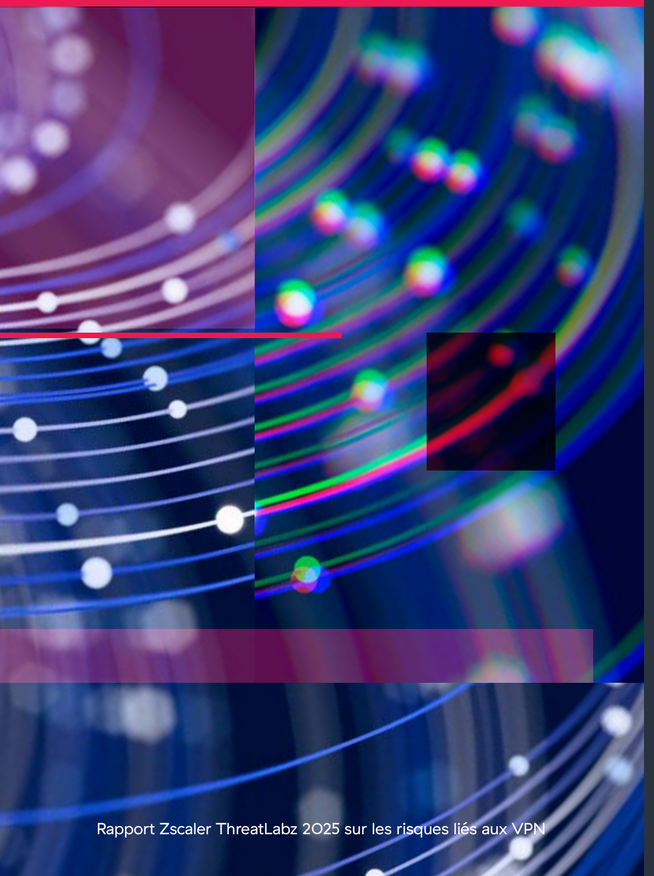
zscaler™ | Cybersecurity INSIDERS

Rapport Zscaler ThreatLabz 2025 sur les risques liés aux VPN

Sommaire



Note de synthèse

Le rapport Zscaler ThreatLabz 2025 sur les risques liés aux VPN offre un aperçu précis de l'évolution des risques associés aux réseaux privés virtuels (VPN). Il souligne l'urgence de migrer vers des architectures Zero Trust, en réponse à des entreprises qui s'efforcent de répondre de manière pérenne à leurs besoins en sécurité. Autrefois considéré comme essentiel pour les accès distants, le VPN est devenu une cible privilégiée des cybermenaces, passant du statut d'outil essentiel à celui de risque majeur pour la sécurité des entreprises. Ce rapport, qui s'appuie sur les observations de plus de 600 professionnels de l'informatique et de la sécurité, révèle un tournant crucial dans le paysage de la cybersécurité : plus de la moitié des entreprises interrogées ont subi des attaques imputables à des vulnérabilités de VPN au cours de la seule année écoulée, soulignant ainsi le besoin urgent pour une nouvelle approche adaptée aux environnements de travail hybrides actuels.

En 2025, le mécontentement des utilisateurs à l'égard des VPN traditionnels a été un catalyseur de changement : les entreprises reconnaissent désormais que le déploiement continu de patchs pour restaurer ces vulnérabilités est une course qu'elles ne peuvent plus gagner. Cette prise de conscience favorise l'adoption généralisée du modèle Zero Trust, qui promet un contrôle d'accès granulaire et réduit considérablement les risques de sécurité. 81 % des entreprises envisagent désormais de déployer des stratégies Zero Trust d'ici 2026, et 65 % prévoient de supprimer complètement leurs VPN sur cette même période. De plus, les frustrations opérationnelles, telles que la lenteur des connexions, les déconnexions fréquentes et la complexité des processus d'authentification, n'ont fait qu'ajouter à l'urgence, entraînant une forte demande pour des solutions Zero Trust qui assurent des accès fluides et sécurisés.

Toutes ces évolutions s'inscrivent dans un contexte de menaces optimisées par l'IA. En effet, l'essor des cyberattaques qui font appel à l'IA aura un impact sans précédent sur la sécurité des VPN. Les hackers vont de plus en plus tirer parti de l'IA pour détecter automatiquement les vulnérabilités des VPN, facilement identifiables par scan sur l'Internet public. Des techniques telles que le « password-spraying » (piratage par une utilisation de mots de passe communs) et le développement rapide d'exploits permettront aux acteurs malveillants de compromettre les identifiants d'accès au VPN à plus grande échelle. À une étape ultérieure de la chaîne d'attaque, les techniques d'évasion optimisées par IA compliqueront davantage la détection des intrusions via VPN en amont de tout dommage majeur. Les risques liés aux VPN ne feront donc que s'amplifier à mesure que les menaces basées sur l'IA se développeront, incitant les entreprises à adopter des mesures de sécurité proactives et accélérant la transition déjà en cours vers des solutions Zero Trust.

En reconnaissant ces changements, le rapport ThreatLabz ne se contente pas d'illustrer le déclin des VPN, qui sont passés du statut d'outils indispensables à celui de handicap, mais fournit également des informations décisionnelles aux entreprises qui tentent de s'y retrouver dans ce paysage en pleine mutation.

Principales conclusions

1. L'obsolescence des VPN s'accélère :

Pas moins de 65 % des entreprises prévoient de remplacer leurs services VPN au cours de l'année à venir, un chiffre qui progresse de 23 % par rapport à 2024. Cette tendance s'explique principalement par l'incapacité des VPN à répondre aux exigences de sécurité et de conformité des entreprises modernes : ces VPN accentuent les risques plutôt que de les juguler.

2. Les préoccupations liées aux cyberattaques et aux ransomwares exploitant les VPN sont croissantes :

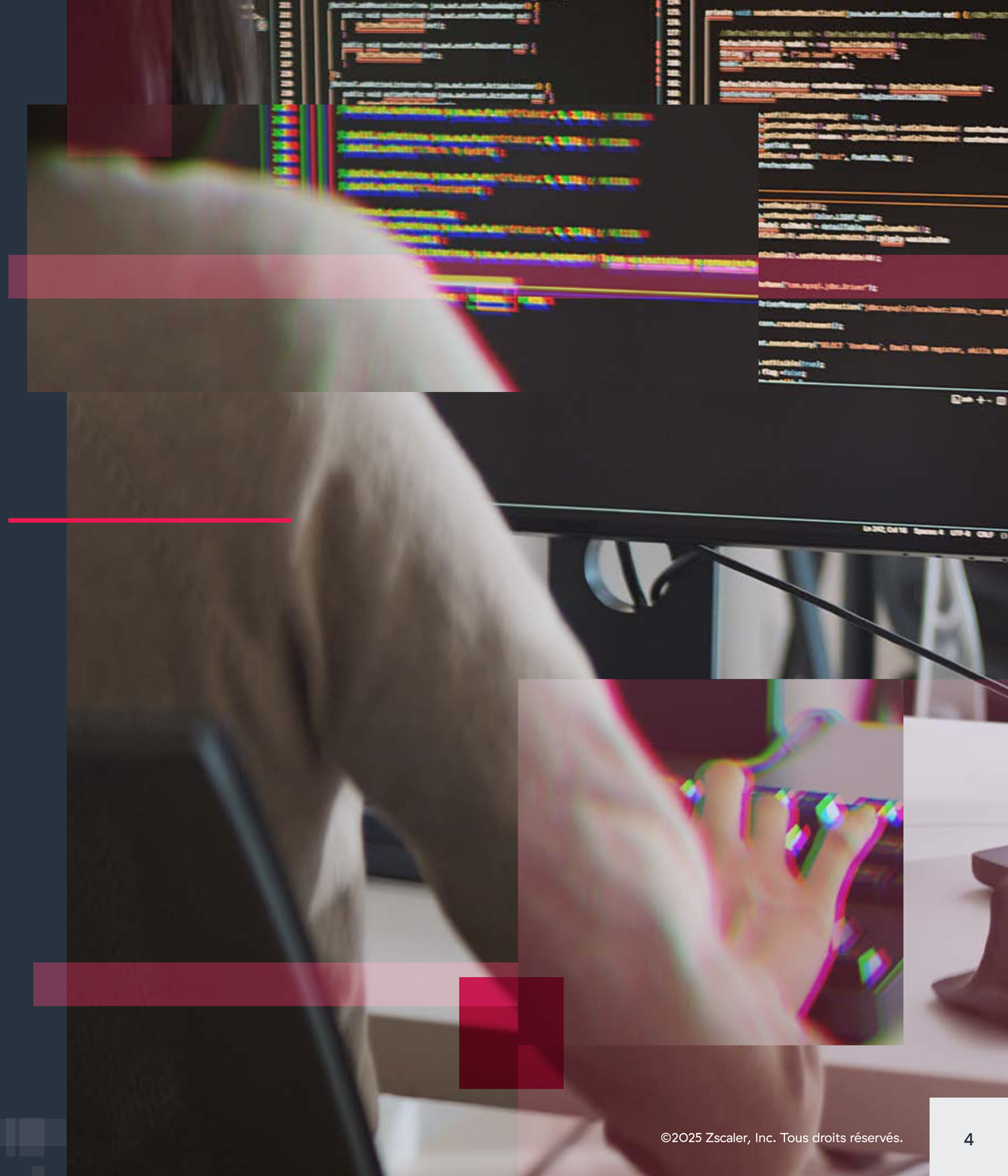
L'année dernière a été marquée par une augmentation inquiétante des cyberincidents liés aux vulnérabilités des VPN, 56 % des entreprises ayant signalé des violations de ce type, ce qui représente une hausse alarmante par rapport aux chiffres précédents. Par ailleurs, 92 % des personnes interrogées craignent que les vulnérabilités non corrigées des VPN débouchent directement sur des attaques de ransomware. Ces résultats confirment la tendance selon laquelle, face à la difficulté de restaurer les vulnérabilités à un rythme effréné, les entreprises ont besoin d'une refonte complète de leur sécurité afin de pallier ces failles critiques et d'atténuer les risques permanents liés à l'utilisation des VPN.

3. Le mécontentement des utilisateurs finaux invite à repenser la sécurité :

La frustration des utilisateurs face aux carences des VPN, qu'il s'agisse de performances atones ou de la complexité (voire dysfonctionnement) de l'authentification, influence de plus en plus les stratégies de sécurité des entreprises. Ce mécontentement des utilisateurs finaux encourage une transition vers des architectures Zero Trust qui offrent un accès sécurisé et permanent, sans les inconvénients traditionnels associés aux VPN.

4. Migrer du VPN vers le Zero Trust : du concept à la mise en œuvre

Reflet d'un changement stratégique majeur, 81 % des entreprises s'orientent activement vers le déploiement de frameworks Zero Trust dans l'année à venir. Cette transition est cruciale : le Zero Trust n'est plus considéré comme un idéal théorique, mais comme une nécessité pratique pour remplacer les VPN tout en renforçant la sécurité dans des environnements informatiques dynamiques et multisites.



Risques liés aux VPN : 81 % des entreprises passeront au Zero Trust d'ici 2026

Les VPN ont été conçus pour fournir un accès à distance, mais les temps ont changé, tout comme les hackers. Aujourd'hui, les VPN servent souvent de passerelle d'entrée aux attaques de ransomware, au vol d'identifiants et au cyberespionnage en raison de vulnérabilités qu'il est difficile de corriger rapidement, du modèle de confiance implicite qui fournit un accès complet au réseau et d'autorisations d'accès trop laxistes. Les vulnérabilités de sécurité constituent le principal défi lié aux VPN auquel sont confrontées les entreprises (selon 54 % des personnes interrogées), ce qui souligne le fait que les hackers exploitent régulièrement des failles non corrigées ou contournent les protections pour infiltrer les réseaux.

Les risques sont encore plus importants avec l'accès des tiers au VPN. 93 % des personnes interrogées s'inquiètent des backdoors introduites par les connexions VPN externes : en effet, les assaillants exploitent de plus en plus des identifiants de tiers pour pénétrer les réseaux sans être détectés. Il ne s'agit pas seulement d'un accès initial : les VPN peuvent donner lieu à des incidents plus dévastateurs. Contrairement aux solutions Zero Trust qui appliquent des politiques granulaires pour empêcher les déplacements au sein des réseaux, les VPN offrent un accès étendu, permettant aux hackers de se déplacer latéralement et d'élever leurs privilèges. Globalement, 71 % des personnes interrogées considèrent le déplacement latéral des menaces comme une préoccupation majeure, reconnaissant qu'il amplifie la portée et l'impact d'une violation.

Ces défis, associés à des préoccupations quotidiennes telles que la médiocrité des performances, la complexité de l'authentification et la fréquence des déconnexions, éclairent sur les raisons qui incitent les entreprises à délaisser les VPN au profit de modèles Zero Trust. Le rapport 2025 sur les risques liés aux VPN, basé sur les observations de 632 professionnels de l'informatique et de la cybersécurité, se propose de dresser un état des lieux de l'utilisation des VPN en 2025 afin de mieux appréhender les risques et les défis inhérents. Le rapport fournit également aux entreprises des recommandations de bonnes pratiques pour améliorer leur posture de cybersécurité et leur approche en matière d'accès à distance sécurisé.

Les conclusions de ce rapport proposent aux responsables informatiques et de la sécurité des observations factuelles sur les raisons de supprimer les VPN obsolètes et d'adopter une architecture Zero Trust moderne fournie depuis le cloud. Passer d'une confiance implicite à une validation continue de cette confiance n'est plus une option ; il s'agit désormais d'un impératif de sécuriser les entreprises multisites modernes, de simplifier les environnements informatiques et de garantir une expérience utilisateur fluide.

Préoccupations liées à la sécurité des VPN

Obsolescence des VPN : risques de sécurité et frustrations des utilisateurs

Les entreprises qui continuent à faire appel aux VPN pour leurs accès à distance s'exposent de plus en plus à des failles de sécurité, à des opérations peu efficaces et à un mécontentement croissant parmi les utilisateurs finaux. Cette réalité accentue le sentiment que les VPN appartiennent à une époque révolue en matière d'accès sécurisé.

Le principal défi, à savoir les risques liés à la sécurité et à la conformité, cité par 54 % des personnes interrogées, accentue la vulnérabilité critique des VPN face aux ransomwares, à l'élévation des privilèges et aux déplacements latéraux des menaces. Les hackers considèrent les VPN comme des maillons faibles à exploiter, tandis que les entreprises peinent à corriger ces systèmes obsolètes au rythme imposé par les menaces avancées.

La frustration des utilisateurs a atteint son paroxysme : 51 % des personnes interrogées identifient les performances médiocres des VPN (lenteur de la connexion, déconnexions et protocoles d'authentification fastidieux) comme un frein à la productivité. Les VPN restent un fardeau opérationnel, 41 % des personnes interrogées citant des difficultés de gestion et 37 % signalant leur coût de maintenance élevé. Ces chiffres illustrent à quel point les VPN sont devenus gourmands en ressources. Ils creusent les budgets informatiques et obligent les équipes à consacrer un temps inutile à des tâches de dépannage répétitives.

Exit les approches traditionnelles, place au Zero Trust

Un récent incident de sécurité rappelle de manière brutale à quel point les VPN sont vulnérables. En janvier 2025, un groupuscule de cyberespionnage chinois a exploité avec succès une faille de type « zero day » dans le VPN Pulse Secure d'Ivanti, obtenant un accès non autorisé aux réseaux de l'entreprise. Cette attaque, l'une des nombreuses visant la technologie VPN ces derniers mois, met en évidence les raisons pour lesquelles les entreprises ne peuvent plus se contenter des modèles d'accès traditionnels pour défendre leurs infrastructures.

Face à ces défis, de nombreux fournisseurs de VPN traditionnels ont commencé à commercialiser des machines virtuelles présentes dans le cloud en tant

S'affranchir des VPN n'est plus une option, mais un impératif immédiat. Les entreprises doivent passer à des frameworks Zero Trust qui fournissent un accès sur la base du moindre privilège et une segmentation granulaire des accès. Ces architectures fournies depuis le cloud contribuent à réduire la surface d'attaque des entreprises, à améliorer l'expérience utilisateur et à simplifier l'environnement informatique, trois avantages que les VPN ne peuvent tout simplement pas offrir.

Quels sont, selon vous, les défis majeurs de vos outils VPN ?

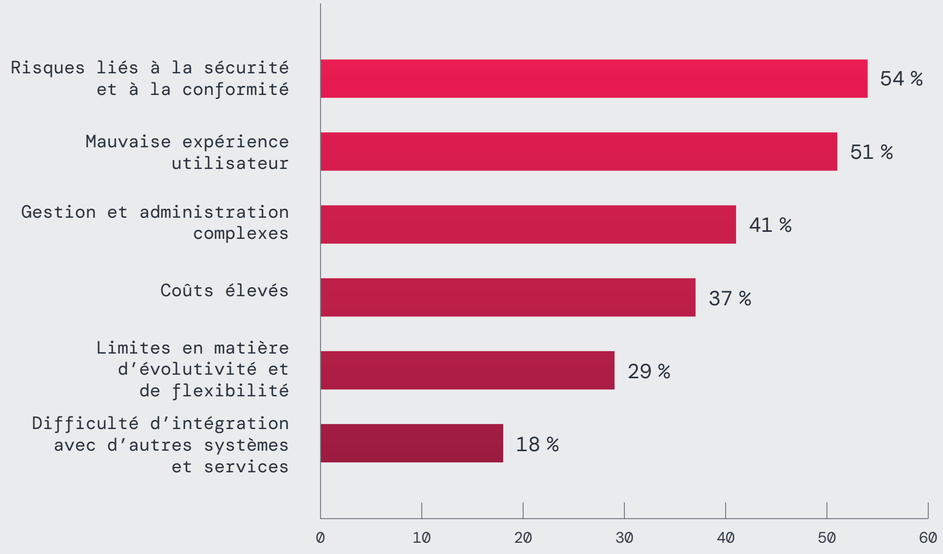


Illustration 1 : défis majeurs du VPN

que solutions Zero Trust. Cependant, les services VPN hébergés dans le cloud restent fondamentalement les mêmes d'un point de vue architectural : il s'agit de services connectés à Internet avec une adresse IP publique qui peut être compromise. Exemple concret : le secteur a récemment connu un bond du volume de scans ciblant plus de vingt mille adresses IP VPN publiques hébergées par l'un des plus grands fournisseurs de sécurité. Ce type d'activité indique généralement que des hackers se préparent à exploiter des vulnérabilités encore inconnues dans les ressources VPN ciblées. En d'autres termes, si vous êtes accessible, vous êtes vulnérable. C'est pourquoi, d'un point de vue de l'architecture, une technologie VPN basée sur le cloud ne peut pas respecter les principes du Zero Trust, quoique prétende son fournisseur.

Ransomware et VPN : des risques qui se cumulent

Les groupuscules de ransomware continuent d'exploiter les vulnérabilités des VPN avec une précision dévastatrice, en exploitant à la fois les vulnérabilités de type « zero day » et les faiblesses connues, avant que les entreprises ne puissent déployer des patchs de sécurité. Les VPN sont devenus une proie facile pour les hackers en raison de leur adoption généralisée et de leur dépendance à des modèles de confiance obsolètes.

Dans l'ensemble, 92 % des personnes interrogées ont exprimé leur vive inquiétude face aux ransomwares qui ciblent les vulnérabilités non corrigées des VPN, soulignant un besoin critique pour des mécanismes de protection plus robustes. Ces données expliquent pourquoi les VPN sont désormais considérés comme des risques plutôt que comme des outils fiables permettant de maîtriser les cyber-risques modernes.

Des exemples du terrain viennent confirmer ces craintes. En janvier 2023, plusieurs entreprises du secteur de la santé aux États-Unis ont été victimes d'une attaque de ransomware exploitant une vulnérabilité non corrigée de Citrix NetScaler (CVE-2023-4966). Cette faille a permis aux assaillants d'infiltrer les systèmes, de perturber le fonctionnement des hôpitaux, de verrouiller des dossiers des patients et de contraindre les établissements à modifier leurs soins d'urgence critiques, les résultats de cette vulnérabilité qui n'a pas été corrigée à temps. Cet incident illustre ce risque omniprésent que représentent les VPN non corrigés. Les acteurs malveillants recherchent régulièrement des systèmes exposés, s'assurant de pouvoir exploiter les vulnérabilités avant que les entreprises n'appliquent les patchs nécessaires, ce qui expose ces dernières à des risques de compromission, de perturbation opérationnelle et de pertes financières.

Les entreprises doivent sortir de ce cercle infernal de patching pour adopter des stratégies de défense proactives, adaptées à l'évolution des menaces. Les frameworks Zero Trust privilégient un contrôle d'accès basé sur l'identité et la vérification continue du niveau de confiance, ce qui réduit considérablement le risque d'attaque par ransomware, même lorsque les vulnérabilités ne sont pas corrigées. Les systèmes de détection automatisés et les politiques dynamiques limitent davantage les violations potentielles, empêchant les hackers de se déplacer latéralement ou d'élever leurs privilèges.

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

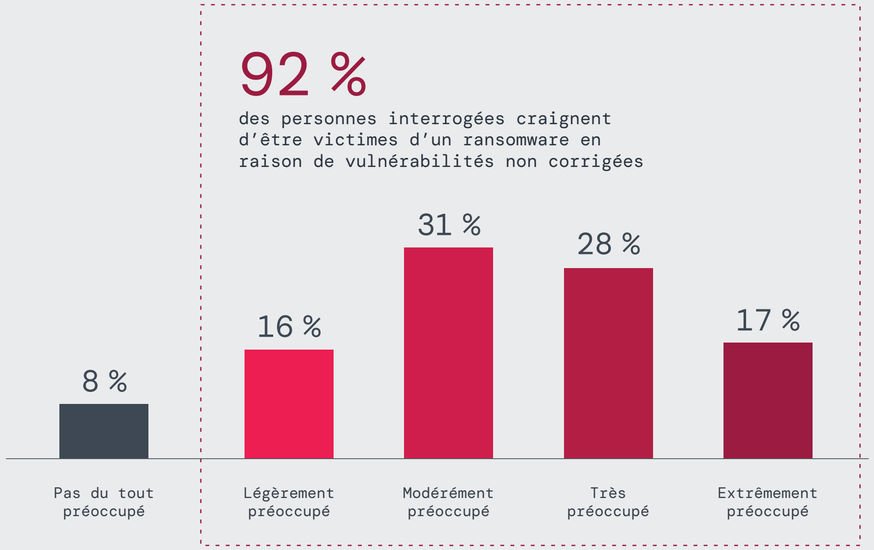


Illustration 2 : Préoccupations vis-à-vis des attaques de ransomware

VPN et déplacement latéral : un impact plus large des incidents

Au-delà de permettre une compromission initiale par le biais de ransomwares et autres menaces, les VPN facilitent le déplacement latéral de ces menaces, une technique d'attaque redoutable. Les hackers exploitent l'accès étendu qu'offrent les VPN pour élever leurs privilèges et s'infiltrer plus profondément dans les réseaux cibles, souvent avec des conséquences dévastatrices.

71 % des personnes interrogées ont exprimé un certain niveau de préoccupation à l'égard de ce risque, 32 % d'entre elles se déclarant très préoccupées. Ces inquiétudes sont justifiées, car les VPN accordent généralement un accès étendu au réseau, ce qui permet aux hackers de se déplacer sans être détectés, d'élever leurs privilèges et d'exfiltrer des données sensibles une fois à l'intérieur du réseau.

En septembre 2024, des hackers ont exploité plusieurs vulnérabilités de type « zero day » dans la solution Cloud Service Appliance (CSA) d'Ivanti, notamment CVE-2024-8963 et CVE-2024-8190, pour pirater plusieurs entreprises, comme l'ont confirmé la Cybersecurity and Infrastructure Security Agency (CISA) et le FBI. Les hackers ont contourné les mesures de contrôle en place, exécuté des commandes arbitraires, collecté des informations d'identification et implanté des scripts web shells, ce qui leur a permis de se déplacer latéralement au sein des réseaux. Malgré les incidents de sécurité antérieurs impliquant les VPN Ivanti, ces nouveaux exploits démontrent que l'application de correctifs ou la refonte des solutions VPN traditionnelles ne permettent toujours pas de remédier aux failles de sécurité fondamentales inhérentes aux modèles d'accès à distance au réseau.

Dans quelle mesure craignez-vous que des hackers se déplacent latéralement sur votre réseau suite à une compromission de VPN ?

89 % des personnes interrogées sont préoccupées par les déplacements latéraux des assaillants

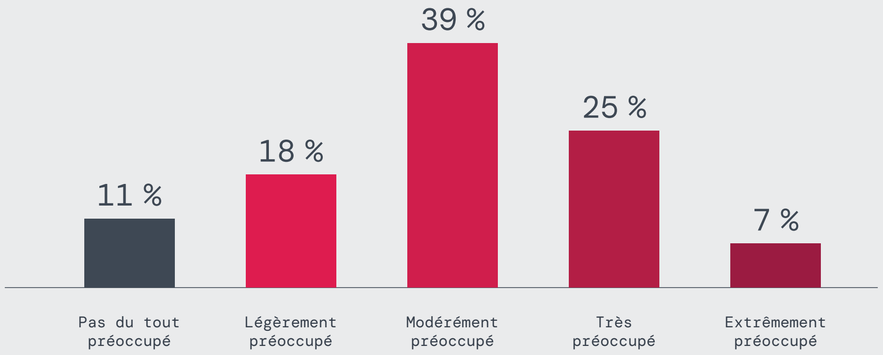


Illustration 3 : Préoccupations des entreprises concernant le déplacement latéral sur le réseau en cas de compromission d'un VPN

Pour juguler ces risques, les entreprises doivent passer d'un accès par VPN à un accès réseau Zero Trust (ZTNA) et à une segmentation stricte. Contrairement aux VPN, qui accordent aux utilisateurs un accès réseau étendu, le ZTNA fournit un accès au niveau des applications en fonction de l'identité et du contexte, garantissant que les utilisateurs ne peuvent accéder qu'aux ressources spécifiques dont ils ont besoin. Cette approche empêche les déplacements latéraux même en cas d'accès initial, réduisant ainsi considérablement la surface d'attaque et le rayon d'action potentiel des incidents. De plus, la micro-segmentation du réseau renforce la sécurité en cloisonnant les systèmes critiques et en empêchant toute communication non autorisée entre les ressources compromises et celles sécurisées.

Vulnérabilités CVE liées aux VPN de 2020 à 2025 : des vulnérabilités plus graves

Aucun logiciel n'est à l'abri de failles de sécurité, et il ne faut pas s'attendre à ce qu'il le soit. Cependant, dans le cas de la technologie VPN, les vulnérabilités, en particulier les menaces de type « zero day », peuvent être particulièrement dommageables. En effet, les acteurs malveillants peuvent facilement identifier les infrastructures VPN vulnérables et les pirater avant qu'un correctif ne soit publié ou appliqué. Le signalement des CVE est une approche pertinente, car cet effort communautaire aide les fournisseurs et les clients à suivre les bonnes pratiques et à améliorer leurs pratiques de cybersécurité, grâce à l'application de correctifs et à la divulgation des vulnérabilités. La manière dont ces CVE sont découvertes et les informations qu'elles contiennent reflètent l'évolution du paysage des menaces.

Zscaler ThreatLabz a analysé 411 vulnérabilités CVE liées aux VPN de 2020 à 2025, telles que signalées dans le programme CVE de MITRE. Les résultats indiquent que les vulnérabilités des VPN se sont progressivement développées au cours de la première moitié de cette décennie. Ces CVE couvrent un large éventail de failles des VPN, de l'exploitation d'interfaces de gestion Web via des injections de commandes et des validations de données malveillantes en entrée, aux défaillances cryptographiques et aux attaques DoS et DDoS. Les vulnérabilités VPN récentes ne manquent pas, et beaucoup d'entre elles ont déjà donné lieu à des failles de sécurité majeures.

Nombre de ces CVE sont critiques. En 2024, par exemple, 60 % des 83 vulnérabilités VPN signalées par le NIST affichaient un score CVSS de gravité élevée ou critique. Parallèlement, les vulnérabilités d'exécution de code à distance (RCE), qui permettent aux hackers d'exécuter des commandes arbitraires et potentiellement de compromettre le système, constituaient les CVE de VPN les plus courantes. Autrement dit, loin d'être anodines, la majorité des CVE de VPN sur l'année écoulée ont rendu leurs utilisateurs extrêmement vulnérables à des exploits relativement simples à réaliser. De plus, nombre de ces CVE étaient des exploits de type « zero day ». Si les CVE de 2025 sont encore peu nombreuses en ce début d'année, des vulnérabilités majeures ont déjà été révélées, telles que deux exploits de type « zero day », CVE-2025-0282 et CVE-2025-0283.

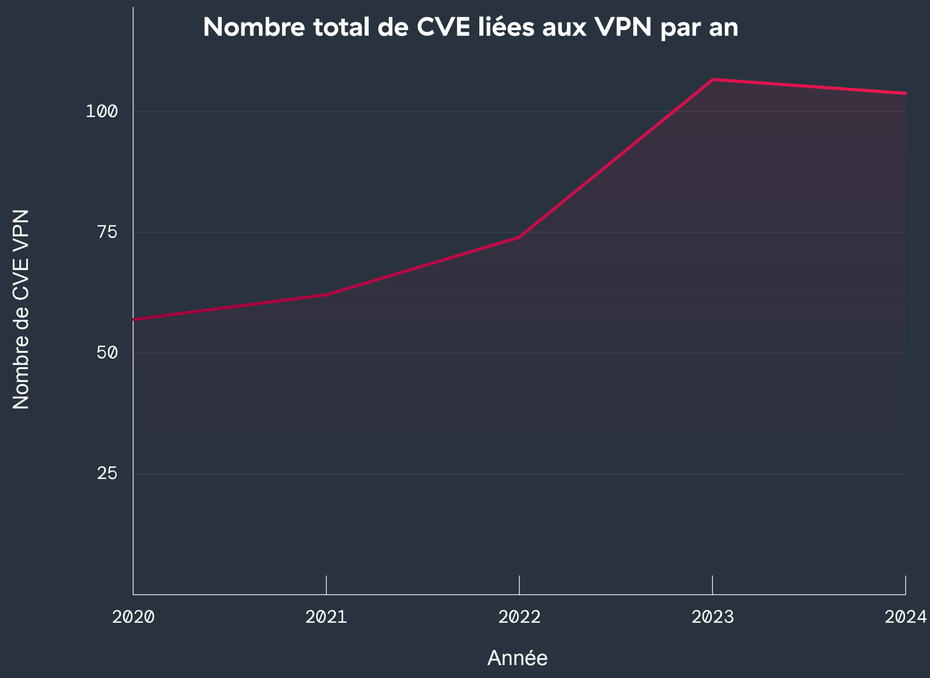


Illustration 4 : Nombre total de CVE VPN pour chaque année, de 2020 à 2024

1. Le RCE demeure la principale menace

- **Observation :** les vulnérabilités RCE (exécution de code logiciel à distance) sont en tête de liste sur les quatre années, avec 32 cas rien qu'en 2024. Le RCE est associé à 149 CVE, en incluant les données de 2025, ce qui en fait le type de vulnérabilité le plus fréquent et le plus critique.
- **Conséquence :** les vulnérabilités RCE permettent aux hackers d'exécuter des commandes arbitraires sur les dispositifs VPN, ce qui peut entraîner une compromission intégrale des systèmes. Les entreprises doivent se concentrer en priorité sur l'application de correctifs et la sécurisation des systèmes vulnérables à ces exploits.

2. L'élévation des privilèges progresse régulièrement au fil du temps

- **Observation :** le nombre de CVE qui donnent lieu à une élévation de privilèges est en constante évolution (66,7 %), culminant en 2024 avec 20 vulnérabilités.
- **Conséquence :** les hackers exploitent de plus en plus les failles des VPN pour élever leurs privilèges et prendre le contrôle de l'administration de systèmes. Les entreprises doivent sécuriser leurs configurations système et strictement encadrer les accès privilégiés.

3. Les vulnérabilités de déni de service (DoS) bondissent de 200 %

- **Observation :** les CVE liés au DoS ont triplé, passant de 9 en 2020 à 27 en 2024, pour devenir le deuxième type de CVE ayant le plus d'impact ces dernières années, avec 85 CVE au total, données de 2025 incluses.
- **Conséquence :** les attaques DoS gagnent en sophistication, faisant des systèmes VPN des cibles privilégiées pour perturber les opérations. Les entreprises devraient adopter des mesures de limitation de débit et de régulation du trafic pour maîtriser ces risques.

4. Les fuites d'informations sensibles sont plus rares, mais demeurent critiques

- **Observation :** bien que relativement moins courantes, avec 41 CVE au total, les vulnérabilités liées à la fuite d'informations sensibles exposent des identifiants, des clés de chiffrement et des données utilisateur critiques.
- **Conséquence :** l'impact est particulièrement préjudiciable en matière de confidentialité et de conformité. Les entreprises doivent appliquer un chiffrement robuste, des pratiques de codage sécurisé et une surveillance du trafic afin de détecter et de prévenir les fuites de données.

5. Le nombre de vulnérabilités liées au contournement de l'authentification est en constante augmentation

- **Observation :** les incidents de contournement de l'authentification ont été relativement peu nombreux, mais constants, passant de 4 en 2020 à un pic de 6 en 2023, puis à 4 vulnérabilités en 2024, pour un total de 30 CVE sur la période étudiée.
- **Conséquence :** les assaillants ciblent les failles de l'authentification multifactorielle (MFA) et des processus de connexion pour usurper l'identité des utilisateurs. Les entreprises doivent renforcer leurs processus de MFA et surveiller les comportements anormaux de connexion.

Principales tendances : types d'impact des CVE

Afin de comprendre les dommages potentiels de ces vulnérabilités si elles sont exploitées, ThreatLabz a évalué les CVE de VPN sur 5 catégories d'attaques : exécution de code à distance (RCE), élévation de privilèges, fuite d'informations, déni de service (DoS) et contournement de l'authentification. Certaines catégories regroupent des profils distincts d'attaques, mais néanmoins étroitement liés : par exemple, le contournement de l'authentification inclut les attaques qui peuvent contourner l'authentification à deux ou plusieurs facteurs, ainsi que celles qui contournent les mesures d'authentification de base. En général, la correction de toute vulnérabilité RCE doit être une priorité pour les entreprises.

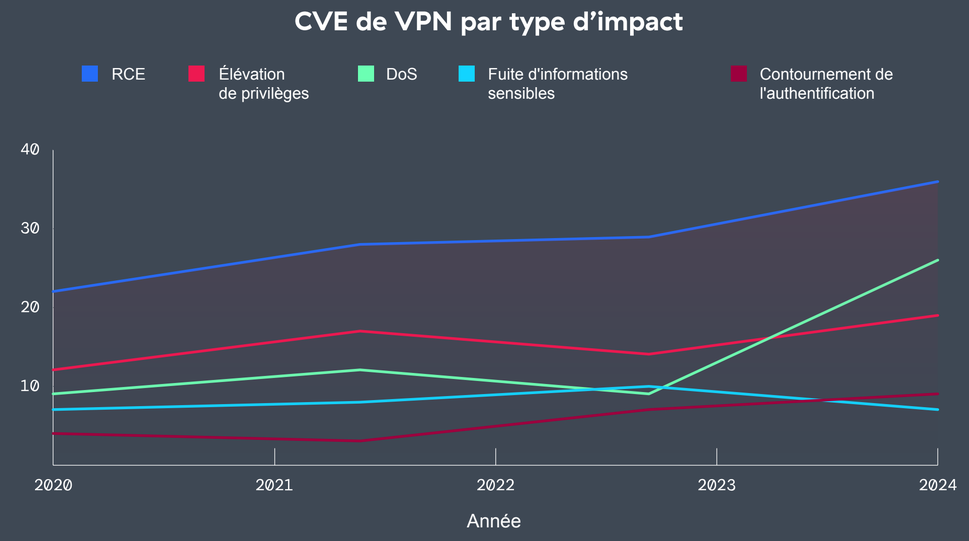


Illustration 5 : Type d'impact des CVE de VPN de 2020 à 2024, couvrant les RCE, l'élévation des privilèges, les DoS, les fuites d'informations sensibles et le contournement de l'authentification

Principales tendances : vulnérabilités critiques des VPN

Au-delà des types d'impact, ThreatLabz a également analysé la gravité des CVE de VPN pour chaque année. **Globalement, ThreatLabz a observé une augmentation de 38,9 % de ces CVE présentant des scores CVSS de gravité ÉLEVÉE ou CRITIQUE entre 2020 et 2024.** En effet, 66,3 % de tous les CVE en 2024 relevaient d'une gravité ÉLEVÉE ou CRITIQUE, ce qui indique un impact potentiellement grave pour les entreprises lorsque ces CVE sont exploités avant d'être corrigés. De plus, ThreatLabz a analysé les tendances critiques des différents types de vulnérabilités représentées dans les données CVE. Cela devrait aider les entreprises à mieux se défendre contre l'évolution des menaces liées aux VPN.

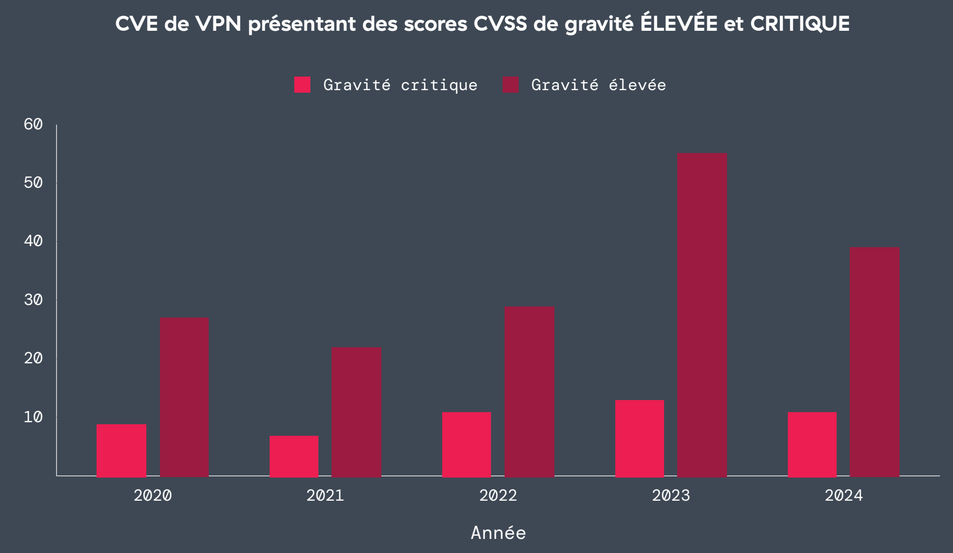


Illustration 6 : volume de CVE de VPN avec des scores CVSS de gravité ÉLEVÉE et CRITIQUE de 2020 à 2024

1. Compromission croissante des interfaces de gestion Web

- **Tendance :** les vulnérabilités d'injection de commandes et de validation de données malveillantes en entrée ont progressé de manière constante, ce qui témoigne de l'intérêt croissant des hackers pour les portails d'administration et de gestion, tant du point de vue des administrateurs que des utilisateurs finaux. De par leur architecture, ces interfaces sont exposées à Internet et sont susceptibles d'être compromises par des acteurs malveillants.
- **Escalade :** déjà présentes en 2020–2021, ces vulnérabilités se sont considérablement intensifiées à partir de 2022, suggérant que les hackers considèrent ces interfaces de gestion comme des cibles attrayantes et accessibles, notamment en raison de pratiques à risque en matière de codage et de sécurité.

2. Authentification généralisée et contournements de l'authentification multifacteur

- **Tendance :** les attaques ciblant spécifiquement les méthodes d'authentification, notamment les contournements de la MFA, le détournement de sessions et la gestion incorrecte de sessions, progressent de manière régulière.
- **Escalade :** les années précédentes (2020–2021) ont principalement donné lieu à des contournements d'authentification plus simples. De 2023 à 2025, ceux-ci ont évolué vers des attaques plus avancées, automatisées et persistantes visant explicitement les faiblesses de l'authentification multifactorielle, ce qui témoigne de la volonté des hackers de contourner les mesures de sécurité renforcées.

3. Progression des exploits d'élévation des privilèges en local

- **Tendance :** les vulnérabilités d'élévation des privilèges en local sont devenues plus fréquentes et graves.
- **Escalade :** ce qui n'était au départ que des erreurs de configuration mineures en 2020–2021 s'est intensifié en 2024–2025 pour donner lieu à des méthodes d'élévation des privilèges plus sophistiquées, telles que le détournement de DLL, qui donnent aux hackers un accès système plus profond.

4. Sophistication croissante des attaques DoS et DDoS

- **Tendance :** les attaques DoS ont évolué, passant de la simple paralysie de ressources (2020–2021) à des techniques sophistiquées d'amplification des DDoS (2024–2025).
- **Escalade :** les hackers, qui se contentaient auparavant de perturber le trafic à l'aide de paquets mal formatés, ont désormais recours à des attaques amplifiées et plus sophistiquées, reflétant une escalade stratégique visant à maximiser les perturbations opérationnelles.

5. Défaillances de chiffrement persistantes et plus nombreuses

- **Tendance :** les problématiques de chiffrement, à l'instar d'une validation incorrecte des certificats, d'une divulgation de clés et d'une vérification TLS insuffisante, se sont considérablement intensifiées.
- **Escalade :** à partir de 2022, une augmentation notable des vulnérabilités de chiffrement a été observée, avec un pic en 2024–2025 et des failles de gravité élevée. Cette hausse démontre l'intérêt stratégique des adversaires pour tirer parti de faiblesses liées au chiffrement afin de compromettre la confidentialité des VPN.

Préoccupations liées à la sécurité des VPN (suite)

Les défis liés à la segmentation

Face au risque que représentent les déplacements latéraux, de nombreuses entreprises tentent de limiter la propagation des attaques par le biais de la segmentation. Bien qu'il s'agisse d'un mécanisme de défense essentiel pour réduire la surface d'attaque, sa mise en œuvre est souvent complexe.

L'enquête met en évidence des défis, avec 51 % des entreprises anticipant ou subissant une complexité en matière de configuration de cette segmentation. En outre, 39 % d'entre elles font état d'un déficit d'expertise et de ressources, tandis que 24 % sont confrontées à des performances atones, ce qui indique que les architectures réseau existantes sont mal outillées pour permettre ces contrôles d'accès granulaires requis par les environnements informatiques actuels.

Les défis liés à la segmentation ont joué un rôle notable dans l'attaque de ransomware contre MGM Resorts en 2023, au cours de laquelle les hackers ont obtenu un accès initial grâce à des techniques d'ingénierie sociale, pour ensuite se déplacer latéralement en raison d'une segmentation insuffisante. Cet incident a lourdement perturbé les opérations de l'hôtel, les distributeurs automatiques de billets et les systèmes de jeux du casino, causant à la société un préjudice estimé à 100 millions de dollars. Ce cas montre comment une segmentation déficiente permet aux hackers de se déplacer d'un système critique à un autre, amplifiant ainsi l'impact d'une intrusion initiale.

Pour remédier à ces carences, les entreprises doivent adopter des modèles de segmentation basés sur le cloud et axés sur l'identité, qui simplifient l'application des politiques et réduisent les opérations manuelles. Contrairement à une segmentation réseau traditionnelle, qui repose sur des règles de pare-feu et des configurations VLAN complexes, une approche Zero Trust permet une segmentation dynamique basée sur l'identité de l'utilisateur, la posture de l'appareil et des évaluations de risques en temps réel. Ainsi, seuls les utilisateurs autorisés peuvent accéder à des applications spécifiques tout en préservant la sécurité du réseau dans son ensemble.

Quelles sont les problématiques rencontrées par votre entreprise lors de la mise en œuvre de la segmentation ?

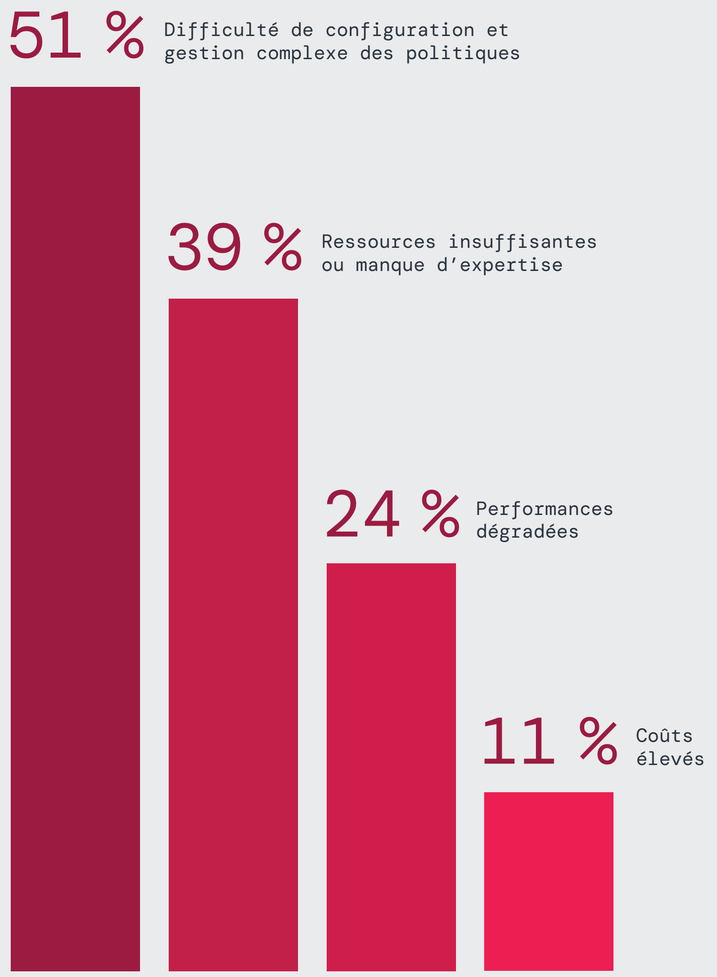


Illustration 7 : Principaux défis auxquels les entreprises sont confrontées lors de la mise en œuvre de la segmentation

Les VPN accentuent les risques de cybersécurité lors des fusions et acquisitions

Au-delà des défis de sécurité quotidiens, les transitions informatiques majeures, notamment suite à des fusions et acquisitions d'entreprises, induisent des risques supplémentaires et élargissent les surfaces d'attaque. Ces transitions impliquent souvent la fusion de réseaux, d'applications et d'identités disparates, ce qui peut s'accompagner de vulnérabilités, d'erreurs de configuration et de fonctionnalités de sécurité héritées et peu efficaces.

Près des deux tiers (64 %) des personnes interrogées se disent préoccupées par les cybermenaces lors de fusions et acquisitions, et reconnaissent les failles de sécurité qu'elles entraînent lors des intégrations informatiques.

Le piratage de données subi par Capita en 2023 en est un parfait exemple : des assaillants ont exploité les failles de sécurité suite à une acquisition d'entreprise pour obtenir un accès non autorisé à des données sensibles. L'incident est imputable à un manque d'harmonisation des politiques de sécurité entre les entités fusionnées, ce qui a permis aux acteurs malveillants de se déplacer latéralement vers le réseau nouvellement intégré. Cet incident souligne à quel point des contrôles de sécurité incohérents, l'accès VPN traditionnel et les environnements non segmentés créent des conditions propices aux cyberattaques lors des fusions/acquisitions.

Pour maîtriser ces risques lors de fusions et acquisitions, les entreprises doivent auditer leur cybersécurité, appliquer un accès sur la base du moindre privilège et segmenter leur infrastructure. Contrairement aux modèles d'accès basés sur un VPN, le Zero Trust empêche que les environnements informatiques qui doivent fusionner héritent de droits d'accès étendus, réduisant ainsi efficacement le risque de déplacement latéral et d'élévation des privilèges. En remplaçant les VPN et les défenses basées sur le périmètre par des contrôles d'accès basés sur l'identité et qui valident chaque demande d'accès, les entreprises sécurisent leurs environnements informatiques existants et ceux nouvellement intégrés.

Êtes-vous préoccupé par la vulnérabilité de votre entreprise aux cyberattaques suite à une fusion/acquisition ?

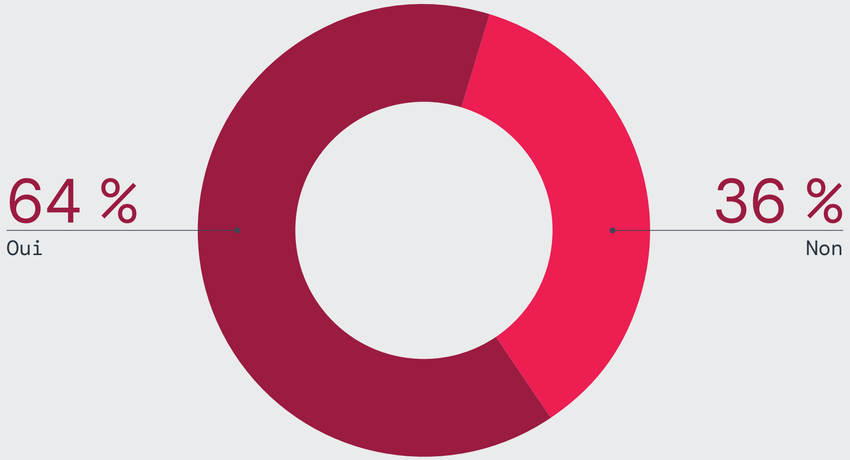


Illustration 8 : Préoccupations des entreprises concernant les cyberattaques suite à une fusion ou une acquisition

Accès de tiers par VPN : une backdoor pour les hackers

L'accès de tiers est devenu l'un des points d'entrée à disposition des assaillants. De par leur conception, les VPN traditionnels offrent un accès réseau étendu suite à l'authentification, étendant ce privilège aux fournisseurs et partenaires externes. Cette pratique crée des zones d'ombre que les hackers sont prompts d'exploiter. Ceux-ci peuvent tirer parti d'identifiants volés ou faibles, d'erreurs de configuration et de vulnérabilités non corrigées pour pirater ces connexions jugées fiables. Avec 93 % des personnes interrogées exprimant des inquiétudes concernant les vulnérabilités liées aux backdoors, l'accès de tiers représente une bombe à retardement pour les entreprises qui font appel à des modèles d'accès statiques basés sur la confiance.

Cette inquiétude est d'ailleurs parfaitement fondée. En août 2024, Enterprise Financial Group (EFG) a été victime d'une importante violation de données qui a exposé les informations personnelles de près de 20 000 clients. L'exaction a été attribuée à des vulnérabilités dans le VPN tiers qu'utilisait EFG, que les hackers ont exploitées pour infiltrer le réseau et accéder à des données sensibles. Cet incident souligne à quel point les VPN de tiers créent des failles de sécurité que les hackers peuvent utiliser pour s'introduire dans les réseaux d'entreprise.

Les entreprises doivent commencer par auditer les accès de tiers par VPN et appliquer des politiques de contrôle plus strictes, telles qu'un accès limité dans le temps, une inspection de bout en bout du trafic (de l'appareil à l'application) et une authentification adaptative. La transition vers un modèle Zero Trust permettra d'appliquer un accès spécifique à chaque application, garantissant que les partenaires externes ne disposent que d'un accès minimal nécessaire. De plus, une surveillance continue et des politiques basées sur les risques peuvent considérablement atténuer les vulnérabilités liées aux tiers.

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

93 % Des personnes interrogées sont préoccupées par le fait que des accès par VPN de tiers puissent servir de backdoor vers le réseau d'entreprise

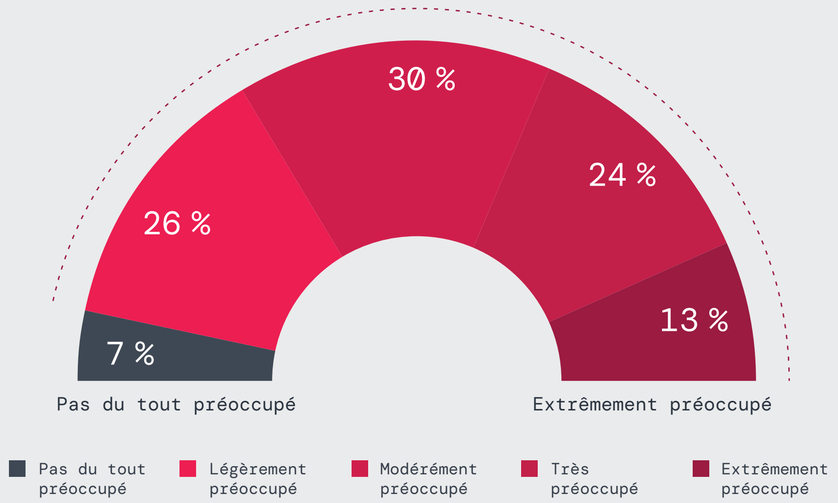


Illustration 9 : Préoccupations des entreprises concernant les accès de tiers par VPN qui facilitent les cyberattaques

Défis et failles des mesures de protection traditionnelles

Les outils traditionnels rendent les applications privées plus vulnérables

La sécurisation des applications privées contre des menaces Web de plus en plus sophistiquées, telles que les ransomwares, le vol d'identifiants et l'utilisation malveillante d'API, est devenue une priorité pour les entreprises modernes. Pourtant, nombre d'entre elles continuent de faire appel à des outils obsolètes, peu adaptés pour contrer les menaces actuelles.

Selon l'enquête, les pare-feux (84 %), les pare-feux d'applications Web (58 %) et les VPN (43 %) restent les principaux moyens de défense des entreprises contre les attaques Web. Cependant, les hackers contournent de plus en plus ces outils, en exploitant les dispositifs sans patchs, les erreurs de configuration et les carences des modèles de sécurité périmétrique, démontrant ainsi que ces défenses traditionnelles peinent à juguler les menaces modernes.

De récentes violations de sécurité mettent en évidence les failles de ces défenses basées sur le périmètre. En août 2024, un groupe de pirates informatiques chinois, baptisé Salt Typhoon, a infiltré des opérateurs américains de télécommunications, dont AT&T et Verizon, en exploitant des vulnérabilités dans des périphériques réseau et des routeurs sans patchs. Cette attaque a compromis les métadonnées sensibles de plus d'un million d'utilisateurs, démontrant que des cybercriminels sophistiqués peuvent contourner les mesures de sécurité traditionnelles telles que les pare-feux et les VPN.

La seule solution viable pour protéger efficacement les applications privées consiste à s'affranchir des défenses obsolètes basées sur le périmètre et à adopter des modèles d'accès Zero Trust. Les architectures Zero Trust éliminent toute dépendance à une sécurité basée sur le réseau, permettant aux utilisateurs de se connecter directement aux applications dans le cadre de politiques d'accès granulaire, appliquées de manière stricte et basées sur le moindre privilège. Contrairement aux pare-feu et aux VPN, les architectures Zero Trust permettent aux utilisateurs de se connecter directement aux applications grâce à un accès granulaire fondé sur le principe du moindre privilège. Cette approche déjoue les tentatives d'accès non autorisées et prévient les déplacements latéraux, le détournement de sessions et le vol d'identifiants, autant de tactiques couramment utilisées par les hackers pour contourner les défenses traditionnelles basées sur le périmètre.

Quels produits utilisez-vous pour protéger vos applications privées contre les attaques Web ?

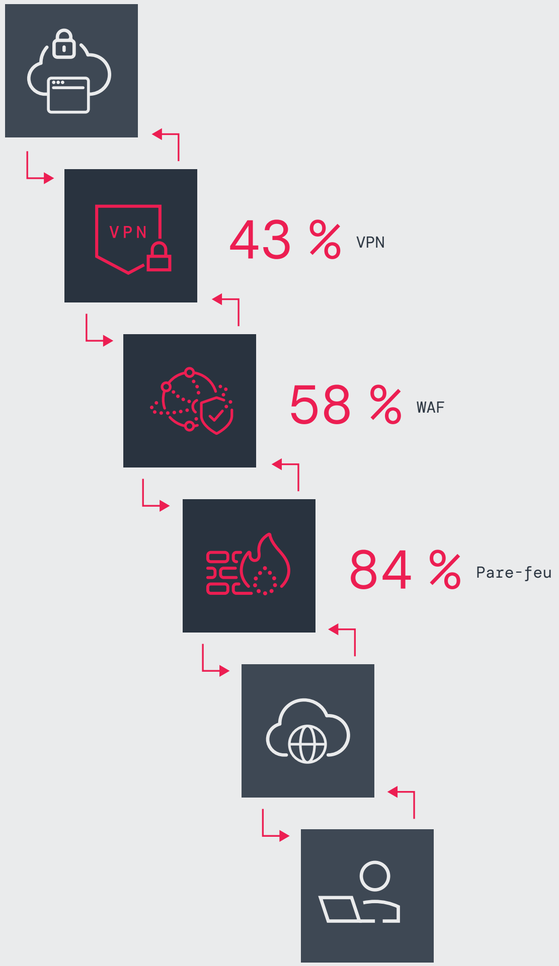


Illustration 10 : Produits de sécurité utilisés par les entreprises pour protéger leurs applications privées contre les menaces Web

Contrôle d’accès et environnements de VPN : une protection limitée

54 % des entreprises interrogées déclarent utiliser un NAC pour sécuriser l’accès par VPN aux ressources privées. Cette fonctionnalité n’a toutefois pas encore empêché les violations et les exploits généralement associés aux vulnérabilités des VPN, ce qui souligne l’incapacité du NAC à répondre aux risques systémiques liés à un modèle qui attribue une confiance par défaut à toute entité présente sur le réseau.

Les solutions NAC appliquent un contrôle de la posture des dispositifs, une authentification et une segmentation du réseau. Cependant, elles ne répondent pas aux problématiques de sécurité fondamentales liées aux VPN, telles que les autorisations d’accès étendues, les risques de déplacement latéral et un modèle de confiance implicite.

Les récentes violations démontrent que même avec un système NAC, les vulnérabilités des VPN restent d’actualité. En novembre 2023, le ministère américain de l’Énergie a confirmé un incident de sécurité majeur impliquant une compromission d’identifiants VPN qui a permis à des hackers de contourner les contrôles d’accès et d’infiltrer des systèmes internes sensibles. Ce cas met en évidence la manière dont les hackers peuvent exploiter directement les faiblesses du VPN, par le biais d’informations d’identification volées, de vulnérabilités non corrigées ou de détournement de sessions, ce qui limite l’efficacité du NAC tant que le modèle de confiance reste inchangé.

Utilisez-vous un contrôle d’accès NAC (Network Access Control) entre votre VPN et vos ressources privées ?

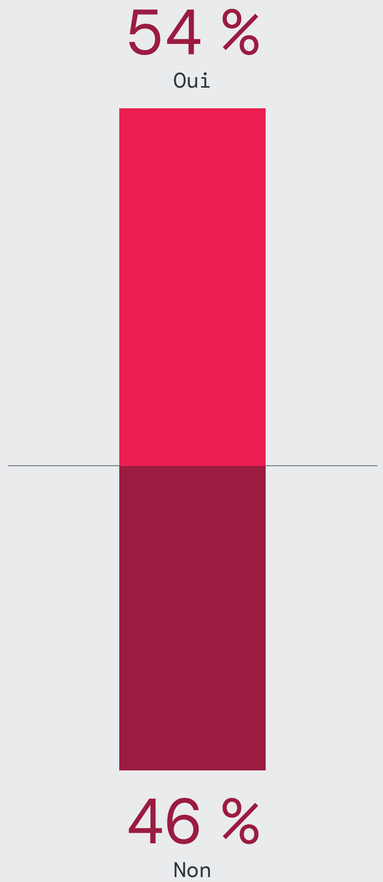


Illustration 11 : Part d’entreprises utilisant un NAC entre leurs VPN et leurs ressources privées

Pour pallier les limites des architectures NAC et VPN traditionnelles, les entreprises doivent adopter un modèle de sécurité Zero Trust. Le Zero Trust élimine toute confiance étendue au réseau en permettant aux utilisateurs de se connecter directement à des applications spécifiques dans le cadre de politiques continuellement validées liées à l’identité, à la posture des appareils et au contexte. Le Zero Trust bloque les accès non autorisés et prévient les déplacements latéraux, déjouant ainsi les hackers avant qu’ils ne puissent élever leurs privilèges ou exfiltrer des données.

Expérience utilisateur des VPN et problématiques de gestion

Performance médiocre des VPN : des utilisateurs frustrés et des équipes informatiques débordées

Les VPN ne constituent pas seulement un risque pour la sécurité ; ils sont également une source majeure d'insatisfaction chez les utilisateurs. Les utilisateurs finaux expriment de plus en plus leur frustration face aux performances médiocres des VPN, qui freinent la productivité et accentuent la pression sur les équipes informatiques.

La lenteur des connexions constitue la plainte la plus courante (23 %), soulignant la mauvaise réputation des VPN en matière de latence, de congestion et de performances médiocres lors de l'accès aux applications cloud depuis le domicile des télétravailleurs. Les problématiques d'authentification constituent également un important sujet de préoccupation : 20 % des personnes interrogées mentionnent la complexité des processus de connexion et 17 % rencontrent des difficultés d'accès aux applications en raison d'erreurs d'authentification.

Ces problèmes de performances perturbent les opérations quotidiennes, nuisent à la productivité et engorgent le service de support informatique, qui doit gérer de multiples demandes de dépannage. Ce problème ne fait que s'aggraver à mesure que les environnements de télétravail et hybrides gagnent en complexité.

Le remplacement des VPN par un accès réseau Zero Trust (ZTNA) élimine la congestion de la bande passante et améliore considérablement l'expérience utilisateur en permettant des connexions directes, sécurisées et sans latence aux applications. Contrairement aux VPN, qui acheminent tout le trafic via une passerelle centrale et créent des congestions, le ZTNA permet un accès direct et sécurisé aux applications, sans dégradation des performances. En adoptant un contrôle d'accès basé sur l'identité, une vérification continue et une sécurité fournie depuis le cloud, les entreprises éliminent non seulement les frustrations courantes liées aux VPN, mais renforcent la productivité de leurs collaborateurs et allègent la charge informatique liée au dépannage et au support des VPN.

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

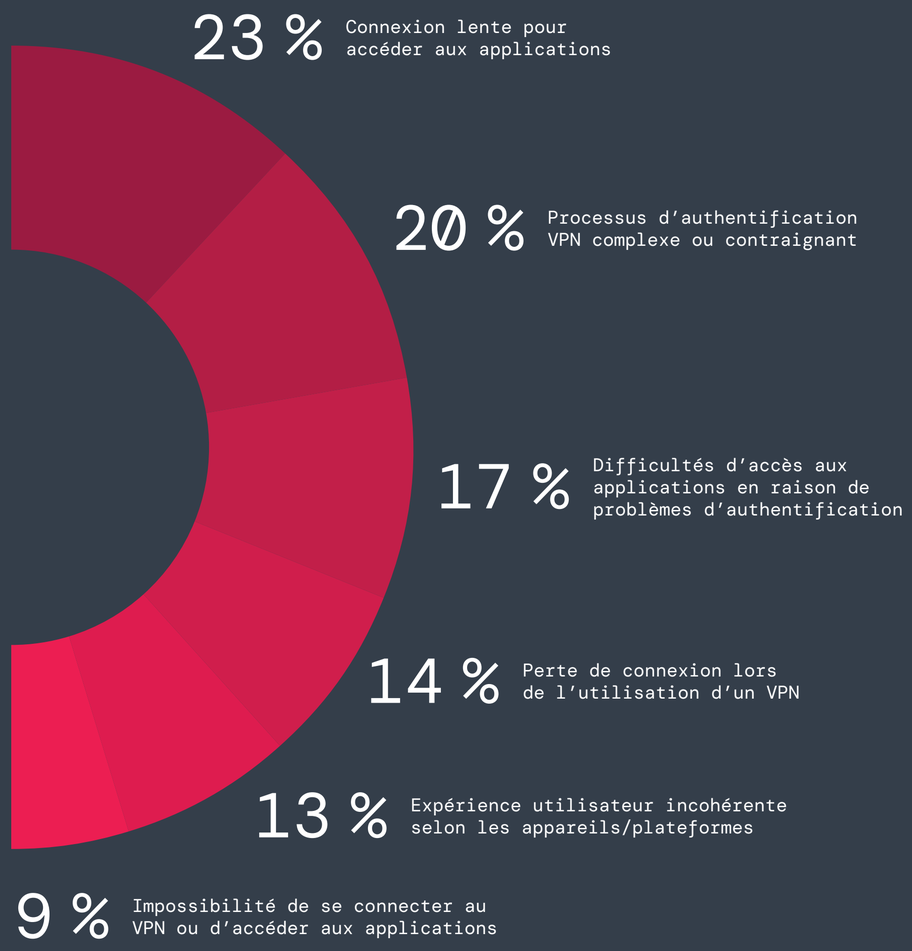


Illustration 12 : Plaintes les plus courantes parmi les utilisateurs de VPN

Gestion des VPN : équipes informatiques débordées et vulnérabilités

Les VPN pèsent sur les équipes informatiques, avec leurs vulnérabilités de sécurité persistantes, des demandes de maintenance qui mobilisent les ressources et des modèles d'accès obsolètes qui ne correspondent plus aux besoins des environnements d'entreprise actuels axés sur le cloud. La principale préoccupation de ces équipes (52 %) concerne les failles de sécurité susceptibles d'entraîner des incidents, soulignant les risques permanents liés au vol d'identifiants, aux exploits logiciels non corrigés et aux hackers qui exploitent l'accès VPN pour se déplacer latéralement, sans contraintes. Ces risques soulignent les raisons pour lesquelles les VPN sont de plus en plus considérés comme des outils d'accès à risque.

Les VPN sont devenus un fardeau financier et opérationnel pour les équipes informatiques, 41 % des personnes interrogées soulignant les coûts exorbitants des ressources liées à leur maintenance. Un processus incessant de déploiement de patchs, de dépannage et de surveillance des logs est indispensable pour sécuriser une infrastructure obsolète. Mais cette approche peut être épuisante pour les équipes, jusqu'à les empêcher de se concentrer sur des activités à plus forte valeur ajoutée.

Autre faiblesse critique, citée par 35 % des personnes interrogées, les VPN sont incapables d'appliquer des contrôles d'accès granulaires. Au lieu d'accorder un accès précis et basé sur l'identité à des applications spécifiques, les VPN fournissent souvent une connectivité réseau étendue et illimitée, ce qui accentue considérablement le risque de menaces internes et de déplacements latéraux des hackers. En outre, 26 % pointent la surcharge opérationnelle liée à la gestion des concentrateurs VPN et autres dispositifs, illustrant la complexité de la maintenance des appliances matérielles, des tunnels réseau et des passerelles d'accès afin de maintenir la connectivité à distance. Ces complexités sont particulièrement ingérables à une époque où les environnements cloud natifs et de télétravail requièrent des solutions plus agiles et évolutives.

Quelles sont les préoccupations les plus couramment exprimées par votre équipe informatique/de sécurité concernant les VPN ?

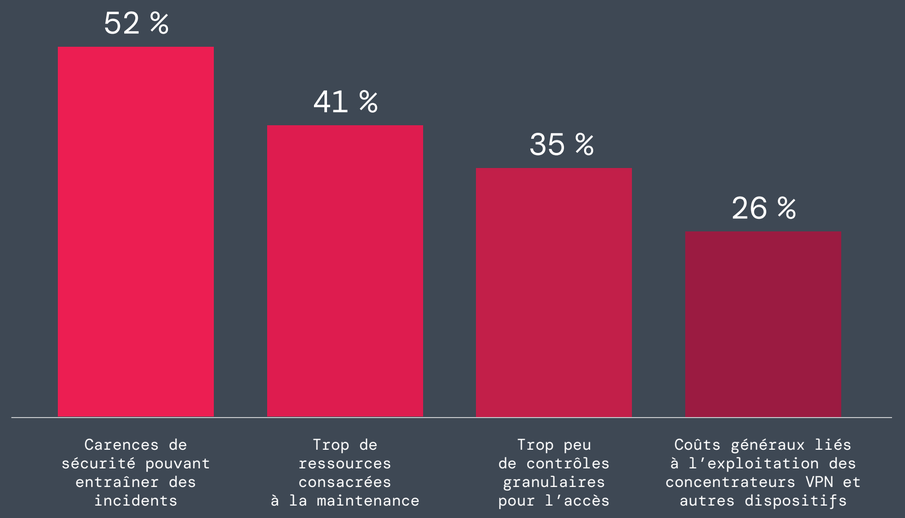


Illustration 13 : Principales préoccupations des équipes informatiques et de sécurité pour la prise en charge des VPN

Pour relever ces défis, les entreprises doivent passer d'un accès VPN classique à un modèle Zero Trust fourni dans le cloud qui remet en cause le principe de confiance implicite, réduit les surfaces d'attaque et simplifie les opérations informatiques. L'adoption du Zero Trust allège les coûts opérationnels liés aux VPN, simplifie la gestion des accès et minimise les risques de sécurité à grande échelle. Les équipes informatiques sont libérées du fardeau d'une maintenance permanente, ce qui leur permet de se concentrer sur des initiatives de sécurité proactives tout en offrant une expérience utilisateur plus rapide et plus fluide.

La gestion fastidieuse des VPN

La gestion de l'infrastructure VPN continue de peser lourdement sur les équipes informatiques, dont les principales préoccupations portent sur la fiabilité, les performances et les coûts de maintenance. Le dépannage des problématiques de connectivité et de stabilité VPN reste le principal défi, cité par 54 % des personnes interrogées. Les équipes informatiques sont confrontées à des difficultés récurrentes pour assurer la disponibilité permanente des VPN, mais aussi gérer les échecs de connexion, sources de perturbations généralisées, de productivité altérée, de sécurité aléatoire et de frustration parmi les collaborateurs.

Arbitrer entre performances du VPN et expérience utilisateur reste un défi majeur (50 %) : les VPN sont souvent source de latence, de déconnexions intempestives et de performances aléatoires, en particulier dans les environnements orientés cloud. De plus, 47 % des professionnels de l'informatique soulignent que la nécessité de déployer fréquemment des patchs et les coûts en ressources associés représentent un obstacle majeur, mettant en évidence les défis opérationnels liés à la maîtrise des vulnérabilités persistantes et à la maintenance de systèmes obsolètes.

Ces défis ont contribué à différents incidents majeurs. De décembre 2023 à début 2024, plusieurs agences gouvernementales américaines ont été ciblées par une attaque menée par VPN. Des retards dans l'application de correctifs pour une vulnérabilité connue ont permis à des acteurs malveillants de pirater un logiciel VPN obsolète et d'obtenir un accès non autorisé au réseau. Cet épisode met en évidence le risque associé à un patching retardé, même au sein d'entreprises disposant d'équipes informatiques dédiées. Il démontre qu'une sécurité partielle des VPN expose les secteurs critiques à des menaces en constante évolution.

L'infrastructure VPN mobilisant d'importantes ressources informatiques dans le cadre du dépannage de la connectivité, de l'application des correctifs de sécurité et de l'optimisation des performances, les entreprises doivent reconsidérer la viabilité à long terme de leur accès basé sur les VPN. En remplaçant les concentrateurs VPN et les appliances réseau telles que les pare-feux et les NAC par une architecture cloud native, les équipes informatiques éliminent les goulets d'étranglement de l'infrastructure, réduisent le nombre de patchs à mettre en oeuvre et évitent de devoir intervenir manuellement à chaque échec de connexion.

L'accès sur la base du moindre privilège, régi par des politiques, garantit que les utilisateurs se connectent uniquement aux applications autorisées, sans avoir à gérer des règles de pare-feu ou des politiques complexes de segmentation du réseau. En passant à un modèle Zero Trust fourni dans le cloud, les entreprises éliminent les goulots d'étranglement liés aux VPN tout en garantissant un accès transparent et basé sur des politiques aux applications. Elles s'affranchissent ainsi de la gestion fastidieuse de l'infrastructure réseau, des correctifs logiciels ou du dimensionnement du réseau.

Quelles sont vos trois principales préoccupations en matière de gestion de votre infrastructure VPN ?

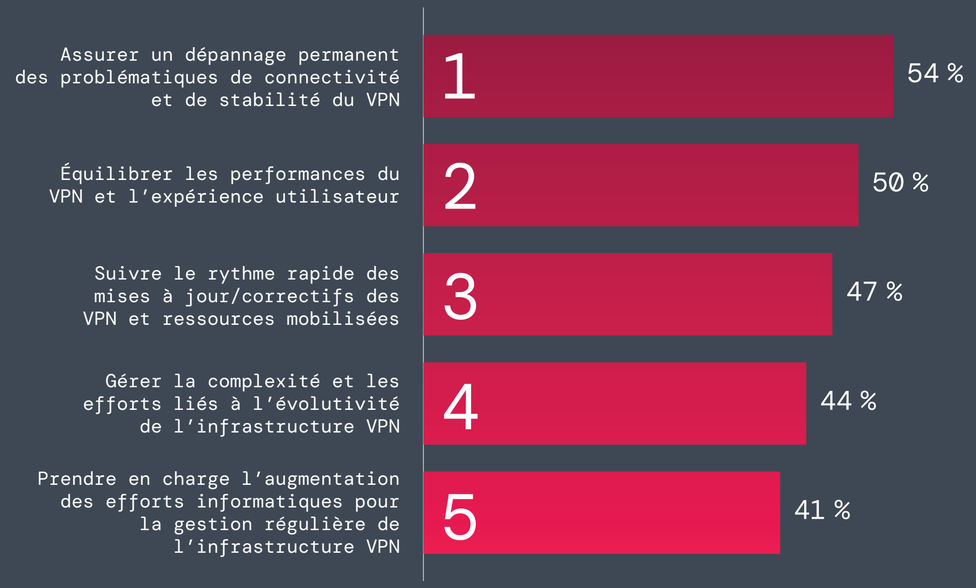


Illustration 14 : Principales préoccupations des équipes informatiques chargées de la gestion de l'infrastructure VPN

Contrôles d’accès trop laxistes aux VPN : une faille de sécurité critique

La cause principale de nombreux risques de sécurité liés aux VPN réside dans la manière dont ces VPN définissent l’accès. Au lieu de fournir un accès précis et spécifique à une application, de nombreuses entreprises accordent un accès réseau étendu, adossé à un modèle de confiance implicite et qui expose leurs systèmes critiques.

Les résultats de l’enquête révèlent que 52 % des entreprises dépendent encore de modèles d’accès obsolètes à l’image de règles statiques de pare-feu réseau statiques (28 %) ou d’un accès pervasif pour les utilisateurs authentifiés (24 %). Ces modèles obsolètes permettent aux assaillants de se mouvoir furtivement sur les réseaux, d’élever leurs privilèges et d’exfiltrer des données critiques une fois l’accès initial obtenu.

De récents incidents soulignent les dangers d’un accès aussi large et laxiste. Au début de l’année 2024, Global Affairs Canada (GAC) a subi un incident de sécurité majeur lié à la compromission d’un VPN utilisé par les collaborateurs pour accéder au siège social d’Ottawa. Les hackers ont exploité des vulnérabilités du VPN pour obtenir un accès non autorisé au réseau et, potentiellement, à des informations sensibles. L’événement a démontré qu’un accès réseau sans restriction et avec des privilèges trop élevés constitue un vecteur idéal pour qu’une menace se déplace latéralement et se propage.

Pour tempérer ces risques, les entreprises ne doivent accorder aucune confiance implicite et appliquer des contrôles d’accès granulaires, basés sur l’identité. La migration d’un modèle d’accès étendu vers une segmentation directe au niveau des applications garantit qu’un utilisateur donné n’accèdera qu’aux ressources spécifiques requises dans le cadre de son rôle, ce qui réduit considérablement la surface d’attaque et prévient les déplacements latéraux.

Comment définissez-vous l’accès des utilisateurs de VPN aux applications ?

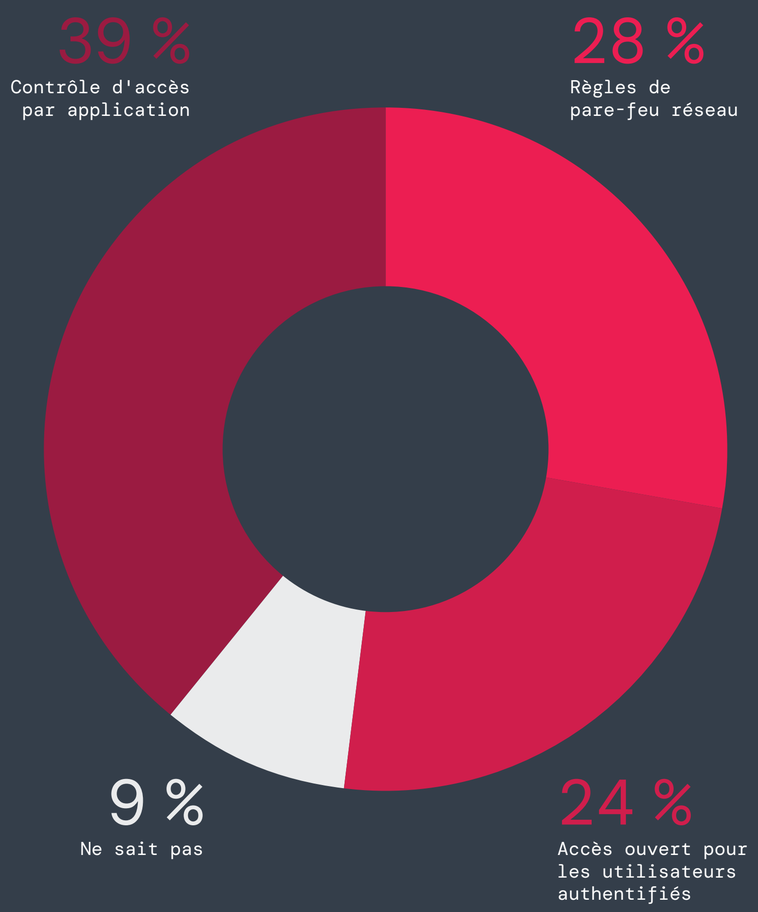


Illustration 15 : les façons dont les entreprises définissent l’accès des utilisateurs de VPN aux applications

Remplacement du VPN : migrer vers un accès intrinsèquement sécurisé

La multiplication des vulnérabilités de sécurité, la nécessité d'offrir une expérience utilisateur et les coûts de maintenance élevés des VPN incitent les entreprises à accélérer leur transition vers des technologies d'accès sécurisé modernes telles que le ZTNA. Cette évolution témoigne d'une prise de conscience croissante de l'incapacité des VPN de répondre aux exigences actuelles en matière de sécurité et d'opérationnel IT.

L'enquête confirme cette dynamique, 65 % des personnes interrogées déclarant que leur entreprise remplace ou prévoit de remplacer ses VPN au cours de l'année à venir.

À mesure qu'elles s'affranchissent des VPN, les entreprises doivent privilégier des modèles de sécurité fournis depuis le cloud et qui imposent un accès granulaire au niveau des applications en remplacement d'une connectivité réseau étendue. Le ZTNA élimine les risques liés au VPN : les utilisateurs n'accèdent qu'aux ressources dont ils ont besoin, en fonction de leur identité et de leur posture de sécurité, et ne sont jamais positionnés sur le réseau corporate. Cette approche renforce la sécurité, simplifie les opérations et améliore l'expérience utilisateur, ce qui rend le remplacement des VPN à la fois urgent et indispensable pour les entreprises modernes.

Quels sont vos projets pour remplacer votre service VPN actuel ?

65 %

des entreprises ont planifié le remplacement de leurs services VPN actuels

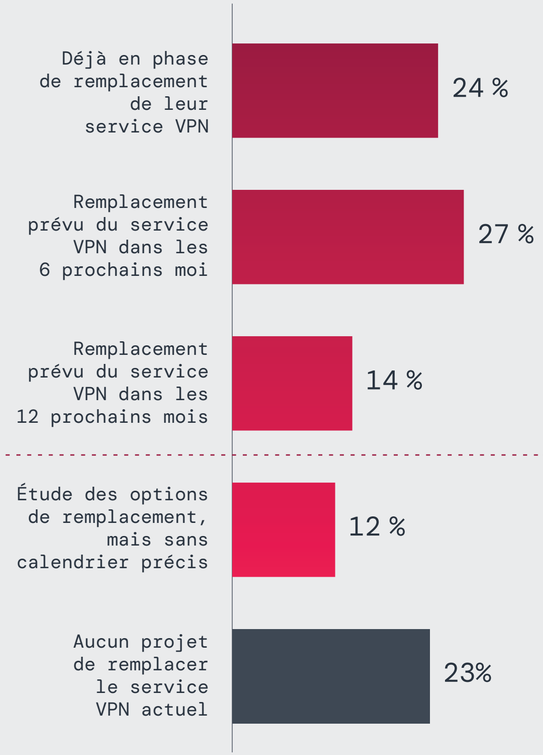
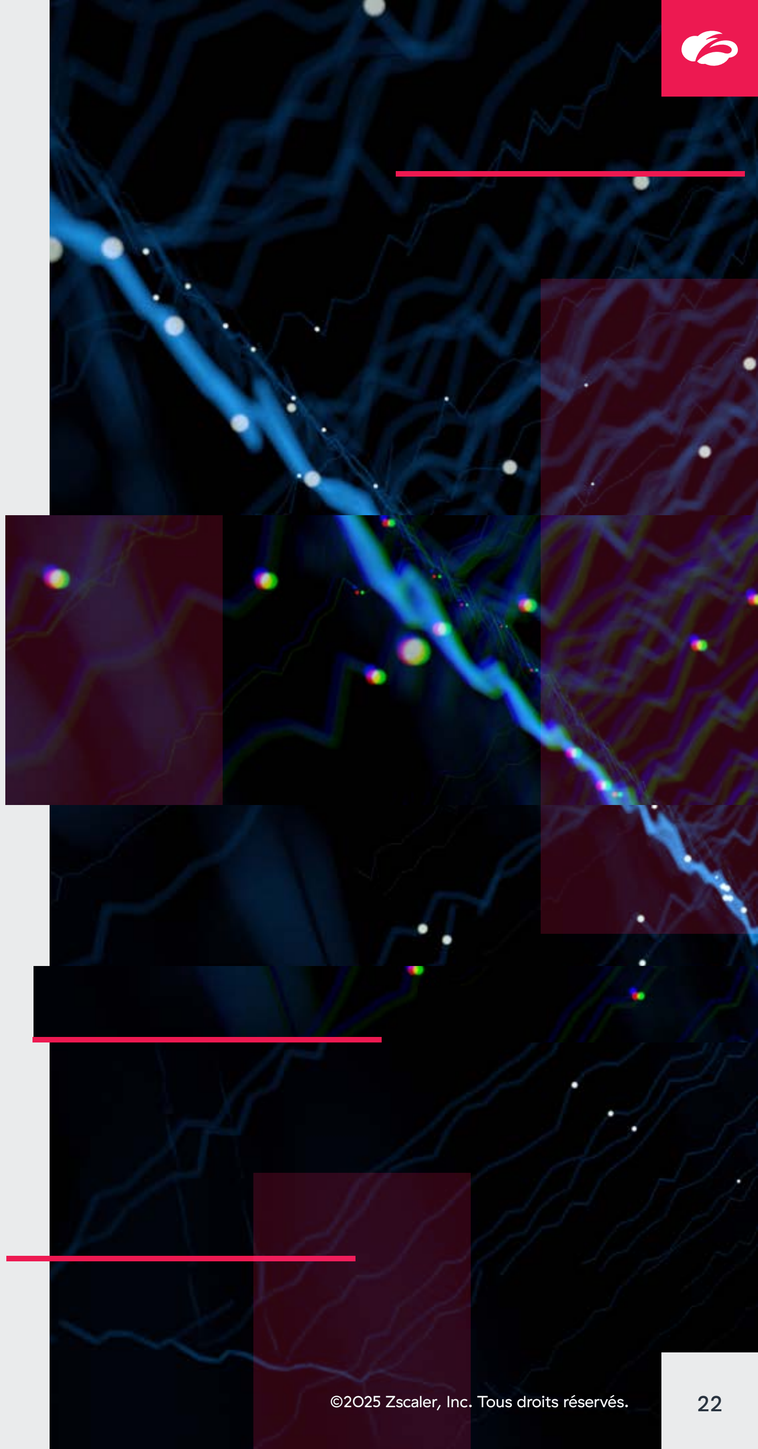


Illustration 16 : Projets des entreprises visant à remplacer leurs services VPN existants.



Adoption du Zero Trust

Le Zero Trust remplace le VPN à grande échelle

Alors que la tendance au remplacement des VPN s'accélère, la grande majorité des entreprises se tournent vers des architectures Zero Trust pour instituer un contrôle d'accès granulaire, réduire leur surface d'attaque et améliorer la productivité des utilisateurs. Les résultats de l'enquête soulignent la dynamique de ce changement de paradigme : 81 % des personnes interrogées ont l'intention d'adopter le Zero Trust dans le courant de l'année. Parmi celles-ci, 35 % déploient déjà des solutions Zero Trust, 24 % prévoient de le faire dans les six mois et 22 % ont planifié leur déploiement pour l'année prochaine, preuve que le Zero Trust s'impose comme la principale stratégie du secteur pour remplacer les technologies d'accès traditionnelles telles que les VPN.

Une adoption réussie du Zero Trust exige une coordination entre les équipes de sécurité et les équipes métiers. Les entreprises doivent mener des audits de risques afin d'identifier les points d'accès les plus vulnérables, qu'il s'agisse d'accès à distance, d'intégrations avec des tiers ou d'applications critiques. Cette connaissance permet de planifier le déploiement du Zero Trust en conséquence. L'application automatisée des politiques peut accélérer la transition vers le Zero Trust tout en réduisant les coûts administratifs.

Quels sont les projets de stratégie Zero Trust pour votre entreprise ?

96 % des entreprises ont déjà mis en œuvre, planifient ou ont adopté une stratégie Zero Trust

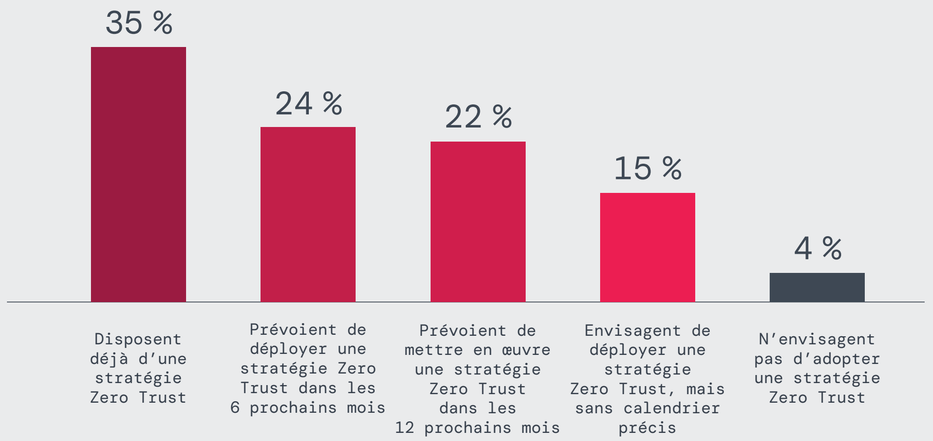


Illustration 17 : Projets des entreprises pour le déploiement d'une stratégie Zero Trust.

Priorités du Zero Trust : le télétravail favorise son adoption

L'abandon des VPN traditionnels témoigne d'une transformation majeure : les entreprises se tournent vers des architectures Zero Trust pour pallier leurs failles de sécurité, simplifier leurs opérations informatiques et répondre aux demandes de collaborateurs distants et disséminés. Cette orientation stratégique positionne le Zero Trust comme une solution moderne qui permet de maîtriser les risques liés aux VPN et de simplifier la gestion de la sécurité.

Les résultats de l'enquête indiquent que la sécurisation des collaborateurs distants constitue la principale motivation de ce changement, 37 % des entreprises mentionnent la sécurité du télétravail et 28 % la sécurité du travail hybride. Cette évolution reflète une tendance plus large vers des modèles de sécurité qui offrent un accès direct et spécifique à chaque application. Cette approche se veut plus simple que de gérer plusieurs produits distincts, comme c'est souvent le cas dans les configurations VPN traditionnelles.

Le déploiement du Zero Trust renforce non seulement la sécurité, mais allège également la charge opérationnelle liée à la gestion de multiples outils de sécurité. En unifiant les politiques et les contrôles de sécurité au sein d'un système consolidé, les entreprises peuvent réduire leurs coûts d'administration et simplifier leurs opérations. Par exemple, une plateforme Zero Trust qui exécute plusieurs actions lors d'une seule analyse peut éliminer le besoin de faire appel à différents outils, simplifiant ainsi l'expérience utilisateur tout en assurant une sécurité robuste.

Pour sécuriser de manière efficace les effectifs distants et hybrides à l'aide d'une architecture Zero Trust, les entreprises doivent privilégier des fonctionnalités de sécurité intégrées, ce qui est source de simplification. Le déploiement d'une plateforme Zero Trust unifiée permet de consolider différentes fonctions de sécurité, en remplacement d'une utilisation de plusieurs produits autonomes de sécurité. Cette approche améliore la sécurité et l'efficacité opérationnelle, permettant aux équipes informatiques de se concentrer sur des projets plus stratégiques que de devoir gérer un ensemble complexe d'outils de sécurité.

Quel est le principal cas d'utilisation pour déployer le Zero Trust ?

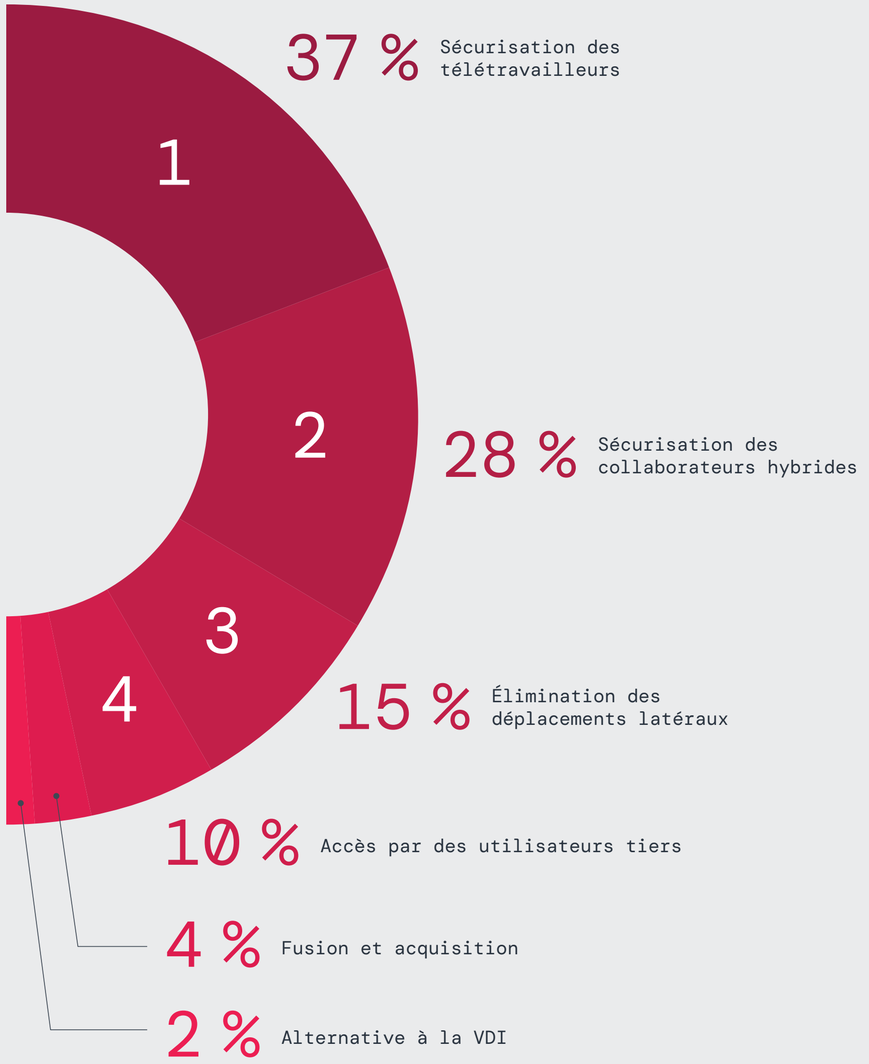


Illustration 18 : Principaux cas d'utilisation des solutions Zero Trust par les entreprises

Principaux avantages de remplacer les VPN par le Zero Trust

L'adoption de solutions Zero Trust transforme la sécurité des entreprises et offre des avantages considérables qui vont au-delà d'un accès sécurisé. Elle simplifie les tâches de gestion, améliore les performances et l'évolutivité, réduit considérablement la surface d'attaque et optimise l'efficacité des ressources. Les entreprises qui remplacent les modèles VPN par le Zero Trust ne se contentent pas de mettre à niveau leurs outils ; elles pérennisent l'ensemble de leur stratégie d'accès à distance.

La majorité des personnes interrogées (76 %) considèrent l'amélioration de la sécurité et de la conformité comme le principal avantage, ce qui confirme que le Zero Trust remplace l'accès implicite au réseau et réduit l'exposition aux ransomwares, au vol d'identifiants et aux risques de déplacement latéral.

En outre, 64 % des personnes interrogées citent la simplification de la gestion, l'évolutivité et l'expérience utilisateur comme principaux avantages : le Zero Trust supprime les charges opérationnelles liées à la gestion des concentrateurs VPN, à l'application régulière de patchs et au dépannage des accès.

Près de la moitié (45 %) des personnes interrogées citent le remplacement du VPN par une solution Zero Trust comme une étape cruciale vers une architecture Zero Trust complète. Parallèlement, 34 % soulignent l'évolutivité et la flexibilité supérieures du Zero Trust qui en font une solution plus efficace pour sécuriser les collaborateurs distants et hybrides. D'autres avantages contribuent à la création de valeur du Zero Trust : amélioration de l'expérience utilisateur (32 %), intégration transparente entre les systèmes informatiques et de sécurité (28 %) et réduction des coûts opérationnels grâce à des économies de ressources (18 %). Collectivement, ces avantages illustrent les raisons pour lesquelles les entreprises délaissent rapidement les VPN traditionnels au profit du Zero Trust.

ManpowerGroup, un leader mondial de solutions de gestion des ressources humaines, est un cas d'école en matière de sécurisation des accès grâce au Zero Trust. Pour accompagner ses nombreux télétravailleurs, l'entreprise a remplacé son infrastructure VPN traditionnelle par une solution Zero Trust de Zscaler. En seulement 18 jours, ManpowerGroup a étendu l'accès sécurisé aux applications à plus de 30 000 utilisateurs, assurant une continuité d'activité et une baisse spectaculaire de 97 % des demandes de support. Cette opération met en évidence la capacité d'une architecture Zero Trust à évoluer rapidement, à simplifier les opérations et à générer des résultats mesurables en termes de productivité et de sécurité.

Si vous avez remplacé votre VPN par une solution Zero Trust, quels sont, selon vous, les principaux avantages par rapport à l'ancienne infrastructure VPN ?

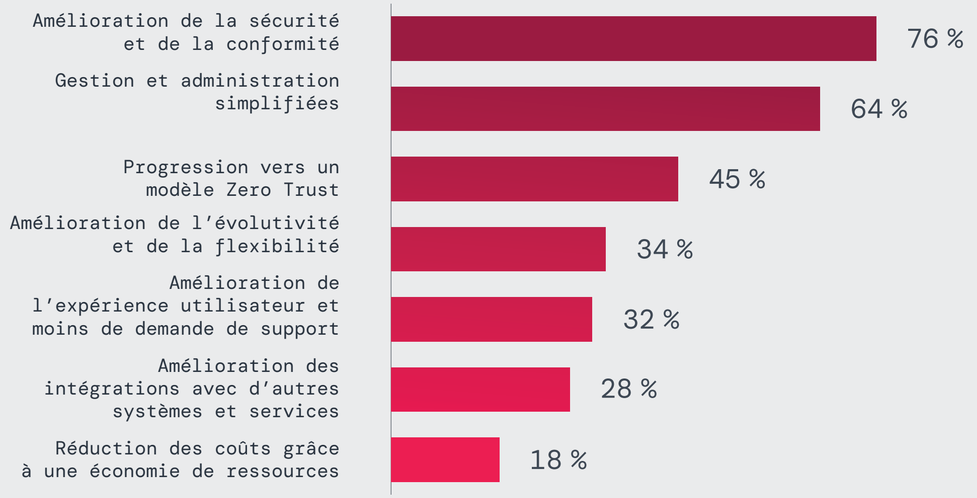


Illustration 19 : Principaux avantages, selon les entreprises, d'une solution Zero Trust par rapport à leur ancienne infrastructure VPN

L'adoption du Zero Trust doit commencer par des modifications qui visent à éliminer l'accès réseau via un VPN au profit de connexions directes vers les applications, ceci afin de limiter le risque de déplacement latéral. Les entreprises peuvent privilégier le remplacement des accès traditionnels pour les cas d'utilisation critiques, tels que la sécurisation des connexions des utilisateurs distants et tiers. Dans un second temps, les capacités Zero Trust peuvent être étendues à l'ensemble de leur écosystème informatique. L'automatisation des politiques d'accès, basée sur un ensemble de règles, et l'intégration d'une sécurité basée sur l'identité simplifieront davantage la gestion du Zero Trust tout en favorisant une évolutivité pour prendre en charge une infrastructure multisite. Ces frameworks intelligents permettent aux équipes informatiques de maintenir un contrôle de sécurité en temps réel sans sacrifier l'agilité ni l'efficacité.

Prévisions des risques liés aux VPN pour 2025

Les vulnérabilités VPN critiques continueront d'émerger

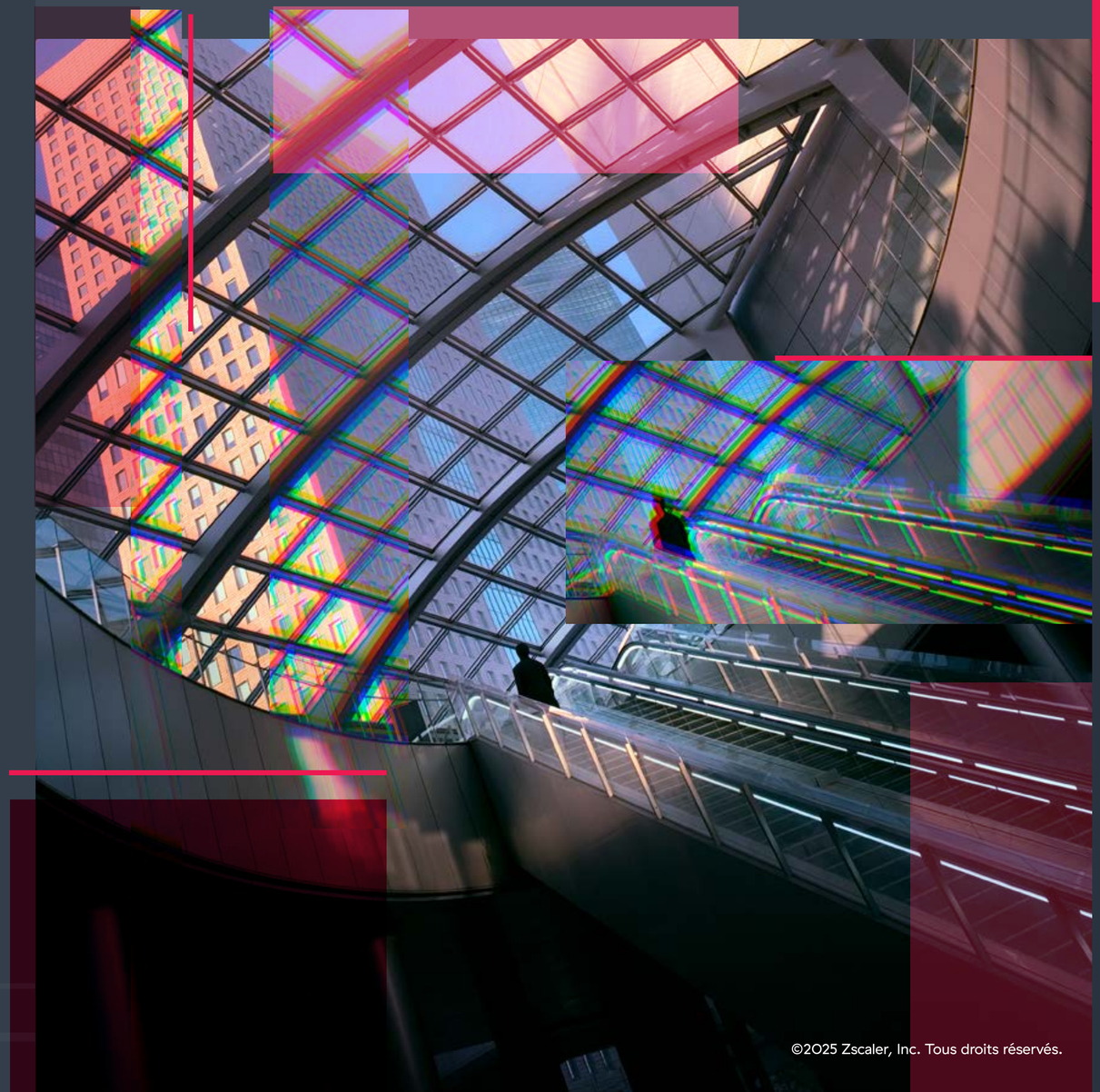
La recrudescence du nombre d'exploits de VPN ces dernières années s'accélérera en 2025. Les technologies VPN sont une cible de choix pour les hackers, car elles exposent les infrastructures d'entreprise à Internet, ce qui facilite la détection et l'exploitation des vulnérabilités. Même si les entreprises s'efforcent de corriger les failles VPN, les hackers continueront de découvrir et d'exploiter de nouvelles vulnérabilités de gravité élevée, comme l'illustre l'incident de sécurité subi par Ivanti Pulse Secure de janvier 2025. Les chercheurs en sécurité tout comme les cybercriminels analysent activement les infrastructures VPN, ce qui donnera lieu à la divulgation de nouvelles vulnérabilités CVE critiques.

Les groupuscules de ransomware intensifieront leurs attaques contre les VPN

Alors que 92 % des personnes interrogées se disent préoccupées par les vulnérabilités VPN non corrigées, les auteurs de ransomware continueront d'exploiter les failles VPN connues et de type « zero day » comme principale méthode d'accès initial. Les groupuscules RaaS (Ransomware-as-a-service) recherchent régulièrement des VPN exposés comportant des vulnérabilités non corrigées, ce qui leur permet de déployer des ransomwares avant que les équipes informatiques ne puissent réagir. La campagne de ransomware de janvier 2025 visant des entreprises du secteur de la santé aux États-Unis a démontré que les failles de sécurité des VPN offrent aux hackers un accès direct aux systèmes sensibles. À mesure que ces attaques s'automatisent, la transition vers une sécurité Zero Trust deviendra plus urgente.

Les déplacements latéraux via les VPN favoriseront des attaques plus destructrices

Les hackers exploitent l'accès étendu qu'offrent les VPN pour se déplacer latéralement, élever leurs privilèges et exfiltrer des données. Il s'agit là de l'une des techniques les plus efficaces des cybercriminels et de certains états-nations malveillants. Avec 71 % des entreprises préoccupées par ce risque, la segmentation du réseau est souvent considérée comme une solution efficace, mais néanmoins complexe à mettre en oeuvre. De nombreuses entreprises ne disposent pas du personnel qualifié pour gérer efficacement la segmentation, ce qui rallonge considérablement la réalisation d'un tel projet. Pour atténuer ces difficultés, les entreprises doivent adopter une segmentation Zero Trust, qui impose un accès strict sur la base du moindre privilège aux applications, éliminant ainsi les possibilités de déplacement latéral sans avoir à déployer et gérer une segmentation réseau traditionnelle.



L’accès des tiers par VPN reste un vecteur majeur de menaces

Alors que 93 % des personnes interrogées se disent préoccupées par les vulnérabilités des VPN de tiers, les hackers continueront de cibler les points d’accès externes vulnérables. Le détournement d’identifiants de tiers et une mauvaise configuration des accès VPN donnent lieu à des passerelles d’entrée pour les cybercriminels. L’incident subi par Enterprise Financial Group (EFG) de 2024 illustre comment les hackers exploitent des liens VPN tiers pour infiltrer les environnements d’entreprise. De nombreuses entreprises ne disposent pas d’une visibilité suffisante sur les autorisations d’accès accordées aux tiers, ce qui complique l’application des politiques de sécurité. Pour maîtriser ces risques, les entreprises doivent adopter un modèle Zero Trust, qui impose un accès strict sur la base du moindre privilège et une vérification continue de toutes les connexions provenant de l’externe.

Les exploits VPN optimisés par l’IA vont progresser

L’essor des cyberattaques optimisées par IA aura un impact sans précédent sur la sécurité des VPN. Les hackers exploiteront de plus en plus l’IA pour mener des reconnaissances automatisées, des piratages à l’aide de mots de passe communs (« password-spraying »), et développer rapidement des exploits, ce qui leur permettra de pirater des identifiants VPN à grande échelle. Les techniques de contournement optimisées par l’IA compliqueront davantage la détection des intrusions via VPN en amont de tout dommage. Parallèlement, les solutions de sécurité des VPN optimisées par l’IA peuvent donner lieu à des failles de sécurité fortuites, ouvrant la voie à de nouveaux vecteurs d’attaque que les cybercriminels ne manqueront pas d’exploiter. Face à la montée en puissance des menaces qui font appel à l’IA, les entreprises doivent adopter des mesures de sécurité proactives telles que la vérification continue des identités et le contrôle d’accès Zero Trust.

Des failles majeures liées aux VPN feront la une de l’actualité

Dans le droit fil de plusieurs incidents très médiatisés en 2024, les entreprises seront soumises à une pression accrue pour divulguer leurs cyberincidents liés aux VPN. Avec les nouvelles réglementations de la SEC imposant la transparence sur les risques de cybersécurité, les entreprises victimes d’exploits VPN seront exposées à un contrôle réglementaire renforcé et à d’éventuelles sanctions financières. Les VPN restant un principal point d’entrée pour les attaques, les entreprises seront contraintes de réévaluer leurs modèles d’accès existants, accélérant ainsi l’adoption d’une sécurité Zero Trust.

Les investissements dans le Zero Trust vont progresser avec le déclin des VPN

Avec 65 % des entreprises ayant déjà remplacé ou prévoyant de remplacer leurs VPN dans l’année, les investissements dans la sécurité Zero Trust s’accélèrent, remodelant fondamentalement le paysage de l’accès à distance. Les exigences réglementaires et les obligations en matière de cyberassurance incitent les entreprises à se détourner des VPN, ces outils traditionnels ne répondant plus aux exigences de sécurité, d’évolutivité et de conformité. L’adoption du Zero Trust réduit non seulement les risques cyber, mais élimine également les coûts élevés liés à la maintenance des concentrateurs VPN, aux appliances réseau et aux cycles continus de patching. En conséquence, les VPN sont de plus en plus perçus comme obsolètes, ce qui incite l’ensemble du secteur à adopter des modèles de sécurité Zero Trust.

Ces prévisions mettent en évidence un consensus croissant : les entreprises qui retardent l’adoption du Zero Trust resteront extrêmement vulnérables à mesure que vont se multiplier les exploits liés aux VPN. L’avenir de l’accès sécurisé dépend de la capacité à maîtriser proactivement les risques, et non d’une application réactive de correctifs. Il est donc temps d’en finir avec les VPN.

Bonnes pratiques pour un accès sécurisé

Réduire les risques liés aux VPN et renforcer la sécurité Zero Trust

1. **Supprimer l'accès réseau pour minimiser la surface d'attaque**
   Empêchez les hackers d'exploiter les points d'entrée réseau exposés en remplaçant progressivement les VPN et les accès via le réseau par une connectivité directe et spécifique aux applications. L'enquête révèle que 54 % des entreprises citent les risques de sécurité comme le principal défi lié aux VPN, ce qui renforce la nécessité de supprimer toute dépendance aux VPN et aux modèles de sécurité basés sur des pare-feux qui exposent les entreprises aux attaques.

2. **Prévenir les compromissions initiales grâce à une prévention intégrée des menaces**
   Inspectez l'ensemble du trafic chiffré et non chiffré afin de neutraliser les exploits de type « zero day », les malwares et les payloads de ransomware avant qu'ils n'atteignent les utilisateurs. Alors que 92 % des entreprises se disent préoccupées par les ransomwares qui exploitent les vulnérabilités des VPN, l'inspection du trafic en temps réel et la neutralisation des menaces sur la base de politiques s'avèrent essentielles. Un modèle de sécurité cloud native évite d'avoir à recourir à des pare-feux sur site et réduit la surface d'attaque.

3. **Renforcer l'authentification et la sécurité des identités**
   Protégez-vous du phishing à l'aide d'une authentification multifacteur (MFA) par identifiants FIDO2, biométrie ou jeton matériel, pour ainsi valider l'accès des utilisateurs. Évitez les méthodes d'authentification traditionnelles, telles que la MFA par SMS et les notifications push, que les hackers savent contourner. Intégrez une sécurité fondée sur l'identité avec vérification continue plutôt que de vous contenter d'une authentification unique et ponctuelle.

4. **Appliquer un accès sur la base du moindre privilège et d'éléments de contexte avec ZTNA**
   Remplacez l'accès VPN général par un accès réseau Zero Trust (ZTNA) afin de garantir que les utilisateurs se connectent uniquement aux applications autorisées, et jamais au réseau lui-même. Des contrôles d'accès granulaires, limités dans le temps (JIT ou « Just-in-Time ») et basés sur l'identité, la posture des dispositifs et l'analyse des risques en temps réel garantissent que les utilisateurs ne peuvent accéder qu'à ce dont ils ont besoin, quand ils en ont besoin.

5. **Éliminer les déplacements latéraux grâce à la segmentation Zero Trust**
   Connectez les utilisateurs directement aux applications, et non au réseau, pour empêcher les hackers de se déplacer d'un système à un autre suite à l'obtention d'un accès initial. La segmentation Zero Trust et la micro-segmentation basée sur l'identité garantissent qu'un hacker ne peut se déplacer vers d'autres ressources suite à une compromission initiale, ni élever ses privilèges. Le ZTNA élimine les tunnels VPN, qui sont un facteur majeur de déplacements latéraux.

6. **Sécuriser les accès tiers et externes grâce à des contrôles basés sur l'identité**
   Appliquez un accès sur la base du moindre privilège aux tiers et partenaires externes, en appliquant des contrôles de session stricts, des vérifications de la posture des dispositifs et un monitoring continu. Le remplacement des VPN de tiers par le ZTNA réduit considérablement l'exposition aux risques de compromission des identifiants de tiers. Ce changement est appréciable pour les 93 % d'entreprises préoccupées par les risques liés à l'accès de tiers par VPN.

7. **Renforcer la protection des données grâce à des politiques Zero Trust intégrées**
Déployez un contrôle inline de protection contre la perte de données (DLP) et de sécurité des accès au cloud (CASB) pour inspecter, chiffrer et empêcher le transit non autorisé de données. Un framework de sécurité Zero Trust garantit que tout le trafic utilisateur est inspecté et contrôlé, même pour les applications SaaS et dans les environnements cloud.

8. **Déployer une sécurité optimisée par l'IA et une surveillance continue**
Utilisez des analyses temps-réel et optimisées par l'IA, une technologie de leurre et une détection comportementale automatisée pour stopper les menaces avant qu'elles ne se concrétisent. Les solutions ZTNA évaluent les risques en temps réel, empêchant tout accès aux applications sensibles à partir d'un compte compromis. La traque proactive quotidienne des menaces et les contrôles d'accès basés sur les risques réduisent considérablement l'impact des violations.

9. **Évaluer et adapter en permanence la posture de sécurité**
Menez des évaluations automatisées des risques, des tests d'intrusion et des simulations d'attaques afin d'ajuster dynamiquement les politiques de sécurité Zero Trust. Les erreurs de configuration de la sécurité et le défaut d'application des politiques sont des vecteurs majeurs d'incidents. Une application automatisée des politiques de sécurité est donc indispensable pour réduire les erreurs humaines.

10. **Éliminer l'infrastructure VPN et automatiser l'application des politiques de sécurité**
Supprimez le besoin de concentrateurs VPN, de gestion des règles de pare-feu et de listes de contrôle d'accès manuelles en adoptant un modèle Zero Trust fourni dans le cloud. Le ZTNA permet d'appliquer des politiques de sécurité dynamiques qui s'adaptent en temps réel aux exigences de conformité, aux mises à jour réglementaires et à l'évolution des cybermenaces, sans configuration manuelle ni déployer de nouveau matériel.

En appliquant ces bonnes pratiques, les entreprises éliminent les risques de sécurité liés aux VPN. Ils capitalisent sur un framework de sécurité Zero Trust résilient, garantissant une validation continue de la sécurité, des accès sur la base du moindre privilège et une gestion proactive des menaces.

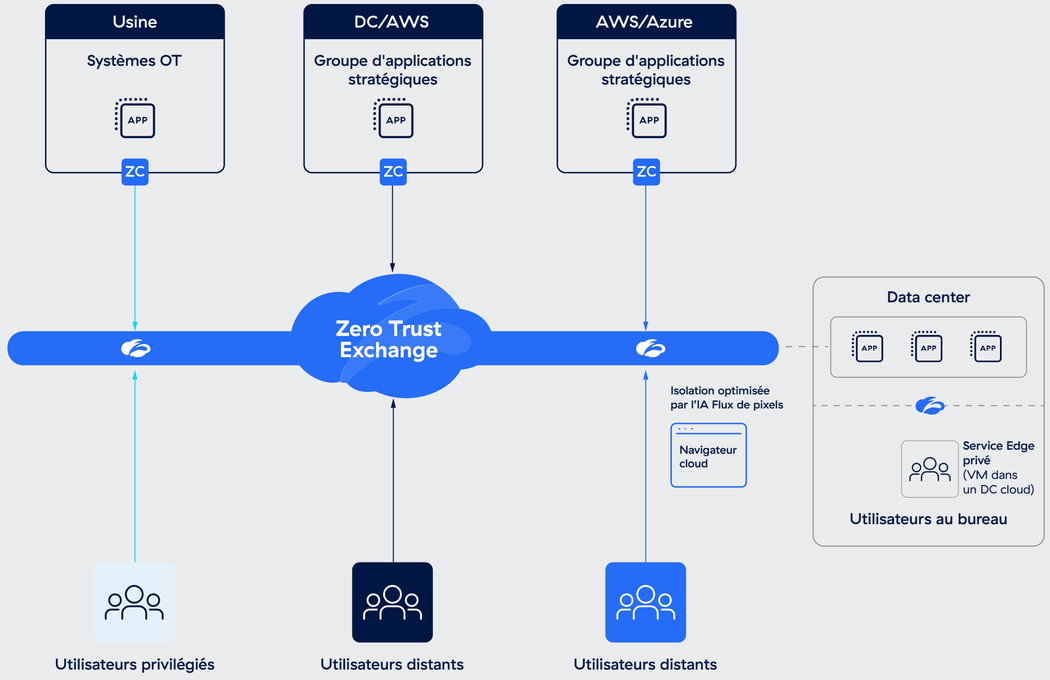
Comment Zscaler transforme l'accès sécurisé

En positionnant les utilisateurs directement sur le réseau corporate, les VPN et pare-feu traditionnels élargissent considérablement la surface d'attaque d'une entreprise. Cet accès étendu facilite la tâche des hackers qui peuvent exploiter les vulnérabilités, s'introduire dans le réseau et se déplacer en interne. Alors que les menaces continuent d'évoluer et que le travail hybride se généralise, le recours à ces technologies obsolètes pose des risques de sécurité critiques qui exigent des solutions plus sécurisées et flexibles.

Zscaler Private Access™ (ZPA) offre une alternative sécurisée et évolutive aux solutions d'accès à distance traditionnelles telles que les VPN. Solution cloud native, ZPA permet un accès Zero Trust à tous les utilisateurs en leur offrant une connectivité directe aux applications privées. Afin de minimiser la surface d'attaque, les applications sont protégées par la plateforme Zscaler Zero Trust Exchange™. Cette approche élimine les déplacements latéraux grâce à une segmentation utilisateur-application optimisée par l'IA et protège contre les menaces sophistiquées grâce à une inspection intégrée du trafic, ainsi qu'à la protection des applications et des données.

ZPA peut être déployé en quelques heures pour remplacer les VPN et les outils d'accès à distance traditionnels par une plateforme Zero Trust globale. Adossé au plus vaste cloud de sécurité au monde, ZPA offre une connectivité rapide, fiable et à faible latence aux utilisateurs, quelle que soit leur localisation dans le monde. Son architecture cloud native garantit une évolutivité optimale et répond de manière transparente aux besoins des équipes disséminées et hybrides, présentes sur différentes zones géographiques.

Avec ZPA, les entreprises peuvent adopter en toute confiance des modèles de travail hybrides, sachant que leurs ressources sont protégées, leurs utilisateurs productifs et leurs opérations informatiques pérennes.



Principaux avantages de Zscaler Private Access (ZPA)

Minimiser la surface d'attaque pour prévenir les attaques de ransomware

Les vulnérabilités des VPN exposent les entreprises à des utilisateurs malveillants, susceptibles de mener des attaques de ransomware et de détourner des identifiants. ZPA élimine ce risque en masquant toutes les applications derrière Zero Trust Exchange et en accordant aux utilisateurs un accès direct et Zero Trust uniquement aux applications autorisées. En empêchant les utilisateurs non autorisés (y compris les fournisseurs et partenaires externes) d'identifier les applications et de se déplacer latéralement, ZPA constitue une protection efficace contre les attaques de ransomware. La solution permet un accès à distance sécurisé à toutes les applications, y compris les applications privées, les applications connectées au réseau telles que la VoIP et les applications serveur–client. De plus, ZPA minimise l'impact des perturbations en optimisant la continuité d'activité et aide les entreprises à se conformer à des exigences de conformité strictes.

Éliminer le déplacement latéral des menaces

ZPA applique le principe du moindre privilège en connectant directement les utilisateurs à des applications spécifiques et en empêchant l'accès aux autres applications du réseau. Cette solution fournit des perspectives visuelles sur les accès des utilisateurs aux applications et les politiques appliquées, améliorant ainsi la visibilité et le contrôle. La segmentation ZPA optimisée par l'IA génère automatiquement des recommandations pour la segmentation des applications et les politiques, simplifiant ainsi la mise en œuvre de la segmentation tout en garantissant une sécurité robuste et évolutive.

Bénéficier d'une visibilité et d'analyses granulaires

ZPA fournit une visibilité détaillée et en temps réel sur l'utilisation des applications, le comportement des utilisateurs et les schémas d'accès. Les équipes informatiques peuvent utiliser ces données pour surveiller, auditer et identifier rapidement les menaces potentielles, afin de renforcer leur sécurité globale. Ces éléments peuvent également contribuer à garantir la conformité réglementaire.

Fournir un accès sans client pour restaurer les vulnérabilités liées aux tiers

L'accès sans client de ZPA simplifie l'accès des tiers en permettant aux sous–traitants et aux partenaires de se connecter en toute sécurité aux applications via n'importe quel navigateur, sans installer de client spécifique. Cette solution cloisonne les appareils non gérés par rapport au réseau d'entreprise, protège les données sensibles et s'intègre au navigateur Google Chrome Enterprise pour une sécurité renforcée des dispositifs BYOD. Cette approche moderne réduit les coûts, minimise les risques liés à l'accès des tiers et permet de se passer d'une gestion VDI traditionnelle.

Prévenir la compromission des applications privées

ZPA minimise le risque de compromission des applications privées et de perte de données en effectuant une inspection inline complète du trafic des applications privées. De solides capacités de protection contre la perte de données garantissent la sécurité des informations sensibles tout en bloquant les accès non autorisés En rendant les applications invisibles depuis l'Internet public et en permettant des connexions sécurisées entre les utilisateurs et les applications selon les principes du Zero Trust, ZPA renforce la sécurité globale. La solution réduit la surface d'attaque, empêche le déplacement latéral et prévient les intrusions.

Simplifier la gestion des politiques et accélérer le déploiement

ZPA simplifie les opérations informatiques en simplifiant le déploiement de l'accès à distance, la gestion des politiques et la segmentation utilisateur–application. Les tâches auparavant chronophages, telles que l'intégration des utilisateurs, l'application de correctifs et la gestion des mises à niveau, s'effectuent désormais en quelques minutes, ce qui réduit considérablement la charge de travail informatique. Grâce à une gestion centralisée et à des recommandations de politiques d'automatisation, ZPA permet aux équipes informatiques d'améliorer leur efficacité, de maîtriser la complexité et de se concentrer sur les initiatives stratégiques plutôt que sur des opérations quotidiennes.

Appliquer un contrôle d'accès basé sur la posture des appareils

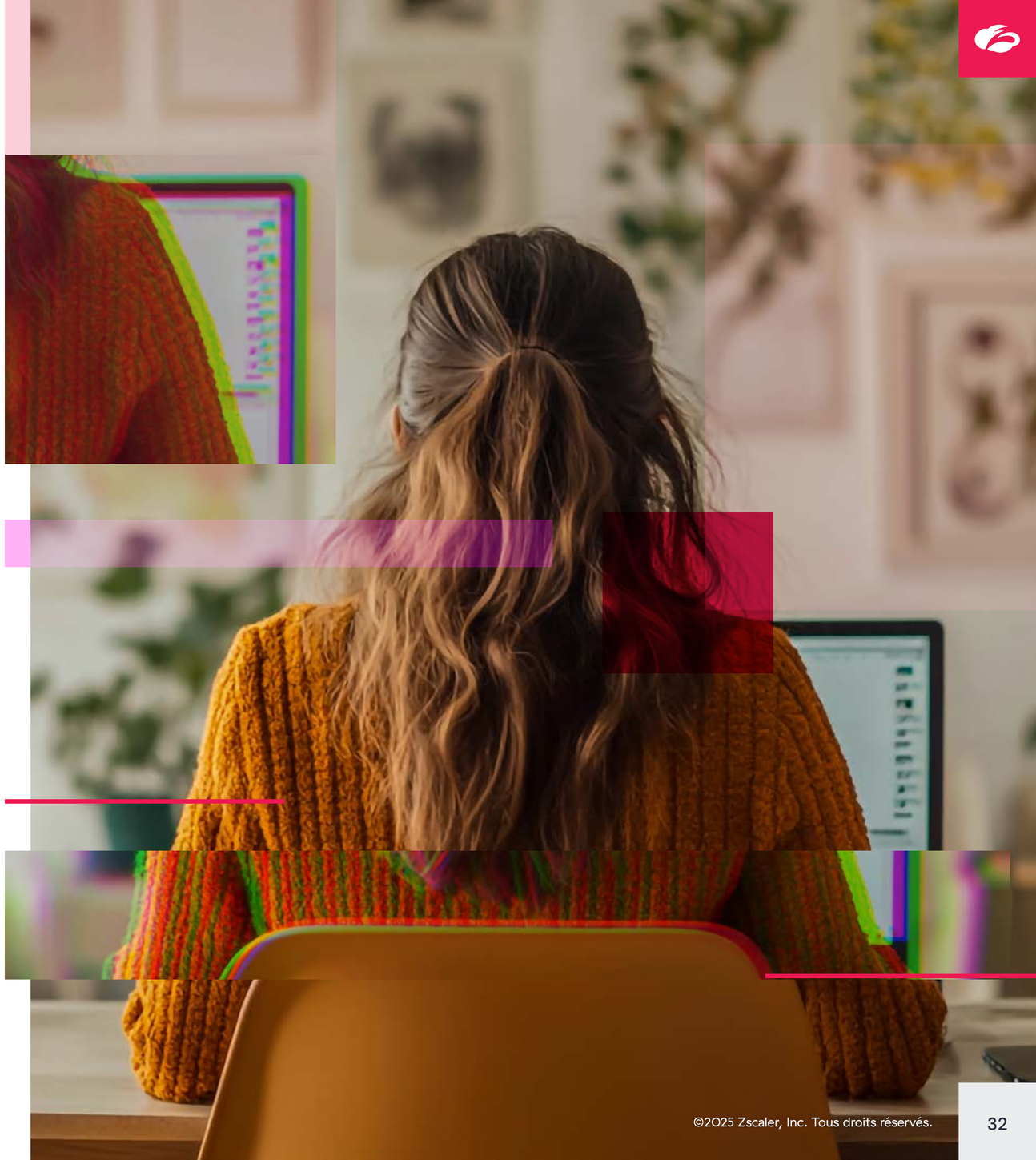
ZPA s'intègre aux outils d'évaluation de la posture des terminaux afin de vérifier la posture de sécurité des appareils des utilisateurs avant de leur accorder l'accès. Ainsi, seuls les appareils conformes peuvent se connecter, ce qui atténue les risques liés aux appareils non gérés ou compromis.

Offrir un expérience utilisateur optimale

ZPA optimise l'expérience utilisateur en fournissant une connectivité rapide, fluide et sécurisée aux applications d'entreprise. Contrairement aux VPN qui effectuent un backhauling du trafic via un data center centralisé, ZPA permet des connexions directes entre l'utilisateur et l'application, via Zero Trust Exchange.
Cette approche réduit considérablement la latence et améliore les performances des applications, que les utilisateurs travaillent sur site, à distance ou en déplacement. En minimisant les connexions multiples et la dépendance aux logiciels clients, ZPA simplifie l'accès et stimule la productivité. De plus, les capacités de surveillance proactive de ZPA simplifient la résolution des problématiques, garantissant un accès permanent et de qualité à tous les utilisateurs.

Réduire le coût total de possession

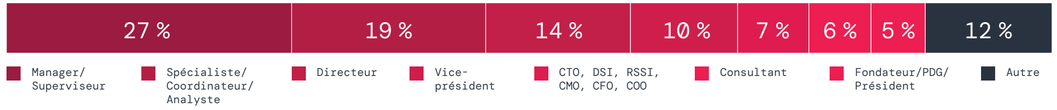
ZPA réduit considérablement le coût total de possession en éliminant le besoin de faire appel à plusieurs produits autonomes (VPN, pare–feu, NAC, concentrateurs VPN...) Conçu sur une architecture cloud native Zero Trust, ZPA supprime les coûts d'infrastructure liés au support matériel, à la maintenance et aux mises à jour. Sa simplicité de gestion et l'application automatisée des politiques réduisent les coûts opérationnels, en offrant aux équipes informatiques de solides gains en matière de temps, de productivité, de sécurité et d'évolutivité.



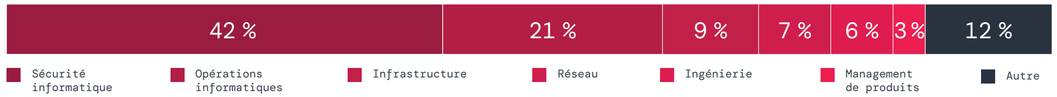
Méthodologie et données démographiques

Ce rapport s'appuie sur une enquête exhaustive menée début 2025 auprès de 632 professionnels de l'informatique et de la cybersécurité. Il examine les risques liés à la sécurité des VPN, les tendances en matière d'accès au sein des entreprises et l'adoption des architectures Zero Trust. Les profils interrogés sont des cadres, des professionnels de la sécurité informatique et des responsables d'infrastructures réseau issus de divers secteurs d'activité. Les conclusions de ce rapport offrent des informations factuelles sur le déclin des VPN et la migration vers le Zero Trust.
Elles proposent des perspectives essentielles aux entreprises qui modernisent leurs stratégies de sécurité des accès.

Niveau de poste

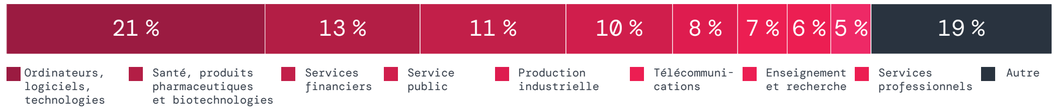


Département



Effectif d'entreprise

Secteur



À propos de Zscaler

Zscaler (NASDAQ : ZS) aide les entreprises à accélérer leur transformation numérique en renforçant leur agilité, leur productivité, leur résilience et leur sécurité. Sa plateforme Zero Trust Exchange™, conçue selon les principes du SASE, protège des milliers de clients contre les cyberattaques et la perte de données en assurant une connexion sécurisée entre utilisateurs, dispositifs et applications, partout dans le monde. Adossé à plus de 160 centres de données répartis à l'échelle mondiale, Zero Trust Exchange™ s'impose comme la plus vaste plateforme de sécurité cloud native. Pour en savoir plus, rendez-vous sur **www.zscaler.com/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 contre les menaces avancées via 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 la 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, VOTRE SOURCE FIABLE DE PERSPECTIVES FACTUELLES SUR LA CYBERSÉCURITÉ

Cybersecurity Insiders fournit des perspectives éprouvées et validées par des tiers, afin de permettre aux responsables de la cybersécurité d'éclairer leurs décisions stratégiques. Forts de plus de 10 années de recherches et d'études menées auprès d'un réseau mondial de plus de 600 000 professionnels de la cybersécurité, nous fournissons des informations décisionnelles qui aident les décideurs à appréhender l'évolution des menaces, à évaluer les technologies émergentes et à élaborer des stratégies innovantes en toute confiance.

Nous transformons les observations de nos recherches en des résultats concrets pour les fournisseurs de cybersécurité. Ces derniers gagnent en crédibilité, visibilité et en confiance en faisant appel à nos services à fort impact, qu'il s'agisse d'études de marché quantitatives, de webinaires de leadership d'opinion, de guides de bonnes pratiques destinés aux RSSI, d'évaluations de produits, d'articles pratiques qui guident les acheteurs de technologies, ou encore de distinctions au service de l'image de marque.

Nous pouvons également assurer la distribution de ces contenus de valeur pour aider les marques technologiques à se positionner en tant qu'acteurs de confiance, à gagner en notoriété et à développer leur activité commerciale sur un marché de la cybersécurité concurrentiel.

En savoir plus : **cybersecurity-insiders.com**

Holger Schulze
PDG et fondateur
de Cybersecurity Insiders

zscaler™ | Zero Trust Everywhere

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange™, basé sur le SSE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

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