Livre blanc

Pourquoi les leaders de l'informatique doivent-ils adopter une stratégie ZTNA (Zero Trust Network Access)

Faciliter l'activité digitale tout en protégeant les données

Si la technologie a longtemps été considérée comme un moteur nécessaire à l'avancée de l'entreprise, elle est aujourd'hui reconnue comme un véritable pilote de l'activité, capable de générer de nouvelles synergies et opportunités de revenus. De manière analogue, le rôle du leader informatique a évolué, les RSSI, DSI et directeurs techniques rejoignant le comité de direction pour se concentrer sur les projets technologiques et les mener à bien.

Les principaux facteurs de ce changement ont été l'explosion de l'adoption du cloud public par les entreprises, notamment Azure, AWS et Google Cloud, et l'utilisation généralisée d'appareils mobiles appartenant aux employés (BYOD) pour le travail. Les entreprises tirent parti de ces technologies pour optimiser les processus de l'entreprise, et pour fournir des produits et services plus rapidement et à un moindre coût global.

Mais qu'en est-il du risque qu'ils véhiculent?

En raison de la migration vers le cloud et de la mobilité, le périmètre de sécurité traditionnel qui protégeait autrefois les utilisateurs et les services internes au sein du réseau d'entreprise a disparu.

De ce fait, lorsque les leaders informatiques demandent un budget pour une nouvelle logistique informatique qui s'arrime au cloud et la mobilité, ils doivent aider le conseil d'administration à voir le lien entre le risque et son impact potentiel sur les revenus des entreprises. Ils doivent communiquer de manière efficace le coût d'une violation de données, le coût des temps d'arrêt des infrastructures essentielles, ainsi que le coût de la perte de la réputation de la marque. En substance, le service informatique doit initier des échanges sur la valeur de l'entreprise que les dirigeants comprendront.

Les leaders informatiques devraient commencer par comprendre le portefeuille de risques de leur entreprise et déterminer le degré d'aversion au risque de leur entreprise. Les applications essentielles à leur activité peuvent être conformes aux normes SOC1 ou ISO 27001 et nécessiter des couches de sécurité supplémentaires. Celles-ci sont considérées comme des infrastructures critiques. Il se peut que certains pays, comme la Chine, doivent être isolés des autres pays. Les infrastructures traditionnelles nécessitant une évaluation continue des correctifs, une seule configuration de pare-feu négligée peut entraîner de gros problèmes pour l'entreprise.

Les défis que doivent relever les leaders technologiques

En fin de compte, pour favoriser les projets d'entreprise clés et combler le fossé entre les besoins des entreprises et les capacités informatiques, les leaders informatiques doivent choisir une technologie qui les aide à surmonter leurs difficultés et qui leur permette de :

1. Faciliter l'exécution du travail et réduire le stress du personnel
2. Offrir une meilleure expérience utilisateur aux employés et aux tiers
3. Réduire les risques qui peuvent menacer la productivité, la propriété intellectuelle et la réputation de l'entreprise
4. Faire preuve de souplesse et d'agilité pour habiliter une entreprise en perpétuelle mutation
5. Accélérer la transformation digitale par l'adoption du cloud public

Identifier les technologies qui permettront d'atteindre ces objectifs est une tâche difficile car, dans certains cas, les résultats souhaités d'une solution peuvent accroître la complexité d'une autre. Par exemple, la décision d'adopter les services cloud et les technologies mobiles permet d'atteindre l'objectif d'une expérience utilisateur rationalisée, mais qu'en est-il de l'objectif de minimiser les risques d'une attaque de cybersécurité ? Les leaders informatiques doivent trouver un juste équilibre entre l'accélération de l'adoption de nouvelles technologies et la garantie de la sécurité des données sensibles. Il est donc essentiel de choisir la bonne technologie au bon moment.

La valeur de ZTNA pour l'entreprise

Gartner recommande aux responsables informatiques d'adopter ZTNA dans le cadre d'une stratégie de Security Service Edge (SSE), afin de fournir une connectivité flexible et sécurisée au personnel hybride. Les services ZTNA fournissent un accès sécurisé aux applications d'entreprise privées pour les utilisateurs distants et ceux qui travaillent au bureau, sans devoir recourir aux technologies VPN traditionnelles.

Les services ZTNA créent une frontière d'accès logique basée sur le contexte et sur l'identité autour d'une application ou d'un ensemble d'applications. Les applications sont cachées et l'accès est limité, par l'intermédiaire d'un courtier de confiance, à un ensemble d'entités nommées. Le courtier vérifie l'identité de l'utilisateur, le contexte et le respect de la politique des participants spécifiés avant de négocier la connexion.
Ainsi, les actifs de l'application ne sont plus visibles sur Internet et la surface d'attaque s'en trouve considérablement réduite.

Gartner

D'ici 2025, au moins 70 % des nouveaux déploiements d'accès à distance seront principalement desservis par ZTNA au détriment des services VPN, contre moins de 10 % à la fin de 2021.

Nous avons abordé précédemment les cinq facteurs clés que les leaders informatiques doivent prendre en compte lorsqu'ils adoptent de nouvelles technologies. Voyons comment ZTNA joue un rôle dans la prise en charge de chacun d'eux :

1. Amélioration de la productivité :

Trois employés à temps plein sur quatre, qui travaillent au bureau, **prévoient de quitter leur emploi cette année**, s'ajoutant aux dizaines de millions d'employés qui ont déjà changé d'emploi au cours de la Grande démission due à la pandémie. Avec la réorganisation massive du personnel, les employeurs repensent la manière de fidéliser et d'attirer les talents, et les responsables informatiques peuvent faire appel à la technologie pour arrêter l'hémorragie tout en préparant le terrain pour l'avenir du travail. La facilité d'utilisation de ZTNA procure des avantages considérables aux utilisateurs puisqu'elle leur évite de devoir lancer un client VPN à chaque fois qu'ils se connectent au réseau, ce qui permet de maintenir une excellente productivité et de limiter au maximum les frustrations. La simplicité de la solution ZTNA, fournie dans le cloud et uniquement sous forme logicielle, facilite sa mise en place et son déploiement. Cette simplicité permet aux services informatiques d'adopter une technologie d'application cloud sécurisée, même sur les appareils mobiles, tout en optimisant la productivité du personnel informatique et de l'ensemble de l'entreprise.

2. Apporter une meilleure expérience utilisateur :

Les utilisateurs actuels travaillent partout : au bureau, à la maison, et même en déplacement. Ces utilisateurs sont souvent un mélange d'employés et de tiers, qui ont tous besoin d'un accès fluide aux applications, quels que soient leur appareil, leur emplacement ou leur réseau. ZTNA veille à ce que chaque utilisateur bénéficie d'une expérience rapide et totalement transparente. Il élimine également le besoin d'un VPN et les ouvertures de session fastidieuses, tout en prenant en charge les utilisateurs tiers et tous les types d'appareils sans devoir recourir à un agent endpoint.

De plus, ZTNA sans client, qui exploite l'accès aux applications privées basé sur des politiques, augmente la productivité car les utilisateurs peuvent se connecter aux applications depuis n'importe quel appareil, indépendamment de leur emplacement.

3. Réduire les risques :

La sécurité reste une préoccupation concernant l'adoption du cloud et le télétravail, car ces derniers peuvent augmenter la probabilité d'une attaque contre les applications critiques pour l'entreprise et l'infrastructure si elle n'est pas traitée avec diligence. Les technologies traditionnelles, centrées sur le réseau, telles que les VPN et les pare-feu, accordent une confiance excessive et doivent être évitées. Ces solutions placent les utilisateurs distants directement sur le réseau, ce qui oblige les serveurs VPN à écouter les appels entrants en provenance d'Internet. C'est pourquoi les VPN sont devenus un cheval de Troie pour les ransomwares. Cela signifie que, qu'il soit à distance ou en local, l'utilisateur dispose d'un accès latéral au réseau. C'est le cas tant des employés que des tiers qui pourraient avoir des pratiques de sécurité moins rigoureuses. Les services ZTNA utilisent des politiques basées sur Zero Trust pour fournir aux seuls utilisateurs autorisés (sur la base de l'identité et de la posture de l'appareil) une connectivité à des applications privées spécifiques exécutées dans un cloud public, un cloud privé ou un data center. La récente évolution de ZTNA, qui est passée d'une simple fourniture de connectivité à une sécurité entièrement intégrée pour protéger les applications contre les menaces internes et les hackers sophistiqués, contribue à l'amélioration de la sécurité globale des entreprises.

4. Agilité et évolutivité fournies dans le cloud :

Actuellement, le nombre d'employés, d'appareils utilisateur, d'applications et de trafic ne cesse d'augmenter. Les services ZTNA fournis dans le cloud sont hébergés par le fournisseur, de sorte que la mise à l'échelle ne constitue plus une préoccupation pour le service informatique. Le service ZTNA gère automatiquement la charge supplémentaire à mesure qu'augmente la demande. Il n'est pas nécessaire de déployer du matériel ou des pare-feu virtualisés supplémentaires, qui ralentiraient les projets d'adoption du cloud public. Une plus grande agilité et une plus grande évolutivité sont essentielles à la réussite d'un responsable informatique, et c'est précisément ce que propose ZTNA.

5. Accélérer la transformation digitale :

Le cloud et la mobilité sont aujourd'hui des priorités pour la majorité des équipes d'entreprise. Cependant, avec de mauvaises solutions, exploiter le cloud en toute sécurité pour une base d'utilisateurs mondiale peut prendre des mois, voire des années. Cela s'explique en partie par la complexité de l'utilisation des technologies traditionnelles de réseau et de sécurité pour permettre l'accès aux applications cloud à partir d'appareils utilisateurs non gérés. ZTNA utilise des logiciels pour réduire cette complexité, ce qui permet de réduire le temps de mise en œuvre de plusieurs mois ou années à quelques heures seulement. Avec ZTNA, les entreprises peuvent rapidement profiter des avantages du cloud et d'une meilleure mobilité.

« Avec les changements que nous avons apportés au cours de notre migration vers le cloud, je suis convaincu que nous serons en position de force pour faire face à toute éventualité. En fin de compte, cette expérience aura un impact durable et changera à terme les anciennes mentalités. Nous ouvrons les yeux sur de nouvelles méthodes de travail tout en révélant l'impact de la technologie, ainsi que la résilience et la créativité de notre personnel. »

Alex Philips, directeur des technologies de l'information, National Oilwell & Varco

En savoir plus sur ZTNA

Les services d'accès au réseau Zero trust (ZTNA) constituent un outil précieux pour les responsables informatiques des entreprises. Chez Zscaler, nous avons développé un service ZTNA appelé Zscaler Private Access (ZPA). Le service utilise notre cloud mondial pour fournir un accès transparent et sécurisé aux applications internes. Exactement ce qu'il faut pour aider l'informatique à passer du statut de « centre de coûts » à celui de héros de la salle du conseil d'administration.

Ne manquez pas de visionner le témoignage de Carlos Cong, directeur principal du groupe Enterprise Technology Services chez Paychex. En effet, cette société a simplifié et accéléré ses intégrations informatiques des fusions et acquisitions avec ZTNA.

Visionner l'histoire de CMA-CGN

Demandez à votre équipe de faire un essai gratuit de 7 jours de la solution ZTNA de Zscaler.

Démarrer une démo ZTNA de 7 jours

Vous avez d'autres questions ? N'hésitez pas à contacter directement nos experts ZTNA à l'adresse **sales@zscaler.com.**

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients, avec une meilleure sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler.**

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