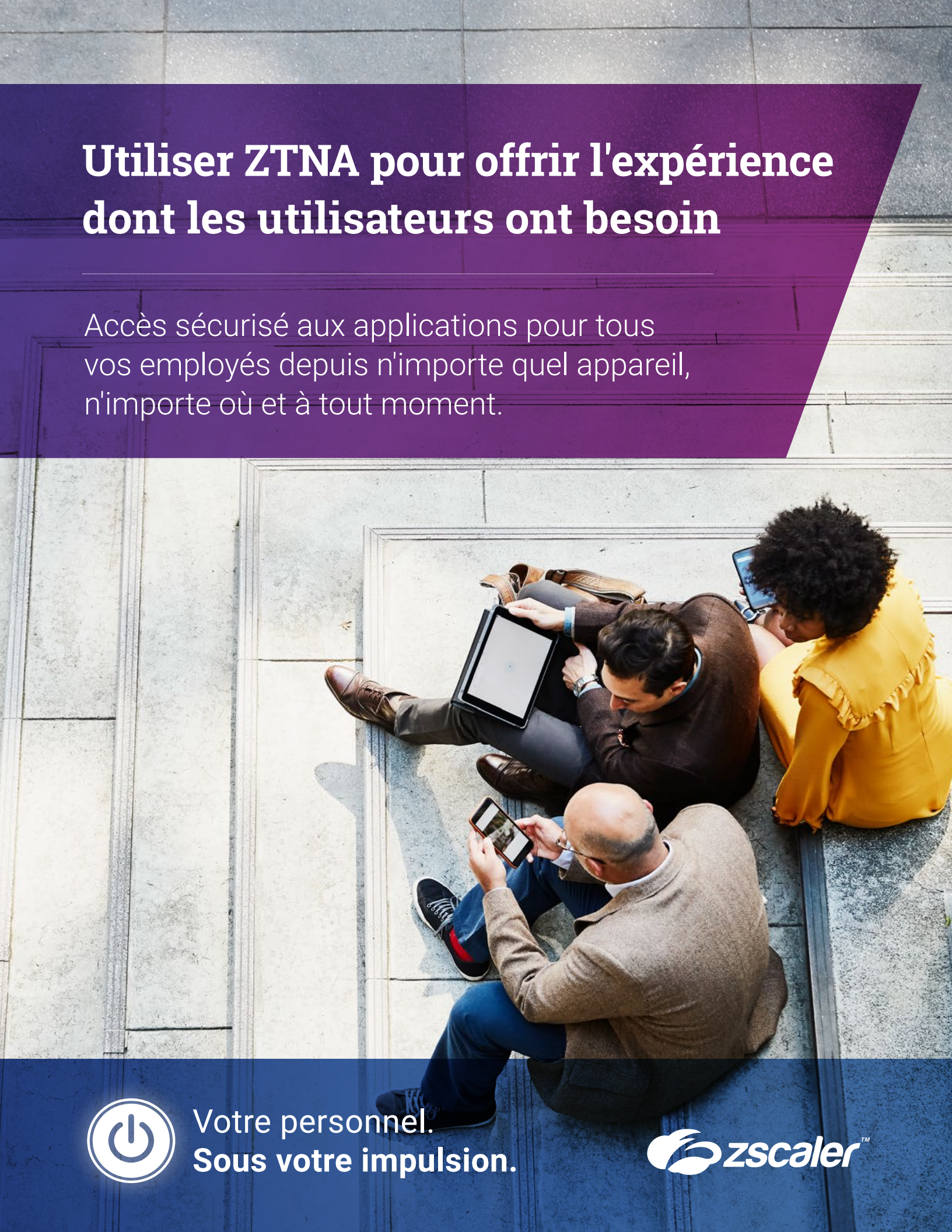
Utiliser ZTNA pour offrir l'expérience dont les utilisateurs ont besoin

Accès sécurisé aux applications pour tous vos employés depuis n'importe quel appareil, n'importe où et à tout moment.



Votre personnel.
Sous votre impulsion.

zscaler™

"Nous voulons que les gens n'aient pas à réfléchir à la manière dont ils auront accès à leurs applications, et nous voulons rapidement valoriser cette capacité avec le moins de frictions possible".

- Mike Towers, CSO Takeda

Votre base d'utilisateurs a évolué

Nous sommes en 2020 et vos employés ne sont plus cloîtrés au bureau. Ils travaillent depuis le domicile, les hôtels, et même les aéroports. Les appareils qu'ils utilisent ne sont plus des appareils BlackBerry gérés qui leur ont été donnés par l'équipe chargée des terminaux. Ils utilisent des smartphones, des tablettes et des ordinateurs portables personnels, à la fois pour les divertissements et le travail.

Vous avez la responsabilité non seulement de sécuriser vos employés, mais aussi les prestataires tiers qui figurent également sur la liste de paie de l'entreprise. Tous ces utilisateurs ont besoin d'un accès identique aux applications privées quels que soient les appareils, emplacements et types d'applications. Fournir l'accès à partir de ces appareils, sans compromettre la sécurité, était jadis mission impossible. Ce n'est plus le cas.

Un coup d'œil sur votre portefeuille d'utilisateurs

Avec une main-d'œuvre diversifiée et désormais répartie dans le monde entier: fournir un accès sécurisé aux applications privées est devenu un véritable défi pour les équipes informatiques. Même si la main-d'œuvre est différente de ce qu'elle était il y a 15 ans, il y a toujours quelque chose qu'elles ont en commun, c'est que tous vos utilisateurs ont besoin d'un accès rapide et fiable aux applications privées pour assurer le bon fonctionnement de l'entreprise. Votre main-d'œuvre moderne peut ressembler à ceci:

Le voyageur

Sam Davis, vice-président des ventes

"Je suis probablement en déplacement environ 75% du temps. Le plus souvent, je suis dans un aéroport, un hôtel ou un site client essayant de faire le travail dans les périodes d'attente. Bien que mon environnement professionnel soit en constante évolution, j'ai toujours besoin d'accéder rapidement à nos ressources commerciales pour pouvoir mieux servir nos clients."

Le local

Danielle Allen, directrice des finances

« Je suis basée dans notre siège social à San Jose, en Californie et je suis, pour la plupart, un employé "de bureau". Je reçois des demandes au quotidien de la part d'autres employés sollicitant leurs paiements. J'utilise constamment nos applications financières et ai besoin d'y accéder rapidement pour pouvoir suivre les demandes.»

L'entrepreneur

Elaina Thalin, Entrepreneur en développement Web

"Je suis sous contrat avec l'entreprise depuis environ 8 mois maintenant. Bien que je ne sois ni une employée ni dans un bureau, j'ai toujours besoin d'accéder à quelques applications privées pour effectuer mon travail. Au cas où je n'y accède pas, je ne peux vraiment pas faire mon travail."

Le télétravailleur

Justin Miller, Directeur du marketing

"Je vis en Floride et suis souvent touché par les alertes météorologiques, y compris les ouragans. À ces moments-là, j'ai dû assurer ma sécurité et celle de ma famille tout en assumant mes responsabilités professionnelles".

Quel que soit le type d'utilisateur ou la fonction, votre personnel doit pouvoir accéder à vos applications privées rapidement et en toute sécurité, où qu'il se trouve. Le service informatique doit être doté de la technologie appropriée pour rendre cela possible et garantir que la sécurité n'entrave pas la productivité des utilisateurs. C'est la raison pour laquelle le VPN n'est pas l'outil idoine pour la main-d'œuvre moderne.

Vos utilisateurs méritent mieux que le VPN

Les VPN ayant été développés il y a plus de 30 ans, ils ne sont plus adaptés à la main d'œuvre moderne, car leur conception de sécurité défectueuse offre une mauvaise expérience utilisateur.

Latence élevée, échelle limitée et mauvaise expérience

Les VPN ont été conçus pour sécuriser l'accès au réseau. Cela signifie que tout le trafic utilisateur est d'abord redirigé vers le data center, même si les applications s'exécutent désormais dans le cloud public. Cela provoque le tromboning du réseau, qui à son tour crée de la latence pour les utilisateurs. De plus, les appliances VPN ont des limitations de capacité utilisateur et peuvent déborder si trop d'utilisateurs accèdent au serveur VPN à la fois.

Connexions répétitives et interrompues

Chaque fois qu'il y a un changement ou une inactivité du réseau, la connexion VPN chute. Pour une main-d'œuvre désormais mobile, cela peut se produire assez fréquemment, entraînant la frustration des utilisateurs et une perte de productivité.

Incertitudes quant au moment d'utiliser un VPN... Ou pas

Il arrive souvent que vos utilisateurs ne sachent même pas quelle est la différence entre vos applications publiques et privées. Aujourd'hui, avec la migration des applications vers le cloud, l'utilisateur est encore plus confus lorsqu'il s'agit de savoir quand, où et comment il devrait utiliser le VPN. Il va sans dire que le VPN n'est ni transparent ni intuitif pour vos utilisateurs.

Tout comme Netflix n'aurait pas pu naître d'une simple connexion de milliers de lecteurs DVD, les solutions d'accès aux applications privées pour un accès en tout lieu et à tout moment doivent être spécialement conçues. Elles doivent être en permanence disponibles, hautement évolutives et centrées sur l'utilisateur. La mise à niveau des appliances VPN dans le data center, leur virtualisation ou leur migration vers le cloud ne résoudra pas les problèmes liés à l'expérience utilisateur ou à la sécurité du réseau que génère un monde mobile. **Une nouvelle approche est indispensable.**

"D'ici 2023, 60% des entreprises élimineront progressivement la plupart de leurs réseaux privés virtuels (VPN) d'accès à distant au profit de ZTNA."

Gartner, Guide du marché pour Zero Trust Network Access
Steve Riley, Neil MacDonald, Lawrence Orans, avril 2019

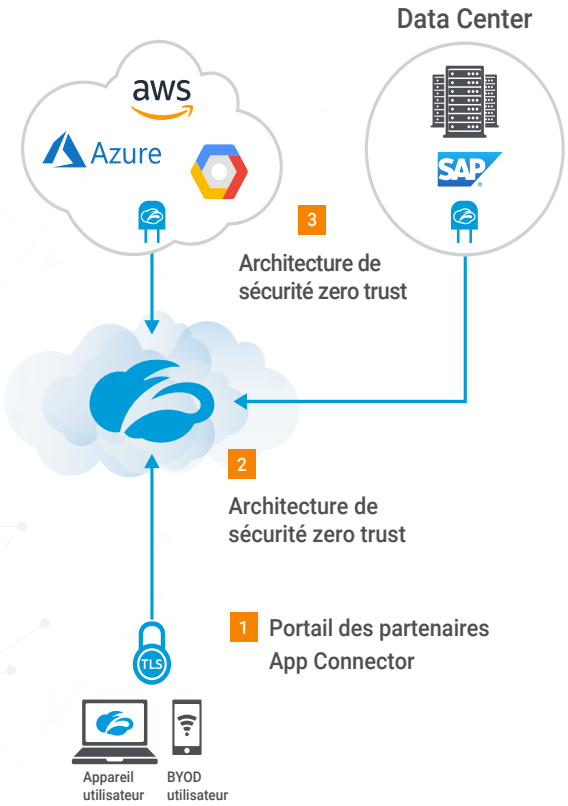
Garantir la productivité des utilisateurs avec ZTNA

Qu'il s'agisse d'accéder à SAP dans le cloud public, par SSH, RDP, un intranet personnalisé ou une application de feuille de temps basée sur le web, l'expérience utilisateur devrait toujours être transparente. C'est pourquoi Gartner recommande aux organisations d'adopter **les technologies ZTNA (Zero Trust Network Access)** pour remplacer les VPN d'accès distant.

Dans la plupart des cas, les services ZTNA sont hébergés dans le cloud et utilisent des politiques pour déterminer quels utilisateurs autorisés ont accès à une application privée spécifique. Ces politiques prennent en compte l'identité de l'utilisateur, son groupe, la posture de l'appareil et plusieurs autres critères.

Étant donné que de nombreux services ZTNA sont entièrement fournis dans le cloud, ils permettent aux utilisateurs de se connecter à l'un des nombreux points de présence mondiaux du service, qui assure ensuite la connexion sécurisée à une application privée. Cela offre une plus grande disponibilité et beaucoup plus d'évolutivité qu'une appliance VPN. Les utilisateurs ne sont jamais placés sur le réseau, et de ce fait le trafic n'est plus redirigé vers un data center. Cela signifie que le service ZTNA rend l'accès transparent à l'utilisateur final tout en vous permettant de minimiser les risques pour votre entreprise.

Architecture ZTNA (Zero Trust Network Access)



1 Zscaler App ou Browser Access

- Redirige le trafic vers le fournisseur IPD pour l'authentification
- Client Connector achemine automatiquement le trafic vers Public Service Edge
- L'accès au navigateur supprime le besoin du client sur l'appareil lors de l'accès aux applications Web

2 ZPA Public Service Edge

- Sécurise la connexion utilisateur-application
- Applique toutes les politiques d'administration personnalisées

3 App Connector

- Se situe devant les applications privées dans le cloud et/ou le data center
- Répond uniquement aux demandes de ZPA Public Service Edge
- Aucune connexion entrante. Répond avec des connexions de l'intérieur vers l'extérieur uniquement



Commencez à offrir l'expérience que les utilisateurs souhaitent

Alors que vous réfléchissez aux moyens de rendre vos utilisateurs productifs, envisagez un service ZTNA.

Ne manquez pas de voir comment Steve Day, EGM de l'Infrastructure, du Cloud et du milieu professionnel à la National Australia Bank, a permis à ses utilisateurs d'être productifs.

Regardez l'histoire de la National Australia Bank

Quelle est la prochaine étape? Prenez notre service ZTNA pour un essai.

Démarrer une démo ZTNA de 7 jours

À propos de Zscaler

Zscaler permet aux plus grandes organisations internationales d'adapter en toute sécurité leurs réseaux et leurs applications à un monde résolument tourné vers le mobile et le cloud. Ses services phares que sont Zscaler Internet Access™ et Zscaler Private Access™, créent des connexions rapides et sécurisées entre les utilisateurs et les applications, et ce quels que soient l'appareil, l'emplacement ou le réseau. Les services Zscaler sont à 100% fournis dans le cloud et offrent simplicité, sécurité renforcée ainsi qu'une amélioration de l'expérience utilisateur inégalables par les appliances traditionnelles ou les solutions hybrides. Adopté dans plus de 185 pays, Zscaler gère une plate-forme multi-entité de sécurité cloud distribuée qui protège des milliers de clients contre les cyberattaques et les pertes de données. Pour en savoir plus, accédez à**zscaler.com** ou suivez-nous sur Twitter **@zscaler**.

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