a déclaré utiliser un VPN moins d'une fois par mois, ce qui confirme l'adoption généralisée de cette technologie.

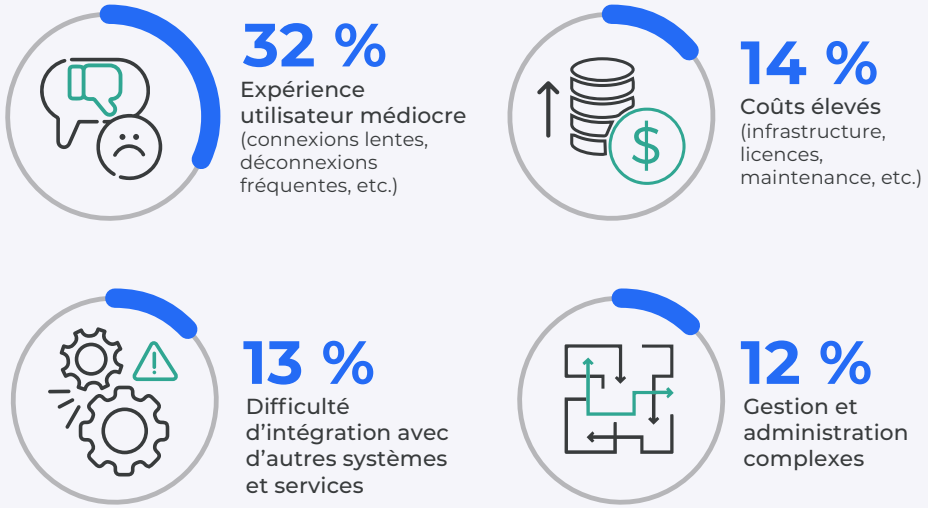
Compte tenu de cette utilisation fréquente, il est essentiel d'assurer une disponibilité constante et une sécurité solide des services d'accès à distance/VPN.

À quelle fréquence vos utilisateurs finaux utilisent-ils un VPN ?



Une expérience utilisateur aléatoire

Quel est le principal problème que rencontre votre entreprise avec son service VPN actuel ?



Évolutivité et flexibilité limitées 11 % | Carence de sécurité et conformité 7 % | Lacunes dans la prise en charge du télétravail et la collaboration 4 % | Autre 7 %

Les performances et l'expérience utilisateur des services VPN ont un impact considérable sur la productivité et l'efficacité opérationnelle globale des entreprises. Un VPN lent ou qui se déconnecte fréquemment peut considérablement perturber les activités de l'entreprise et frustrer les utilisateurs. Les résultats de l'enquête révèlent que le problème le plus important concernant les services VPN porte sur une expérience utilisateur médiocre, 32 % des personnes interrogées évoquant la lenteur des connexions et de fréquentes déconnexions.

Au vu de ces résultats, les entreprises devraient privilégier l'amélioration de l'expérience utilisateur de leurs services d'accès à distance, ce qui pourrait impliquer une augmentation de la capacité des serveurs ou de choisir des solutions d'accès sécurisées, réputées pour leur rapidité et leur stabilité. Il est intéressant de noter que les entreprises ont classé la sécurité comme un problème relativement peu important, malgré les multiples cyberattaques menées contre les VPN au cours des dernières années.

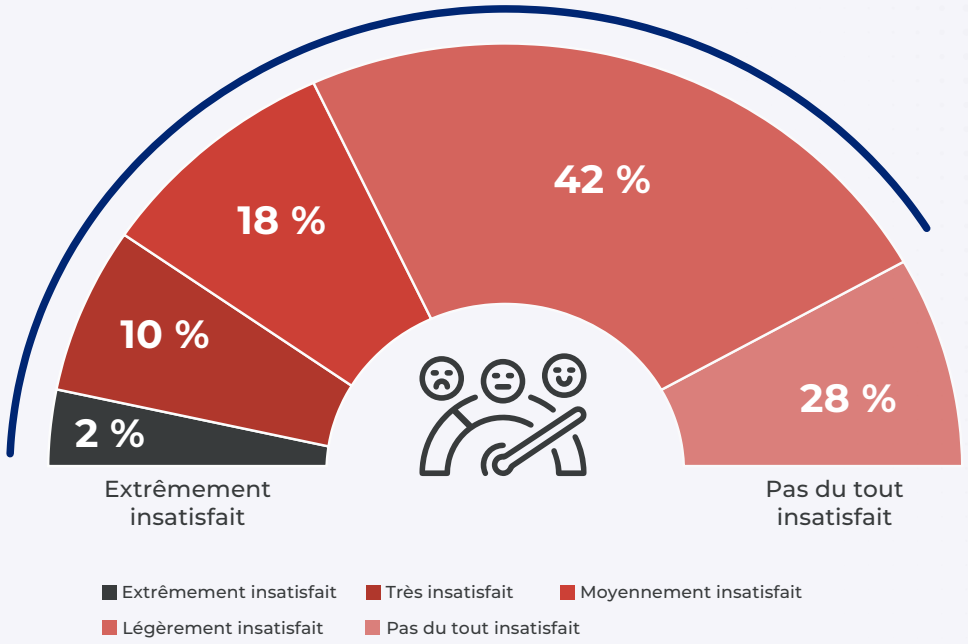
Mécontentement des utilisateurs à l'égard des VPN

Il est essentiel d'évaluer la satisfaction des utilisateurs à l'égard de leur expérience du VPN : tout mécontentement peut obérer la productivité, mais également entraîner un non-respect des politiques de sécurité, ce qui, à son tour, aboutirait à des vulnérabilités en matière de sécurité.

Une grande majorité d'utilisateurs (72 %) se disent insatisfaits de leur expérience du VPN, ce qui souligne la nécessité de disposer de solutions d'accès à distance plus conviviales et plus fiables au sein de l'espace de travail digital.

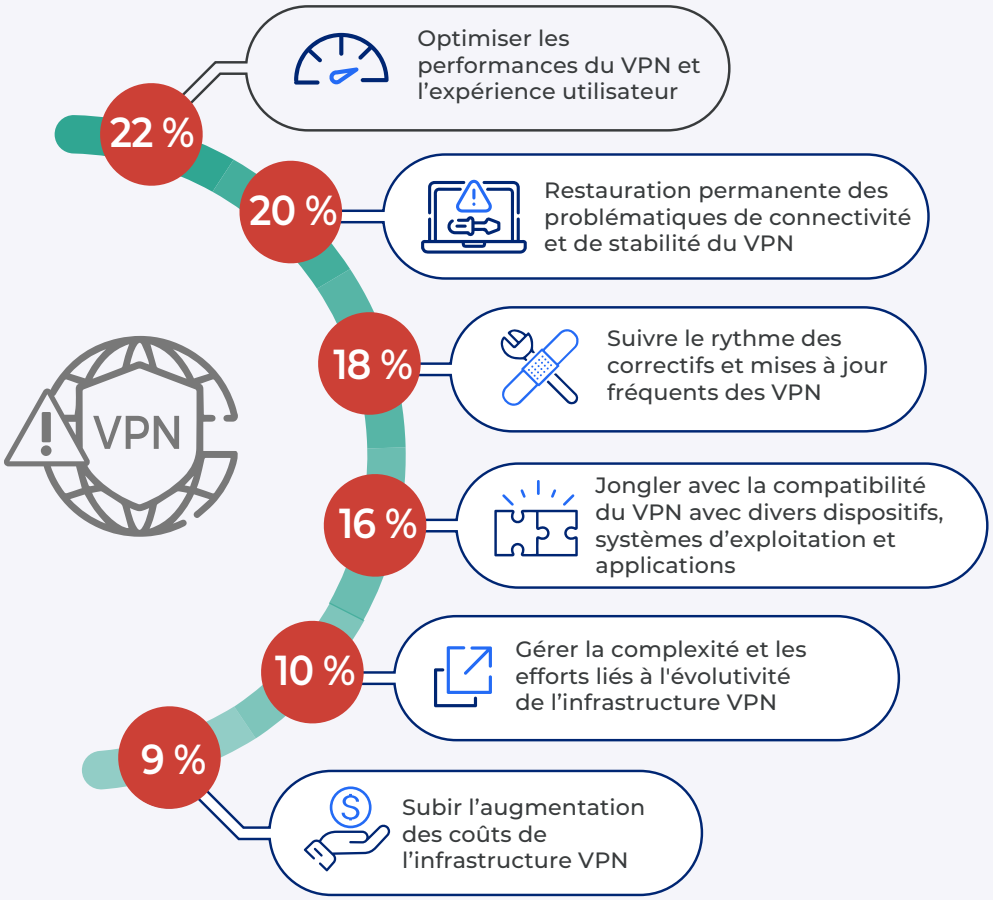
Dans quelle mesure vos utilisateurs sont-ils mécontents de leur expérience VPN ?

72 % des entreprises sont légèrement à extrêmement\ rinsatisfaites de leur expérience VPN



Défis liés à la gestion des VPN

Quel est le principal écueil dans la gestion de votre infrastructure VPN ?



Autres 5 %

L'enquête révèle que le plus grand défi dans la gestion de l'infrastructure VPN, comme l'indiquent 22 % des répondants, est d'assurer les performances du VPN et l'expérience utilisateur.

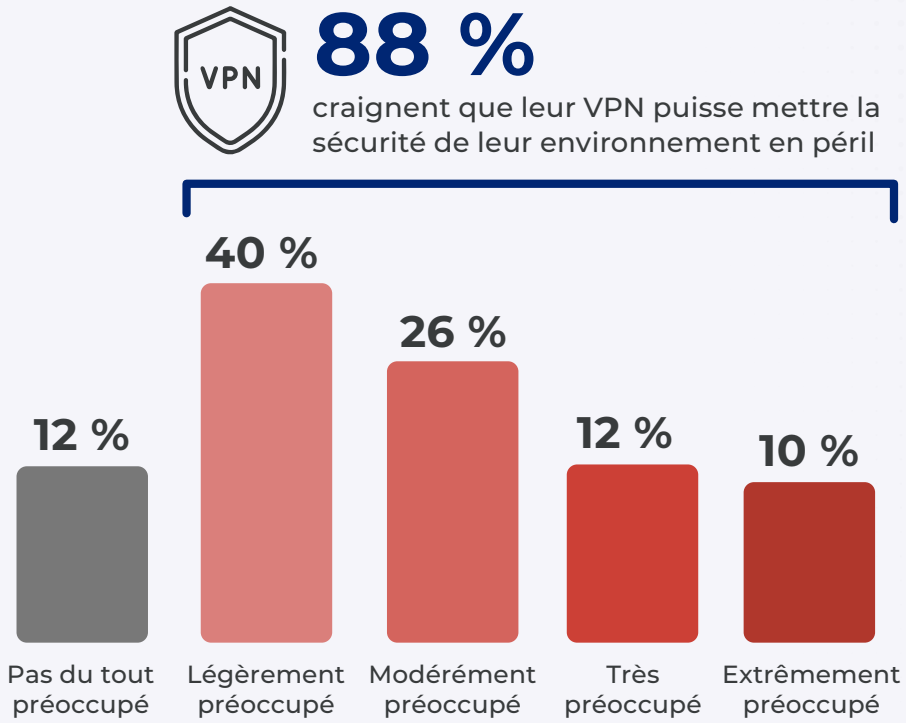
La résolution des problèmes de connectivité et de stabilité du VPN constitue également une préoccupation importante, affectant près de 20 % des personnes interrogées, suivi de près, avec 18 %, par les efforts requis pour gérer les fréquents correctifs et mises à jour des logiciels.Il est intéressant de noter que seuls 9 % des personnes interrogées font du renchérissement des coûts de l'infrastructure VPN leur principal défi.

Préoccupations liées à la sécurité des VPN

Le niveau de sécurité que fournit une solution d'accès à distance est essentiel à la protection des données et des systèmes sensibles des entreprises. Confrontés à des cybermenaces de plus en plus sophistiquées, les VPN peuvent soit renforcer, soit compromettre la posture de sécurité d'une entreprise, en fonction de leur conception et de la qualité de leur gestion.

Les résultats de l'enquête révèlent que la grande majorité des personnes interrogées (88 %) craignent que leur VPN ne mette en péril la sécurité de leur environnement. Il est particulièrement intéressant de noter que 22 % des personnes interrogées se déclarent « très » ou « extrêmement » préoccupées, ce qui indique un niveau de préoccupation important à l'égard des VPN considérés comme de potentiels points faibles pour la sécurité.

Dans quelle mesure craignez-vous que le VPN puisse fragiliser votre capacité à sécuriser votre environnement ?

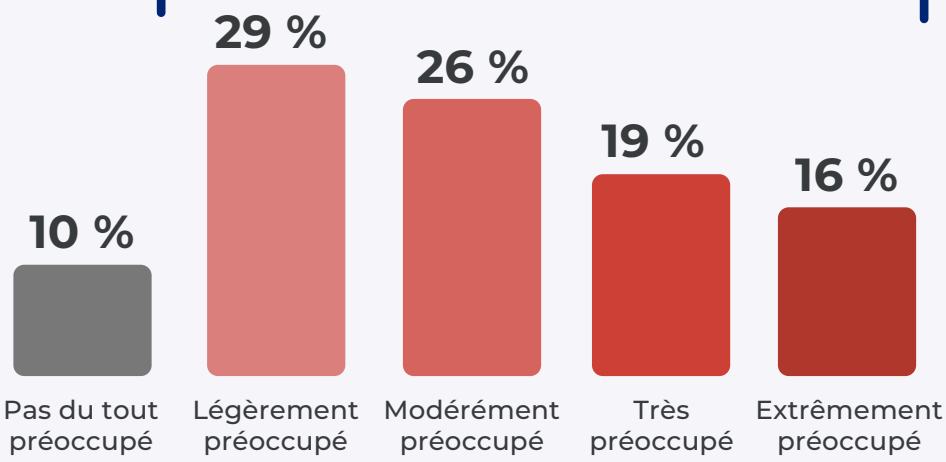


Inquiétudes concernant la sécurité liée à des tiers

Dans quelle mesure êtes-vous préoccupé par le fait que des tiers puissent servir de passerelle à des assaillants pour accéder à votre réseau par le biais de leur accès VPN ?

90 %

sont préoccupées par le fait que des tiers puissent servir de passerelle pour accéder au réseau d'entreprise via un accès VPN



Permettre à des tiers d'accéder à votre réseau par l'intermédiaire d'un VPN est une pratique nécessaire, mais elle soulève des problématiques de sécurité. Étant donné que les entités tierces peuvent ne pas adhérer aux mêmes normes rigoureuses de cybersécurité, elles peuvent potentiellement fournir une porte dérobée aux assaillants en leur permettant d'accéder au réseau d'une entreprise.

Une grande majorité des personnes interrogées (90 %) se sont dites préoccupées par le fait que des tiers puissent servir de portes dérobées pour pénétrer dans leurs réseaux via un accès VPN. Au total, 35 % des personnes interrogées se sont déclarées « très » ou « extrêmement » préoccupées, ce qui suggère que l'accès VPN pour des tiers constitue une source non négligeable d'inquiétude.

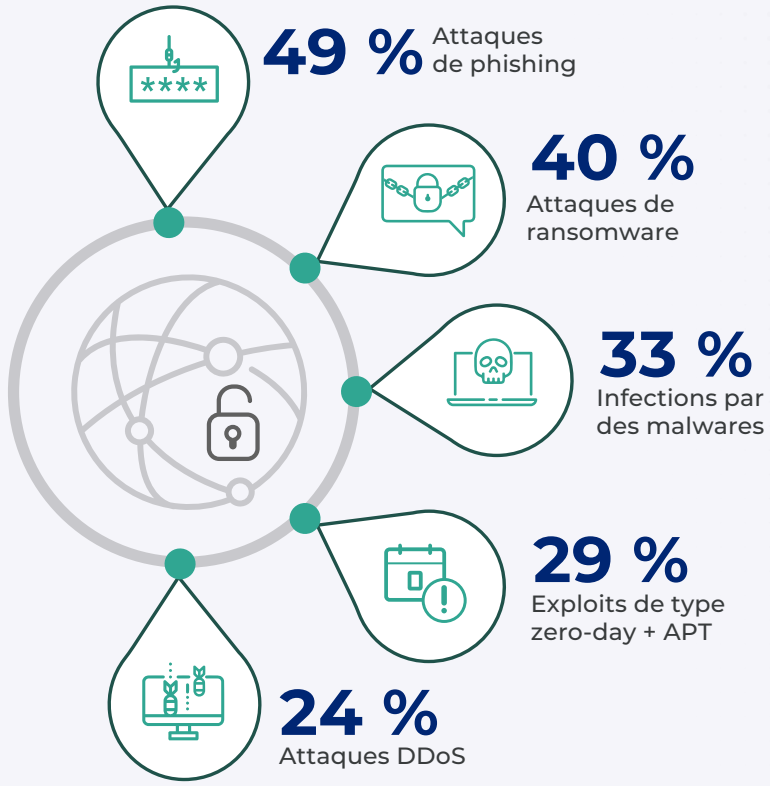
Les entreprises devraient appliquer des mesures de sécurité rigoureuses lorsqu'elles accordent un accès VPN à des tiers. Ceci impliquerait de revoir et de mettre régulièrement à jour les autorisations d'accès, d'appliquer des politiques de mots de passe forts et de surveiller l'activité du réseau pour détecter toute anomalie. En outre, les entreprises devraient s'assurer du respect des politiques de cybersécurité par les tiers et envisager d'utiliser des technologies avancées telles que des architectures Zero Trust, qui n'accordent l'accès que sur la base de ce qui est nécessaire.

Les attaques de phishing représentent la moitié des cyberattaques

Les VPN sont historiquement connus pour leurs vulnérabilités, ce qui oblige les équipes informatiques à patcher en permanence leurs serveurs VPN. Ceci peut potentiellement exposer une entreprise à diverses cyberattaques, les hackers se montrant de plus en plus sophistiqués et créatifs dans leurs techniques.

Les répondants à l'enquête considèrent que les attaques de phishing (49 %) et de ransomware (40 %) sont les types d'attaques les plus à même d'exploiter les vulnérabilités du VPN de leur entreprise. Ces attaques consistent souvent à tromper les utilisateurs pour qu'ils révèlent des informations sensibles ou à déployer des logiciels malveillants qui verrouillent les systèmes jusqu'au paiement d'une rançon.

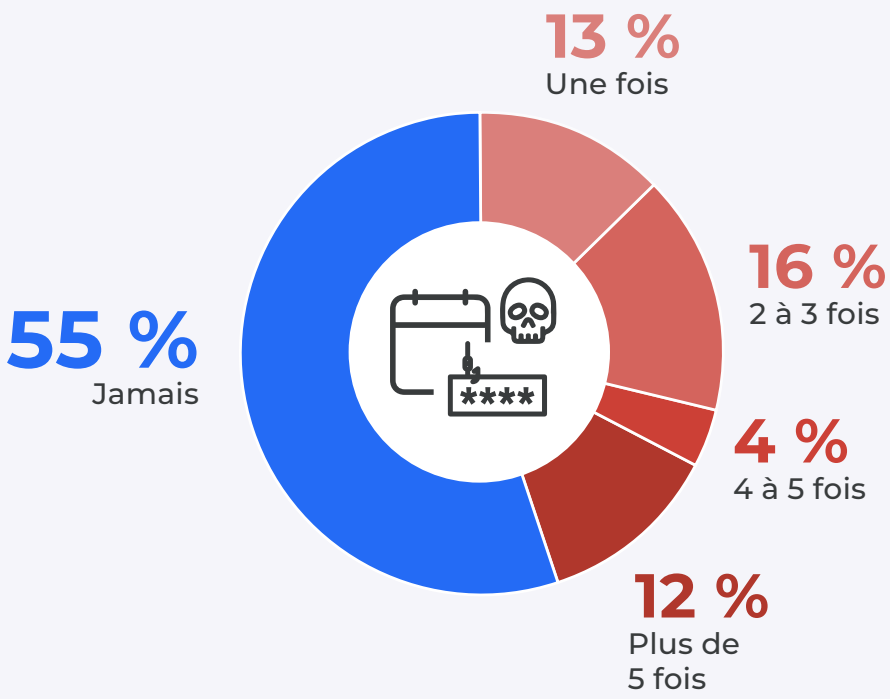
Selon vous, quels types de cyberattaque sont les plus susceptibles d'exploiter les vulnérabilités de votre VPN d'entreprise ?



Attaques de type MitM (man-in-the-middle) 22 % | Attaques par escalade de privilèges 20 % | Attaques par exfiltration de données 18 % | Attaques par force brute 11 % | Cross-site scripting 11 % | Exécution de logiciel à distance 9 %

1 entreprise sur 2 a été victime d'attaques liées au VPN

Au cours des 12 derniers mois, votre entreprise a-t-elle été victime d'une attaque exploitant les failles de sécurité de vos serveurs VPN ?



La sécurité d'un serveur VPN est cruciale pour assurer l'intégrité et la confidentialité des données qu'il traite et héberge. Comme les entreprises dépendent de plus en plus des VPN pour le télétravail, toute vulnérabilité peut devenir une cible de choix pour les assaillants.

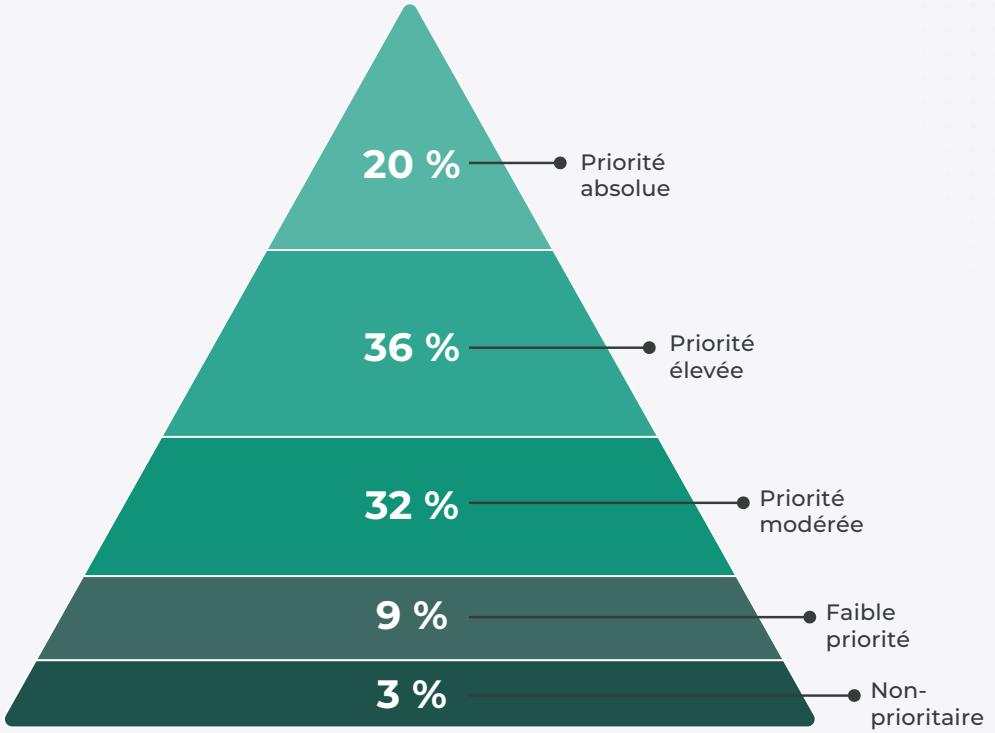
Selon l'enquête, une part non négligeable des entreprises (45 %) ont subi une ou plusieurs attaques sur leurs serveurs VPN au cours des 12 derniers mois. Ces exactions ont exploité des vulnérabilités logicielles des serveurs VPN, soulignant le besoin urgent de solutions d'accès à distance plus sécurisées.

Le Zero Trust est une priorité majeure

L'adoption du Zero Trust, un modèle de sécurité qui consiste à « ne jamais faire confiance, toujours vérifier », est une priorité pour 9 entreprises sur 10.

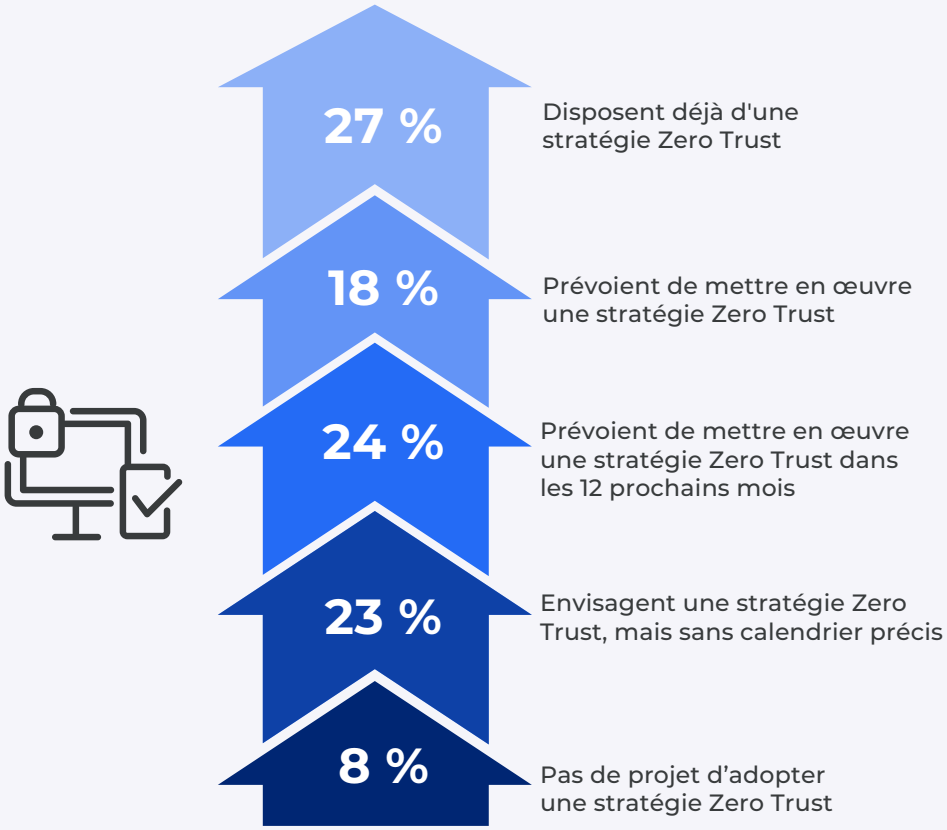
Pour tirer pleinement parti d'une architecture Zero Trust, les entreprises doivent donner la priorité à des pratiques essentielles comme l'authentification multifactorielle, la vérification continue du trafic, la segmentation du réseau, les accès basés sur le moindre privilège et une surveillance continue, autant de leviers qui permettent de renforcer leur posture de sécurité.

Dans quelle mesure l'adoption d'une stratégie Zero Trust est-elle une priorité pour votre entreprise ?



Mettre en œuvre la stratégie Zero Trust est l'objectif principal

Quels sont les projets d'adoption d'une stratégie Zero Trust pour votre entreprise ?



92 % des entreprises ont déjà mis en œuvre (27 %), prévoient de mettre en œuvre (42 %) ou envisagent une stratégie Zero Trust, ce qui démontre qu'elles comprennent son importance et que la notion de Zero Trust est bien plus qu'un buzzword, autrement dit une réalité.

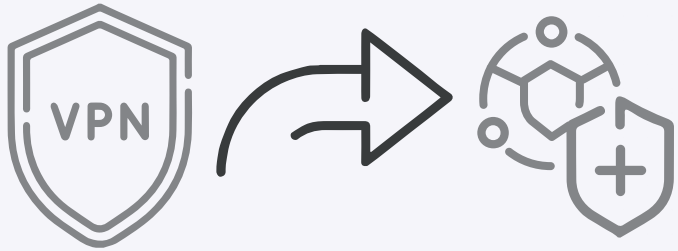
Celles qui n'ont pas encore défini de calendrier de mise en œuvre devraient envisager d'accélérer leurs projets pour préserver leur compétitivité et leur sécurité. Celles qui n'ont pas de plan ou qui sont dans le doute risquent de se faire distancer par des menaces de sécurité cloud en constante évolution.

Du VPN au Zero Trust

La transition des VPN vers des solutions Zero Trust Network Access (ZTNA) marque un virage important dans les stratégies modernes de sécurité cloud, étant donné l'accent mis sur les accès fondés sur le moindre privilège et la microsegmentation inhérente à ZTNA. Quatre entreprises sur dix sont en train de passer au ZTNA, ce qui témoigne d'une réponse active à l'évolution des exigences de sécurité.

Les entreprises qui envisagent de passer au ZTNA doivent impérativement évaluer et choisir les solutions ZTNA qui répondent à leurs exigences de sécurité et à leurs besoins spécifiques. Celles qui n'ont pas encore l'intention d'adopter ZTNA devraient au moins étudier les avantages potentiels de ces solutions pour améliorer leur posture de sécurité cloud. Les modèles hybrides peuvent constituer un compromis avantageux pour les entreprises qui ne sont pas en mesure de basculer complètement, car ils offrent les avantages du ZTNA tout en s'appuyant sur l'infrastructure VPN existante.

Avez-vous l'intention de remplacer votre solution VPN actuelle par une solution Zero Trust Network Access (ZTNA) dans un avenir proche ?



37 %

prévoient de remplacer leur VPN par une solution ZTNA dans un avenir proche

Bonnes pratiques pour votre migration vers le Zero Trust

Nous recommandons les bonnes pratiques suivantes pour passer avec succès d'une infrastructure VPN traditionnelle à une architecture Zero Trust moderne.

Évaluez votre infrastructure actuelle :
commencez par un examen approfondi de votre infrastructure VPN existante. Avec 32 % des utilisateurs qui indiquent des expériences utilisateurs médiocres et 14 % des coûts élevés, il est crucial de comprendre vos problèmes spécifiques avant d'aller de l'avant.

Choisissez la bonne solution :
recherchez une solution Zero Trust qui répond à vos besoins spécifiques. Une solution cloud-native, de type software-defined, peut simplifier la gestion, réduire les coûts et améliorer l'expérience utilisateur, pour ainsi répondre à des problématiques fréquemment rencontrées avec les VPN.

Instaurez un accès basé sur le principe du moindre privilège :
n'accordez aux utilisateurs qu'un accès strictement nécessaire à des ressources spécifiques, en fonction des besoins propres à leur fonction. Il s'agit d'un élément fondamental du Zero Trust.

Privilégiez l'évolutivité :
optez pour une solution qui peut s'adapter à la croissance de votre entreprise. Notre enquête révèle qu'environ 11 % des entreprises sont confrontées à des problèmes d'évolutivité liés à leurs VPN. Une solution basée sur le cloud répond efficacement aux besoins d'évolutivité.

Évaluez et mettez à jour régulièrement vos politiques de sécurité :
prenez l'habitude d'évaluer et de mettre à jour régulièrement vos politiques de sécurité. Vous bénéficierez ainsi d'une posture de sécurité robuste.

Sécurisez l'accès de tous les utilisateurs :
adoptez une solution qui assure un accès sécurisé aux télétravailleurs, aux tiers et aux appareils non gérés. Choisissez une plateforme qui prend en charge n'importe quel utilisateur, n'importe où, sur n'importe quel appareil.

Un processus permanent de contrôle et d'amélioration :
adoptez une stratégie de surveillance continue afin d'identifier les problèmes potentiels et d'y répondre avant qu'ils ne s'aggravent. La détection et la réponse proactives aux menaces sont la clé d'une mise en œuvre réussie du Zero Trust.

Méthodologie et données démographiques

Ce rapport est basé sur les résultats d'une enquête approfondie réalisée en ligne en juin 2022 auprès de 351 professionnels de l'informatique et de la cybersécurité, afin d'identifier les dernières tendances de matière d'adoption de technologies par les entreprises, les défis, les lacunes et les préférences concernant les solutions visant à maîtriser les risques associés aux VPN. Les répondants sont aussi bien des cadres techniques que des professionnels de la sécurité informatique, constituant un échantillon représentatif d'entreprises de tailles diverses actives dans de nombreux secteurs.

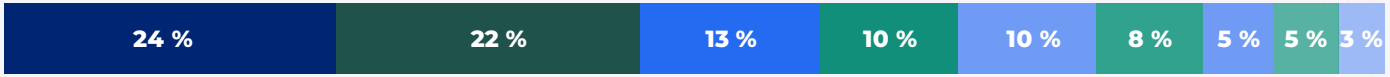
Niveau professionnel

Spécialiste · Manager/Superviseur · Directeur · Consultant · CTO, DSI, RSSI, CMO, CFO, COO · Autre

Département

Sécurité informatique · Opérations informatiques · Ingénierie · Gestion des produits

Rôle principal



Administrateur systèmes · Responsable informatique, directeur · Analyste de sécurité · CSO, RSSI ou VP de la sécurité · Responsable ou directeur de la sécurité · Auditeur · DSI · Administrateur de la sécurité · Analyste des menaces

Taille de l'entreprise

1 250-5 000 · 5 001-20 000 · +20 000

Secteur

Gouvernement · Soins de santé, produits pharmaceutiques et biotechnologie · Ordinateurs et électronique · Services financiers · Logiciels et Internet · Télécommunications · Commerce de détail · Services aux consommateurs · Éducation et recherche · Autres

À propos de Zscaler

Zscaler (NASDAQ : ZS) est un catalyseur de la transformation digitale de ses clients, pour leur permettre de gagner en agilité, productivité, résilience et sécurité. La plateforme Zero Trust Exchange de Zscaler protège des milliers de clients contre les cyberattaques et les pertes de données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications indépendamment de leur localisation. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur la technologie SASE, est la plus importante plateforme de sécurité cloud intégrée au monde.

En savoir plus sur zscaler.fr ou nous suivre sur Twitter @zscaler.com.

zscaler.fr

Cybersecurity INSIDERS

Cybersecurity Insiders fédère plus de 600 000 professionnels de la sécurité informatique et des fournisseurs technologiques de premier plan, pour une résolution intelligente des problèmes et la collaboration, et ainsi relever les défis actuels les plus critiques de la sécurité cloud.

Notre approche consiste à créer et enrichir des contenus qui sensibilisent et informent les professionnels de la cybersécurité sur les dernières tendances, solutions et bonnes pratiques de la sécurité cloud. Qu'il s'agisse d'études détaillées, de critiques objectives de produits, de guides électroniques pratiques, de webinaires ou d'articles de sensibilisation, nous nous engageons à fournir des ressources qui apportent des réponses éprouvées aux défis complexes de la sécurité cloud moderne.

Contactez-nous dès aujourd'hui pour découvrir comment Cybersecurity Insiders peut vous aider à vous démarquer sur un marché très concurrentiel et à stimuler la demande, la visibilité de votre marque et votre présence en tant que leader d'opinion.

Envoyez-nous un e-mail à **info@cybersecurity-insiders.com** ou rendez-vous sur le site **cybersecurity-insiders.com**