Livre blanc

Sécurité et expérience utilisateur, des vecteurs de productivité pour vos collaborateurs hybrides

Introduction

L'avenir du travail s'annonce hybride. Au cours des trois dernières années, de nombreuses entreprises ont opéré une transformation technologique rapide pour intégrer le télétravail. Cependant, il est désormais manifeste que les modèles de travail à distance et sur site présentent tous deux des avantages. La migration soudaine vers le télétravail a révélé aux dirigeants d'entreprise que la collaboration en présentiel présente de réels avantages, en contribuant activement à la cohésion des équipes et à la culture d'entreprise. Parallèlement, ces décideurs ont compris que le télétravail est un levier de productivité et qu'il facilite l'équilibre entre vie professionnelle et vie privée des collaborateurs.

Pour obtenir le meilleur des deux mondes, de nombreuses entreprises incitent désormais leurs collaborateurs à revenir au bureau une partie de leur temps professionnel. Mais elles le font de manière plus souple, plus modulable et plus diversifiée que jamais.

Quelque 77 % des entreprises ont adopté une politique de travail hybride, le modèle le plus courant étant celui d'un travail hybride à la demande, qui permet aux collaborateurs de choisir leurs jours de présence au bureau. Ce modèle offre une flexibilité optimale, ce qui améliore la satisfaction parmi les équipes et, bien souvent, leur productivité.

Ce renforcement de la productivité et du niveau de satisfaction est d'autant plus essentiel que la demande pour des talents qualifiés reste supérieure à l'offre. Malgré les incertitudes économiques, le marché du travail actuel reste historiquement tendu. Ainsi, aux États-Unis, les données recueillies par la U.S. Chamber of Commerce témoignent de 10 millions de postes à pourvoir aux États-Unis contre seulement 6 millions de personnes au chômage. Il en résulte que les entreprises, quelles que soient leur taille ou leur secteur d'activité, peinent à recruter les collaborateurs qui leur font défaut, de l'ouvrier au cadre dirigeant.

La pénurie actuelle de compétences impose aux entreprises d'assurer des expériences technologiques qui contribueront à la satisfaction et à la productivité des collaborateurs, que ces derniers soient au bureau, à domicile ou ailleurs.

Cependant, toutes les entreprises n'ont pas défini de stratégie à long terme qui permettrait à chaque collaborateur, où qu'il se trouve, d'accéder à toutes les applications dont il a besoin pour mener à bien sa mission. Pourtant, cet accès est primordial pour garantir une expérience cohérente, que les applications soient hébergées dans le cloud ou dans un data center privé.

Les entreprises doivent mettre en œuvre des solutions capables d'offrir une expérience utilisateur exceptionnelle tout en protégeant les entreprises contre les risques de cybersécurité. Alors que les entreprises élaborent des stratégies de travail à plus long terme, il devient particulièrement important de veiller à ce que les équipes distantes et sur site bénéficient de la même expérience et du même niveau de sécurité. Cette cohérence doit également s'appliquer lorsque les équipes basculent entre présentiel et distanciel, au gré de leurs impératifs et envies.

Sécuriser les collaborateurs hybrides : les prérequis

Dans le passé, les acteurs du secteur technologique considéraient souvent que sécurité et facilité d'accès aux ressources constituaient des objectifs certes souhaitables, mais intrinsèquement opposés. De nos jours, les solutions modernes basées sur le cloud permettent de fournir aux utilisateurs un accès rapide et transparent aux applications, sans pour autant compromettre la sécurité. Les professionnels de l'informatique peuvent ainsi arbitrer entre une protection permanente contre les menaces et une connectivité à faible latence, quelle que soit la localisation de leurs équipes.

Dans le cadre de l'adoption du travail hybride, ces solutions permettent de répondre aux deux critères essentiels de réussite, en assurant à la fois la **sécurité** et des **expériences utilisateur optimales**. Examinons plus en détail ce que cela implique.

Expérience utilisateur

Les réseaux traditionnels en étoile n'ont pas été conçus pour répondre aux besoins d'un personnel hybride, ni pour améliorer sa productivité. Les réseaux conçus selon cette topologie appliquent des politiques de sécurité par le biais d'un panel de dispositifs de sécurité et de pare-feu situés dans

un data center centralisé au sein de l'entreprise. La totalité du trafic doit ainsi être acheminée via ce hub. Ce backhauling ralentit les performances des applications, ce qui est particulièrement problématique pour les logiciels de visioconférence et autres outils de collaboration modernes. Ceux-ci fonctionnent mal en cas de latence, alors qu'ils jouent un rôle essentiel dans les workflows du quotidien.

Les architectures de sécurité traditionnelles ne peuvent tout simplement pas garantir un accès à distance transparent aux ressources. Dans ce contexte, des solutions contraignantes doivent être déployées, telles que les réseaux privés virtuels (VPN), assorties de procédures de connexion complexes. Cela signifie que, par nécessité, les télétravailleurs devront accéder aux applications critiques et à d'autres ressources d'une manière très différente que s'ils étaient au bureau.

Les équipes étant de plus en plus disséminées, les équipes informatiques ont également plus de difficultés à suivre et à résoudre les problématiques qui affectent leurs utilisateurs finaux. Les outils existants de surveillance des appareils, des réseaux et des applications ne disposent que d'une vision fragmentée sur la chaîne de fourniture applicative. D'où des zones d'ombre entre l'appareil de l'utilisateur et l'application. Pour renforcer leur visibilité, les équipes IT opérationnelles et de support doivent exporter et mettre en corrélation les données provenant de plusieurs outils. Et ce, manuellement. Conséquence de ce manque de visibilité de bout en bout sur l'expérience digitale, les équipes informatiques opèrent souvent dans un contexte d'urgence. Elles sont constamment contraintes de résoudre des problèmes après en avoir été informées, au lieu de pouvoir les identifier et les résoudre de manière proactive, avant tout impact sur les utilisateurs.

Il est donc nécessaire de disposer d'une solution qui offre un accès rapide et transparent à Internet et aux applications privées et SaaS (Software-as-a-Service) depuis tout endroit, pour garantir en permanence une expérience optimale à l'ensemble des collaborateurs. D'un point de vue technique, le peering direct, qui établit le chemin le plus court possible entre les utilisateurs et leurs applications de destination, peut remplir cette fonction. En supprimant tout besoin de VPN et de pare-feu, le peering direct réduit considérablement la latence.

Des solutions permettant aux équipes informatiques de surveiller les expériences digitales en temps réel sont également nécessaires afin d'évaluer en temps réel l'expérience des utilisateurs finaux. Il est ainsi possible d'optimiser les performances avant même que les utilisateurs ne subissent une quelconque problématique.

Sécurité

L'adoption à grande échelle du télétravail a conduit à une expansion de la surface d'attaque, avec de nombreux nouveaux appareils tentant de se connecter aux réseaux d'entreprise pour accéder aux ressources. Les acteurs malveillants s'en prennent désormais aux VPN et aux pare-feu, cherchant des moyens de contourner les protections limitées qu'ils offrent. Une fois parvenus à leurs fins, ils disposent d'un accès total au réseau et à l'ensemble des ressources qui s'y trouvent, exposant ainsi potentiellement les données les plus précieuses de l'entreprise.

Pour une prévention efficace des violations de données au sein des écosystèmes informatiques complexes d'aujourd'hui, le moment est venu d'éliminer le concept d'accès au réseau dans son ensemble. En effet, l'accès ne devrait être accordé qu'à des applications individuelles, une par une, selon les besoins. Cette approche est cohérente avec le principe de microsegmentation, clé de voûte d'une sécurité Zero Trust. Le respect de ce principe empêche une menace de se propager en interne, lorsque les acteurs malveillants utilisent un seul compte compromis comme tremplin pour accéder à d'autres ressources de l'entreprise.

D'autre part, les applications internes ne sont plus visibles depuis l'Internet public. En substance, c'est la surface d'attaque qui est éliminée.

Les pare-feu traditionnels sont incapables de détecter les menaces véhiculées par le trafic chiffré, alors que précisément, la plupart des attaques sont aujourd'hui chiffrées. Une nouvelle approche capable d'inspecter l'ensemble du trafic, indépendamment de son origine ou de sa destination, ou du fait que les appareils concernés appartiennent à des collaborateurs ou à l'entreprise, est désormais essentielle pour une protection efficace des données.

De nouvelles solutions s'imposent également pour permettre aux équipes de sécurité d'appliquer des politiques de protection des données cohérentes de manière transparente, même au sein des environnements multisites .

Zscaler Zero Trust Exchange : permettre un accès réseau Zero Trust universel pour les applications et les utilisateurs

Un nombre toujours plus important d'entreprises adoptent le Zero Trust pour sécuriser leurs collaborateurs désormais hybrides. Zscaler a conçu Zero Trust Exchange pour aider ces entreprises à offrir un accès sécurisé aux applications qui permettent aux collaborateurs de rester productifs, tout en minimisant les coûts et la complexité. Créé pour offrir une sécurité Zero Trust à l'échelle de l'entreprise, Zero Trust Exchange applique le principe d'un accès sur la base du moindre privilège et veille à ce qu'aucun utilisateur ou application ne soit intrinsèquement considéré comme fiable. Ces principes de sécurité sont activés à partir d'une plateforme unique qui sécurise toutes les communications des utilisateurs, des instances et des appareils, quels que soient leur localisation ou le réseau utilisé.

Le ZTNA au service des équipes hybrides

Le concept d'accès réseau Zero Trust (ZTNA ou Zero Trust Network Access) a rapidement gagné en popularité au cours des dernières années, les entreprises cherchant à pallier leurs failles de sécurité tout en prenant en charge les collaborateurs hybrides et distants. Présenté pour la première fois par l'analyste Gartner, le concept ZTNA implique la création d'une frontière d'accès logique basée sur l'identité et le contexte autour des applications et des ressources de l'entreprise. Pour faire respecter cette frontière, les services ZTNA établissent des connexions entre les utilisateurs et les applications autorisés, avec un accès strictement conforme à des politiques de sécurité basées sur le Zero Trust.

Les avantages du ZTNA vont bien au-delà de sa capacité à remplacer les VPN, s'étendant aux utilisateurs qui se connectent depuis leur bureau ou à distance. Avec un ZTNA universel, les utilisateurs bénéficient du même niveau de sécurité Zero Trust, qu'ils travaillent sur site ou à domicile.

Pour concrétiser un ZTNA universel, les fonctionnalités ZTNA doivent être étendues de manière à ce qu'elles fonctionnent tant pour les utilisateurs sur site que pour les utilisateurs à distance, en garantissant que leur expérience utilisateur ou leur sécurité est la même. Dans cette optique, une solution doit être en mesure de fournir le même accès direct et sécurisé, de l'utilisateur à l'application, à la fois dans le cloud et pour les utilisateurs locaux accédant aux applications hébergées dans le data center de l'entreprise.

Zero Trust Exchange est une plateforme cloud native qui permet des connexions rapides et sécurisées à Internet, aux applications privées et SaaS, sur site ou à distance, tout en optimisant l'expérience des utilisateurs et des administrateurs. Zero Trust Exchange a été conçu pour réussir l'arbitrage entre expérience utilisateur et sécurité, grâce aux avantages suivants :

- Accès rapide et fluide, quel que soit le lieu de connexion : Zero Trust Exchange veille à ce que le trafic emprunte toujours le chemin le plus court entre les utilisateurs et les destinations grâce à un peering direct avec les applications SaaS. D'autre part, l'accès s'effectue via l'intermédiaire (broker) le plus proche de l'utilisateur tout en éliminant le besoin de VPN et de pare-feu.
- Maîtrise des risques pour l'entreprise : en fournissant un accès direct aux applications, Zero Trust Exchange applique la microsegmentation, créant des connexions individuelles entre les utilisateurs et les applications afin de réduire la surface d'attaque et empêcher la propagation des menaces sur le réseau, même en cas de piratage des comptes d'utilisateurs.
- Expériences digitales optimales : Zero Trust Exchange permet aux équipes informatiques d'anticiper toute expérience utilisateur médiocre, grâce à une surveillance des expériences digitales pour renforcer les performances. Cela permet de résoudre rapidement les problématiques liées aux applications, au réseau et aux appareils avant tout impact sur la productivité.

Zero Trust Exchange de Zscaler constitue la solution idéale pour un ZTNA universel, avec Zscaler Private Access (ZPA) Private Service Edge. Cette solution étend tous les avantages de Zscaler Zero Trust Exchange aux applications privées hébergées dans le data center de l'entreprise. En étendant l'ensemble des fonctionnalités de Zero Trust Exchange au data center privé ou au cloud public, ZPA Private Service Edge permet de réduire la latence, d'améliorer les performances applicatives pour les utilisateurs au bureau, et d'appliquer des politiques de sécurité Zero Trust. Avec ZPA Private Service Edge, ces politiques sont appliquées au plus proche de l'edge, ce qui permet aux utilisateurs locaux et distants de bénéficier d'expériences identiques, qu'ils accèdent à des applications hébergées dans le data center ou dans le cloud.

Zscaler Zero Trust Exchange permet aux entreprises de mettre en œuvre une véritable posture de sécurité Zero Trust, et ce de manière rentable et efficace, tout en répondant à l'ensemble des besoins de sécurité et de performances des collaborateurs hybrides modernes.

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les appareils et les applications, quelle que soit leur localisation. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange est la plus grande plateforme cloud de sécurité SSE proposée en mode inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

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