Rapport Zscaler ThreatLabz 2024 sur les risques liés aux VPN

Cybersecurity INSIDERS

Alors que l'adoption du modèle Zero Trust gagne du terrain, découvrez les principales tendances en matière de sécurité des VPN, de risques et d'expérience utilisateur.

Sommaire

Synthèse

L'environnement de travail moderne, multisite et orienté cloud, fait évoluer les méthodes d'accès, des réseaux privés virtuels (VPN) traditionnels vers des frameworks de sécurité plus pertinents comme le Zero Trust. Traditionnellement, les VPN fournissaient un accès à distance essentiel pour interconnecter des utilisateurs ou des sites. Cependant, la sophistication croissante des cybermenaces ainsi que la généralisation du télétravail et des technologies cloud ont révélé certaines vulnérabilités des VPN. En raison de leur architecture traditionnelle, les VPN accordent, après validation des identifiants de connexion, un accès trop étendu au réseau, ce qui renforce le risque de cyberattaques en cas de piratage de ces identifiants.

Des exploits récents médiatisés, liés à des appliances VPN, ont mis en évidence des vulnérabilités critiques (notamment CVE-2023-46805, CVE-2024-21887 et CVE-2024-21893) affectant des secteurs d'activité critiques, à l'instar de celui de la défense américaine. Ces vulnérabilités permettent aux hackers de contourner l'authentification, d'exécuter des commandes avec des privilèges élevés et de rendre leurs attaques persistantes même après la réinitialisation des dispositifs infectés. En réponse, l'agence américaine CISA (Cybersecurity and Infrastructure Security Agency) a émis une directive d'urgence aux agences fédérales du pays, pour qu'elles déconnectent immédiatement les dispositifs VPN concernés en raison des risques de sécurité importants associés.

Par le biais du décret 14028, le gouvernement américain impose désormais l'adoption d'architectures Zero Trust pour renforcer la cybersécurité, en remplacement des VPN traditionnels. Cette directive, qui fait partie d'une stratégie globale visant à renforcer la cybersécurité nationale américaine, demande aux agences fédérales de déployer une stratégie Zero Trust, qui vérifie chaque demande d'accès au réseau, quelle qu'en soit l'origine. L'Office of Management and Budget (OMB) soutient également cette initiative par une stratégie fédérale Zero Trust détaillée, qui souligne un vrai changement de culture : la confiance implicite accordée aux accès par VPN devient caduque, au profit d'une vérification continue de tous les accès. Ces directives et recommandations reflètent un consensus au sein de la communauté de la cybersécurité selon lequel le Zero Trust fournit une défense plus robuste contre les cybermenaces complexes et évolutives, une nécessité soulignée par les vulnérabilités et exploits récents liés aux VPN traditionnels.

En conséquence, les entreprises adoptent rapidement le modèle Zero Trust, qui n'accorde aucune confiance intrinsèque à un utilisateur ou appareil à l'intérieur ou à l'extérieur du périmètre réseau, et qui procède à une vérification granulaire de chaque demande d'accès. Ce modèle est efficace pour empêcher les déplacements latéraux au sein des réseaux, une méthode privilégiée par les hackers pour propager leur attaque suite à l'intrusion initiale.

Basé sur une enquête menée auprès de 647 professionnels de l'informatique et experts en cybersécurité, ce rapport explore de nombreux défis liés aux VPN, en matière de sécurité et d'expérience utilisateur. Il révèle la complexité de la gestion actuelle des accès et la vulnérabilité des entreprises face à différents profils d'attaque qui mettent à mal leur posture de cybersécurité. Le rapport présente également des modèles de sécurité plus sophistiqués, en particulier le modèle Zero Trust, qui s'est fermement imposé comme un framework robuste et évolutif pour sécuriser et accélérer la transformation digitale.

Nous remercions Zscaler pour sa contribution à cette enquête sur les risques liés aux VPN. L'expertise de ses équipes en matière de solutions Zero Trust et d'accès sécurisé nous a permis d'enrichir nos conclusions. Nous sommes convaincus que les enseignements de ce rapport seront précieux pour les professionnels de l'informatique et de la cybersécurité dans leur démarche vers une sécurité Zero Trust.

Merci à vous.
Holger Schulze, fondateur, Cybersecurity Insiders

« Au cours de l'année écoulée, de nombreuses vulnérabilités VPN critiques ont servi de passerelle d'entrée à des attaques menées contre de grandes entreprises et administrations. Face à ce scénario qui se répète, il est crucial que les entreprises anticipent le fait que les acteurs malveillants exploiteront de plus en plus ces ressources traditionnelles (appliances physiques ou format virtualisé) exposées à Internet et qui leur permettent de se déplacer latéralement sur les réseaux plats traditionnels. Il est essentiel de passer à une architecture Zero Trust, qui réduit considérablement la surface d'attaque en éliminant les technologies traditionnelles telles que les VPN et les pare-feu, applique des contrôles de sécurité cohérents avec une inspection TLS et limite le périmètre d'impact et le préjudice des incidents grâce à des technologies de segmentation et de leurre. »

– DEEPEN DESAI, RESPONSABLE DE LA SÉCURITÉ, ZSCALER

Principales conclusions

Les attaques contre les VPN progressent.

56 % des entreprises ont subi une ou plusieurs cyberattaques liées aux VPN au cours de l'année écoulée, contre 45 % l'année précédente, ce qui met en évidence la fréquence et la sophistication croissantes des attaques ciblant les VPN.

La grande majorité des entreprises adoptent le Zero Trust.

78 % des entreprises prévoient de déployer une stratégie Zero Trust au cours des 12 prochains mois. Parallèlement, 62 % des entreprises conviennent que les VPN vont à l'encontre des stratégies Zero Trust.

La plupart des entreprises émettent des doutes concernant la sécurité des VPN.

91 % des personnes interrogées ont exprimé leurs inquiétudes quant au fait que les VPN mettent en péril leur sécurité informatique. Des incidents récents illustrent les risques liés à l'exploitation d'infrastructures VPN obsolètes ou non patchées.

Les VPN ne font pas le poids face aux ransomwares, malwares et attaques DDoS.

Les personnes interrogées ont identifié les ransomwares (42 %), les malwares (35 %) et les attaques DDoS (30 %) comme les principales menaces exploitant les vulnérabilités des VPN, ce qui souligne l'ampleur des risques auxquels les entreprises sont confrontées en raison des carences des architectures VPN traditionnelles.

Le risque de déplacement latéral ne peut être ignoré.

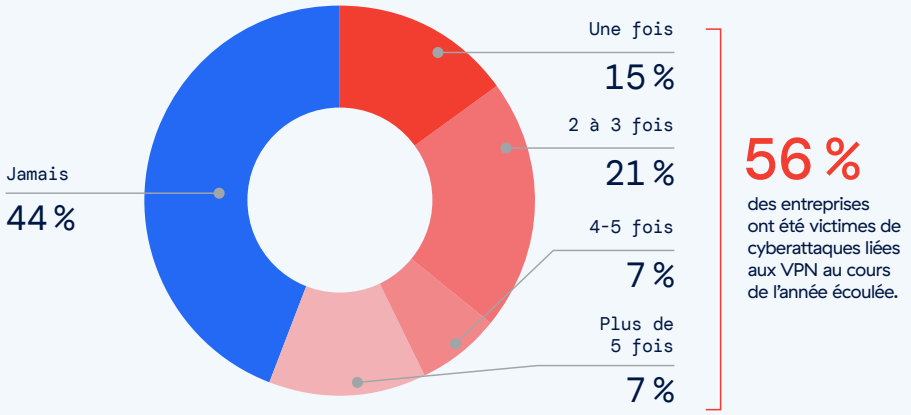
53 % des entreprises victimes d'un incident lié à une vulnérabilité VPN affirment que les hackers se sont déplacés en interne, ce qui démontre l'échec d'un confinement du point initial de compromission et souligne les risques que présentent les réseaux plats traditionnels.

Défis de sécurité des VPN

Recrudescence des attaques contre les VPN

La fréquence et la sévérité des attaques exploitant les vulnérabilités des VPN mettent en évidence l'impuissance des mesures de cybersécurité conventionnelles et soulignent les risques d'un réseau exposé. Notre enquête révèle que 56 % des entreprises ont subi des cyberattaques au cours de l'année écoulée qui ont tiré parti des vulnérabilités des VPN, soit un bond par rapport aux 45 % de l'année précédente. Fait alarmant, 41 % des entreprises ont déclaré avoir subi au moins deux attaques liées au VPN, ce qui dénote de graves failles de sécurité.

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

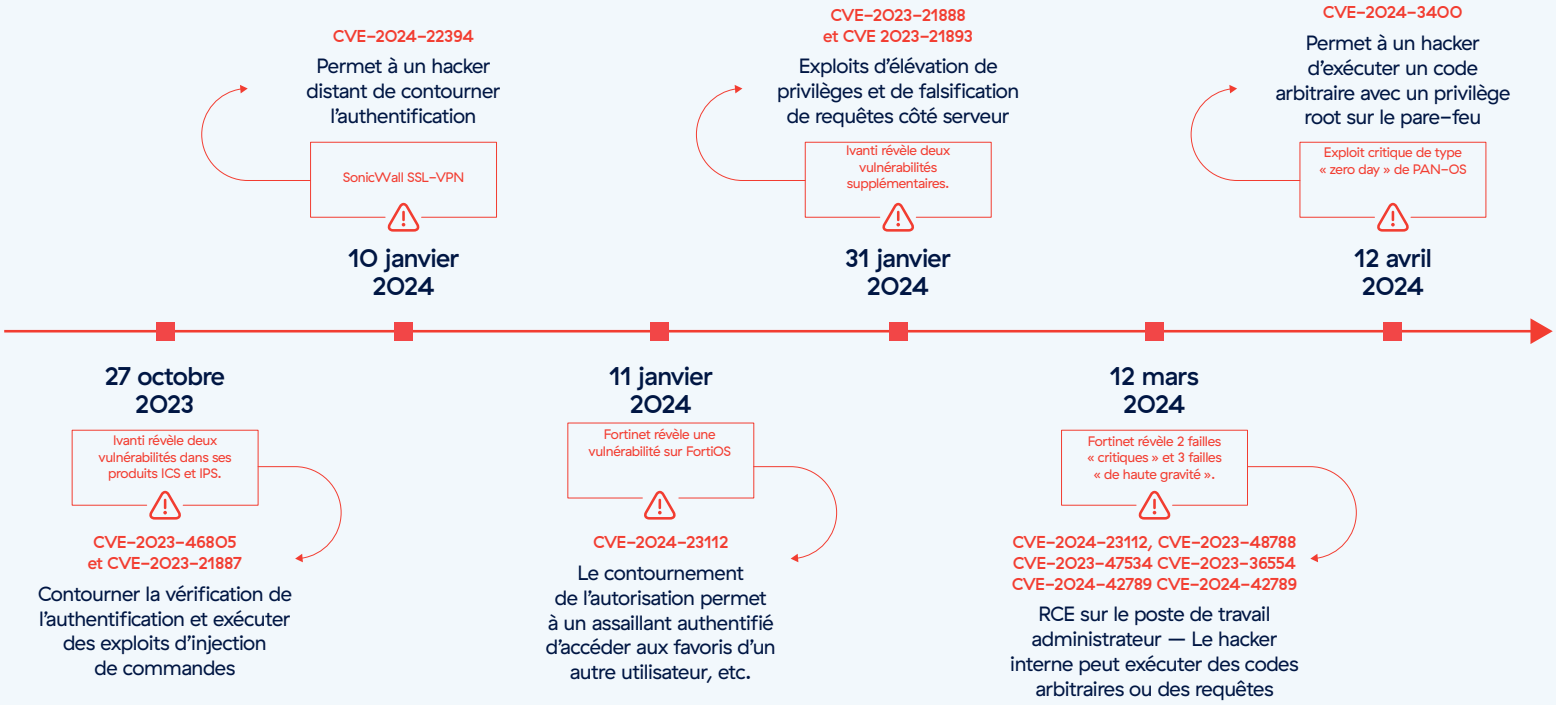


Les tendances récentes confirment que les attaques contre les VPN deviennent plus fréquentes, mais aussi plus sophistiquées. Par exemple, la multiplication des cas de ransomware exploitant les vulnérabilités des VPN, en particulier à la suite de la divulgation publique de celles-ci, met en évidence les carences critiques des VPN traditionnels. Ces vulnérabilités constituent, pour les assaillants des passerelles pour infiltrer les réseaux et s'y déplacer en interne, entraînant des violations de données et des perturbations opérationnelles.

Principales vulnérabilités des VPN au cours de l'année écoulée

Compte tenu des récentes vulnérabilités CVE critiques affectant les produits de VPN, il n'est guère surprenant que les entreprises signalent davantage d'exploits. Bien entendu, aucun fournisseur ni technologie particulière ne peut être à l'abri de vulnérabilités logicielles. Dans le cas du VPN, le défi pour les entreprises est que chaque vulnérabilité CVE est un point de défaillance unique pour la sécurité unique de l'entreprise : une tête de pont qui permet aux hackers de compromettre une ressource VPN, de s'ancrer de manière persistante sur le réseau, de se déplacer latéralement sur celui-ci et de détourner des données. Si les vulnérabilités CVE des VPN continuent à progresser au même rythme, elles constitueront un risque persistant pour les entreprises qui font appel à cette technologie pour leur connectivité à distance.

Une série de vulnérabilités CVE récentes met en évidence des carences d'architecture



Analyse des défis de sécurité du VPN

Les résultats de l'enquête reflètent de réelles préoccupations concernant le risque des VPN pour la sécurité, faisant écho aux tendances actuelles et aux vulnérabilités toujours plus nombreuses à affecter les VPN. Une écrasante majorité des personnes interrogées (91 % contre 88 % en 2023) se disent préoccupées par des VPN qui mettent en péril leur sécurité informatique, soulignant ainsi que les entreprises sont davantage sensibilisées aux risques associés aux VPN.

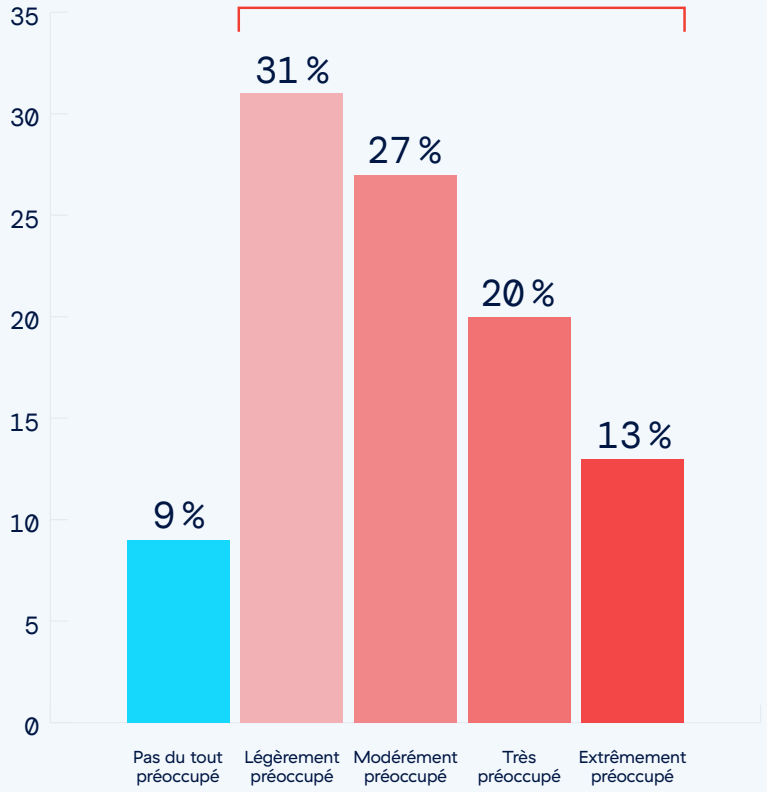
Cette inquiétude est justifiée par les exploits récents ciblant les VPN Ivanti, lorsque des hackers ont exploité des vulnérabilités pour infiltrer les réseaux et exfiltrer des données sensibles. Ces incidents, impliquant des vulnérabilités telles que CVE-2024-21888 et CVE-2024-21893, mettent en évidence les risques liés à la maintenance et à la sécurisation d'infrastructures VPN obsolètes ou sans patch. De plus, l'architecture inhérente aux VPN présente des risques de sécurité importants dans l'univers digital étendu d'aujourd'hui. Alors que les entreprises adoptent de plus en plus les services cloud et que les modèles de télétravail évoluent, les VPN sont confrontés à de nouveaux défis de sécurité, notamment la gestion de droits d'accès étendus et la sécurisation d'une surface d'attaque en expansion.

Ces vulnérabilités et contraintes architecturales soulignent un changement crucial dans la perception de la sécurité des VPN, dans la droite ligne des tendances de cybersécurité plus larges qui préconisent des frameworks plus dynamiques et plus résilients tels que le Zero Trust.

Les entreprises innovantes évoluent vers des architectures Zero Trust pour s'octroyer un contrôle plus granulaire et réduire considérablement leur surface d'attaque en ne conférant aucune confiance implicite aux entités, que celles-ci soient à l'intérieur ou à l'extérieur du périmètre réseau. L'adoption d'une telle stratégie répond aux vulnérabilités immédiates des VPN traditionnels et s'aligne sur une approche proactive de cybersécurité, essentielle pour s'adapter à l'évolution des menaces.

Dans quelle mesure craignez-vous que le VPN fragilise votre capacité à sécuriser votre environnement IT ?

91 % des entreprises craignent que leur VPN puisse mettre la sécurité de leur environnement en péril.

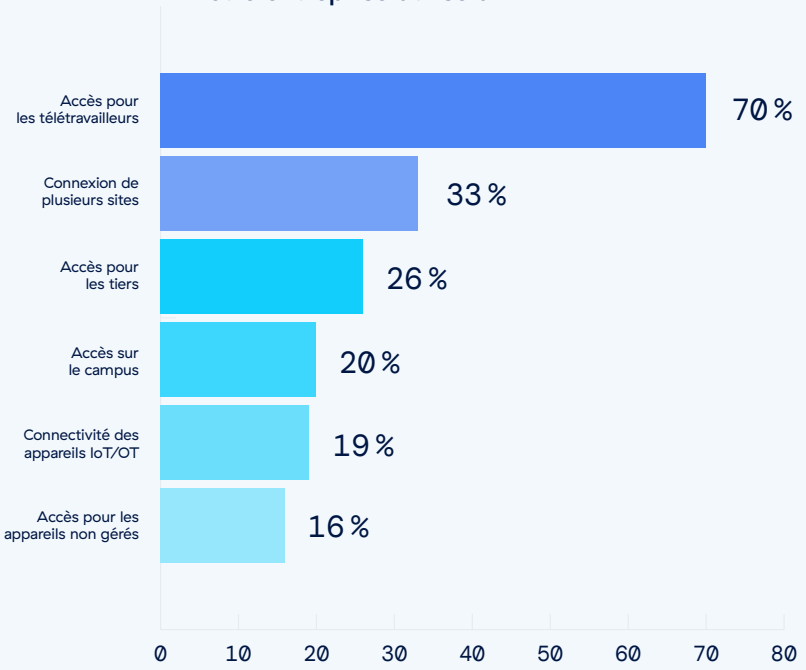


Principaux scénarios pour un accès sécurisé

Comprendre pourquoi les entreprises utilisent des VPN est essentiel, pour mettre en évidence la manière dont elles privilégient un accès sécurisé lors de différents scénarios. Il s'agit également d'identifier les cas d'utilisation réseau les plus exposés aux risques de sécurité, et donc les domaines qui nécessitent des stratégies de sécurité d'accès plus robustes et innovantes.

Près de 70 % des entreprises utilisent des VPN principalement pour sécuriser l'accès de leurs collaborateurs distants. L'accès à distance, aujourd'hui généralisé, est une cible privilégiée des cyberattaques. 33 % des entreprises utilisent des VPN pour interconnecter plusieurs sites. Le risque est que ces connexions servent de vecteurs de cyberattaques si elles ne sont pas correctement sécurisées. 26 % des entreprises ont mentionné l'accès pour les tiers, ce qui complique davantage la sécurité en raison des postures de sécurité différentes de chaque partie prenante externe et d'un déficit de contrôle sur les politiques de sécurité. Enfin, 20 % des entreprises utilisent des VPN pour accéder à leur campus d'entreprise, et 19 % pour la connectivité des dispositifs IoT/OT.

Quelle est la principale raison pour laquelle votre entreprise utilise un VPN ?



Face aux menaces actuelles, les VPN ne présentent plus un niveau satisfaisant de sécurité. En effet, ils opèrent selon des modèles de confiance obsolètes qui accordent un accès étendu au réseau sur simple authentification de l'utilisateur. Cet accès étendu expose les entreprises à des risques majeurs. Il permet aux assaillants potentiels de s'immiscer sur le réseau via un point d'entrée unique, pour ensuite se mouvoir et exfiltrer des données sensibles via le réseau.

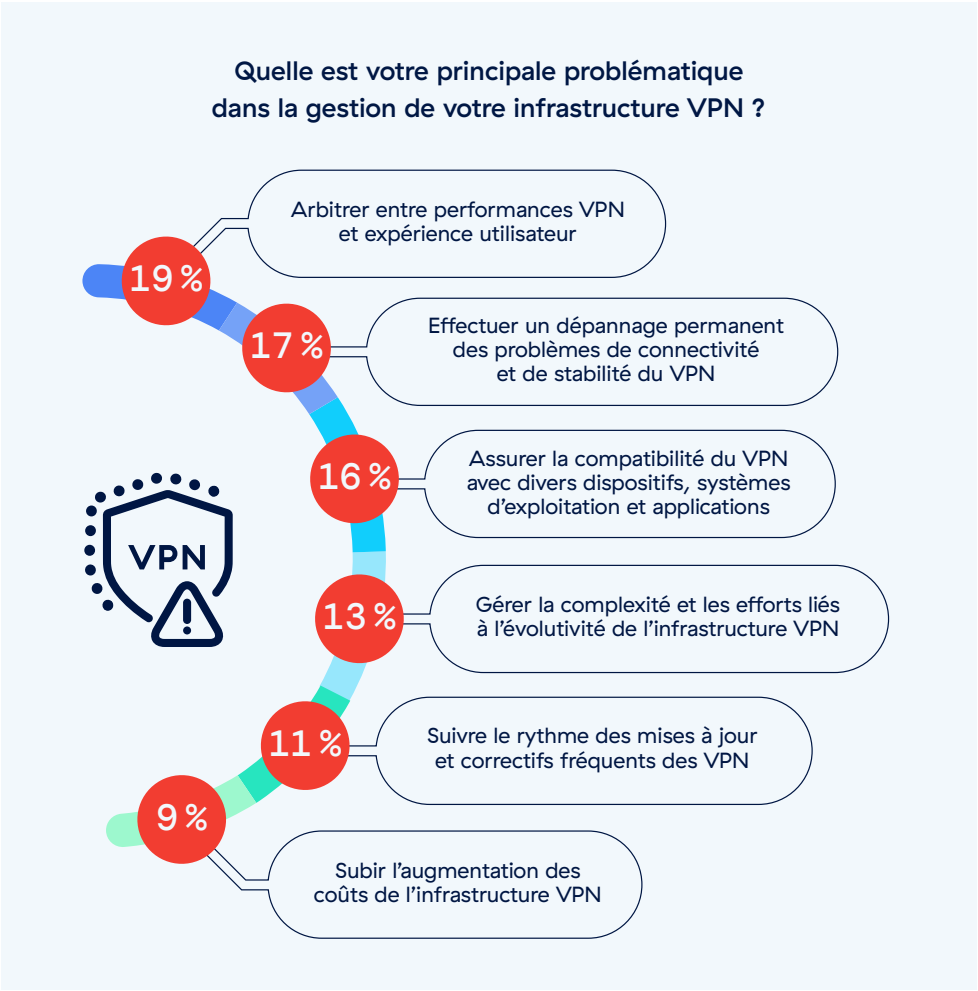
Gestion, performances et expérience utilisateur des VPN

Défis liés à la gestion des VPN

Outre les risques de sécurité, la gestion des infrastructures VPN présente d'importants défis pour les équipes informatiques. En effet, le besoin pour des solutions d'accès robustes est plus important au sein d'un environnement de travail désormais multisite et orienté cloud. Le principal défi de gestion que rencontrent les professionnels de l'informatique est d'arbitrer entre performances du VPN et expérience utilisateur (19 %). Cet enjeu est crucial, car il impacte directement la productivité : un VPN qui ralentit le réseau ou dont l'utilisation s'avère trop contraignante pèsera sur la satisfaction des collaborateurs et sur l'efficacité des processus métiers.

La deuxième préoccupation la plus courante, citée par 17 % des personnes interrogées, porte sur le traitement en continu des problématiques de connectivité et de stabilité du VPN. Ces problèmes sont non seulement chronophages pour les équipes informatiques, mais provoquent également des perturbations frustrantes pour les utilisateurs. Parmi les autres défis notables, citons le manque de compatibilité des VPN avec une large gamme d'appareils, de systèmes d'exploitation et d'applications, ce que 16 % des professionnels de l'informatique considèrent fastidieux. De plus, 13 % des personnes interrogées sont confrontées à la complexité et à la faible évolutivité de l'infrastructure VPN, un problème crucial à mesure que les entreprises se développent et que leurs besoins s'accentuent dans un contexte de pénurie de professionnels qualifiés en cybersécurité.

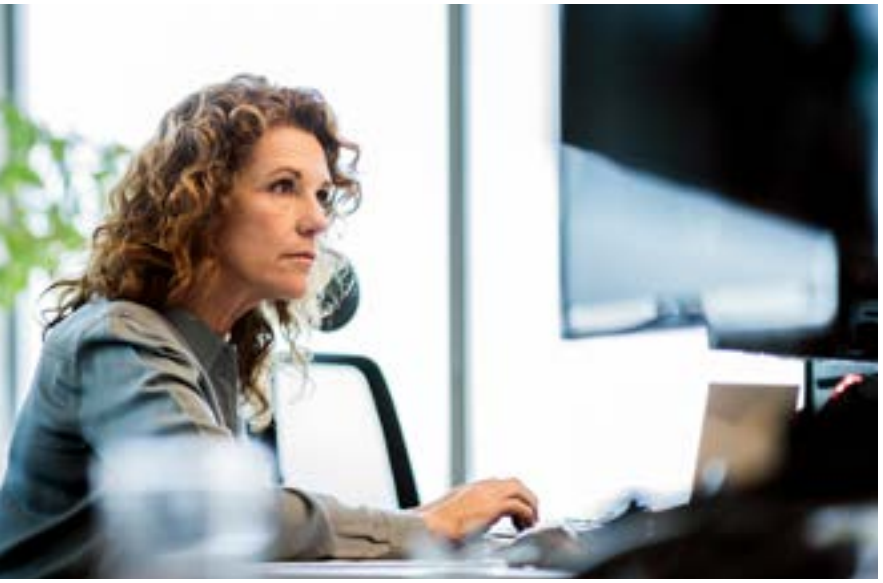
Ces perspectives soulignent la nécessité qu'ont les entreprises d'explorer des alternatives plus agiles, conviviales et moins gourmandes en ressources, telles que les modèles d'accès réseau Zero Trust (ZTNA). ZTNA assure un contrôle plus granulaire, offre davantage d'évolutivité et favorise une réduction des coûts de gestion, ce qui en fait une alternative pertinente au VPN traditionnel dans le paysage dynamique de la cybersécurité moderne.



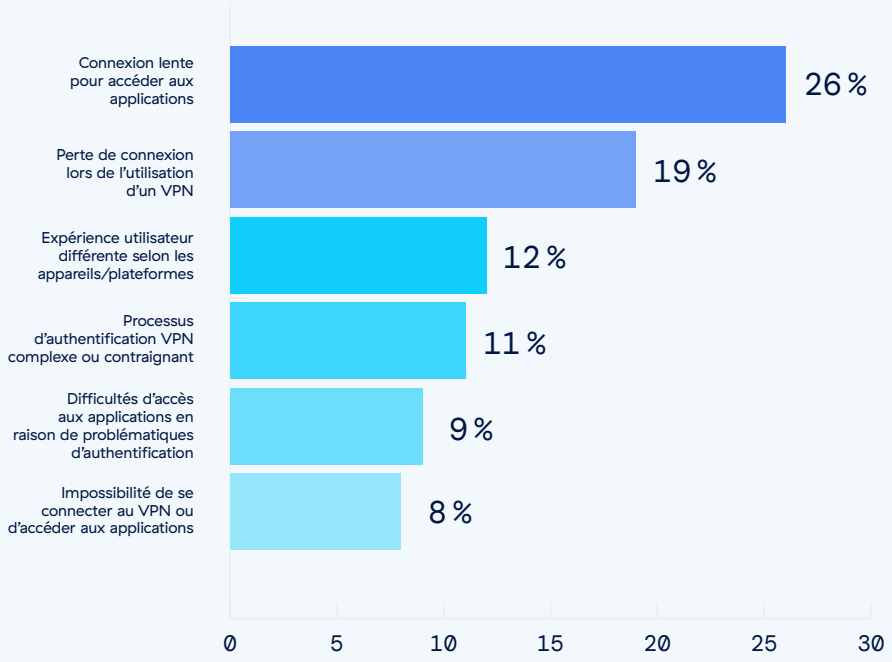
Défis courants pour les utilisateurs de VPN

La plainte la plus fréquente des utilisateurs de VPN, comme l'ont mentionné 26 % des personnes interrogées, porte sur la lenteur de la connexion. Ces performances médiocres illustrent un problème critique de productivité et de satisfaction des utilisateurs : en effet, des connexions lentes grèvent le bon fonctionnement des tâches de routine et l'accès aux ressources cloud, en particulier en environnement de télétravail.

Les pertes de connexion VPN représentent le deuxième problème le plus courant, cité par 19 % des personnes interrogées. Ce défaut peut perturber les tâches et les communications en cours, affectant considérablement l'expérience utilisateur et la continuité des opérations métiers. La divergence de l'expérience des utilisateurs selon leur dispositif, signalée par 12 % des utilisateurs, plaide en faveur d'accès dont les performances sont plus uniformes.

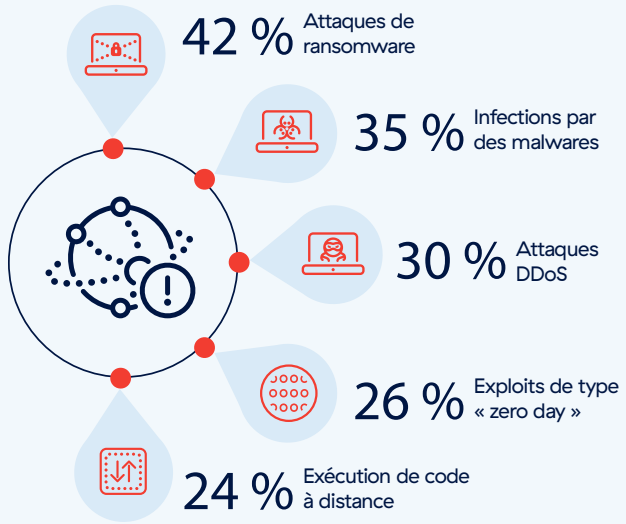


Quelle est la plainte la plus fréquente formulée par vos utilisateurs lorsqu'ils accèdent à des applications via un VPN ?



Pour répondre à ces préoccupations, les entreprises doivent envisager des solutions d'accès réseau qui offrent davantage de stabilité et de cohérence entre les différents dispositifs et plateformes. La mise en œuvre d'une architecture Zero Trust peut se révéler particulièrement efficace, car elle améliore la sécurité sans nuire aux performances. Le Zero Trust garantit que les problèmes de connexion ne compromettent pas la sécurité, et qu'un contrôle d'accès strict s'adapte et s'applique à différents environnements utilisateur.

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



Pour pallier ces vulnérabilités, les entreprises doivent adopter des mesures de sécurité proactives telles que le modèle Zero Trust. Le Zero Trust applique des contrôles d'accès rigoureux et une vérification continue de toutes les connexions réseau, quelle que soit leur origine. Cette stratégie tempère les risques associés à de nombreuses attaques ciblant les faiblesses du VPN, en limitant les déplacements latéraux et en déployant un contrôle d'accès robuste.

Exploits des vulnérabilités du VPN

La diversité des cyberattaques qui exploitent les faiblesses des VPN met en évidence l'ampleur des risques qui affectent les entreprises. L'enquête révèle que 42 % des personnes interrogées identifient les attaques de ransomware comme les plus probables pour exploiter les vulnérabilités du VPN, mettant en évidence leur impact majeur et leur fréquence régulière. Viennent ensuite les infections par malwares, signalées par 35 % des personnes interrogées, et les attaques DDoS, signalées par 30 % des répondants, qui compromettent la disponibilité, ainsi que la confidentialité et l'intégrité des systèmes.

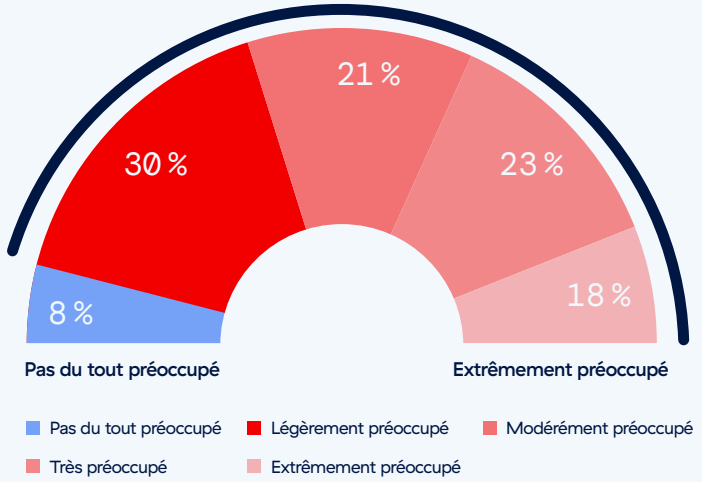
Risques liés à l'accès de tiers aux VPN

L'enquête souligne une préoccupation majeure concernant l'accès de tiers aux VPN, considérée comme une vulnérabilité de sécurité du réseau. Un pourcentage notable (92 %) des personnes interrogées exprime leur appréhension face à ce risque, un chiffre en légère hausse par rapport aux 90 % de 2023. Cette perspective fait de l'accès des tiers un point d'entrée pour les cybermenaces.

De nouvelles informations sur les vulnérabilités et les incidents sur des VPN ont encore confirmé ces préoccupations. Les VPN traditionnels fournissent généralement un accès étendu au réseau après validation des informations d'identification, ce qui présente des risques si la sécurité des fournisseurs tiers est compromise.

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

92 % des entreprises sont préoccupées par le fait que des tiers puissent servir de passerelle pour accéder à leur réseau d'entreprise via un accès VPN.



Les entreprises doivent accélérer leur transition des VPN traditionnels vers des architectures Zero Trust. Ce changement implique de mettre en œuvre des systèmes qui vérifient rigoureusement les demandes d'accès en fonction de l'identité et du contexte, ce qui permet de restreindre les fournisseurs à des ressources spécifiques essentielles à leurs tâches.

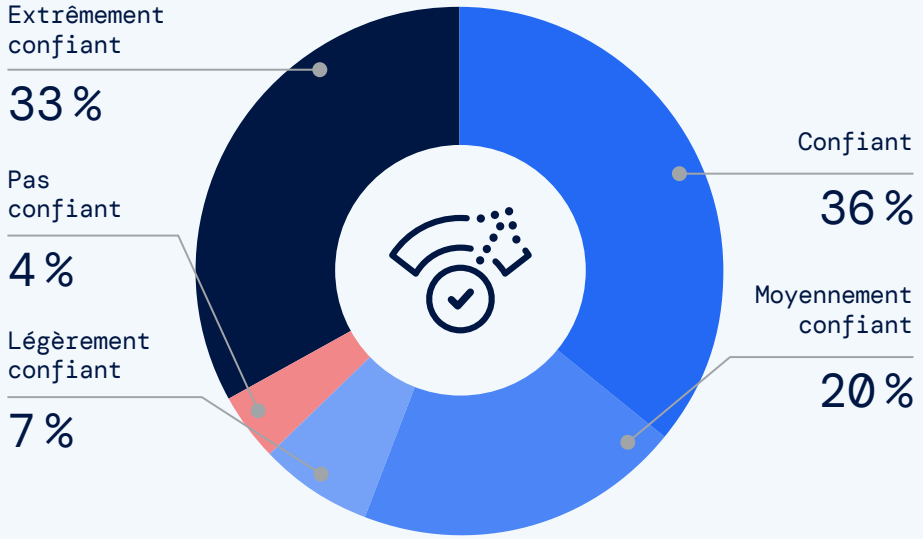
Problématiques de sécurité liées à l'infrastructure VPN

Confiance excessive dans la sécurité des VPN

La recrudescence récente des vulnérabilités des VPN met en évidence un décalage entre la sécurité perçue et le risque réel. Des exploits récents et de grande ampleur qui ont affecté les produits VPN soulignent que les entreprises, même celles qui sont bien préparées, pourraient sous-estimer les capacités des cyber-adversaires exploitant les vulnérabilités de la technologie VPN. 69 % des personnes interrogées déclarent être très confiantes dans la capacité de leur entreprise à gérer les vulnérabilités des VPN, ce qui n'est pas vraiment en phase avec la recrudescence des menaces liées à des assaillants compétents qui exploitent très rapidement les carences les plus anodines. Une confiance excessive peut être particulièrement risquée compte tenu de la complexité et de la persistance des exploits VPN récents, comme le prouvent les incidents impliquant des groupes parrainés par des États-nations et des gangs de cybercriminels ciblant des systèmes restés sans patch pendant de longues périodes.

Les entreprises doivent repenser leurs opérations de sécurité en intégrant des évaluations rigoureuses des vulnérabilités, des mises à jour fréquentes et une sensibilisation des collaborateurs à la sécurité. Il est recommandé d'adopter une approche de sécurité qui ne repose pas exagérément sur les VPN pour assurer une protection complète. Cette approche devrait associer un monitoring avancé, une détection des anomalies et les principes du Zero Trust.

Dans quelle mesure êtes-vous confiant dans la capacité de votre entreprise à détecter et restaurer les vulnérabilités VPN qui l'exposent à des attaques de cybersécurité ?

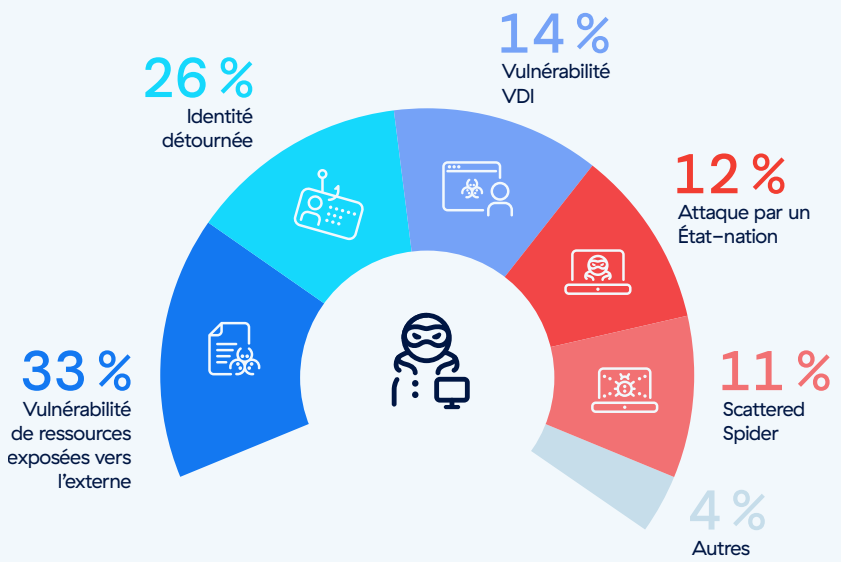


Vecteurs d'attaque des ransomwares

L'enquête identifie clairement les vulnérabilités des ressources exposées vers l'externe comme étant le vecteur potentiel d'attaque par ransomware le plus préoccupant, mentionné par 33 % des personnes interrogées. Ce chiffre atteste de la réalité de risques associés aux services réseau et applications Web exposés, qui constituent souvent le premier point d'entrée des attaques par ransomware.

Le détournement d'identité suit de près, avec un score de 26 %, soulignant le rôle du piratage d'informations pour permettre aux hackers de contourner les mesures de sécurité et d'obtenir l'accès permettant de diffuser les payloads de ransomwares. Les inquiétudes concernant les vulnérabilités des infrastructures de postes de travail virtuels (VDI) et les attaques menées par des États-nations, ressortant à respectivement 14 % et 12 %, mettent en évidence la diversité des menaces de ransomware contre lesquelles les entreprises doivent se protéger. Scattered Spider (un groupe cybercriminel qui utilise des tactiques d'ingénierie sociale sophistiquées, notamment le phishing, le spam de demande d'authentification multifacteur et le SIM swapping), préoccupe 11 % des personnes interrogées.

Quelle votre principale préoccupation concernant les ransomwares ?



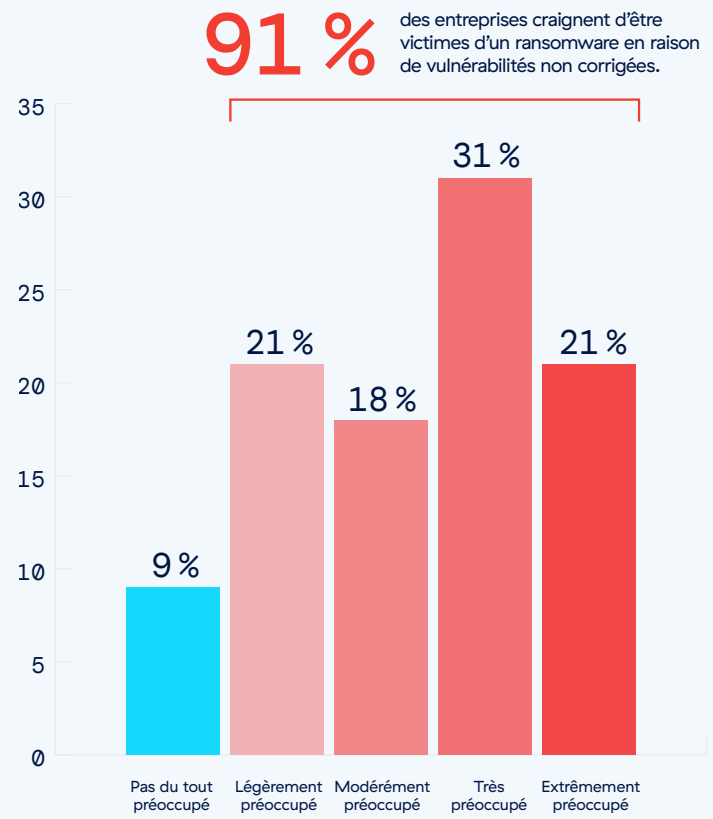
Les entreprises doivent renforcer leurs défenses et leurs protocoles de gestion des identités. La mise en œuvre de processus complets de gestion des vulnérabilités et l'adoption d'un modèle de sécurité Zero Trust peuvent réduire efficacement le risque d'attaques de ransomware, en leur refusant l'accès aux ressources réseau et en les empêchant de se propager en interne.

Préoccupations liées aux ransomwares

Les résultats de l'enquête révèlent que 52 % des personnes interrogées sont très ou extrêmement préoccupées par la menace de ransomware liée à des vulnérabilités non corrigées. Cette inquiétude est justifiée, car les vulnérabilités non corrigées demeurent un des principaux vecteurs d'attaque des ransomwares. Des analyses récentes révèlent qu'une part importante des attaques de ransomware exploite ces vulnérabilités, avec des conséquences particulièrement graves par rapport à d'autres types de cyberattaques.

Les groupuscules spécialisés dans le ransomware gagnent en sophistication, nombre d'entre eux utilisant désormais des tactiques avancées capables d'exploiter rapidement les vulnérabilités récemment découvertes, avant que les entreprises ne puissent les corriger. Ce cycle d'exploitation rapide réduit considérablement la fenêtre de prise en charge des vulnérabilités critiques et souligne le besoin urgent de mesures de sécurité avancées qui réduisent la surface d'attaque.

Dans quelle mesure craignez-vous d'être ciblé par un ransomware en raison de vulnérabilités non corrigées ?



Déplacement latéral dans les attaques visant les VPN

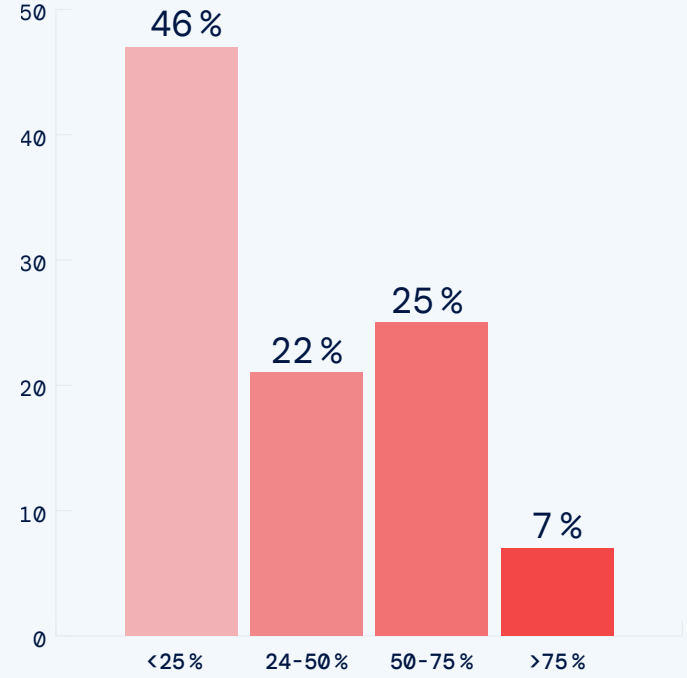
La plupart des personnes interrogées (53 %) rapportent que plus de 25 % des attaques liées aux VPN donnaient lieu à des déplacements latéraux, démontrant l'échec du confinement au niveau du point initial de compromission. Près d'un tiers (32 %) ont constaté des déplacements latéraux dans plus de la moitié des attaques, ce qui témoigne de difficultés majeures à contrôler la propagation de la menace une fois que les hackers franchissent les défenses du réseau.

Les déplacements latéraux constituent un risque important des VPN, puisque les assaillants peuvent obtenir un accès réseau étendu similaire à celui d'un utilisateur authentifié. Cela leur permet de se mouvoir furtivement sur le réseau et de cibler les zones sensibles.

En ce sens, les VPN peuvent aggraver les risques et étendre la portée d'une attaque au-delà de son point d'entrée initial. Pour résoudre cette problématique, une segmentation stricte s'impose, idéalement avec le déploiement du Zero Trust pour sécuriser le trafic entre les utilisateurs et les applications, ainsi qu'un monitoring permanent. Ainsi, le rayon d'action du déplacement latéral est considérablement réduit, permettant ainsi un accès granulaire à un plus petit ensemble d'applications pour chaque utilisateur, ce dernier n'ayant aucune visibilité sur les autres applications.

La sophistication croissante des attaques exploitant les vulnérabilités des VPN souligne la nécessité d'évoluer vers le Zero Trust. En appliquant des contrôles d'accès stricts et une validation continue, le modèle Zero Trust limite les déplacements latéraux non autorisés et améliore la sécurité des environnements digitaux en expansion.

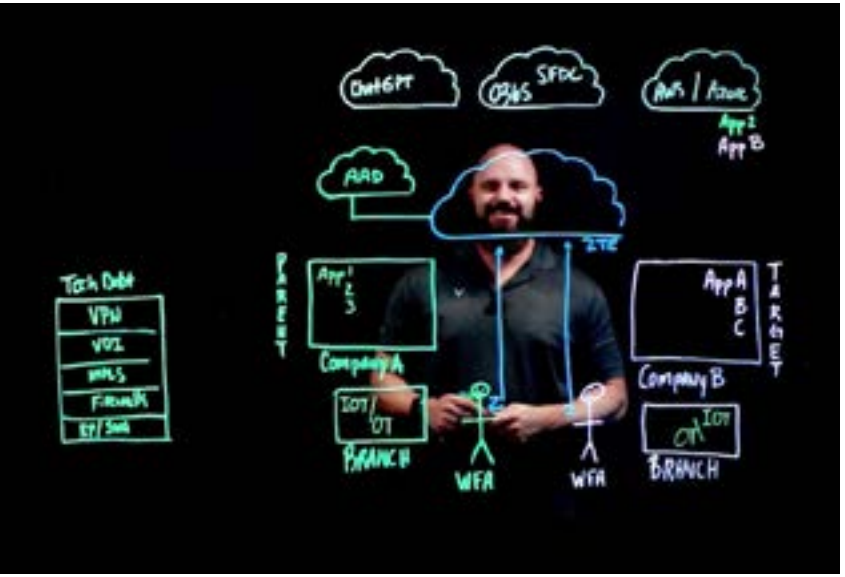
Sur l'ensemble des attaques subies par votre entreprise, quel est le pourcentage de menaces qui se sont propagées latéralement après avoir obtenu un accès grâce à un VPN ?



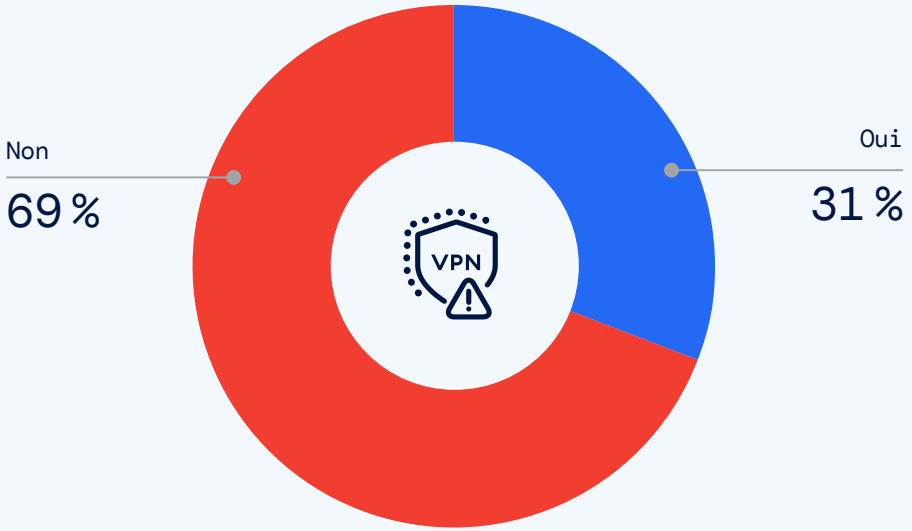
Préoccupations liées à la sécurité des VPN après une opération de fusion et d'acquisition

Les préoccupations relatives à l'impact des fusions et acquisitions sur l'infrastructure VPN existante mettent en évidence les vulnérabilités potentielles qui découlent de changements organisationnels et de l'intégration de réseaux hétérogènes.

69 % des personnes interrogées expriment leur crainte à l'égard des cyberattaques suite à une opération de fusion et acquisition, ce qui témoigne d'une inquiétude généralisée à l'égard des risques de sécurité associés à ces opérations corporate. Ce sentiment traduit une compréhension claire que les activités de fusion et acquisition peuvent déstabiliser les environnements de sécurité existants, renforçant ainsi l'exposition aux cybermenaces.



Craignez-vous que votre infrastructure actuelle soit victime d'une attaque suite à une opération de fusion et acquisition ?



Les périodes de transition pendant les activités de fusion et d'acquisition offrent aux entreprises l'opportunité de remplacer progressivement les technologies VPN obsolètes et vulnérables par des architectures Zero Trust. Plus précisément, les architectures Zero Trust renforcent la sécurité en fournissant une segmentation complète de l'environnement entre les utilisateurs et les applications, entre les instances entre elles, entre les sites distants, ainsi qu'entre les dispositifs, qu'il s'agisse de dispositifs gérés, non gérés, de dispositifs IoT ou de systèmes OT. Cette approche renforce la sécurité pendant et après une transition grâce à une vérification rigoureuse de tous les utilisateurs et dispositifs, une segmentation complète et une application stricte des contrôles d'accès sur la base du moindre privilège.

Adoption du Zero Trust par les entreprises

Progrès dans l'adoption du Zero Trust

L'enquête reflète une tendance majeure, celle de l'adoption d'un framework de sécurité Zero Trust, en tant que levier pour améliorer la cybersécurité des entreprises. 31 % des personnes interrogées mettent déjà en œuvre le modèle Zero Trust (contre 27 % en 2023), dans un effort proactif pour mieux protéger les ressources du réseau.

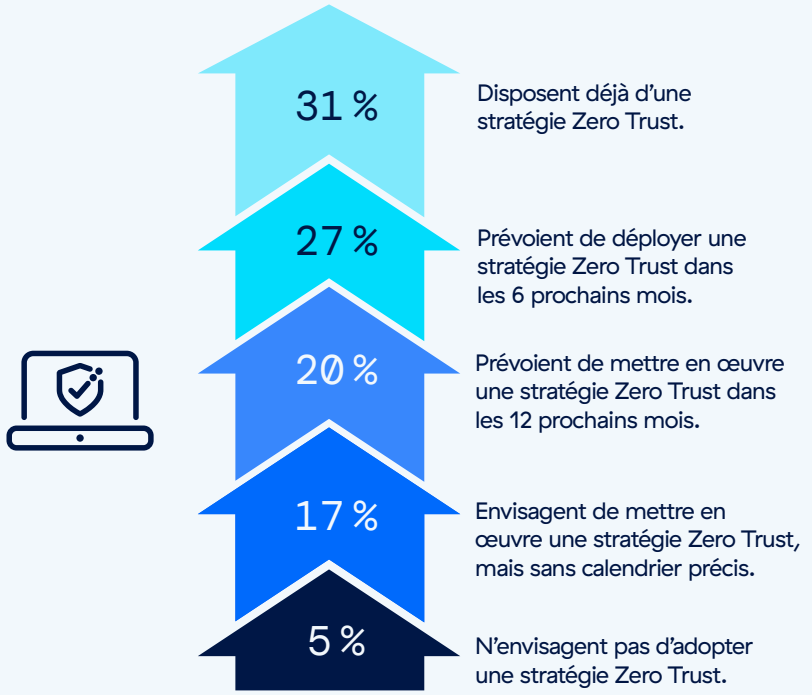
De plus, 27 % des entreprises prévoient de déployer une stratégie Zero Trust au cours des six prochains mois (contre 18 % en 2023), tandis 20 % des entreprises envisagent cette transition au cours des 12 prochains mois, démontrant un engagement général en faveur d'une adoption du Zero Trust dans un avenir proche. D'ailleurs, plus des trois quarts des personnes interrogées (78 %) reconnaissent l'urgence et les avantages du Zero Trust.

Cependant, 17 % des personnes interrogées étudient la possibilité d'une stratégie Zero Trust mais ne disposent pas de calendrier précis (contre 23 % en 2023), ce qui met en évidence certaines hésitations ou difficultés potentielles dans la planification ou l'initiation de la démarche Zero Trust. Seule une part modeste (5 %) déclare ne pas prévoir d'adopter le Zero Trust (contre 8 % en 2023), peut-être en raison d'un manque de ressources.

Une analyse par taille d'entreprise indique que les grandes entreprises interrogées, en particulier celles qui comptent plus de 20 000 employés, sont davantage susceptibles d'adopter des stratégies Zero Trust, et ce, de manière plus rapide, 33 % d'entre elles les ayant déjà mis en œuvre. En revanche, les petites entreprises comptant entre 1 000 et 5 000 employés affichent un taux d'adoption légèrement inférieur (29 %), ce qui suggère que l'envergure et la disponibilité des ressources peuvent influencer le rythme et le périmètre d'un projet Zero Trust.

Les entreprises qui hésitent encore ou envisagent d'adopter le modèle Zero Trust devraient commencer par évaluer leur posture de sécurité actuelle et leur architecture réseau afin d'identifier leurs besoins spécifiques et les défis potentiels associés.

Quels sont vos projets pour l'adoption d'une stratégie Zero Trust au sein de votre entreprise ?

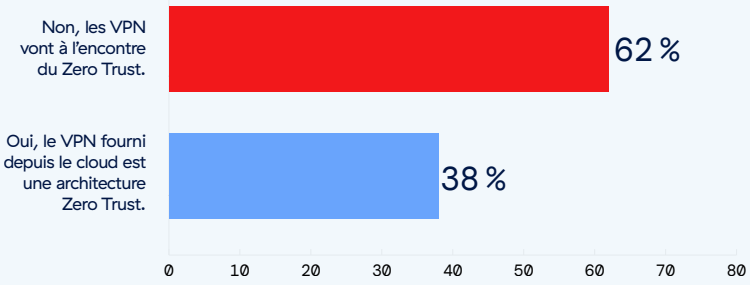


Absence de sécurité Zero Trust avec les VPN

Les résultats de l'enquête reflètent une méconnaissance sur la compatibilité des VPN avec les frameworks de sécurité Zero Trust. La plupart des personnes interrogées (62 %) estiment que les VPN vont à l'encontre du Zero Trust, ce qui confirme que les architectures VPN traditionnelles ne s'alignent pas sur les principes du Zero Trust. À l'inverse, 38 % des personnes interrogées considèrent que les VPN, en particulier les plateformes cloud, sont compatibles avec les architectures Zero Trust.

Si ce point de vue peut s'expliquer par le fait que les fournisseurs de VPN affirment que leurs solutions cloud intègrent les principes du Zero Trust, ces allégations doivent faire l'objet d'une analyse critique. Le simple fait d'héberger un service VPN dans le cloud, par exemple, ne confère pas automatiquement des attributs du Zero Trust. La sécurité Zero Trust exige davantage qu'un simple environnement d'hébergement sécurisé : elle impose de migrer des défenses basées sur le périmètre vers un modèle où la sécurité se veut dynamique, granulaire et contextualisée.

Pensez-vous qu'il est possible de concrétiser une sécurité Zero Trust avec des VPN ?



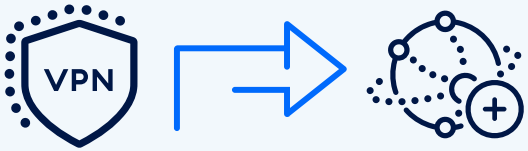
Une véritable sécurité Zero Trust implique une validation continue de tous les utilisateurs et dispositifs, l'application du principe d'accès sur la base du moindre privilège et la segmentation du trafic pour empêcher les déplacements latéraux, autant de fonctionnalités absentes des VPN traditionnels, même ceux basés sur le cloud. Par conséquent, les entreprises doivent vérifier que tout VPN prétendument « Zero Trust » intègre réellement ces principes fondamentaux, au-delà donc des promesses marketing.

Passer du VPN au Zero Trust NEtwork Access (ZTNA)

Les résultats de l'enquête révèlent que la plupart des entreprises opèrent un changement stratégique, 53 % des personnes interrogées indiquant leur intention de remplacer leurs solutions VPN existantes par des solutions ZTNA dans un avenir proche. Le ZTNA propose une approche plus flexible et plus sécurisée en appliquant des politiques basées sur le contexte de l'utilisateur, sa localisation et la sécurité de son dispositif. Aucune confiance ne lui est accordée sur le simple fait qu'il est présent sur le réseau. Ceci contraste avec les VPN traditionnels qui accordent généralement un accès étendu à un réseau, créant ainsi des failles de sécurité.

Pour les 53 % d'entreprises qui s'orientent vers le ZTNA, il est crucial d'assurer une transition fluide en planifiant des évaluations complètes des risques, en mettant à jour les politiques d'accès et en sensibilisant les utilisateurs aux nouveaux protocoles. Quant aux 47 % d'entreprises qui n'envisagent pas encore de déployer le ZTNA, elles devraient évaluer leurs défis de sécurité actuels et se demander si le ZTNA pourrait les résoudre plus efficacement qu'un VPN.

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



53 %

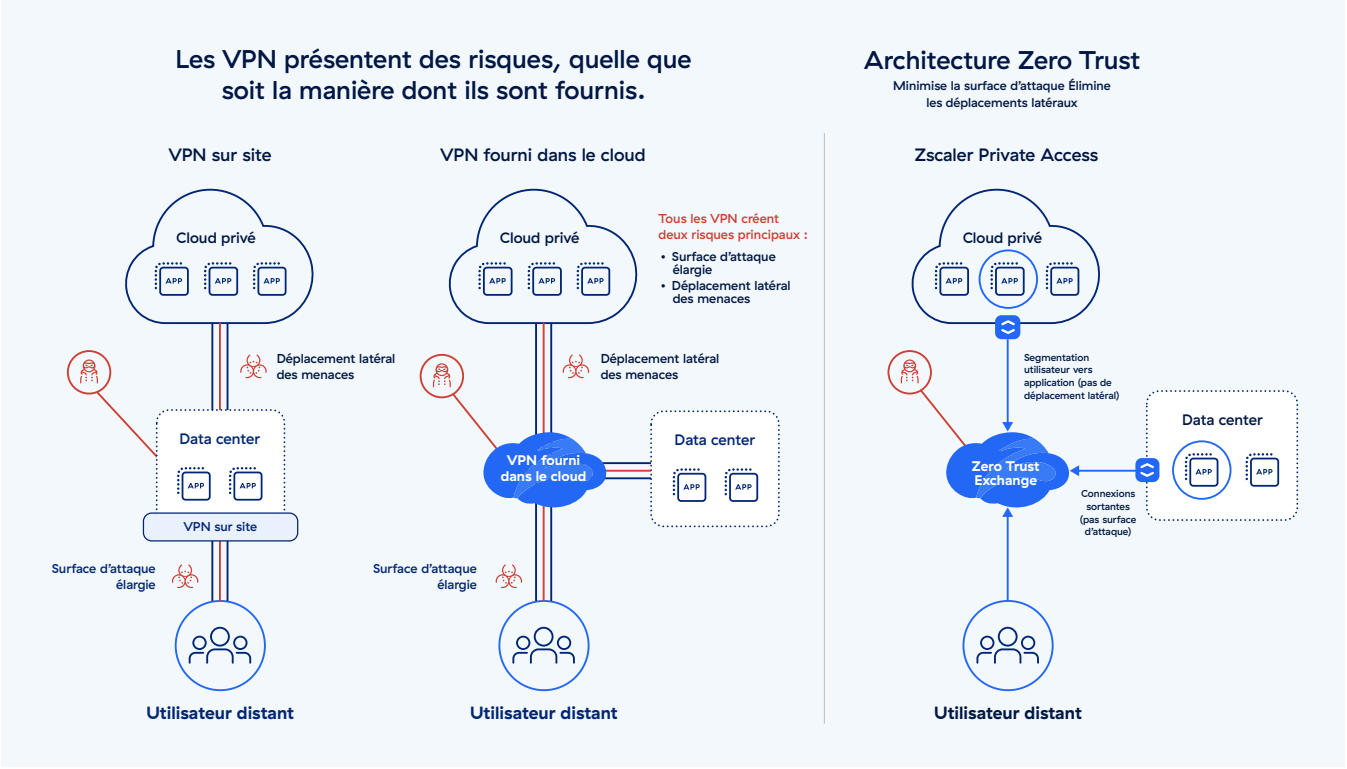
prévoient de remplacer leur VPN par une solution ZTNA dans un avenir proche.

Pourquoi le Zero Trust est plus sécurisé que le VPN

Sur le plan architectural, le Zero Trust et le ZTNA sont plus sécurisés que les VPN traditionnels, principalement en raison d'un framework de sécurité robuste qui n'accorde jamais une confiance intrinsèque à une connexion. Les architectures traditionnelles basées sur les VPN sont susceptibles de présenter un point de défaillance unique (SPOF). Lorsqu'un VPN ou un appareil est compromis (par exemple via une nouvelle vulnérabilité CVE), les acteurs malveillants peuvent exploiter la confiance généralement accordée sur un réseau plat pour accéder à l'ensemble de celui-ci, se déplacer latéralement, détourner des données et exécuter des ransomwares. C'est pourquoi les professionnels de la sécurité sont de plus en plus préoccupés par les risques de sécurité liés aux VPN.

Les VPN sur site et fournis depuis le cloud présentent des vulnérabilités de sécurité similaires. De plus, les VPN introduisent davantage de complexité, ce qui entraîne des coûts inutiles et des tâches fastidieuses telles que le provisioning des utilisateurs, la gestion des tables de routage, le dépannage de la connectivité, l'application de correctifs, ainsi que la surveillance et l'optimisation des performances.

Dans une architecture Zero Trust, aucune connexion n'est considérée comme fiable par défaut. Les utilisateurs se connectent directement aux applications, jamais au réseau sous-jacent. De plus, chaque connexion est automatiquement interrompue, quelle que soit son origine, avant d'être vérifiée par sept couches de sécurité Zero Trust. L'architecture Zero Trust permet aux entreprises de segmenter complètement et précisément leurs environnements : entre les utilisateurs et les applications, entre les instances elles-mêmes, entre les sites distants et entre les appareils, y compris les dispositifs IoT et OT.



Différences et avantages principaux

Surface d'attaque considérablement réduite
Une architecture Zero Trust permet une connectivité interne qui rend les ressources critiques, les applications, les serveurs et autres ressources invisibles depuis l'Internet public tout en éliminant le besoin d'utiliser des technologies vulnérables comme les VPN et les pare-feu. Les entreprises peuvent ainsi fournir une connectivité hybride à leur personnel tout en réduisant considérablement leur surface d'attaque. En revanche, les architectures basées sur VPN et pare-feu obligent les entreprises à étendre leur surface d'attaque en réponse à une connectivité plus large.

Vérification en continu
Les modèles Zero Trust imposent une validation permanente de la sécurité des informations d'identification et de la posture de sécurité avant d'accorder l'accès aux ressources, ce qui complique considérablement l'accès des entités non autorisées aux informations et systèmes sensibles. En revanche, avec les VPN, l'utilisateur ou l'appareil dispose souvent d'un accès étendu aux ressources du réseau une fois que l'accès lui a été accordé.

Accès sur la base du moindre privilège
Le Zero Trust applique des politiques d'accès sur la base du moindre privilège, garantissant que les utilisateurs et les appareils n'ont accès qu'aux ressources nécessaires à leurs rôles spécifiques. Ceci minimise le risque de menaces internes et de déplacements latéraux au sein d'un réseau, qui sont des vulnérabilités courantes dans les environnements de VPN.

Accès granulaire et segmentation
En dissociant les ressources réseau en segments distincts (entre les utilisateurs et les applications, entre instances et entre dispositifs), le modèle Zero Trust confine d'éventuelles intrusions à des zones plus restreintes, réduisant ainsi considérablement l'impact d'une attaque. Bien que les entreprises tentent souvent de segmenter leurs environnements réseau, il s'agit d'un processus opérationnel complexe et coûteux qui, en pratique, reste souvent inachevé, nécessite des centaines de règles de pare-feu distinctes et expose des zones réseau plus larges aux utilisateurs authentifiés.

Accompagner les collaborateurs hybrides d'aujourd'hui
Le Zero Trust permet d'étendre facilement un accès ultra-rapide aux applications privées pour les utilisateurs sur site et distants, les sites distants et les partenaires tiers.

Amélioration de l'expérience utilisateur et simplification
Le Zero Trust améliore l'expérience utilisateur en éliminant le besoin d'acheminer l'ensemble du trafic distant vers un point central du réseau, ce qui pourrait aboutir à une congestion du réseau comme dans le cas des VPN. Cette architecture est mieux à même de répondre aux exigences d'évolutivité des réseaux modernes, notamment en matière de politiques IoT et BYOD. De plus, le modèle Zero Trust allège les coûts de gestion en automatisant les fonctions de sécurité et en simplifiant l'application des politiques de sécurité sur l'ensemble du réseau.

Ces avantages architecturaux font du Zero Trust une alternative intéressante aux VPN traditionnels, en particulier face à des menaces actuelles toujours plus sophistiquées. Pour les entreprises qui cherchent à renforcer leurs défenses en matière de cybersécurité, l'adoption d'une approche Zero Trust procure une infrastructure de sécurité plus robuste, flexible et évolutive.

Prévisions concernant les VPN pour 2024 et au-delà

1 Les vulnérabilités et les exploits graves liés aux VPN vont se multiplier

Compte tenu de la fréquence, de la gravité et de l'ampleur des vulnérabilités VPN révélées au cours de l'année écoulée, les entreprises doivent s'attendre à ce que cette tendance se poursuive. Les acteurs malveillants et les chercheurs en sécurité sont conscients du risque accru des vulnérabilités critiques affectant les produits VPN. En réponse, ils en recherchent activement d'autres, ce qui rend probable la découverte de nouvelles vulnérabilités CVE dans les mois et années à venir.

2 Les attaques médiatisées menées via des VPN vont se retrouver sous le feu des projecteurs

Dans le droit fil de notre première prévision, nous verrons davantage de grandes entreprises divulguer des incidents résultant de l'exploitation de vulnérabilités des VPN. Ceci s'explique en partie par les nouvelles directives de la SEC qui obligent les entreprises américaines cotées en bourse à divulguer ces violations et leur impact. Comme nous l'avons vu, les acteurs malveillants créent systématiquement des portes dérobées dans les environnements cibles. Ils identifient les vulnérabilités d'un VPN afin de les exploiter ultérieurement, même après correction de ces vulnérabilités. À mesure que l'année avance, de plus en plus de ces vulnérabilités seront divulguées dans les documents déposés auprès de la SEC et feront sans doute la une de l'actualité.

3 La multiplication des offres de VPN optimisés par IA alimentera les préoccupations en matière de sécurité et de confidentialité.

Conséquence des progrès constants de l'IA, les solutions VPN optimisées par IA vont inonder le marché. Les entreprises doivent évaluer ces offres avec prudence. Au-delà des promesses de meilleures performances, l'intégration de l'IA amplifiera les risques de sécurité et donnera aux assaillants de nouvelles opportunités d'exploiter les vulnérabilités du VPN. En outre, l'analyse approfondie des données, qui accroît le risque d'exposition des informations sensibles, suscitera des craintes concernant la protection de la vie privée.

4 Les attaques de type password-spraying vont continuer à se développer

Les assaillants trouveront de nouveaux moyens de tirer parti de mots de passe peu sécurisés et d'identifiants de connexion VPN par défaut, via des attaques de password-spraying (utilisation de mots de passe communs pour tenter d'accéder à plusieurs comptes de VPN). Dans ces attaques, les hackers essaient le même mot de passe sur de nombreux comptes VPN jusqu'à ce qu'ils parviennent à se connecter, obtenant ainsi un accès non autorisé. Les entreprises doivent s'attendre à la persistance d'attaques similaires, car de nombreuses violations récentes et très médiatisées liées au VPN ont effectivement été exploitées à l'aide de cette technique.

5 Les dépenses des entreprises se détourneront du VPN au profit du Zero Trust

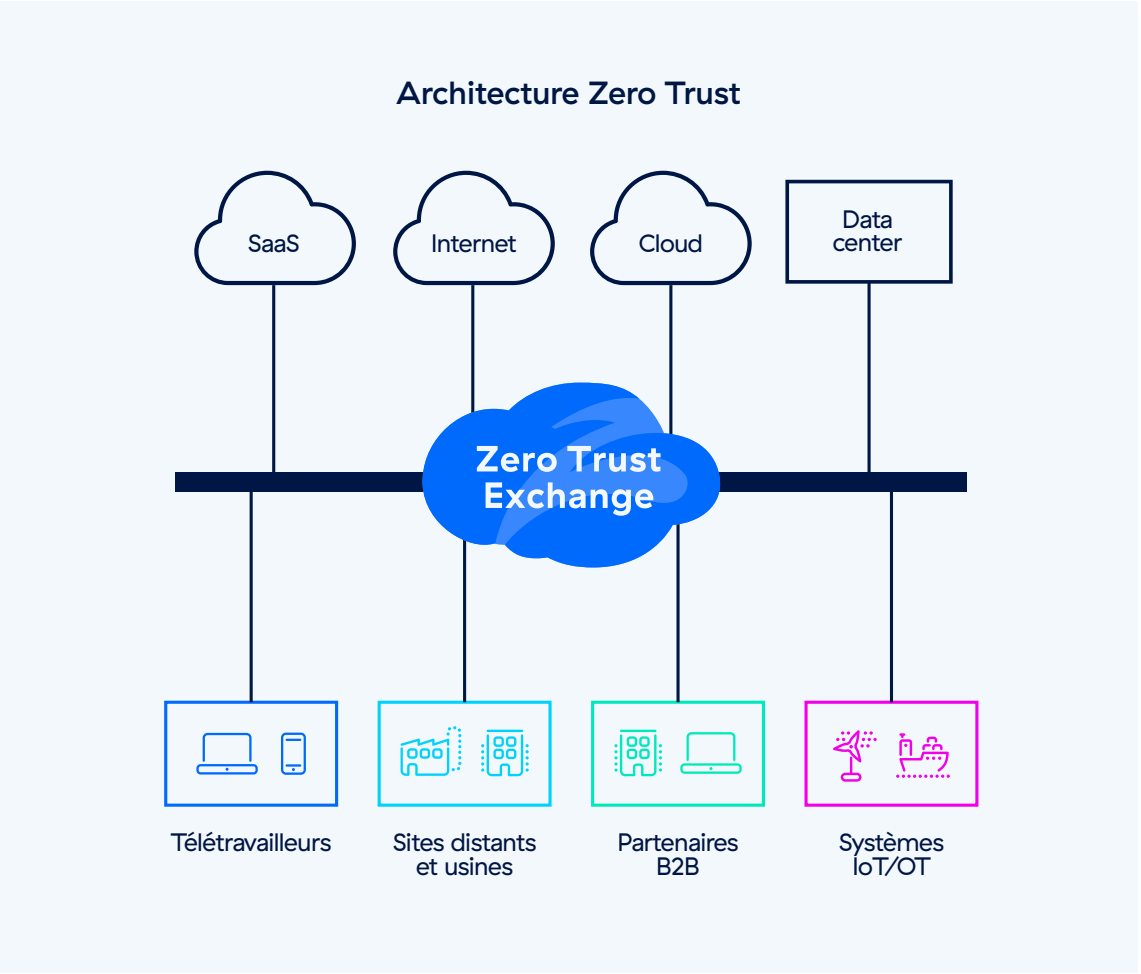
Bien que les VPN permettent depuis longtemps aux entreprises de se connecter à distance, les problèmes constants et croissants de sécurité de cette technologie vont rendre plus difficile la justification des dépenses sur le long terme. À présent que les entreprises s'accordent à penser sur le Zero Trust est l'architecture à privilégier pour la sécurité et la connectivité, elles investiront dans des initiatives Zero Trust afin de sécuriser les collaborateurs distants.

Comment Zscaler facilite le remplacement du VPN et l'adoption du Zero Trust

Les pare-feu traditionnels et les VPN génèrent une vaste surface d'attaque qui permet aux hackers de voir et cibler les ressources exposées. En positionnant les utilisateurs sur le réseau et en leur permettant d'accéder à n'importe quelle application présente, les approches traditionnelles donnent aux hackers un accès facile aux données sensibles. Elles rendent fastidieux de sécuriser l'accès ou le partage des ressources avec des fournisseurs, des sous-traitants et autres tiers. En outre, elles renchérissent les coûts et la complexité, et sont trop lentes pour satisfaire les besoins des collaborateurs distants modernes.

La plateforme Zscaler Zero Trust Exchange™, le plus vaste cloud de sécurité inline au monde, connecte en toute sécurité les utilisateurs, les instances, les dispositifs IoT/OT, et les partenaires B2B, sans besoin d'étendre l'accès au réseau.

Zscaler Private Access™ (ZPA™), composant essentiel de Zero Trust Exchange, fournit un accès direct aux applications privées dissimulées derrière la plateforme Zero Trust Exchange. Cette configuration permet de minimiser la surface d'attaque, de segmenter chaque connexion entre un utilisateur et une application, d'éliminer les déplacements latéraux, d'offrir une protection des applications privées, d'inspecter le trafic et de neutraliser les menaces de type « zero day ». Autant d'atouts pour renforcer votre posture de sécurité. Service cloud natif, ZPA peut être déployé en à peine quelques heures pour remplacer les outils d'accès à distance traditionnels tels que les VPN et les VDI.



Réseau Zero Trust

ZPA permet un accès granulaire et segmenté avec une connectivité sortante vers les applications et instances privées. En outre, ZPA propose un panel complet de services de contrôle d'accès, notamment une segmentation optimisée par IA des connexions entre les utilisateurs et les applications (avec des recommandations automatisées pour les politiques d'accès utilisateur et les segments d'applications), une segmentation des connexions entre instances, un accès à distance privilégié, le composant Private Service Edge, l'accès par navigateur et davantage.

Protection contre les cybermenaces

ZPA offre des capacités avancées de cyber-protection pour sécuriser votre entreprise. Il s'agit notamment de fonctionnalités de protection des applications qui s'appuient sur une inspection de sécurité pour déjouer les attaques applicatives les plus répandues et les vulnérabilités de type « zero day », ainsi que d'une technologie de leurre qui attire les hackers avec des applications factices et facilite la détection des menaces sophistiquées.

Protection des données

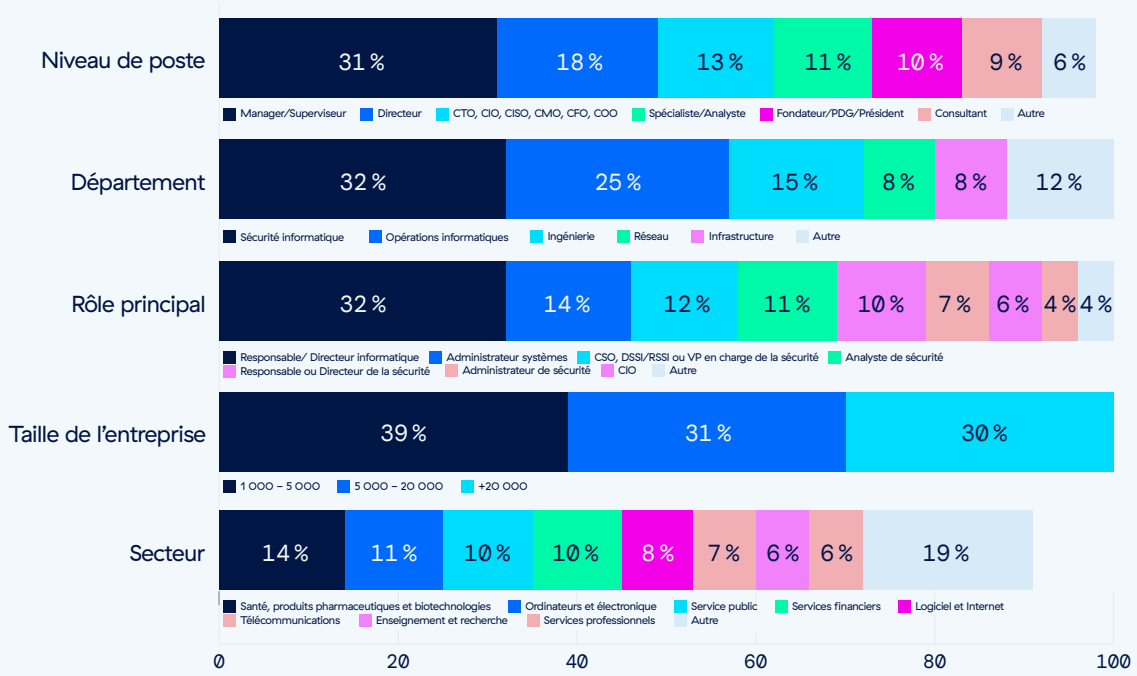
ZPA offre une protection globale des données et empêche la perte de données sur tous les canaux grâce à une prévention des pertes de données (DLP) Web, à une DLP sur les terminaux et à une fonction d'isolation du navigateur qui empêche les fuites de données par les utilisateurs vulnérables et les terminaux BYOD.

Bonnes pratiques pour juguler les risques liés aux VPN

- **Minimiser la surface d'attaque :** fournissez un accès direct aux applications, en garantissant que les applications et les utilisateurs sont invisibles depuis Internet, empêchant ainsi les hackers de les identifier et de les cibler pour obtenir un accès initial.
- **Prévenir la compromission initiale :** inspectez l'ensemble du trafic inline pour déjouer automatiquement les exploits de type « zero day », les malwares et autres menaces sophistiquées.
- **Neutraliser les accès non autorisés :** faites appel à une authentification multifacteur (MFA) robuste, à l'instar de mots de passe ou des jetons OTP, de données biométriques ou d'informations d'identification FIDO2 pour valider les demandes d'accès des utilisateurs. À l'inverse, les méthodes MFA faibles utilisent souvent des questions de réinitialisation de mot de passe.
- **Un accès sur la base du moindre privilège :** restreignez les autorisations pour les utilisateurs, le trafic, les systèmes et les applications sur la base de l'identité et du contexte : vous garantissez ainsi que seuls les utilisateurs autorisés peuvent accéder aux ressources approuvées (une sécurité supplémentaire en cas de compromission de l'authentification MFA ou de détournement d'identifiants).
- **Éliminer les déplacements latéraux :** connectez les utilisateurs directement aux applications, et non au réseau, afin de limiter le rayon d'action d'un incident potentiel et de maîtriser le risque de déplacement latéral des menaces.
- **Neutraliser les utilisateurs compromis et les menaces internes :** activez l'inspection et la surveillance inline afin de détecter les utilisateurs compromis ayant accès à votre réseau, à vos applications privées et à vos données.
- **Prévenir les pertes de données :** inspectez les données en mouvement et au repos pour contrer le détournement de données lors d'une attaque.
- **Déployer des défenses actives :** déployez des leurres et traquez quotidiennement les menaces pour neutraliser les attaques en temps réel.
- **Testez votre posture de sécurité :** procédez régulièrement à des évaluations de risques par des tiers et organisez des activités spécifiques en équipe pour identifier et traiter les lacunes de votre programme de sécurité. Demandez à vos fournisseurs de services et à vos partenaires technologiques d'en faire autant et partagez leurs informations avec votre équipe de sécurité.

Méthodologie et données démographiques

Ce rapport est basé sur les résultats d'une enquête approfondie menée en ligne en avril 2024 auprès de 647 professionnels de l'informatique et de la cybersécurité, afin d'identifier les 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 personnes interrogées sont aussi bien des décisionnaires techniques que des professionnels de la sécurité informatique, constituant un échantillon représentatif d'entreprises de différentes tailles diverses et actives dans de nombreux secteurs.



À propos de Zscaler

Zscaler accélère la transformation digitale et permet à ses clients 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 des données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossé à un écosystème de plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur www.zscaler.fr.

À propos de ThreatLabz

ThreatLabz est l'organisme de recherche en sécurité de Zscaler. Cette équipe experte est responsable de la traque de nouvelles menaces et s'assure de la protection optimale des milliers d'organisations qui utilisent la plateforme mondiale Zscaler. Au-delà des recherches sur les malwares et des analyses comportementales, l'équipe ThreatLabz s'investit dans la recherche et le développement de nouveaux prototypes qui assurent une protection avancée contre les menaces sur la plateforme Zscaler. Elle mène régulièrement des audits de sécurité interne pour s'assurer que les produits et l'infrastructure de Zscaler répondent aux normes de conformité de sécurité. ThreatLabz publie régulièrement des analyses approfondies sur les menaces nouvelles et existantes sur son portail, research.zscaler.com.

À propos de Cybersecurity Insiders

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

Notre approche consiste à élaborer 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 distinguer sur un marché très concurrentiel et à favoriser la visibilité de votre marque et votre positionnement en tant que leader d'opinion.

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

Explorez votre monde, en toute sécurité.

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients 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 des données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossé à un écosystème de plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.fr**.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr