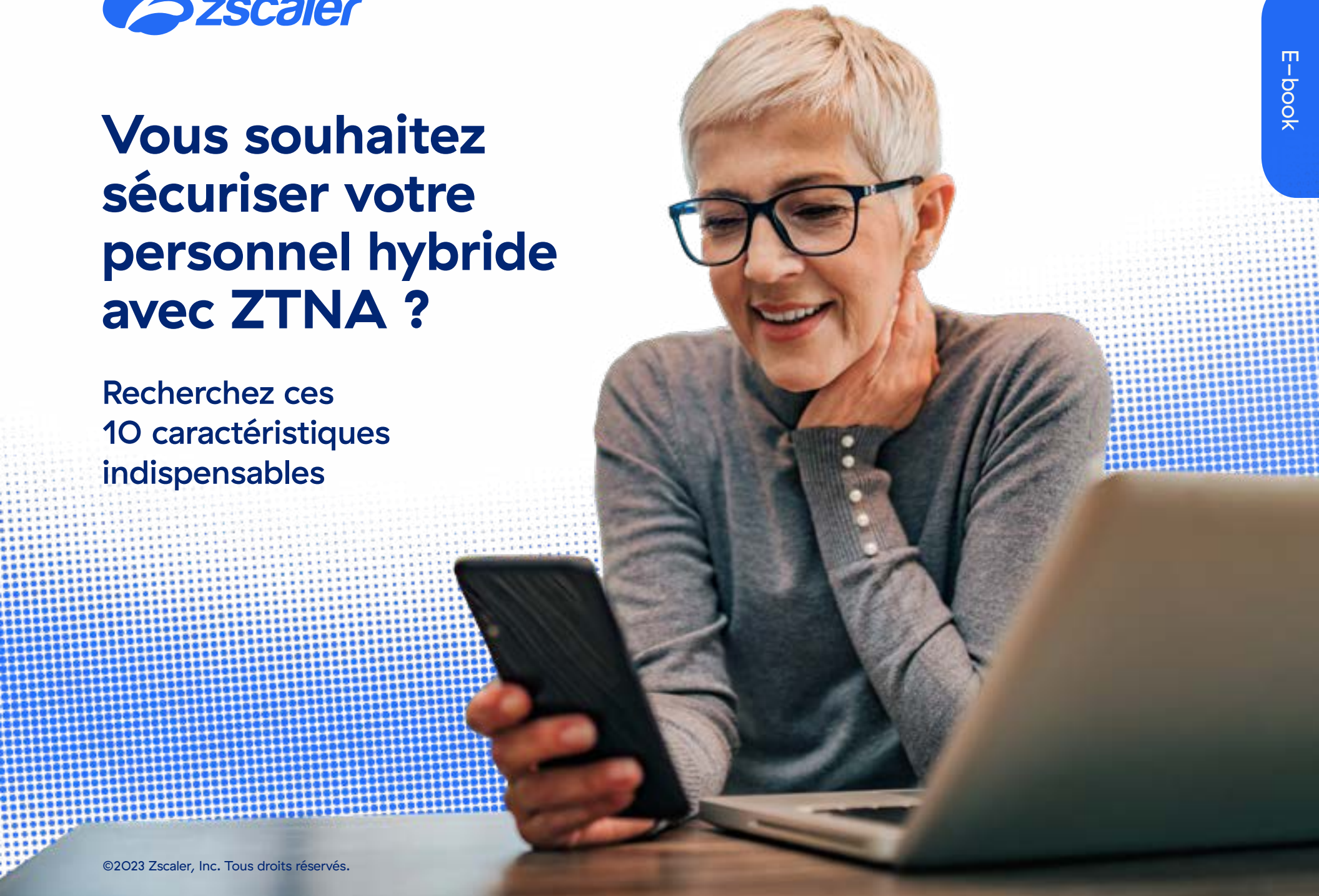
E-book

Vous souhaitez sécuriser votre personnel hybride avec ZTNA ?

Recherchez ces 10 caractéristiques indispensables



E-book

Sommaire

Introduction 3

Qu'est-ce que Zero Trust Network Access (ZTNA) ? 4

N° 1 : Éliminer la surface d'attaque en rendant les applications invisibles sur l'Internet public 5

N° 2 : Assurer une connectivité homogène depuis n'importe où 6

N° 3 : Appliquer l'accès sur la base du moindre privilège 7

N° 4 : Maintenir la productivité des utilisateurs en détectant et en résolvant rapidement les problèmes liés aux applications, au réseau et aux appareils 8

n° 5 : Prévenir les déplacements latéraux grâce à la microsegmentation des applications 9

N° 6 : Prendre en charge l'accès sécurisé pour les appareils BYOD (appareils personnels utilisés dans un cadre professionnel) et ceux appartenant à l'entreprise 10

N° 7 : Arrêter les attaques et bloquer les menaces grâce à l'inspection complète inline du contenu 11

N° 8 : S'intégrer de manière harmonieuse à un large éventail de fournisseurs et de solutions d'identité 12

N° 9 : Incorporer une technologie de tromperie intégrée pour déjouer les hackers 13

N° 10 : Permettre un déploiement rapide et aisé 14

Découvrez par vous-même pourquoi Zscaler Private Access est la plateforme ZTNA la plus déployée au monde 15

Introduction

Le monde du travail évolue. La productivité des employés ne dépend plus des mêmes facteurs qu'il y a quelques années. Alors qu'un nombre croissant d'entreprises adoptent le travail hybride et le télétravail, elles déplacent un nombre croissant d'applications critiques vers le cloud afin de pouvoir profiter pleinement de la flexibilité, de l'évolutivité et de l'efficacité qu'il propose.

Toutefois, la transformation des écosystèmes informatiques s'accompagne de nouveaux défis en matière de sécurité. L'adoption à grande échelle du travail hybride et du télétravail, ainsi que l'utilisation croissante du cloud et l'augmentation de l'accès mobile, peuvent étendre la surface d'attaque, en particulier si ces changements ne s'accompagnent pas d'un désengagement des solutions de sécurité traditionnelles (comme les VPN et les pare-feu) et des approches obsolètes. Outre l'extension de la surface d'attaque, cette situation limite la visibilité des équipes de sécurité, ce qui complique les enquêtes sur les incidents et la résolution des problèmes.

Un nouveau modèle de sécurisation des environnements technologiques s'impose, mieux adapté aux besoins actuels en matière de sécurité et de connectivité. C'est précisément ce que propose le Zero Trust, dont l'adoption est actuellement en plein essor dans tous les secteurs d'activité et toutes les zones géographiques.

Un nombre croissant d'entreprises choisissent l'accès réseau Zero Trust (ZTNA ou Zero Trust Network Access) pour renforcer leur sécurité dans le cadre du travail hybride. ZTNA fournit un cadre clair et parfaitement défini à suivre sur la voie du Zero Trust. Selon le cabinet d'analyse Gartner, le marché du ZTNA se développe à une vitesse fulgurante. Il connaît actuellement une croissance de plus de 60 % d'une année sur l'autre.

Les entreprises mentionnent le remplacement des VPN comme leur principale motivation pour déployer le ZTNA.

Qu'est-ce que Zero Trust Network Access (ZTNA) ?

ZTNA désigne un ensemble de technologies et de fonctionnalités qui permettent aux utilisateurs distants d'accéder de manière sécurisée à des applications internes et/ou privées.

ZTNA fonctionne sur un modèle adaptatif de confiance, où celle-ci n'est jamais implicite, et où l'accès est accordé selon le principe du « besoin de savoir » et du moindre privilège, défini par des politiques granulaires.

Alors qu'un nombre croissant d'entreprises se tournent vers des applications et des infrastructures fournies dans le cloud, beaucoup cherchent à unifier leurs services de sécurité avec une plateforme unique fournie dans le cloud. C'est ce que l'on appelle le Security Service Edge (SSE), qui regroupe les capacités du SWG (Secure Web Gateway), du CASB (Cloud Access Security Broker) et de ZTNA. Gartner recommande aux responsables de la sécurité et de la gestion des risques de définir leur stratégie d'adoption du SSE en adoptant ZTNA. En ce sens, ZTNA constitue souvent une première étape déterminante sur la voie de la sécurité fournie dans le cloud.

De nombreuses entreprises se tournent vers ZTNA pour remplacer les infrastructures VPN qui se révèlent peu performantes à grande échelle ou qui exposent l'entreprise à un risque de sécurité plus élevé dans la mesure où leur présence élargit la surface d'attaque. Mais ZTNA ne se limite pas à remplacer les VPN : cette solution permet aux entreprises d'éliminer les appliances traditionnelles (et leurs frais de gestion), offre aux utilisateurs un accès rapide et direct aux applications, évolue en souplesse et améliore le contrôle et la visibilité administratifs.

Cependant, tous les produits ou solutions ZTNA disponibles sur le marché ne se valent pas. Pour bénéficier de tous ces avantages et de bien d'autres encore, vous devez rechercher un produit ou une solution capable d'accomplir les dix tâches suivantes.

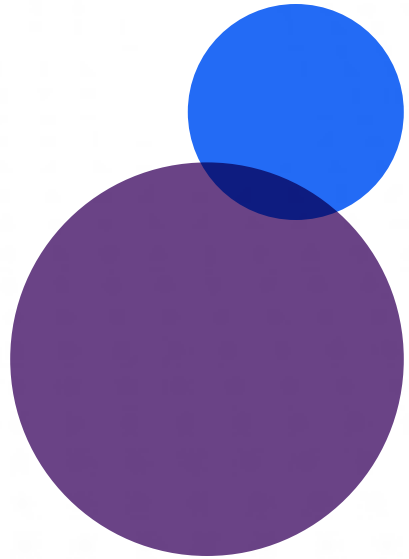
N° 1 : Éliminer la surface d'attaque en rendant les applications invisibles sur l'Internet public

Dans les architectures réseau traditionnelles en étoile, un hacker qui parvient à percer le périmètre de sécurité peut aisément découvrir les applications.

Une fois à l'intérieur du réseau, les acteurs malveillants peuvent facilement localiser les applications et les autres ressources en effectuant une simple recherche.

Dans le cadre d'une véritable solution ZTNA, l'accès aux applications est accordé sur une base individuelle par le biais de la segmentation. Même si un hacker accède à l'une de vos applications, il lui est donc impossible d'en découvrir d'autres dans votre environnement.

Toutes les applications sont dissimulées derrière la plateforme ZTNA qui négocie la connectivité directe. Les hackers ne pouvant pas cibler ce qu'ils ne peuvent pas voir, une solution ZTNA doit dissimuler les identités des sources en obscurcissant leurs adresses IP. En substance, ces connexions internes rendent l'ensemble de votre écosystème d'applications invisible. De la sorte, les hackers ne peuvent pas lancer d'attaques ciblées contre des applications individuelles.



N° 2 : Assurer une connectivité homogène depuis n'importe où

77 % des entreprises modernes ont adopté ou souhaitent adopter le travail hybride.

Les architectures réseau traditionnelles s'appuient sur des liaisons MPLS coûteuses entre les filiales et le data center central, et connectent les utilisateurs distants par le biais de VPN. À mesure que le travail hybride et le télétravail se généralisent, l'utilisation de réseaux VPN crée des problèmes de performances parce qu'ils ne peuvent pas évoluer.

En revanche, ZTNA isole complètement l'accès aux applications de l'accès au réseau, éliminant ainsi le besoin de liaisons MPLS et de VPN. Recherchez un ZTNA proposé sous la forme d'un service fourni dans le cloud, car il n'est plus nécessaire d'acheminer le trafic vers le data center de l'entreprise. Au lieu de cela, les utilisateurs bénéficient d'un accès rapide et direct aux applications indispensables à leur productivité.

Gardez à l'esprit qu'un fournisseur de ZTNA disposant de data centers partout dans le monde pourra trouver le chemin de connectivité le plus court entre les utilisateurs et les applications. Des connexions aussi proches que possible de la périphérie garantissent une expérience utilisateur de premier ordre à vos employés.

N° 3 : Appliquer l'accès sur la base du moindre privilège

L'accès sur la base du moindre privilège est un principe clé de la philosophie Zero Trust. Sa définition est simple : les utilisateurs ne se voient accorder que le niveau d'accès minimal nécessaire à l'exécution de leurs tâches, et rien de plus.

La création d'une architecture de sécurité capable de prendre en charge cette approche peut s'avérer difficile sans la solution ZTNA adéquate. La solution doit intégrer des mécanismes robustes d'authentification de l'identité de l'utilisateur, comprendre le contexte de l'appareil et avoir la capacité d'appliquer une segmentation très granulaire de l'utilisateur à l'application dans ses contrôles. Pour ce faire, ZTNA doit permettre des intégrations étroites avec toutes les principales plateformes de fournisseurs d'identité (IdP).

Recherchez une solution ZTNA capable d'appliquer les politiques informatiques et commerciales en connectant les utilisateurs vérifiés uniquement aux applications qu'ils sont autorisés à utiliser, et non au réseau. Cet accès doit être étendu de la même manière aux utilisateurs distants et sur site, quel que soit leur emplacement, les contrôles de sécurité devant être les mêmes pour tous les utilisateurs, où qu'ils se trouvent.

Zscaler a permis à 18 000 employés de la ville de Los Angeles de télétravailler en toute sécurité.

N° 4 : Maintenir la productivité des utilisateurs en détectant et en résolvant rapidement les problèmes liés aux applications, au réseau et aux appareils

Careem a amélioré son temps moyen de réponse (MTTR) de 62 % grâce à la surveillance de l'expérience digitale de Zscaler.

L'adoption de Zero Trust exige une segmentation granulaire du réseau, en particulier si les équipes tentent de la déployer à l'aide de VPN existants.

Il s'agit là d'une tâche complexe d'un point de vue technique. D'autres obstacles s'ajoutent encore dans le domaine de l'expérience utilisateur. Lorsque les réseaux sont segmentés de cette manière, les équipes du réseau et du service d'assistance peuvent difficilement, voire pas du tout, obtenir les informations sur les performances des appareils et des applications des utilisateurs finaux dont elles ont besoin pour garantir une expérience utilisateur optimale.

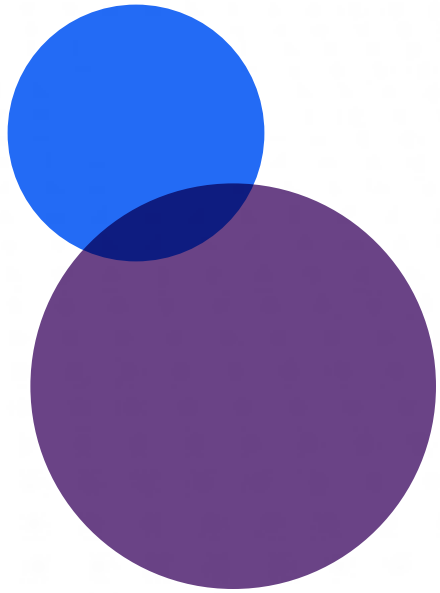
Une solution ZTNA doit proposer des fonctionnalités clés qui permettront aux équipes de résoudre ce problème. Elle doit rassembler des mesures sur la santé des appareils des utilisateurs, les performances du réseau et la disponibilité des applications, et les présenter dans un tableau de bord convivial qui permet aux équipes d'assistance aux utilisateurs d'identifier et de résoudre les problèmes avant que les utilisateurs ne les remarquent.

N° 5 : Prévenir les déplacements latéraux grâce à la microsegmentation des applications

Une solution ZTNA doit protéger vos données, vos flux de travail, vos services et vos ressources grâce à une microsegmentation définie par logiciel. Cela signifie que les utilisateurs doivent être connectés directement aux applications, et non au réseau.

En suivant cette approche, les équipes de sécurité n'ont plus à s'inquiéter des déplacements latéraux sur le réseau. Si un compte d'utilisateur ou une application venait à être compromis, le hacker ne pourrait pas aller plus loin pour compromettre d'autres ressources de l'entreprise.

Avec ZTNA, la connexion à une application ou à une ressource particulière ne devrait jamais impliquer automatiquement l'accès à d'autres ressources.



Careem
a amélioré son temps moyen de réponse (MTTR) de 62 % grâce à la surveillance de l'expérience digitale de Zscaler.

N° 6 : Prendre en charge l'accès sécurisé pour les appareils BYOD (appareils personnels utilisés dans un cadre professionnel) et ceux appartenant à l'entreprise

Recherchez une solution ZTNA capable de prendre en charge à la fois l'accès avec agent et sans agent, aussi bien pour les employés que pour les tiers.

Recherchez une solution ZTNA capable de prendre en charge à la fois l'accès avec agent et sans agent, aussi bien pour les employés que pour les tiers. ZTNA peut ainsi permettre aux partenaires et aux fournisseurs d'accéder de manière harmonieuse à vos ressources, tout en permettant aux employés d'utiliser leurs propres appareils (y compris leurs appareils mobiles) à des fins professionnelles, et ce en toute sécurité.

Avec la généralisation des appareils non gérés, votre solution ZTNA doit également pouvoir prendre en charge l'accès sans client. Si ce n'est pas le cas, vous ne pourrez protéger que vos propres employés sur les appareils fournis par l'entreprise. Dans le monde moderne, centré sur la mobilité, il s'agit d'une contrainte considérable.

N° 7 : Arrêter les attaques et bloquer les menaces grâce à l'inspection complète inline du contenu

Pour bénéficier de la visibilité complète indispensable au blocage de toutes les menaces, une solution ZTNA doit être en mesure d'effectuer une inspection complète inline du contenu.

Cela signifie que le service sera en mesure d'inspecter l'ensemble du trafic (y compris le trafic chiffré SSL qui est utilisé pour masquer la transmission de contenus dangereux tels que les ransomwares, les spywares et les virus) et de n'autoriser que les communications légitimes connues. Cette inspection inline doit s'appuyer sur des renseignements sur les menaces provenant d'un large éventail de signaux mondiaux pour être en mesure de bloquer les ransomwares, le phishing et les menaces de type « zero day », tout comme les attaques avancées.

Vous souhaitez connaître les menaces que ZTNA devrait être en mesure de contrer ? Le Top 10 de l'OWASP représente un large consensus d'experts sur les risques de sécurité les plus critiques pour les applications Web. Une solution ZTNA devrait fournir une couverture complète des techniques de hacking les plus couramment employées, y compris l'injection SQL, le Cross-Site Scripting, les scanners d'environnement et de port, et l'empoisonnement des cookies.

Zscaler permet de bloquer les menaces du Top 10 de l'OWASP et d'autres risques de sécurité connus pour les applications Web, y compris l'injection SQL et le Cross-Site Scripting.

N° 8 : S'intégrer de manière harmonieuse à un large éventail de fournisseurs et de solutions d'identité

Zscaler s'intègre étroitement avec des fournisseurs d'identité tels que Microsoft et Okta, ainsi qu'avec des plateformes de détection et de réponse des terminaux (EDR) telles que CrowdStrike.

La sécurité Zero Trust commence par la vérification de l'identité de l'utilisateur qui tente d'accéder à une application ou à une autre ressource.

Alors qu'un nombre croissant d'entreprises adoptent des stratégies cloud-first pour prendre en charge les environnements de télétravail actuels, elles se tournent vers de nombreux partenaires de gestion de l'identité et de l'accès (IAM), et de gouvernance et d'administration des identités (IGA) pour soutenir leur capacité à gérer l'authentification et les identités des utilisateurs tout au long de leur cycle de vie.

Il va sans dire qu'une solution ZTNA doit s'intégrer à vos partenaires IAM et IGA actuels. Mais recherchez un fournisseur qui a établi de solides partenariats avec tous les meilleurs fournisseurs de solutions technologiques du secteur si vous souhaitez pérenniser votre stratégie d'identité et d'authentification.

N° 9 : Incorporer une technologie de tromperie intégrée pour déjouer les hackers

La technologie de tromperie constitue une nouvelle catégorie de solutions de cybersécurité.

Elle permet de détecter rapidement les menaces réelles avec de très faibles taux de faux positifs. Elle déploie des leurres réalistes (par exemple, des domaines, des bases de données, des répertoires, des serveurs, des applications, des fichiers, des informations d'identification, des fils d'Ariane) dans un réseau, aux côtés d'actifs réels, qui servent d'appâts. Dès qu'un hacker interagit avec un leurre, la technologie commence à recueillir des informations dont elle se sert pour générer des alertes extrêmement précises.

La technologie de tromperie peut améliorer la capacité de votre équipe de sécurité à détecter les menaces, générer de meilleures informations sur les risques auxquels votre entreprise est exposée, en temps réel, et vous permettre de mieux surveiller ce qui serait autrement des zones d'ombre dans votre environnement. Les leurres agissent comme des déclencheurs dans un environnement Zero Trust, détectant les utilisateurs compromis ou les tentatives de déplacement latéral sur le réseau.

S'agissant d'une technologie émergente, peu de fournisseurs de ZTNA ont pour l'instant intégré des plateformes de tromperie, mais les leaders du secteur ont déjà franchi le pas.

KuppingerCole a désigné Zscaler comme l'un des leaders des plateformes de tromperie distribuées.

N° 10 : Permettre un déploiement rapide et aisé

Contrairement à d'autres solutions technologiques dont le déploiement peut prendre des semaines ou des mois, la solution ZTNA leader du secteur peut être déployée n'importe où en quelques jours seulement.

Zscaler a permis à la ville de Los Angeles de fournir un accès sécurisé au télétravail à 18 000 employés en moins de deux semaines.

Découvrez par vous-même pourquoi Zscaler Private Access est la plateforme ZTNA la plus déployée au monde.

Zscaler Private Access (ZPA) fait tout cela et bien plus encore. Basée sur l'unique architecture Zero Trust de Zscaler, la solution ZPA applique le principe du moindre privilège pour fournir aux utilisateurs des connexions directes et sécurisées aux applications privées, tout en éliminant les accès non autorisés et les déplacements latéraux. Service fourni dans le cloud, ZPA peut être déployé en quelques heures, remplaçant les VPN et outils d'accès à distance traditionnels par une plateforme Zero Trust moderne et globale.

Zscaler Private Access offre les avantages suivants :

- **Sécurité sans égal bien au-delà de ce que les VPN et des pare-feu traditionnels peuvent réaliser :** les utilisateurs se connectent directement aux applications, et non au réseau, ce qui minimise la surface d'attaque et élimine la possibilité de déplacement latéral.
- **Fin de la compromission des applications privées :** la meilleure protection des applications en son genre, avec prévention inline, tromperie et isolation des menaces, permet de minimiser le risque de compromission des comptes utilisateurs.
- **Productivité supérieure pour les équipes hybrides modernes :** un accès ultra-rapide aux applications privées s'étend de manière transparente aux utilisateurs distants, aux bureaux de l'entreprise, aux filiales et aux partenaires tiers.
- **Plateforme ZTNA unifiée pour les utilisateurs, les charges de travail et les appareils :** les employés et les partenaires peuvent se connecter en toute sécurité aux applications privées, aux services et aux appareils OT/IoT au sein de la plateforme ZTNA la plus complète du secteur.

Vous souhaitez en savoir plus ? ? Demandez sans plus attendre une démonstration gratuite.

Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale des entreprises pour les rendre plus agiles, productives, résilientes et sécurisées. 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. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange basé sur le 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. (siège) • 120 Holger Way • San Jose, CA 95134

zscaler.fr