Retour au bureau : moderniser l’espace de travail avec le Zero Trust



© 2025 Zscaler, Inc. Tous droits réservés.

LIVRE BLANC

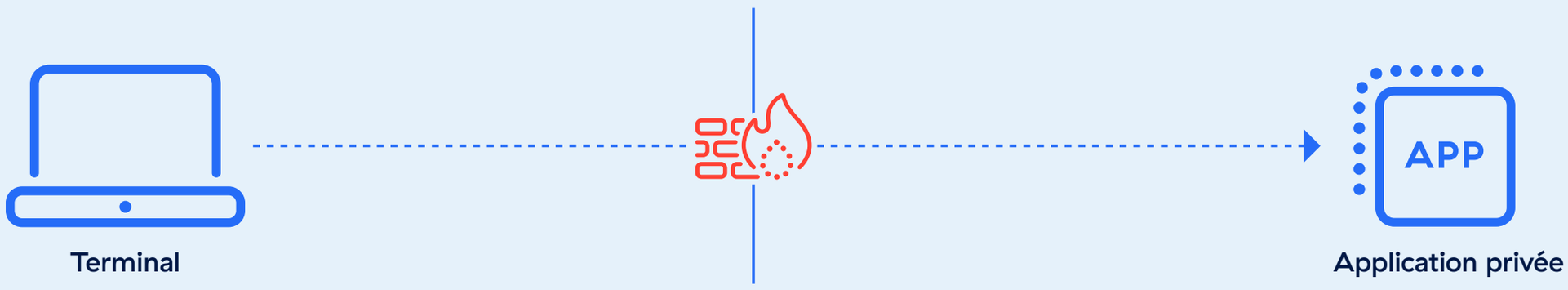
Le retour au bureau ne signifie pas un retour en arrière. Les employés reviennent au bureau, mais pas les applications ni les données. Des années de travail à distance et hybride ont renforcé l'usage des applications cloud et la familiarité des employés avec celles-ci. De retour au bureau, les employés exigent la même fiabilité et la même réactivité des services informatiques, voire davantage. Revenir à « la façon dont nous avons toujours Travaillé » ne répondra pas à cette attente.

La migration des applications et des données vers le cloud impose de repenser la sécurité sur site, sans nuire à la productivité. Le Zero Trust, initialement adopté pour sécuriser le télétravail, offre les mêmes avantages aux équipes sur site et doit être vu comme un pilier du lieu de travail moderne.

Sécurité des bureaux traditionnels : faire confiance aux murs

Les réseaux d'entreprise étaient conçus comme des forteresses : toute personne ou tout appareil à l'intérieur des murs physiques du bureau était présumé digne de confiance, car situé dans le « périmètre » de sécurité. Ce modèle fonctionnait lorsque les systèmes de bureau étaient statiques et que chacun se connectait à une infrastructure commune.

Dans le modèle traditionnel de sécurité réseau basé sur le périmètre, la connexion au bureau de l'agence place le poste de travail sur le réseau de confiance :



Dans ce modèle, accéder au réseau signifiait accéder à toutes les applications, ressources et données qu'il contenait. Pour limiter le risque qu'un utilisateur ou un appareil non autorisé se connecte au réseau de confiance, les entreprises utilisaient des outils comme le contrôle d'accès réseau (NAC), par exemple refuser la connexion d'un appareil dépourvu de certificat délivré par la PKI de l'agence.

C'est un progrès, mais insuffisant comparé à un modèle de sécurité fondé sur la segmentation et le principe du moindre privilège. En effet, l'approche du réseau de confiance se caractérise encore par :

- Un accès large et sans restriction
- Des contrôles limités et peu précis
- Des vulnérabilités du réseau interne

© 2025 Zscaler, Inc. Tous droits réservés.

Ces caractéristiques du modèle de « réseau de confiance » (privilèges d'accès étendus, segmentation limitée et visibilité intrinsèque des réseaux internes) ne sont plus adaptées face aux menaces actuelles. Dans un contexte marqué par des cyberattaques toujours plus sophistiquées, des menaces internes et la prolifération des outils d'accès à distance, les modèles de sécurité périmétriques ne suffisent plus à répondre aux vulnérabilités modernes. Les hackers exploitent ces faiblesses, ils contournent les contrôles de segmentation insuffisants, se déplacent latéralement une fois dans le réseau et utilisent souvent des identifiants légitimes pour passer inaperçus. Cette situation impose un véritable changement de paradigme qui consiste à abandonner la logique de « confiance par défaut » au profit des principes du Zero Trust, qui vérifient et valident dynamiquement chaque tentative d'accès, quel que soit l'utilisateur, l'appareil ou l'application.

Les entreprises ont besoin d'une approche qui :

- Réduit la surface d'accès grâce à des connexions granulaires, propres à chaque application
- Applique des politiques dynamiques, fondées sur l'identité et l'état de l'appareil
- Évalue en continu chaque tentative d'accès, sans relâche ni exception

Il ne s'agit pas d'une architecture avant-gardiste. Elle existe déjà sous la forme de l'architecture de réseau Zero Trust (ZTNA), conçue à l'origine pour sécuriser le télétravail

Un environnement de travail Zero Trust

Avec l'essor du télétravail et la migration massive des applications vers le cloud, les fondements traditionnels de la confiance se sont effondrés. Le Zero Trust, qui remplace la notion de « faire confiance par défaut » par « vérifier systématiquement », s'est imposé comme l'approche la plus efficace pour donner aux utilisateurs l'accès dont ils ont besoin.

Dans le contexte du retour au bureau, le Zero Trust devient plus pressant que jamais. Ces dernières années, la majorité des applications et des services informatiques ont migré vers le cloud, générant des gains de productivité et d'efficacité opérationnelle. Revenir aux pratiques périmétriques d'avant le cloud est non seulement obsolète, mais aussi incompatible avec les exigences de l'espace de travail moderne.

Zero Trust est plus qu'une simple amélioration de la sécurité, il s'agit d'une opportunité stratégique de réimaginer et de pérenniser le bureau moderne. Cette approche apporte aux entreprises flexibilité, évolutivité et des économies substantielles Qu'il s'agisse de créer une nouvelle succursale, des pôles de collaboration temporaires ou de gérer des équipes hybrides, le Zero Trust élimine le besoin d'infrastructures réseau coûteuses telles que MPLS ou des solutions gérées par les opérateurs de télécommunications. Cela réduit également la dépendance à des dispositifs de sécurité locaux complexes et lourds à maintenir.

Plus important encore, le Zero Trust garantit la pérennité. Avec une base Zero Trust, les entreprises intègrent sans difficulté de nouvelles technologies, sans être freinées par des configurations réseau dépassées. Elles se libèrent ainsi définitivement des pare-feu et autres

Les utilisateurs sont de retour au bureau, mais pas vos applications

© 2025 Zscaler, Inc. Tous droits réservés.

appliances traditionnelles, tout en renforçant durablement leur stratégie de sécurité.

Aujourd'hui, la majorité du travail passe par des applications cloud, même pour les employés qui travaillent au siège. Le bureau n'est plus le centre des activités informatiques. Les employés sur site accèdent aux ressources exactement comme les télétravailleurs.

Ce changement fondamental a introduit plusieurs défis :

- **Les bureaux sont des goulots d'étranglement de la connectivité :** de retour sur site, les utilisateurs redirigent souvent le trafic destiné au cloud via le réseau de l'entreprise, générant une latence inutile et des incidents.

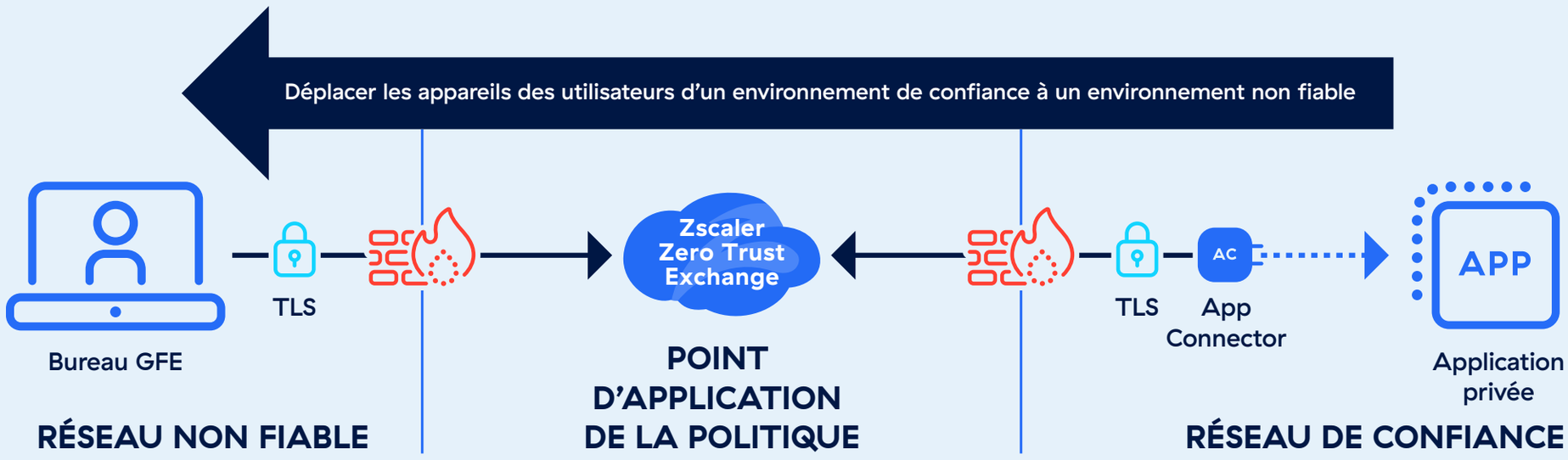
- **L'expérience utilisateur se dégrade :** de retour au bureau, les employés peuvent constater une dégradation des performances des applications. Le réseau n'est pas toujours en cause ; il peut s'agir de lenteur du DNS ou d'un Wi-Fi mal optimisé. Sans visibilité claire, le service informatique avance à l'aveugle pour identifier la source du problème.

- **Des outils de surveillance disparates :** les solutions traditionnelles mesurent surtout la disponibilité du réseau, sans refléter la réalité vécue par l'utilisateur (performances applicatives, latence, état des terminaux).

Repenser les réseaux de bureau

Imaginez un modèle Internet de type café, où les employés se connectent à Internet comme ils le feraient de chez eux. Cette idée peut sembler radicale, mais l'architecture réseau Zero Trust rend déjà ce modèle possible.

Dans ce scénario, la connexion au réseau ne confère aucune confiance implicite. Les postes de travail des utilisateurs ne sont plus considérés comme fiables, ils bénéficient de la même protection que ceux d'un utilisateur en télétravail, avec les mêmes règles d'accès.



Ainsi, se connecter depuis le bureau d'une agence ne devrait pas donner plus de droits qu'une connexion via son fournisseur d'accès domestique. Le réseau devient un simple moyen de transport, sans privilège automatique.

© 2025 Zscaler, Inc. Tous droits réservés.

L'accès et l'autorisation sont basés sur l'identité, l'appareil et l'application (et non l'adresse IP) visée. Ce n'est plus le pare-feu réseau et ses listes de contrôle d'accès (ACL) qui tranchent, mais un point d'application des politiques. Chaque demande est arbitrée selon des règles précises : quelles applications un utilisateur peut consulter, depuis quel appareil, et dans quel contexte.

Ce changement dans l'architecture exige un vrai changement de mentalité.

1. **Étendre les règles aux utilisateurs sur site :** la politique d'accès suit l'utilisateur, et non le réseau auquel il est connecté.

2. **Passer de l'accès réseau à l'accès aux ressources :** avec le Zero Trust, les utilisateurs accèdent directement aux applications via des connexions pilotées par l'identité et les règles de sécurité, sans qu'il soit nécessaire d'ouvrir largement l'accès au réseau.

3. **Traiter le réseau du bureau comme Internet :** le Wi-Fi de votre entreprise devient un « Internet de type café » qui connecte simplement les utilisateurs à Zero Trust Exchange, où les politiques de sécurité prennent le relais. Aucun trafic entrant. Aucune confiance implicite.

4. **Validation continue de la confiance :** Zero Trust évalue chaque demande d'accès de manière dynamique, en tenant compte de la posture de l'appareil, le contexte et les signaux de risque.

La force du Zero Trust est d'offrir une cohérence totale. Les employés n'ont pas à se soucier de savoir s'ils travaillent sur site ou à distance. Ils accèdent toujours aux applications de la même manière, où qu'ils soient. Cette expérience unifiée maintient la productivité des utilisateurs tout en allégeant la gestion informatique.

Meilleure visibilité

Un cadre Zero Trust solide assure une continuité de travail sans heurts, tout en éliminant les risques liés à la confiance implicite et aux infrastructures vieillissantes. La visibilité devient une brique essentielle, au même titre que l'identité, la posture de l'appareil et le contrôle des applications, pour optimiser les performances et résoudre rapidement les problèmes. Elle permet aux équipes informatiques d'optimiser la distribution des applications, de réduire les interruptions et de cibler plus vite les causes des incidents. Une visibilité complète, depuis le terminal jusqu'à la destination, aide les administrateurs à déterminer immédiatement si l'origine du problème se situe chez l'utilisateur, sur le transport ou au niveau du service distant.

Voici quelques scénarios fréquents lors du retour dans des bureaux partagés :

- **Le dilemme du Wi-Fi au bureau :** un employé connecte son ordinateur portable au Wi-Fi de l'entreprise. Aussitôt, Microsft Teams devient inutilisable à cause d'une forte latence, alors que l'application fonctionnait parfaitement à la maison avec une simple connexion haut débit. Est-ce un problème de couverture Wi-Fi, un délai DNS, ou bien un problème avec le serveur Teams lui-même ?

© 2025 Zscaler, Inc. Tous droits réservés.

- **Latence SaaS sur le backhauling d'entreprise :** un utilisateur tente d'accéder à un CRM cloud comme Salesforce. Le trafic est obligé de repasser par le réseau interne, ce qui ajoute une latence due au backhauling.

- **Lacunes de visibilité pour les effectifs hybrides :** n'arrive pas à avoir une vision claire de l'état des appareils, ni de la performance des applications SaaS et des FAI, que ce soit pour les employés sur site ou à distance. Cela entraîne une multiplication des tickets d'incident qui mobilisent inutilement les équipes informatiques.

Un élément clé du bureau Zero Trust est d'intégrer la surveillance de l'expérience numérique dans l'architecture globale.

Zscaler pour le bureau Zero Trust — Pourquoi ?

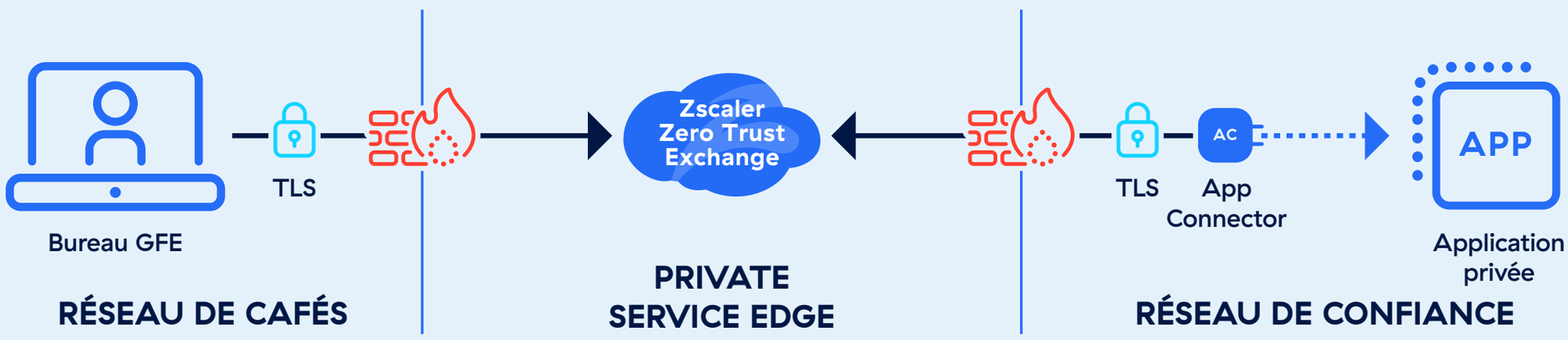
Zscaler est déjà un partenaire éprouvé pour des administrations qui mènent des projets de modernisation. Premier fournisseur de services de sécurité cloud du secteur, Zscaler sert 14 des 15 agences ministérielles américaines, dont le DHS, le DOJ et la GSA en sécurisant leurs réseaux, en simplifiant leurs opérations et en réduisant leurs coûts. Nous sécurisons des millions d'utilisateurs dans des centaines d'institutions à tous les niveaux de gouvernement.

La solution Zscaler for Users regroupe trois grands ensembles de fonctionnalités : réduire les risques, améliorer la productivité et réduire les coûts et la complexité.

- **Accès Internet et SaaS sécurisés (ZIA)** — Le point d'accès de vos utilisateurs à Internet et à l'ensemble des applications, avec une protection intégrée contre les menaces avancées et les fuites de données.

- **Accès sécurisé aux applications privées (ZPA)** — Garantit aux utilisateurs une connexion via le Private Service Edge local, qui établit le lien vers une application privée à travers le réseau de l'agence, sans détour par Internet.

- **Expérience utilisateur numérique (ZDX)** — Apporte une visibilité complète sur l'expérience numérique des utilisateurs, en mesurant la performance depuis le poste de travail jusqu'à l'application SaaS, pour assurer l'excellence opérationnelle au bureau comme à distance.



© 2025 Zscaler, Inc. Tous droits réservés.

Moderniser le lieu de travail grâce au Zero Trust

À mesure que le lieu de travail évolue, la notion même de « bureau » perd de sa pertinence. Qu'ils travaillent au bureau, à domicile ou en déplacement, les utilisateurs doivent bénéficier d'une expérience fluide et sécurisée.

Le retour au bureau offre aux entreprises une occasion unique de moderniser leur infrastructure de travail. Une fondation Zero Trust renforce non seulement la sécurité, mais assure également l'évolutivité, l'agilité et la résilience à long terme. C'est la vision du Zero Trust Office pleinement réalisé, un bureau où la productivité prospère.

Le bureau Zero Trust est dès désormais une réalité accessible. En appliquant aux opérations sur site les mêmes principes que pour le télétravail, les entreprises peuvent considérablement réduire les risques, améliorer l'expérience utilisateur et bâtir une architecture de sécurité pérenne.

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 160 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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

zscaler™

Zero Trust Everywhere