2021

Cybersecurity
INSIDERS

RAPPORT SUR LES RISQUES LIÉS AU VPN

TABLE DES MATIÈRES

VUE D'ENSEMBLE

Pendant près de 30 ans, les VPN (réseaux privés virtuels) se sont avérés incontournables pour permettre aux utilisateurs distants d'accéder au réseau de l'entreprise. Aujourd'hui, le monde digital, où le Zero Trust est un impératif et où les applications ont migré en dehors du périmètre traditionnel, a changé cette réalité.

« À mesure que les entreprises se tournent vers des services plus axés sur le cloud, le VPN d'entreprise devient une technologie vieillissante... Cependant, dans le sillage de la pandémie mondiale du coronavirus, les entreprises se rendent compte qu'elles doivent fondamentalement changer leur façon de travailler ».

- Rob Smith, directeur analyste principal, Gartner

Les technologies VPN qui étaient la clef de voûte de l'accès à distance sont devenues une source de risques, conduisant les entreprises à réévaluer leur stratégie d'accès à long terme ainsi que leur utilisation du VPN. L'expansion mondiale du travail à distance due à la pandémie de COVID-19 a entrainé une augmentation de l'utilisation du VPN et par conséquent, une extension de la surface d'attaque des entreprises. Les acteurs malveillants ciblent les VPN comme en témoignent les innombrables articles récents relatifs aux failles du VPN, ainsi que les près de 500 vulnérabilités de VPN répertoriées dans la base de données CVE.

Pour réaliser ce rapport 2021 sur les risques liés aux VPN, 357 professionnels de la cybersécurité ont été interrogés, afin de recueillir des informations sur l'environnement actuel de l'accès distant, l'état du VPN au sein de l'entreprise, l'augmentation des vulnérabilités du VPN ainsi que le rôle que jouera à l'avenir le concept de Zero Trust pour permettre l'accès aux applications.

PRINCIPALES CONCLUSIONS :

- **93 %** des entreprises utilisent les services VPN, bien que 94 % sachent pertinemment qu'ils sont la cible des cybercriminels pour avoir accès aux ressources du réseau.
- **72 %** des entreprises sont inquiètes quant au fait que le VPN puisse mettre en péril la capacité des services informatiques à maintenir la sécurité de leurs environments.
- **67 %** des entreprises envisagent une alternative d'accès distant au VPN traditionnel.
- Aujourd'hui, **72 %** des entreprises privilégient l'adoption d'un modèle zero trust, pendant que 59 % ont accéléré leurs efforts en raison de l'accent mis sur le travail à distance.

Reconnaissance appuyée à Zscaler pour son soutien dans cet important projet de recherche.

Nous espérons que vous trouverez ce rapport édifiant et utile, alors que vous poursuivez vos efforts dans la protection de vos environnements informatiques.

Cordialement,

Holger Schulze

Holger Schulze
PDG et fondateur
Cybersecurity Insiders

Cybersecurity
INSIDERS

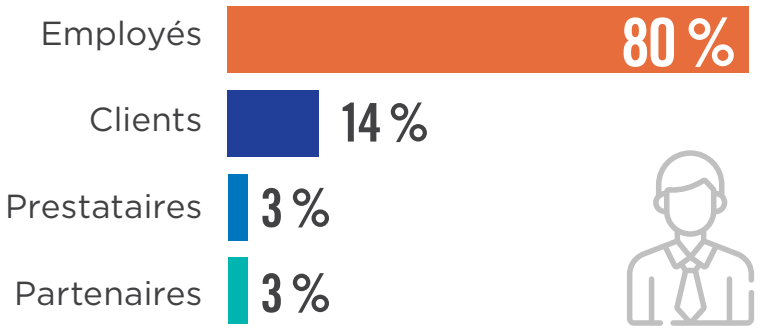
ENVIRONNEMENT D'ACCÈS À DISTANCE

ACCÈS SÉCURISÉ POUR QUI, QUOI...

Pour élaborer un plan visant à soutenir le travail à distance dans un monde moderne, les équipes de sécurité informatique doivent prendre en compte les facteurs suivants : qui accède à leurs applications, à partir de quels appareils et d'où ? Voici ce que l'enquête a mis en évidence.

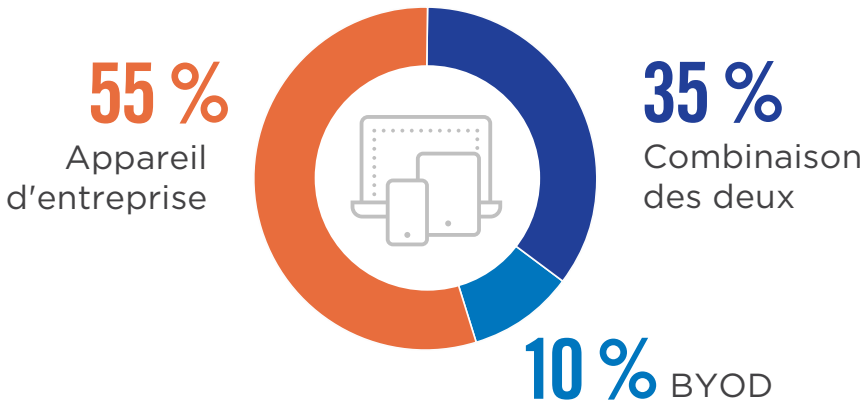
QUI : lorsqu'il s'agit d'exiger un accès sécurisé aux applications d'entreprise, les employés ont la priorité, ce qui n'est pas surprenant. **80 % des entreprises font de l'accès des employés leur principale priorité**, suivi par les clients (14 %), les partenaires et les prestataires (3 % chacun).

Quel est le groupe prioritaire lorsqu'il s'agit de demander un accès sécurisé aux applications commerciales ?



QUOI : lorsqu'on leur demande quel type d'appareils les télétravailleurs utilisent pour se connecter aux ressources et applications de l'entreprise, **45 % des entreprises déclarent que l'utilisation d'appareils personnels/BYOD est autorisée.** L'incapacité à appliquer des mesures de sécurité sur ces appareils BYOD rend plus complexe autant la sécurité des appareils que le contrôle des accès, en particulier dans les scénarios de télétravail.

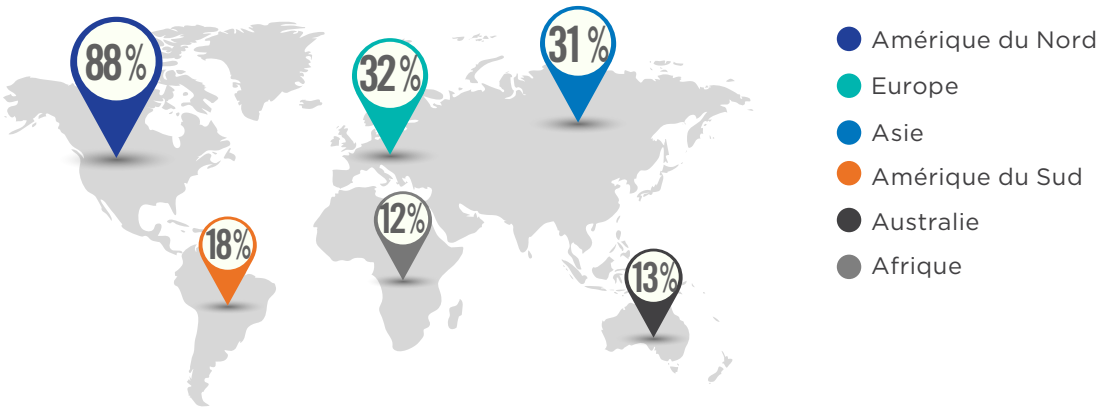
Quels appareils les travailleurs utilisent-ils pour se connecter aux ressources et aux applications de l'entreprise ?



... ET OÙ

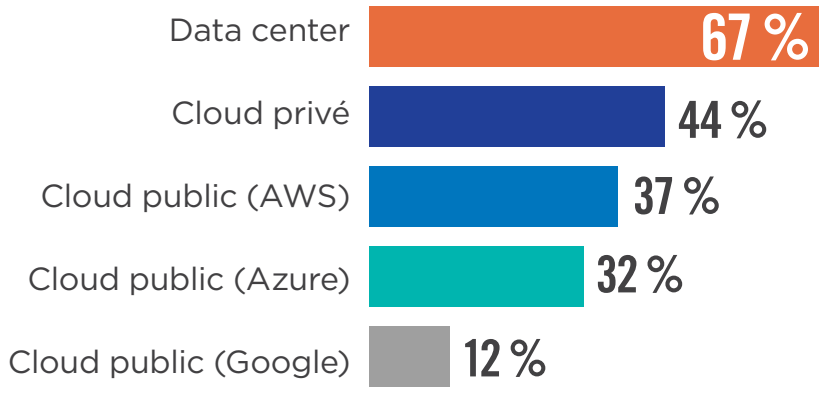
OÙ : les entreprises ayant fait l'objet de l'enquête signalent que **88 % ont des télétravailleurs se connectant de l'Amérique du Nord, 32 % de l'Europe et 31 % depuis l'Asie.** Les utilisateurs étant répartis dans différentes aires géographiques, la prise en charge du travail à distance sécurisé peut devenir un plus grand défi dans la mesure où les normes de sécurité, la disponibilité, les politiques de conformité, etc. varient d'une région à l'autre.

D'où vos télétravailleurs se connectent-ils ?



Qui plus est, cette enquête a révélé que **les applications privées des entreprises sont généralement exécutées dans des data centers (67 %), suivies du cloud privé (44 %), puis des clouds publics (37 % AWS/32 % Azure/12 % Google Cloud Platforms)**. Alors que les entreprises continuent d'adopter une stratégie multicloud, il devient de plus en plus difficile de garantir une sécurité cohérente dans tous les environnements.

Où vos applications privées s'exécutent-elles actuellement ?



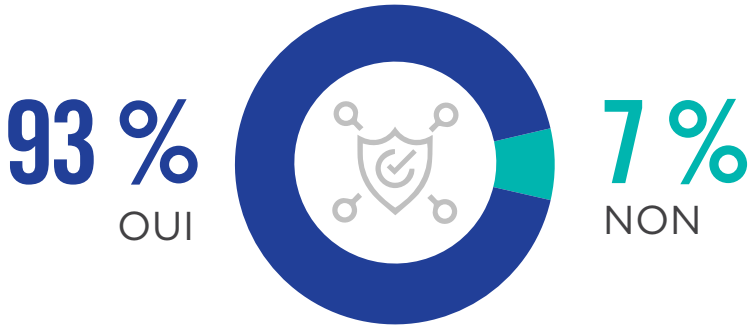
Autre 4 %

ÉTAT DU VPN

UTILISATION DU VPN ET NOMBRE DE PASSERELLES

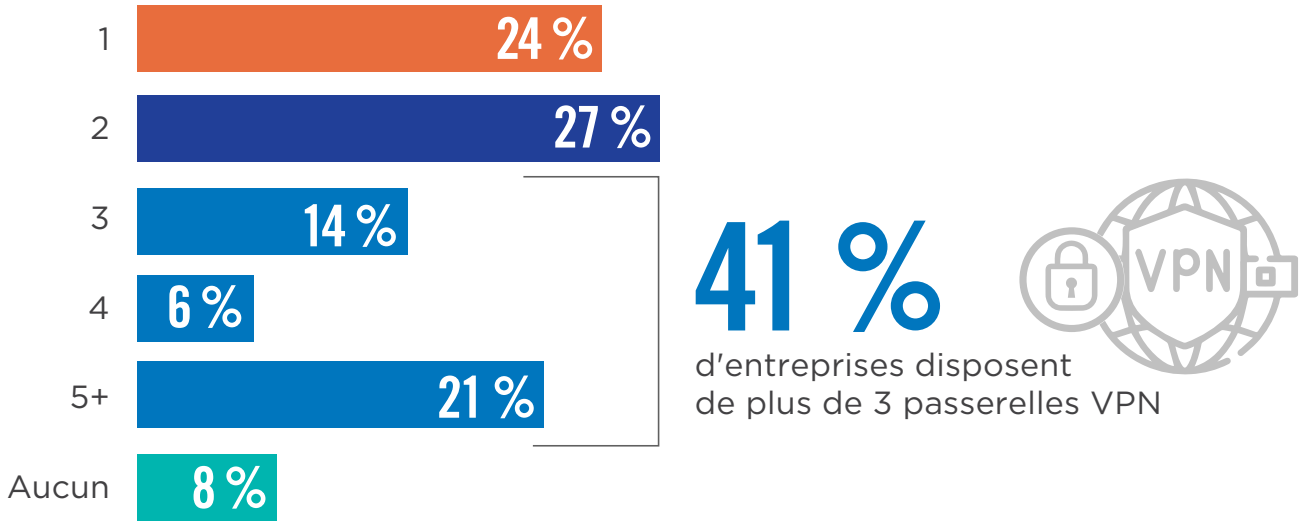
L'adoption de l'accès distant a considérablement augmenté en raison des événements imprévus de 2020. Bien que l'enquête ait révélé que **la grande majorité des entreprises utilisent actuellement un service VPN pour l'accès distant sécurisé (93 %)**, nous avons voulu avoir plus de détails quant à l'état actuel du VPN ainsi que la manière dont 2020 a affecté votre accès à distance.

Utilisez-vous actuellement un service VPN au sein de votre entreprise ?



Lorsqu'on demande aux répondants combien de passerelles VPN entrantes ils ont dans le monde, **41 % des entreprises déclarent en avoir 3 ou plus, et la moitié de ces entreprises déclarent en avoir 5 ou plus.** Chaque passerelle nécessite une pile d'appliances, comprenant souvent le VPN (RAS), un pare-feu interne, un équilibreur de charge interne, un équilibreur de charge global, un DDoS, un pare-feu externe, etc. Plus une entreprise possède de passerelles, plus l'accès distant sécurisé est coûteux et plus il est compliqué pour le service informatique d'administrer et de gérer chaque pile entrante.

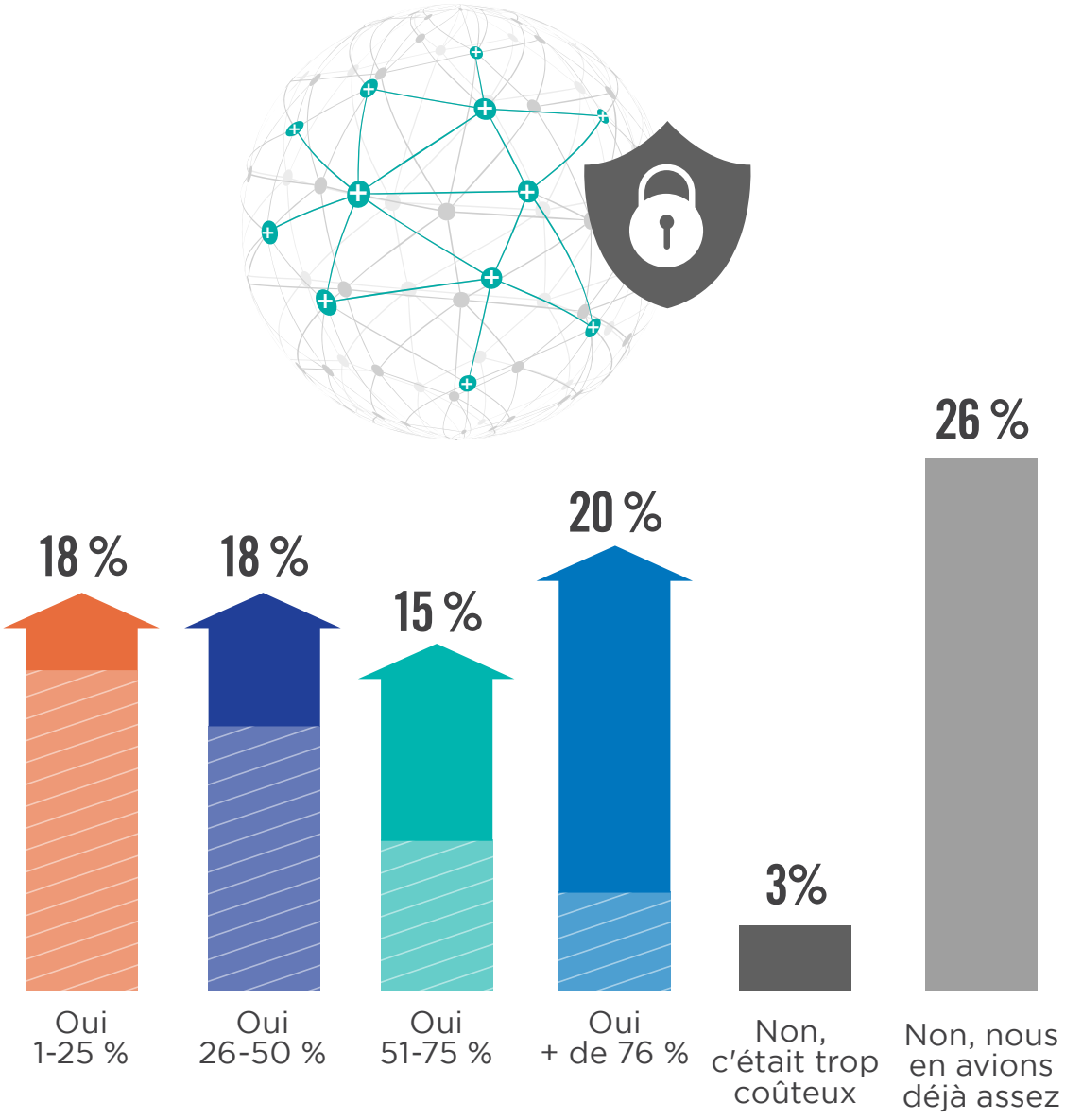
Combien de passerelles VPN entrantes avez-vous dans le monde ?



CAPACITÉ DU VPN ET ÉVOLUTIVITÉ

La pandémie de la COVID-19 a provoqué une augmentation du nombre de travailleurs à distance, **71 % des entreprises ayant déclaré avoir été contraintes d'augmenter leur capacité VPN. Parmi les entreprises qui ont eu besoin d'une bande passante supplémentaire, un tiers d'entre elles ont augmenté la capacité de leur VPN de plus de 50 %**. En revanche, 26 % des entreprises ont déclaré n'avoir pas eu besoin d'augmenter la capacité de leur VPN durant la pandémie. Cela pourrait indiquer que ces entreprises disposaient d'une capacité inutilisée avant l'épidémie et qu'elles dépensaient trop pour leur VPN.

Avez-vous augmenté votre capacité VPN durant la pandémie de la COVID-19 ? Si oui, de quel pourcentage ?



VPN : LES PLUS GRANDS DÉFIS

Si de nombreuses entreprises ont fait confiance au VPN pour un accès distant sécurisé avec un personnel de plus en plus mobile, ce n'est pas sans écueils. **Lorsqu'on leur demande de classer les défis les plus importants auxquels les entreprises sont confrontées avec leur solution d'accès distant, le manque de visibilité sur l'activité des utilisateurs vient en tête, suivi du coût exorbitant de l'infrastructure de sécurité.**

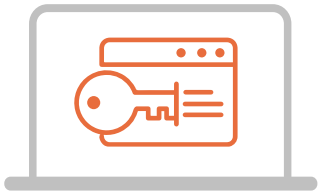
Quel est votre plus grand défi avec votre solution actuelle d'accès distant ?

24 %

Manque de visibilité sur l'activité de l'utilisateur

23 %

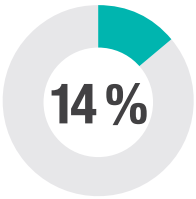
Coûts élevés des appliances/infrastructures de sécurité



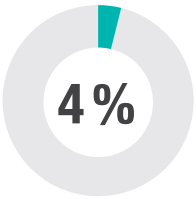
19 %

Exige de donner aux employés et aux tiers l'accès au réseau de l'entreprise

Mauvaise expérience utilisateur due aux backhauling vers les passerelles VPN



Complexité de la gestion des accès distants existants à travers les environnements de cloud public



Incapacité à s'adapter à la demande des utilisateurs

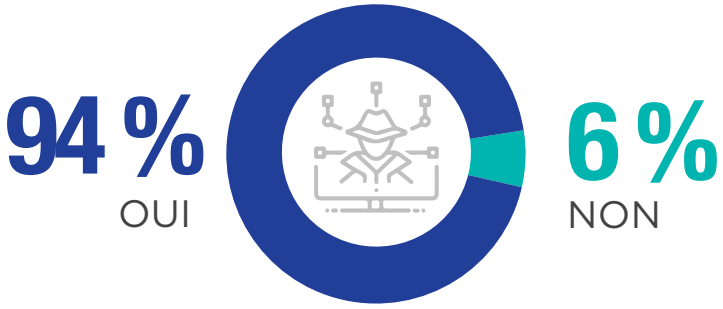
Les utilisateurs ne se connectant plus au bureau, le service informatique perd une part importante de l'activité de l'utilisateur, laissant beaucoup de points d'ombre quant à ce à quoi leurs utilisateurs accèdent. En outre, comme les entreprises ont dû adapter leur VPN en raison de l'augmentation de l'accès distant, le coût élevé des appliances et des infrastructures a grevé de nombreux budgets informatiques.

VULNÉRABILITÉS ET RISQUES LIÉS AU VPN

AUGMENTATION DES MENACES SUR LE VPN

L'explosion du télétravail a donc entraîné une hausse de popularité des attaques ciblées par VPN parmi les cybercriminels qui cherchent à obtenir un accès non autorisé aux ressources du réseau exposées à Internet. En fait, **94 % des entreprises savent que leurs VPN sont vulnérables aux cyberattaques et aux exploits,** pourtant elles continuent de tirer profit de cette technologie tout en étant conscientes du risque.

Savez-vous que les cybercriminels ciblent les VPN pour accéder aux ressources du réseau par le biais d'exploits tels que l'exploitation de codes à distance, de serveurs Windows, de ransomware et d'attaques d'ingénierie sociale ?



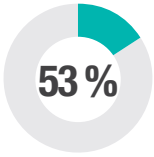
Lorsqu'on les interroge sur les attaques les plus préoccupantes basées sur Internet, **les entreprises s'accordent à dire que l'ingénierie sociale (75 %), les ransomwares (74 %) et les programmes malveillants (60 %) sont les vecteurs d'attaque les plus critiques.** Comme nous l'avons vu dans le passé, il suffit d'un seul appareil infecté ou d'une accréditation subtilisée pour mettre en danger un réseau entier, et c'est la raison pour laquelle les cybercriminels exploitent spécifiquement les utilisateurs qui accèdent au VPN.

Quel type d'attaques basées sur Internet vous préoccupe le plus ?

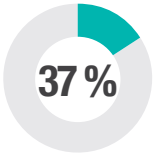
75 %
Ingénierie sociale

74 %
Ransomware

60 %
Programmes malveillants



Code d'exploits distant



Attaques DDoS

Autre 4 %

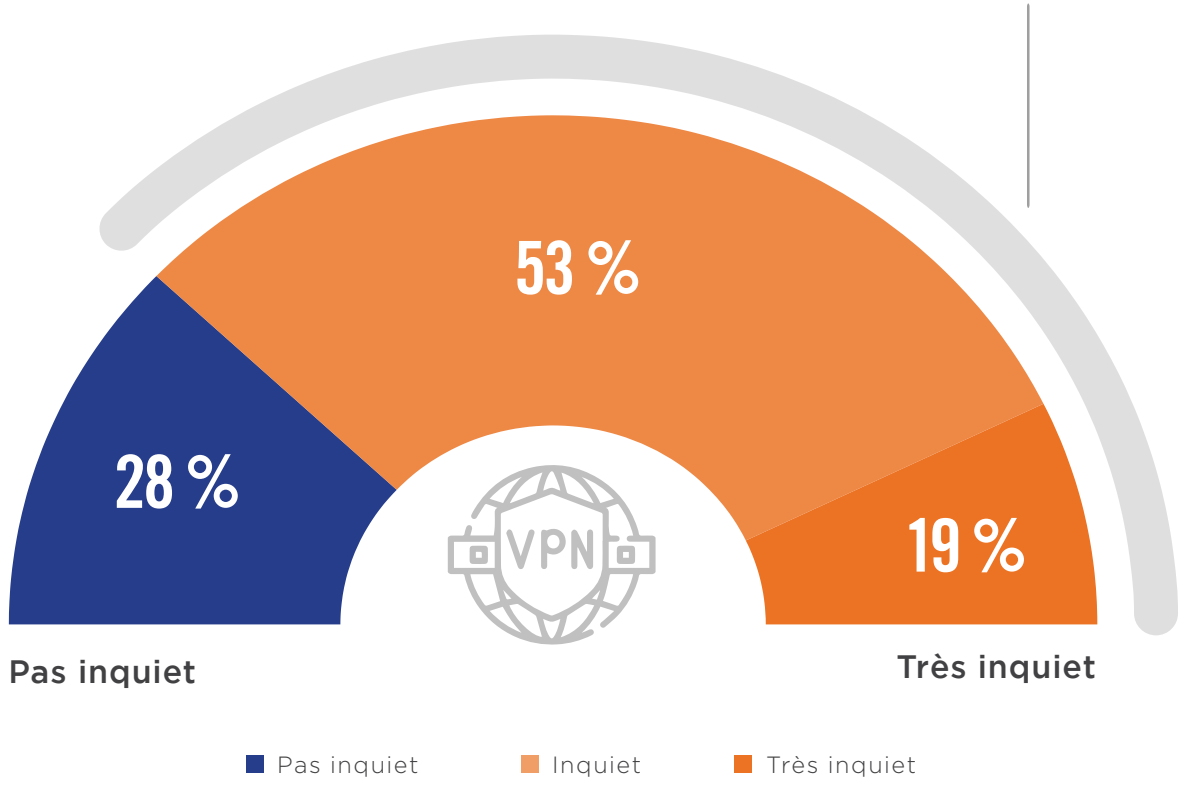
PRÉOCCUPATIONS AUTOUR DE LA SÉCURITÉ DU VPN

Soixante-douze pour cent des entreprises ont exprimé leur inquiétude de voir le VPN compromettre leur capacité à maintenir la sécurité de leurs environnements informatiques. La question se pose à tous les services informatiques : si votre solution d'accès distant sécurisé ne fournit pas le niveau de sécurité escompté, votre stratégie d'accès à distance doit-elle être ajustée ?

Dans quelle mesure craignez-vous que le VPN puisse compromettre votre capacité à assurer la sécurité de votre environnement ?

72 %

s'inquiètent que le VPN puisse compromettre la capacité à assurer la sécurité de l'environnement.



ALTERNATIVES AU VPN

Avec près de trois quart d'entreprises concernées par la sécurité des VPN, **la majorité des entreprises (67 %) envisagent des alternatives d'accès distant au VPN traditionnel.**

Au regard des vulnérabilités et des risques des VPN, 2021 semble être la fin de l'ère des VPN et le début d'une nouvelle ère vers l'adoption d'une stratégie zero trust.

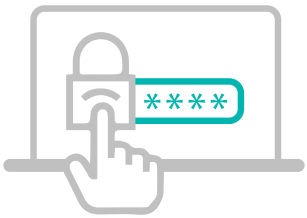
Avez-vous envisagé des alternatives d'accès distant au VPN traditionnel ?

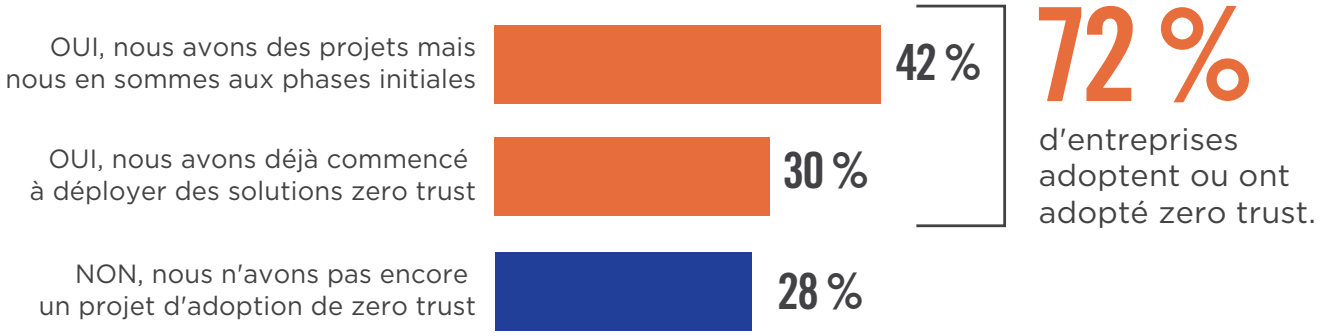
L'AVENIR DE L'ACCÈS DISTANT

ADOPTION ACCÉLÉRÉE DE ZERO TRUST

L'adoption d'une stratégie zero trust via le Zero Trust Network Access (ZTNA) et/ou Zero Trust Architectures (ZTA) a rapidement gagné du terrain ces dernières années. Avec l'augmentation du nombre de travailleurs à distance, **l'adoption de zero trust est devenue une priorité pour de nombreuses entreprises, 72 % d'entreprises confirmant leur intention d'adopter ce modèle.**

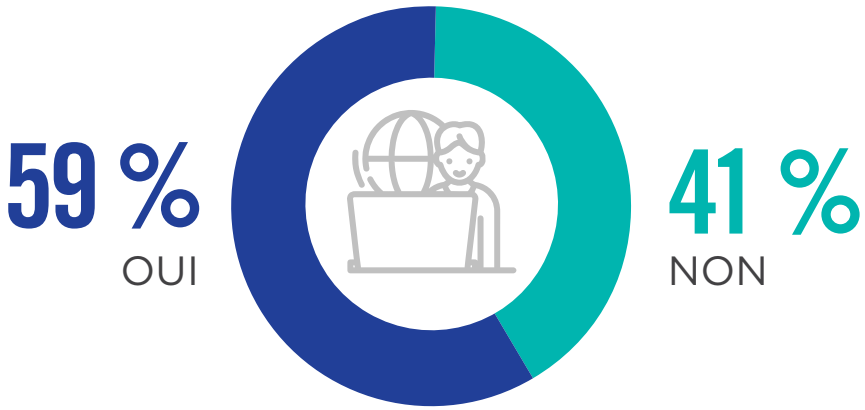
L'adoption d'un modèle zero trust est-elle une priorité pour votre entreprise ?





Non seulement les entreprises font de zero trust une priorité, mais **59 % des entreprises accélèrent également leurs projets zero trust pour une mise en œuvre plus rapide de la technologie au sein de leur entreprise.**

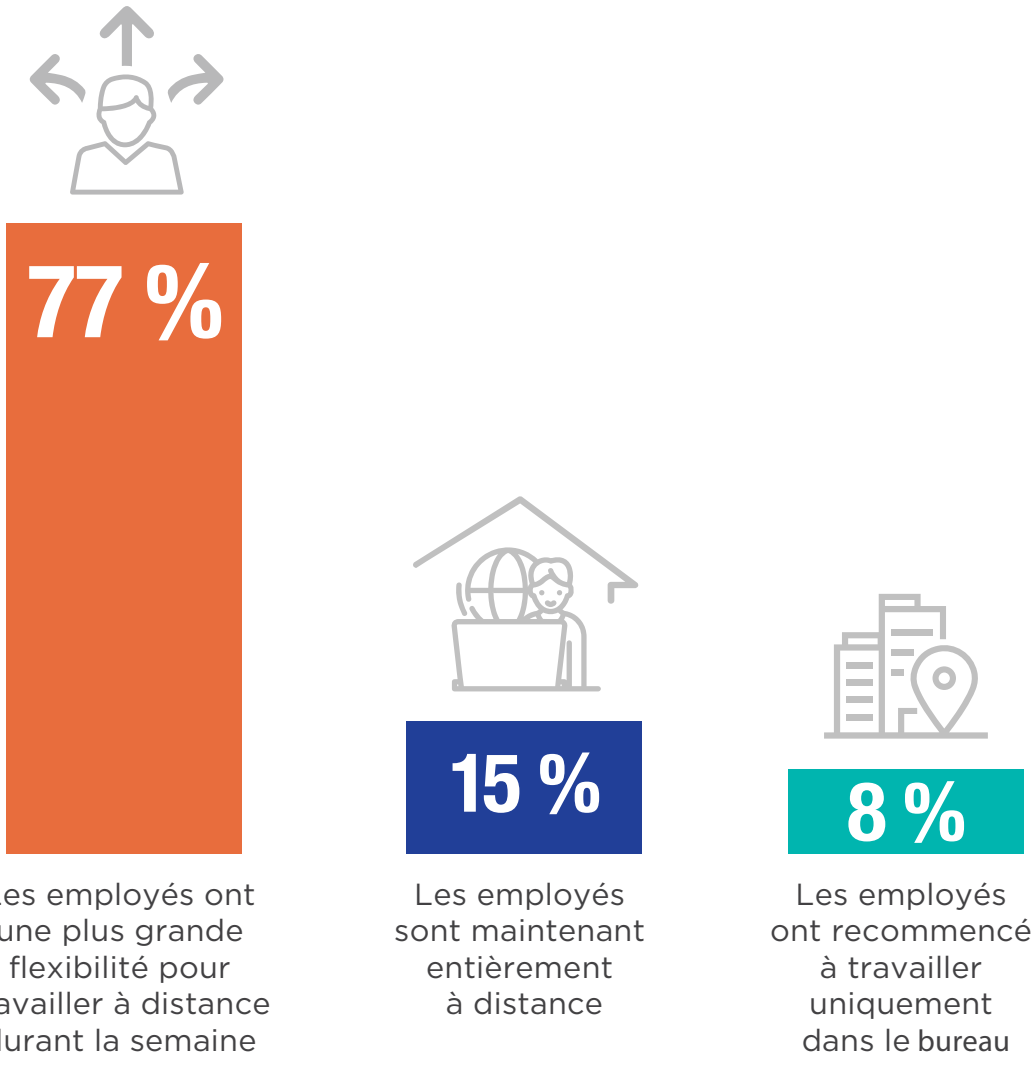
L'accent mis sur le télétravail a-t-il accéléré la priorité des projets zero trust au sein de votre entreprise ?



PROGRESSION DE L'ACCÈS DISTANT

Le passage à zero trust et au télétravail a été un catalyseur pour changer la façon dont les entreprises protègent l'accès distant. Interrogées sur leurs perspectives en matière d'accès distant, **77 % des entreprises déclarent que leur futur personnel sera hybride,** avec une plus grande flexibilité permettant aux utilisateurs de travailler à distance ou au bureau.

A l'horizon 2022, à quoi ressemble l'accès distant dans votre entreprise ?



Les employés ont une plus grande flexibilité pour travailler à distance durant la semaine

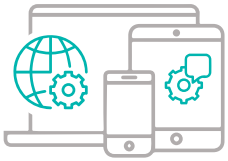
Les employés sont maintenant entièrement à distance

Les employés ont recommencé à travailler uniquement dans le bureau

PRINCIPALES CONCLUSIONS

Alors que le VPN a bénéficié de 30 années sous les feux des projecteurs, l'augmentation des attaques ciblées par VPN, ainsi que l'évolution continue vers la mobilité et le cloud, ont fait comprendre aux entreprises la nécessité de modifier leur stratégie d'accès distant sécurisé, laquelle repose sur les principes de zero trust.

En conclusion, voici les principaux points à retenir :



Avec l'expansion du télétravail, les utilisateurs sont partout, accédant aux applications depuis n'importe quel appareil, et aux applications à la fois dans le data center et le cloud.

Les VPN sont de plus en plus risqués, à mesure que les attaques d'ingénierie sociale, les ransomwares et les programmes malveillants gagnent du terrain, exposant l'entreprise à un risque accru.

Les entreprises sont préoccupées par le niveau de sécurité du VPN et cherchent à adopter une approche moderne d'accès distant, notamment un modèle zero trust.

La majorité des entreprises ont privilégié des plans pour adopter une stratégie zero trust. Alors que de nombreuses entreprises sont prêtes à permettre une main-d'œuvre hybride et la flexibilité du lieu de travail, l'adoption de zero trust devient essentielle.

Le VPN expose-t-il actuellement votre entreprise au risque ?

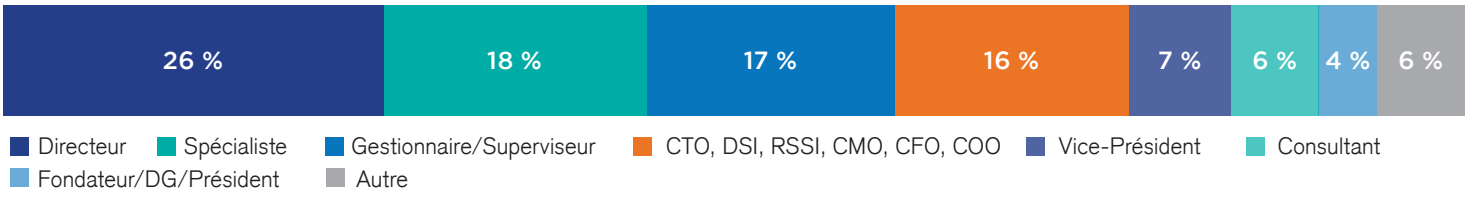
Obtenez une évaluation gratuite des risques et découvrez la surface d'attaque de votre réseau avant que les acteurs malveillants ne le fassent.

DÉCOUVREZ VOTRE SURFACE D'ATTAQUE

MÉTHODOLOGIE ET DONNÉES DÉMOGRAPHIQUES

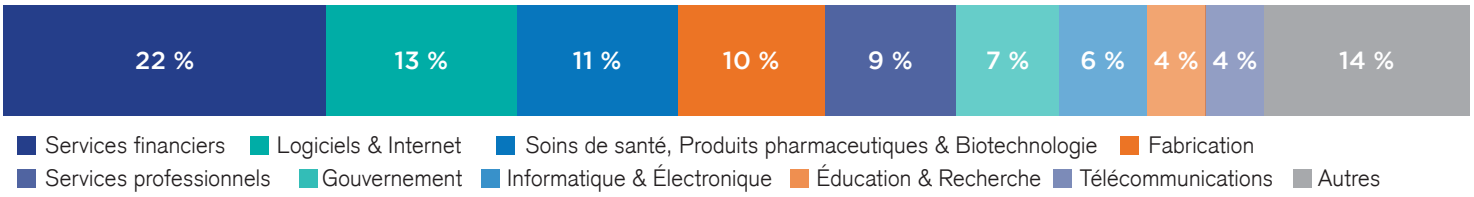
Ce rapport est basé sur les résultats d'une enquête exhaustive en ligne menée en janvier 2021 auprès de 357 professionnels de l'informatique et de la cybersécurité, afin d'identifier les dernières tendances, défis, failles et préférences des entreprises en matière d'adoption de solutions liées au risque du VPN. Les répondants vont des cadres techniques aux professionnels de la sécurité informatique, représentant un échantillon équilibré d'entreprises de tailles diverses dans de multiples secteurs.

NIVEAU PROFESSIONNEL



TAILLE DE L'ENTREPRISE

INDUSTRIE



À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale afin que les clients puissent être plus agiles, plus efficaces, plus résistants et plus sécurisés. 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 appareils, et les applications en tout lieu. Répartis sur plus de 150 data centers à l'échelle mondiale, Zero Trust Exchange basé sur SASE, est la plus grande plateforme de sécurité cloud en ligne dans le monde. Pour en savoir plus, consultez le site zscaler.com ou suivez-nous sur Twitter @zscaler.

zscaler.com