Offrez une expérience de télétravail efficace et sécurisée

Assurez la sécurité et la productivité de vos employés en utilisant le cloud.

zscaler™

Presque toutes les organisations parlent depuis des années des meilleurs moyens de sécuriser une main-d'œuvre à distance, mais en ces temps sans précédent, de nombreuses organisations se trouvent contraintes d'y recourir — immédiatement. Que se passe-t-il lorsque vous êtes soudainement confronté à la nécessité de faire travailler tous vos employés depuis le domicile?

Six exigences pour une main-d'œuvre à domicile productive et sécurisée

La clé de la résilience des entreprises consiste à protéger la santé de vos employés tout en leur donnant les moyens d'être aussi productifs et sécurisés à la maison qu'au bureau. Pour obtenir cette résilience, votre solution d'accès à distance doit répondre à certaines exigences clés.

1. **Toutes les demandes:**
   Accès sécurisé à toutes les applications externes (Internet, SaaS) et internes (data center, Azure, AWS)

2. **Gestion d'accès aux identités cloud:**
   Optimisée pour les intégrations entre appareils, applications SaaS internes et externes

3. **Expérience utilisateur rapide:**
   Une collaboration productive grâce aux outils tels que Microsoft Teams et Zoom

4. **Sécurité et conformité:**
   Protection contre la cybermenace et prévention des pertes de données entre utilisateurs

5. **Déployable en quelques jours:**
   Agilité et simplicité pour un déploiement rapide

6. **Visibilité et dépannage:**
   Visibilité et outils nécessaires pour diagnostiquer les problèmes des utilisateurs lorsqu'ils sont hors réseau

Défis liés au soutien d'un programme de travail à domicile avec une infrastructure informatique traditionnelle

Incapacité à évoluer rapidement

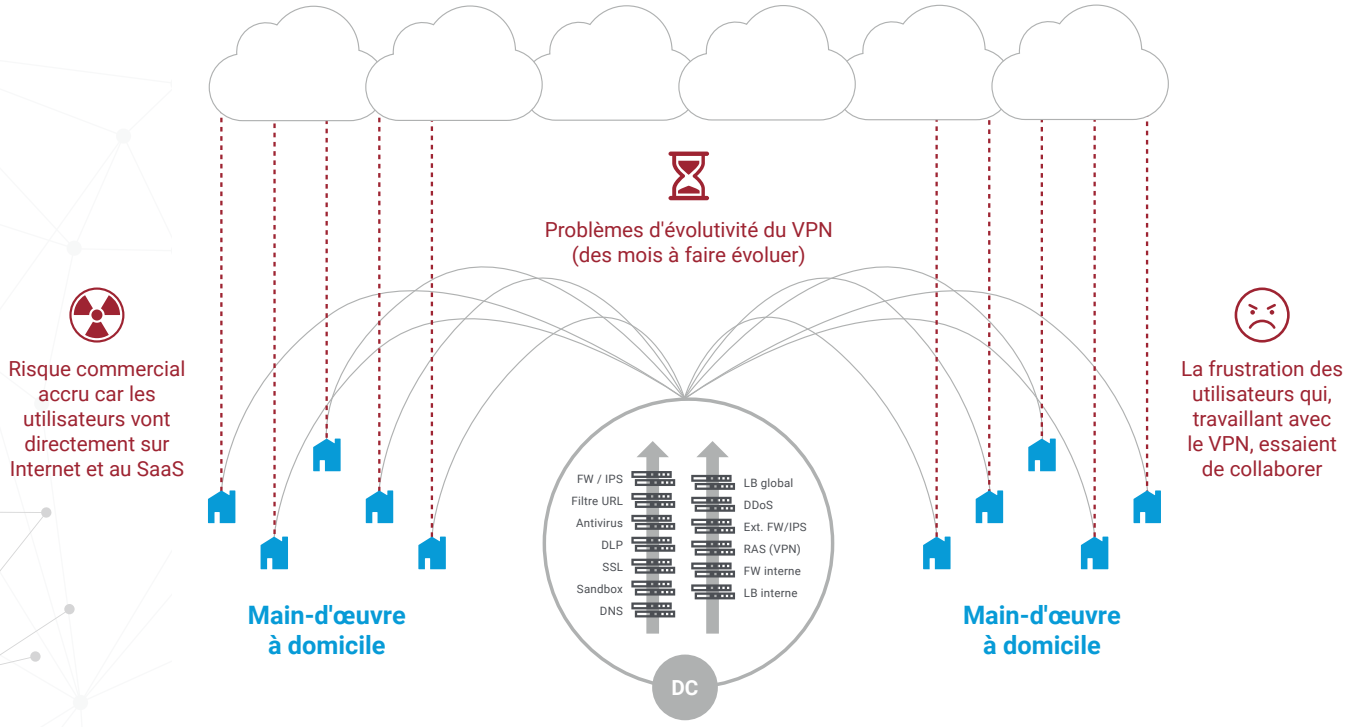
L'acquisition, la configuration, le rangement et l'empilage d'appareils VPN et de passerelles d'appliances supplémentaires pour accueillir une importante main-d'œuvre à domicile peuvent prendre des semaines, voire des mois, avec des perturbations dans la chaîne d'approvisionnement du matériel. De tels retards affectent la productivité des employés, ce qui en retour a une incidence sur les performances de l'entreprise. L'installation de machines virtuelles d'appliances à locataire unique comme solution de rechange augmentera non seulement la complexité, mais vos risques également, car chaque firewall exposé à Internet est une surface d'attaque et a été le point d'entrée de certaines des plus grandes attaques de ransomware.

Exposition accrue aux risques

Bien que le VPN soit nécessaire pour accéder aux applications internes du data center, il n'est pas indispensable pour accéder à Internet et aux applications SaaS. Les utilisateurs à la recherche d'une expérience rapide à domicile accèderont directement à ces applications sans que les contrôles de sécurité appropriés soient en place. Les cybercriminels en sont bien conscients et se sont investis dans le lancement de nouveaux ransomware, des campagnes d'ingénierie sociale sophistiquées et des attaques ciblées.

Mauvaise expérience utilisateur

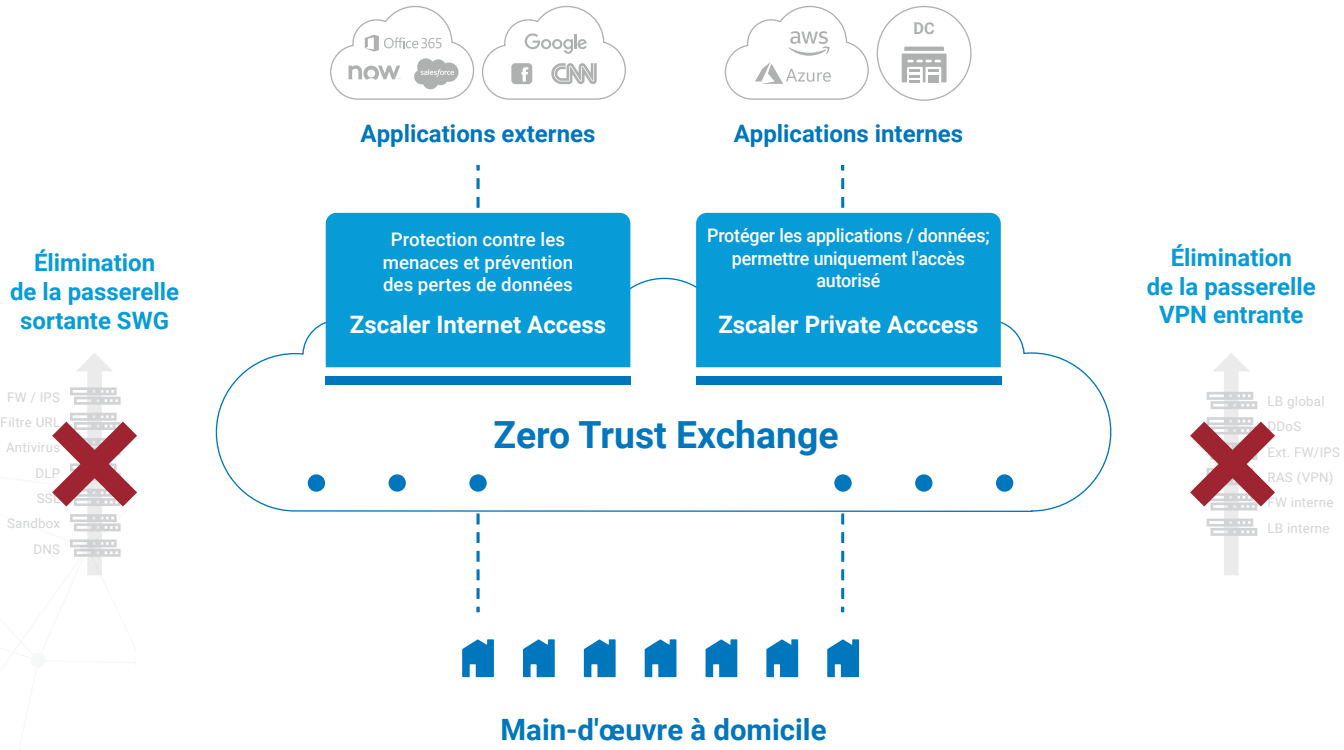
Des applications telles qu'Office 365 et Zoom jouent un rôle essentiel pour faciliter la collaboration et stimuler la productivité d'une main-d'œuvre décentralisée. Le défi est que ces applications SaaS et d'autres ont été conçues pour être accessibles directement. Le backhauling du trafic via une connexion VPN vers une passerelle internet centralisée induit une latence qui est frustrante et, pire encore, inhibe la capacité des utilisateurs à collaborer.



Une expérience de travail à domicile rapide et sécurisée nécessite un cloud de sécurité spécialement conçu

Les entreprises ont transféré des applications et des infrastructures vers le cloud spécifiquement pour son agilité, un avantage essentiel car les organisations doivent se déplacer rapidement et efficacement à tout moment. Lorsque des événements imprévus qui menacent de perturber les affaires se produisent, ce besoin devient encore plus aigu.

En tant que plateforme multi-entité, Zscaler a été conçu dès le départ pour permettre aux clients de se déplacer en toute sécurité dans le monde moderne — le monde dans lequel le cloud est le nouveau data center et Internet le nouveau réseau. Les services de la plate-forme Zscaler ont été développés pour garantir que les entreprises puissent fonctionner dans n'importe quelles conditions, à n'importe quelle échelle, n'importe où dans le monde — à la maison ou au bureau — et sur n'importe quel appareil. Nous disposons de plus de 150 data centers répartis dans le monde entier pour rapprocher la sécurité de nos clients, et nous continuons chaque jour d'augmenter la capacité du cloud.



- **Une architecture multi-entité, native du cloud** qui évolue de manière dynamique
- **Distribution mondiale** à travers plus de 150 data centers répartis sur les six continents
- **Des centaines de partenariats de peering** dans tous les grands échanges Internet
- **Une architecture basée sur proxy** pour une inspection complète du trafic crypté à grande échelle
- **Le Cloud reçoit plus de 120.000** mises à jour de sécurité uniques au quotidien, toutes les 15 minutes et à la demande avec plus de 40 flux de menaces externes
- **Le Cloud traite 95 milliards de transactions** par jour et nous appliquons des modèles AI et ML pour identifier et bloquer les menaces dès leur apparition
- **Les protections sont transmises à chaque utilisateur** dès qu'une menace est détectée n'importe où dans le cloud

Comment Zscaler peut assurer la réussite et la sécurité du télétravail

Permet un accès sécurisé à toutes les applications internes (DC, AWS, Azure) et externes (SaaS, internet)

Pour une expérience de travail à domicile productive, vos employés ont besoin du même niveau de sécurité et d'un accès libre à leurs applications que celui dont ils disposent au bureau. Le défi est que, bien que le VPN soit nécessaire pour accéder aux applications internes, les utilisateurs le désactiveront en cas de problème – performances médiocres ou connexions VPN interrompues – et accéderont à l'internet et aux applications SaaS sans que les contrôles de sécurité appropriés soient en place. Vous pouvez éviter ce risque. Zscaler offre une expérience transparente aux utilisateurs distants sans qu'ils aient besoin de se connecter et de se déconnecter; au contraire, l'accès est continu, indépendamment des changements de connectivité réseau, et la sécurité est appliquée instantanément dans le cloud.

Élimine le VPN et offre une plus grande sécurité ainsi qu'une meilleure expérience utilisateur

Zscaler propose une approche moderne pour sécuriser l'accès aux applications sans les implications en termes de performance du backhauling de trafic via les VPN, qui peuvent rapidement être submergés par des pics d'utilisation. Avec Zscaler, les utilisateurs se connectent localement à leurs applications via le cloud Zscaler, qui est réparti dans 150 data centers dans le monde entier. Les utilisateurs sont protégés par une sécurité complète et l'application de politiques, quel que soit l'endroit où ils se connectent. Une fois Zscaler en place, non seulement vous éliminez le coût élevé de la mise à l'échelle de votre infrastructure de passerelle VPN entrante, mais vous pouvez également commencer à la supprimer progressivement.

S'intègre à la gestion des identités et des accès (IAM) dans le cloud pour un accès conditionnel

La migration des applications et des données de votre entreprise vers le cloud signifie que vous devez pouvoir garder un contrôle optimal quant aux employés qui peuvent accéder à ces ressources cloud. Les solutions de gestion des identités et des accès (IAM) dans le Cloud centralisent les services d'identité et d'authentification, ce qui donne à vos équipes informatiques un plus grand contrôle sur votre environnement Cloud et sa sécurité, et leur permet de suivre quels utilisateurs accèdent à quelles applications, et quand. Zscaler dispose d'une intégration profonde avec les principaux fournisseurs de solutions IAM, notamment Azure AD, Okta et Ping, afin d'appliquer des politiques d'accès contextuelles.

> "ZPA a été un outil déterminant du plan de continuité d'activité de DB Schenker, avec pour corollaire le refus de nos utilisateurs de retourner à des connexions VPN traditionnelles."

DB SCHENKER

Gerold Nagel
SVP, Global Infrastructure Services

Permet en quelques jours aux employés d'être opérationnels—non en semaines ou en mois

Zscaler est un service 100% cloud qui est rapide et facile à déployer car il n'est pas nécessaire d'installer, de configurer ou de gérer des appliances. L'accès est basé sur des politiques d'entreprise hébergées dans le cloud de Zscaler, et le trafic des utilisateurs est transmis localement à Zscaler par l'intermédiaire de Z App, une application légère qui peut être facilement distribuée par des systèmes MDM comme Microsoft Intune; pour les applications web, les utilisateurs n'ont besoin que d'un navigateur pour y accéder.

Zscaler s'intègre avec les fournisseurs d'identité pour authentifier les utilisateurs et appliquer un accès contextuel plutôt que de se fier aux ACL ou aux adresses IP. Les App Connectors, qui sont de petites machines virtuelles, placent en avant des applications internes et utilisent des microtunnels inversés pour connecter un utilisateur à une application autorisée. Zscaler s'occupe de tout le routage et de l'équilibrage de charge, de sorte que vous n'avez pas à vous soucier de la mise à l'échelle de votre infrastructure.

Garantit la sécurité de vos employés et de vos données

Les cybercriminels se sont investis dans le lancement de nouveaux programmes malveillants, des campagnes d'ingénierie sociale sophistiquées, des attaques ciblées, etc. et ils sont bien conscients du fait que de nombreux utilisateurs travaillant à domicile se trouvent généralement sur un réseau d'entreprise derrière un périmètre de sécurité. En déplaçant la sécurité vers un cloud distribué à l'échelle mondiale, Zscaler rapproche l'ensemble de la pile de sécurité Internet (protection avancée contre les menaces, inspection SSL, prévention des pertes de données, sandboxing, isolation du navigateur à distance et CASB) de l'utilisateur pour une expérience rapide et sûre. Peu importe où les utilisateurs se connectent, leur politique de sécurité les suit.

Offre une visibilité et un dépannage rapide pour diagnostiquer les problèmes des utilisateurs

La capacité de surveiller l'activité du réseau devient un défi d'un autre genre lorsque tous vos employés travaillent à domicile, souvent sur des appareils non gérés, et que votre réseau est l'Internet. Outre la visibilité en temps réel des utilisateurs et des applications, vous devez être en mesure de voir exactement ce qui se passe à chaque point entre l'appareil d'un utilisateur et la porte d'entrée d'une application afin d'identifier rapidement la source de toute difficulté à l'origine de problèmes de performances, de manière à pouvoir prendre des mesures correctives.

> "J'ai fait savoir à mon équipe de direction de NOV que les 27.500 utilisateurs pouvaient commencer à travailler à distance grâce à Zscaler. Ils étaient stupéfaits!"

Alex Philips
CIO, National Oilwell Varco

La plateforme Zscaler Cloud Security

Les services Zscaler sont fournis à 100% dans le cloud et offrent un accès rapide, sécurisé et fiable à Internet et aux applications cloud, ainsi qu'aux applications privées dans le data center ou les cloud publics et privés. L'accès est basé sur des politiques commerciales définies par logiciels qui suivent les utilisateurs, quel que soit l'endroit où ils se connectent ou les appareils qu'ils utilisent.

> "L'une des choses que nous fournissons est une approche de type "application par application" pour donner aux gens ce dont ils ont besoin, sans avoir à sur-approvisionner l'accès. Avec la combinaison de ZIA et ZPA, nous sommes beaucoup plus flexibles quant à ce que nous pouvons fournir et puisque nous y faisons passer tout notre trafic, nous savons qu'il peut évoluer."
>
> **Mike Towers**
> CSO, Takeda Pharmaceuticals

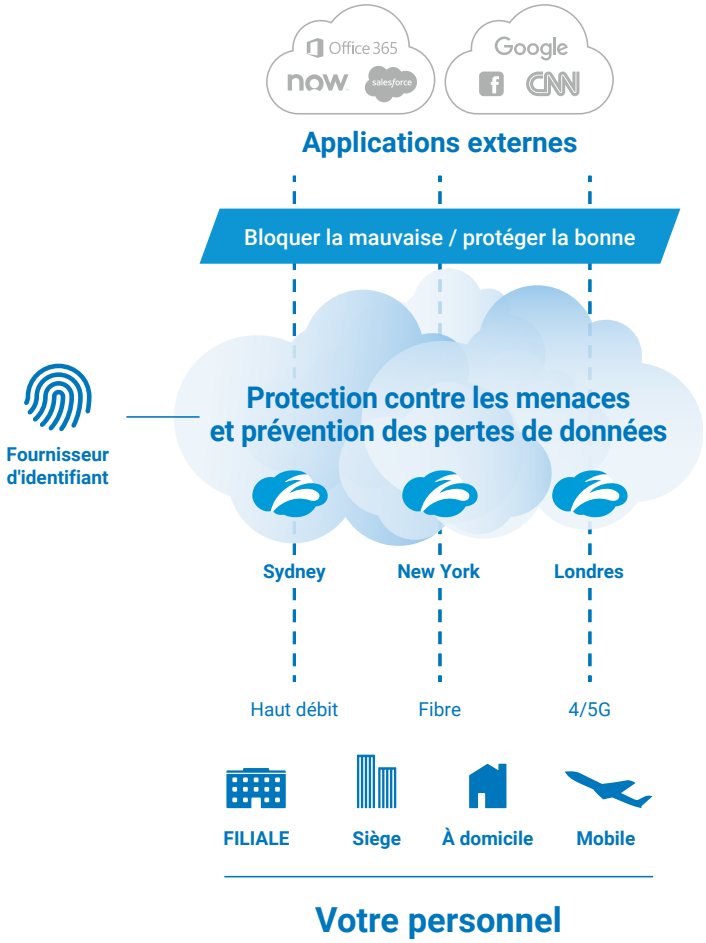
Zscaler Internet Access™ (ZIA™) et Zscaler Private Access™ (ZPA™) constituent la plate-forme Zscaler Cloud Security, qui déplace les passerelles de sécurité entrantes et sortantes vers le cloud. En faisant de Zscaler votre premier saut sur Internet, chaque connexion est sécurisée et les politiques sont appliquées quel que soit l'endroit où les utilisateurs se connectent ou le lieu d'hébergement des applications.

Zscaler Internet Access: votre pile de sécurité en tant que service

Zscaler Internet Access (ZIA) offre à partir du cloud une pile de sécurité complète en tant que service, éliminant ainsi le coût et la complexité des approches traditionnelles de passerelle web sécurisée. En déplaçant la sécurité vers un cloud mondialement distribué, Zscaler rapproche la passerelle Internet des utilisateurs pour une expérience plus rapide. Les organisations peuvent facilement faire évoluer la protection à tous les bureaux ou utilisateurs, quel que soit leur emplacement, et diminuer l'infrastructure des réseaux et des appliances.

Le trafic de votre utilisateur distant est transféré vers Zscaler Cloud via notre légère Zscaler App ou notre fichier PAC. Zscaler Internet Access se situe entre vos utilisateurs et Internet, inspectant chaque octet de trafic inline à travers de multiples techniques de sécurité, même au sein du trafic SSL. Vous bénéficiez d'une protection totale contre les menaces du web et d'Internet. Et grâce à une plateforme de cloud qui prend en charge **le cloud sandboxing**, **un firewall de nouvelle génération**, **la prévention des pertes de données (DLP)**, **l'isolation du navigateur**, et **le CASB**, vous pouvez commencer avec les services dont vous avez besoin aujourd'hui et en activer d'autres au fur et à mesure que vos besoins augmentent.

Pour en savoir plus, lisez **la fiche technique de ZIA** ou regardez cette **vidéo**.

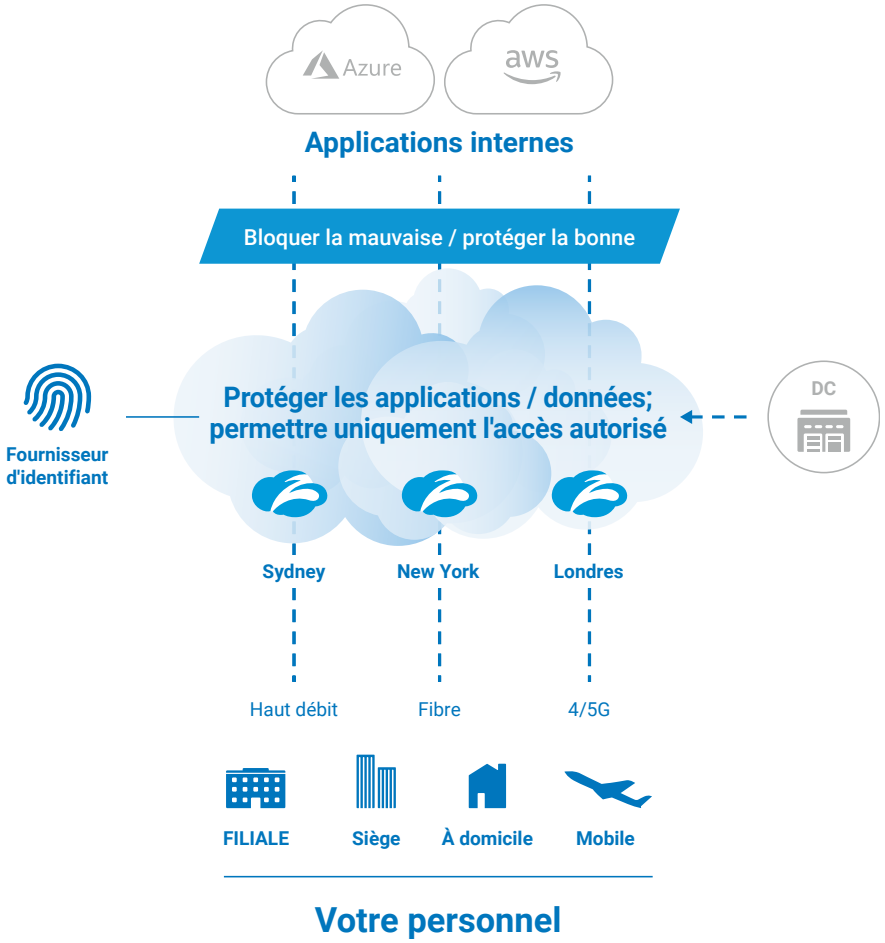


Zscaler Private Access: Une alternative évolutive au VPN

Zscaler Private Access (ZPA) fournit aux utilisateurs un accès rapide et sécurisé aux applications gérées en interne dans le data center et les cloud publics. Pour les utilisateurs, ZPA offre une expérience transparente, ne nécessitant pas de backhauling ou de connexions fastidieuses. Il n'est pas nécessaire d'activer un VPN pour accéder à l'application; il vous suffit d'accéder à l'application et elle fonctionne. L'architecture ZPA offre également des avantages clés en matière de sécurité. Les adresses IP ne sont jamais exposées, ce qui rend impossible les attaques DDoS. Qui plus est, étant donné que les utilisateurs ne sont jamais placés sur le réseau, ZPA réduit le risque de mouvement latéral et de propagation des programmes malveillants.

Comment ça fonctionne ? La ZPA crée un segment sécurisé entre un utilisateur nommé et une application nommée, garantissant que seuls les utilisateurs autorisés ont accès à des applications privées spécifiques. L'accès est basé sur les politiques commerciales que vous définissez dans la console Zscaler Admin. ZPA offre une expérience utilisateur rapide et transparente. Au lieu de se connecter à leur client VPN (et de continuer à le faire chaque fois qu'ils démarrent une session), les utilisateurs ouvrent simplement Zscaler App sur leur ordinateur portable, leur téléphone mobile ou leur tablette, pour des connexions locales rapides.

Pour en savoir plus, regardez cette **vidéo sur tableau blanc** et téléchargez la **fiche technique ZPA**.



Démarrer avec Zscaler est simple et rapide

Les services Zscaler sont à 100% basés sur des logiciels et peuvent être déployés en quelques jours.

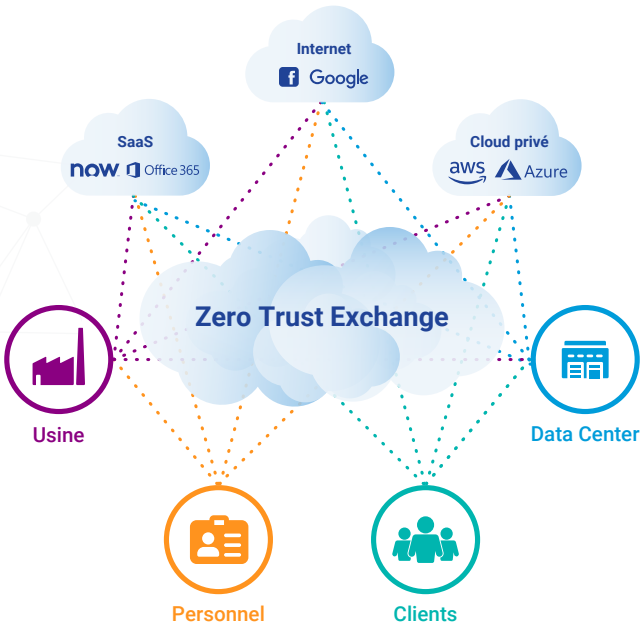
Déployez Zscaler App Connectors, ces petites machines virtuelles qui se placent devant vos applications privées dans le data center ou dans des cloud publics ou privés.

Installez Zscaler App (Z App), une application légère, qui peut facilement être distribuée par le biais de votre solution de gestion des appareils mobiles (MDM). Z App assure la posture de l'appareil de l'utilisateur et étend un microtunnel sécurisé au cloud Zscaler.

Configurez la politique dans la console Zscaler Admin. Vous définissez les politiques d'accès une fois et elles suivent les utilisateurs quel que soit l'endroit où ils se connectent.

Protégez vos employés. Protégez votre entreprise. Alors que les organisations déplacent leurs applications et leur infrastructure vers le cloud et que les utilisateurs quittent le réseau, Zscaler s'est attaché à fournir une sécurité permanente et fournie par le cloud. Aujourd'hui, plus de 400 organisations du Forbes Global 2000 font confiance à Zscaler pour offrir une expérience utilisateur rapide tout en sécurisant toute connexion entre leurs utilisateurs, applications et périphériques, quel que soit le réseau.

Une fois que vous avez mis en place une expérience de travail à domicile productive et sûre, vous pouvez commencer à penser plus largement à votre infrastructure WAN et à la sécurité de votre réseau. Dans le monde moderne du cloud et de la mobilité, le réseau n'est plus le centre de gravité, alors pourquoi continuer à investir dans une infrastructure de sécurité basée sur le réseau?



Zscaler cloud fonctionne comme une bourse Zero trust, permettant une connectivité sécurisée, de n'importe où.

En savoir plus sur les services Zscaler et sur **la façon d'activer vos initiatives de travail à domicile — en toute sécurité.**

www.zscaler.com/continuité des activités

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com