FICHE TECHNIQUE

Zscaler Private Access™

La toute première solution ZTNA optimisé par IA pour doter vos équipes d'un accès rapide, sécurisé et fiable aux applications privées

Zscaler Private Access (ZPA) est une solution cloud native qui offre l'accès Zero Trust à tous les utilisateurs, avec une connectivité directe aux applications privées. La solution minimise la surface d'attaque, élimine les déplacements latéraux des menaces et protège contre les attaques sophistiquées.

Les approches traditionnelles de sécurité réseau ne répondent pas aux besoins de vos collaborateurs hybrides et à ceux de votre entreprise.
Les pare-feu et les VPN traditionnels génèrent une vaste surface d'attaque que les hackers peuvent explorer et exploiter. De plus, les approches traditionnelles positionnent les utilisateurs directement sur votre réseau, ce qui favorise, en cas d'infection, la propagation de menace en interne. Avec des identifiants piratés auprès de vos utilisateurs, les hackers peuvent accéder à vos données sensibles. Recourir à un VPN pour permettre à vos télétravailleurs et à des tiers d'accéder à distance à votre réseau accentuent les risques cyber, offre une expérience utilisateur aléatoire et alourdit les charges d'administration. Il vous faut une approche plus efficace pour fournir un accès sécurisé aux utilisateurs depuis n'importe quel appareil ou lieu.

D'ici 2025, pas moins de 70 % des nouveaux accès à distance déployés seront sécurisés par l'accès réseau Zero Trust (ZTNA) plutôt que par des services VPN, contre moins de 10 % fin 2021, selon Gartner.

Avantages :

- **Remplacement des solutions VPN vulnérables**
  Réduisez votre surface d'attaque et éliminez les déplacements latéraux en connectant les utilisateurs directement aux applications, et non au réseau, ce qui renforce votre posture de sécurité.
- **Prévention des cyberattaques**
  Minimisez le risque de violation en protégeant les applications privées contre les menaces basées sur le Web et liées à l'identité, la protection contre les menaces avancées avec l'inspection inline complète et la prévention des pertes de données.
- **Accompagner vos collaborateurs hybrides**
  Étendez de manière transparente un accès ultra rapide aux applications privées entre les utilisateurs, le siège social, les sites distants et les tiers.
- **Maîtriser la complexité opérationnelle**
  Proposez un accès sécurisé et optimisé, sans produits autonomes coûteux et complexes, grâce à une plateforme ZTNA unifiée et cloud native pour les utilisateurs, les instances et l'OT/IT

Les hackers peuvent facilement contourner les approches traditionnelles de sécurité réseau en tirant parti de la confiance accordée par défaut et de l'accès trop permissif des architectures de sécurité traditionnelles et cloisonnées :

- **L'architecture traditionnelle peine à évoluer et à offrir une expérience utilisateur rapide et transparente :** les VPN requièrent un backhauling, ce qui entraîne des coûts, accentue la complexité et crée une latence qui pèse sur les télétravailleurs.
- **Les pare-feu traditionnels, les VPN, les postes VDI et les applications privées créent une vaste surface d'attaque :** les hackers peuvent identifier et pirater des ressources vulnérables.
- **L'accès à l'ensemble du réseau facilite le déplacement des menaces en interne :** les VPN positionnent les utilisateurs sur votre réseau, ce qui permet aux hackers d'accéder aux données sensibles après avoir infecté un seul dispositif d'utilisateur.
- **Les utilisateurs compromis et les menaces internes peuvent contourner les contrôles traditionnels :** des hackers experts peuvent détourner des identifiants et des identités pour accéder à des applications privées via des outils d'accès à distance traditionnels.

Il est temps de repenser la façon dont nous connectons les utilisateurs de manière sécurisée et homogène aux applications qui leur sont nécessaires, et de faire appel au ZTNA pour redéfinir la sécurité des applications privées.

Zscaler Private Access™ (ZPA)

Première solution ZTNA optimisée par IA du marché, Zscaler Private Access (ZPA) est une solution cloud native qui offre aux utilisateurs un accès Zero Trust et une connectivité directe aux applications privées. Elle permet de minimiser la surface d'attaque en masquant les applications derrière Zero Trust Exchange, en éliminant les déplacements latéraux à l'aide d'une segmentation utilisateur-application optimisée par IA et en assurant une protection contre les attaques sophistiquées, avec une inspection intégrée du trafic et une protection des applications et données. Service cloud natif résilient basé sur un framework SSE (Security Service Edge) global, ZPA se déploie en quelques heures pour remplacer les VPN et les outils d'accès à distance traditionnels, avec des avantages majeur à la clé :

- **Minimiser la surface d'attaque :** les applications sont rendues invisibles depuis Internet, empêchant les utilisateurs et les appareils non autorisés de les identifier. La segmentation des connexions sortantes entre chaque utilisateur et chaque application signifie que les applications et adresses IP ne sont jamais exposées.
- **Définir l'accès sur la base du moindre privilège :** l'accès aux applications est déterminé par l'identité et le contexte, et non par une adresse IP. Les utilisateurs accèdent aux applications sans être positionnés sur le réseau
- **Éliminer les déplacements latéraux :** les applications sont segmentées et les utilisateurs ne peuvent accéder qu'à une application spécifique, ce qui restreint les déplacements latéraux.
- **Neutraliser les cyberattaques grâce à une inspection complète :** le trafic des applications privées est inspecté en mode inline pour empêcher les techniques d'attaque Web les plus courantes.
- **Prévenir la perte de données :** bénéficiez d'une fonction DLP intégrée pour les applications privées, d'une réponse avancée aux incidents et d'une classification des données pour protéger les applications de valeur.
- **Optimiser l'expérience utilisateur :** en connectant les utilisateurs directement aux applications privées, vous éliminez le backhauling lent et coûteux propre aux VPN traditionnels et vous traitez proactivement toute problématique liée à l'expérience utilisateur.

D'ici 2025, pas moins de 70 % des nouveaux accès à distance déployés seront sécurisés par l'accès réseau Zero Trust (ZTNA) plutôt que par des services VPN, contre moins de 10 % fin 2021.*

— Gartner

*Gartner, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales. 8 avril 2022

Principaux cas d’utilisation

Sécuriser l’accès à distance (remplacement du VPN)
Les VPN activés depuis le cloud ou des appliances vous exposent à des cyberattaques. Ils présentent des vulnérabilités et peuvent être piratés. Leur architecture, centrée sur le réseau, entraîne un backhauling du trafic, élargit la surface d’attaque et facilite le déplacement latéral. Les utilisateurs, positionnés directement sur le réseau, peuvent être infectés par un ransomware qui se propagera sur ce réseau. Les VPN sont peu sûrs, lents et leur gestion est complexe.

ZPA pallie les carences de VPN en proposant un accès Zero Trust à tous les utilisateurs, ainsi qu'une connectivité directe aux applications privées. La surface d’attaque est restreinte puisque les applications sont masquées par Zero Trust Exchange. La segmentation utilisateur–application optimisée par IA permet de prévenir les déplacements latéraux. Enfin, c'est la protection contre les attaques sophistiquées qui est assurée grâce à une inspection intégrée du trafic et des fonctions de sécurité des applications et données. ZPA fournit un accès rapide et direct aux applications via plus de 160 points de présence (PoP) répartis dans le monde, sans les risques de sécurité associés au VPN. Le design cloud native de ZPA permet aux équipes informatiques d’éliminer les appliances de passerelles entrantes telles que les équilibreurs de charge, les concentrateurs VPN et autres dispositifs de sécurité, ce qui permet de réduire les coûts, la complexité et les charges de gestion. ZPA fournit un accès Zero Trust à toutes les applications, y compris les applications connectées au réseau telles que la voix sur IP (VoIP) et les applications serveur–client, et même les applications hébergées par des partenaires commerciaux (extranet) pour lesquelles les clients ne peuvent déployer les connecteurs applicatifs de la solution.

Sécuriser l’accès aux applications pour les utilisateurs au bureau et les télétravailleurs
Les utilisateurs actuels ont souvent le choix de travailler depuis leur domicile, un site distant ou au bureau, ce qui remet en question les paradigmes de la sécurité traditionnelle. Les entreprises ont besoin d’un accès ininterrompu aux applications, mais aussi de pérenniser la sécurité Zero Trust en cas de sinistre ou d'accès dégradé à l'infrastructure. Les normes de conformité et de réglementation doivent être respectées pour assurer la continuité de l’activité.

ZPA Private Service Edge vous permet d'introduire la puissance du cloud dans vos locaux, en appliquant les mêmes contrôles de sécurité que vos utilisateurs distants, et avec des performances optimales. En déployant Zscaler Private Service Edge avec des contrôleurs de cloud privé, ZPA permet un basculement entièrement automatisé en mode Continuité d'activité si un dysfonctionnement est détecté. Les politiques et l’authentification sont appliquées même si le cloud ZPA n’est pas accessible.

BYOD et accès des utilisateurs tiers
De manière traditionnelle, l’accès des tiers repose sur des solutions coûteuses, complexes et risquées (VDI, RDP, SSH ou VNC) qui positionnent les utilisateurs directement sur le réseau et exposent les systèmes internes à des dispositifs non fiables.

Les capacités d’accès sans client de ZPA facilitent l’accès des tiers, réduisent les coûts et minimisent les risques. Les tiers, qu'il s'agisse de sous–traitants, de fournisseurs ou de partenaires peuvent utiliser n’importe quel navigateur Web sur leurs propre appareil pour se connecter aux sites Web d'intranet, aux systèmes internes et aux équipements, sans devoir déployer un logiciel client spécifique. Les utilisateurs tiers et les dispositifs non gérés sont ainsi cloisonnés par rapport à votre réseau et vos applications, ce qui garantit la protection des données sensibles contre les opérations non autorisées de copier/coller, d’impression et de téléversement/téléchargement. L’intégration de ZPA et du navigateur Google Chrome Enterprise renforce la sécurité des appareils non gérés/BYOD en vérifiant Chrome Enterprise et en incorporant des informations supplémentaires de posture dans les politiques de ZPA. Avec l’accès sans client, les équipes informatiques offrent une expérience améliorée et plus sécurisée aux utilisateurs, sans subir les coûts de gestion de la VDI traditionnelle. Les fusions, acquisitions et cessions posent souvent de défis en matière d'intégration des réseaux. ZPA accélère ce processus, qui passe de plusieurs mois à quelques semaines. ZPA propose un accès homogène aux applications privées, ce qui élimine le besoin de convergence des réseaux ou d’équipement supplémentaire.

Accès à distance privilégié pour l'OT/IT
Les collaborateurs et fournisseurs tiers doivent accéder régulièrement aux ressources OT/IT pour assurer la haute disponibilité de l'environnement de production et éviter les perturbations résultant d'équipements et de processus défaillants. ZPA permet un accès rapide, sécurisé et fiable aux environnements OT/IT depuis les sites distants, les usines ou tout autre lieu. ZPA for OT/IT fournit un accès à distance cloisonné aux systèmes cibles internes RDP, SSH et VNC, sans installer de client ni faire appel à des serveurs de saut ou des VPN traditionnels.

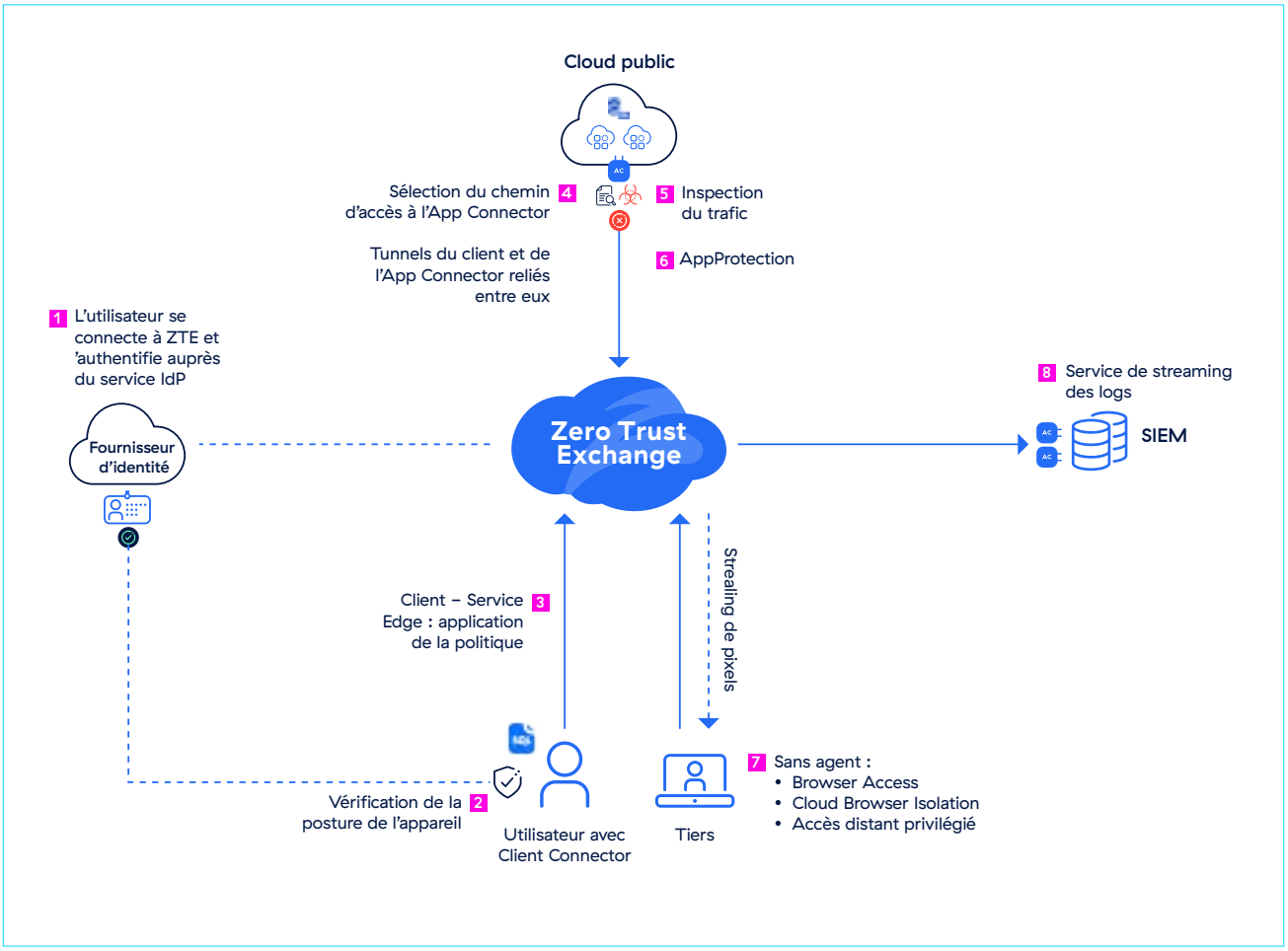
Alternative à la VDI
Les équipes informatiques et de sécurité ne contrôlent pas les dispositifs non gérés, ce qui induit des risques pour l'entreprise. Pour prendre en charge l'accès aux applications à partir d'appareils non gérés, les entreprises ont traditionnellement recours à la VDI. La VDI positionne les utilisateurs directement sur le réseau, exposant les applications internes à des terminaux non gérés. En outre, les dispositifs VDI sont coûteux, difficiles à gérer et ne sont pas évolutifs. Dans le cadre de la transformation numérique, les applications modernes sont généralement basées sur le Web et accessibles par navigateur, tandis que le streaming en continu de toutes les applications via la VDI ne fournit pas une très bonne expérience à l'utilisateur final.

ZPA, une alternative efficace à la VDI, qui offre un accès sécurisé sans agent, basé sur un navigateur, à l'intention des dispositifs non gérés. Les utilisateurs bénéficient d'un accès rapide et homogène aux applications privées via le Service Edge le plus proche. L'architecture ZPA permet un accès direct aux applications, sans positionner l'utilisateur sur le réseau, ce qui sécurise l'accès aux applications privées. ZPA Browser Access permet aux utilisateurs d'utiliser un navigateur Web pour l'authentification de l'utilisateur et l'accès aux applications, sans installer Zscaler Client Connector sur leurs appareils. ZPA assure l'isolation du navigateur, ce qui permet de restituer des pixels/images sur l'appareil de l'utilisateur final, au lieu d'un contenu réel : les données présentes au sein des applications demeurent sécurisées. ZPA permet aux administrateurs de créer des politiques de cloisonnement qui définissent la manière dont un utilisateur peut interagir dans un environnement cloisonné.

Microsegmentation
Les solutions d'accès à distance telles que les VPN accordent un accès complet au réseau et exposent les IP et les applications à Internet. Les VPN étendent le réseau interne aux appareils distants et, de par leur conception, requièrent un trafic entrant, ce qui rend la surface d'attaque visible. Sans une segmentation adéquate du réseau, une intrusion dans un segment pourrait compromettre l'ensemble du réseau de l'entreprise. Cela dit, la mise en œuvre de la segmentation requiert des règles de pare-feu dont la maintenance est complexe. D'autre part, des règles peuvent perturber les applications et compliquer l'accès des utilisateurs de VPN. Dans les grandes entreprises, ceci exige souvent une haute disponibilité, un routage complexe et des liaisons privées onéreuses.

La segmentation applicative optimisée par IA de Zscaler fournit une segmentation précise utilisateur-application et une solution robuste pour un déploiement à grande échelle de politiques cohérentes et l'élimination du déplacement latéral des menaces. Elle vous aide à identifier l'ensemble des applications au sein de votre entreprise et fournit des perspectives sur les utilisateurs qui ont accès aux applications. Elle génère automatiquement des recommandations pour les segments d'applications et les politiques, sur la base de modèles d'apprentissage automatique, ce qui simplifie leur mise en œuvre.

Comment fonctionne ZPA



Fonctionnement

Lorsqu'un utilisateur (collaborateur, fournisseur, partenaire ou sous-traitant) tente d'accéder à une application interne, ZPA garantit une connectivité directe et sécurisée comme suit :

1 L'utilisateur se connecte à Zero Trust Exchange avec le Client Connector et s'authentifie auprès du service de fournisseur d'identité (IdP). Une fois l'authentification réussie, il se reconnecte au Service Edge public, établissant une connexion TLS unique et permanente vers le Service Edge.

2 Après authentification de l'utilisateur et la création d'un tunnel vers le Service Edge, le Client Connector télécharge sa configuration, et notamment le module de contrôle de posture de l'appareil.

3 L'application Zscaler transmet le trafic de l'utilisateur au ZPA Service Edge la plus proche, qui agit en tant que broker pour vérifier les politiques de sécurité et d'accès de l'utilisateur.

4 Deux tunnels sortants, l'un provenant du Client Connector sur l'appareil et l'autre de l'App Connector, sont reliés au niveau du Service Edge.

5 Une fois la connexion établie entre l'appareil de l'utilisateur et l'application, App Connector inspecte automatiquement le trafic pour détecter et neutraliser les menaces potentielles provenant d'utilisateurs ou d'appareils potentiellement compromis.

6 Zscaler AppProtection sécurise les applications privées basées sur le Web et l'identité grâce à une inspection complète de la couche 7, améliorant ainsi la posture de sécurité globale.

7 Les utilisateurs tiers peuvent se connecter à des applications privées via un accès par navigateur intégré ou via Zscaler Browser Isolation qui prend en charge les accès sans client à partir d'appareils non gérés.

8 Log Streaming Service (LSS) diffuse divers logs, dont l'activité des utilisateurs, vers le SIEM.

Un ZPA Service Edge peut être hébergé par Zscaler dans le cloud (ZPA Public Service Edge) ou déployé sur site au sein de votre infrastructure (ZPA Private Service Edge), ce qui permet de raccourcir le chemin vers les applications locales et de favoriser la continuité d'activité.

Fonctionnalités clés

Moteur de politiques basées sur les risques	Validez en permanence les politiques d'accès en fonction de la posture de risque de l'utilisateur, de l'appareil, du contenu ou de l'application. Le moteur de politiques s'assure que seuls les utilisateurs légitimes et authentifiés accèdent aux applications privées.
Accès unifié, avec et sans client	Choisissez la méthode de protection optimale pour votre environnement hybride. L'accès via un client protège les utilisateurs gérés même lorsqu'ils sont en dehors du réseau de l'entreprise, grâce à Client Connector, l'agent léger de Zscaler. L'accès sans client permet aux utilisateurs non gérés de disposer d'un accès fluide aux applications depuis n'importe quel appareil et navigateur Web.
Accès par navigateur	Permettez aux utilisateurs d'appareils personnels (BYOD) et aux utilisateurs tiers d'utiliser librement leurs propres appareils pour accéder de manière transparente et sécurisée aux applications internes, via n'importe quel navigateur Web, sans logiciel client.
ZTNA sur site	Donnez à vos utilisateurs sur site l'expérience du ZTNA en les connectant en toute sécurité aux applications installées dans vos bureaux. Le ZTNA universel garantit un accès et des politiques cohérentes pour tous les utilisateurs, où qu'ils se trouvent et quelles que soient les applications utilisées.
Continuité de l'activité et reprise après sinistre	Assurez un accès permanent aux applications stratégiques, même lors d'un sinistre, grâce à une solution de continuité d'activité, contrôlée par le client ou entièrement managée, qui déploie un chemin d'accès aux applications privées stratégiques par le biais d'une instance de ZPA Private Service Edge.
Identification des applications	Découvrez et répertoriez automatiquement les applications à l'aide de noms de domaine et de sous-réseaux IP spécifiques, vous permettant d'obtenir des informations granulaires sur votre écosystème d'applications privées et sur votre surface d'attaque potentielle.
Segmentation des applications optimisée par IA	Appliquez les recommandations de segmentation optimisées par AA (Apprentissage Automatique) et automatiquement fournies dans ZPA afin d'identifier rapidement et facilement les segments d'applications pertinents et élaborer des politiques d'accès pertinentes. Optimisée par des modèles d'apprentissage automatique entraînés sur des millions de signaux provenant de clients et de vos propres profils d'accès aux applications, la segmentation basée sur l'AA vous aide à minimiser votre surface d'attaque interne.
Segmentation des accès utilisateur vers application	Veillez à ce que tous les accès aux applications soient accordés selon le principe du moindre privilège grâce à la segmentation utilisateur vers application. Fournissez aux utilisateurs autorisés un accès sécurisé à des applications spécifiques sans jamais les positionner sur le réseau. Simplifiez la segmentation du réseau à l'aide de pare-feu internes.
Protection des applications	Protégez les applications privées et l'infrastructure contre les principales attaques grâce à une inspection performante et inline de l'ensemble des charges applicatives afin de détecter toute menace. Identifiez et maîtrisez les risques de sécurité Web connus, tels que les menaces du Top 10 OWASP, ainsi que les vulnérabilités émergentes de type « zero day » qui peuvent contourner les fonctions traditionnelles de sécurité réseau.

Accès distant privilégié	Permettez aux administrateurs et utilisateurs privilégiés de se connecter en toute sécurité aux sites Web intranet, aux systèmes internes et aux équipements sans avoir recours à un VPN, à une infrastructure VDI ou à des outils d'accès à distance (RDP, SSH et VNC).
Protection des données et contre les menaces	Maîtrisez le risque de menaces grâce à une inspection complète du contenu. Identifiez et contrôlez les données sensibles véhiculées par la connexion de l'utilisateur vers l'application.
Identité et authentification unique (SSO)	Intégrez facilement le SSO à votre infrastructure d'identité et d'authentification actuelle pour réduire davantage la complexité.
Accès sécurisé aux applications réseau	Activez cette fonctionnalité pour sécuriser l'accès aux applications connectées au réseau telles que les applications VoIP et serveur–client.
Connectivité IPsec	Activez un accès Zero Trust aux applications des partenaires commerciaux et des fournisseurs (applications extranet) hébergées sur leurs réseaux.

Avantages

Minimiser la surface d'attaque
En éliminant les VPN vulnérables et en rendant les applications invisibles sur Internet, ZPA empêche tout utilisateur non autorisé de les identifier et de les cibler. ZPA crée un segment unique qui regroupe un utilisateur autorisé et une application privée spécifique, en supprimant toute connectivité entrante et en n'autorisant que les connexions sortantes vers les appareils des utilisateurs, via des microtunnels chiffrés. Les administrateurs peuvent découvrir et segmenter automatiquement les applications, les services et les instances indésirables à l'aide d'une fonction d'identification d'applications, ce qui réduit encore davantage la surface d'attaque.

Éliminer les déplacements latéraux
La connectivité, basée sur un accès à moindre privilège, garantit que l'accès aux applications est accordé individuellement, d'un utilisateur autorisé à des applications spécifiques, et non via un accès complet au réseau. Les déplacements latéraux entre les applications ou sur le réseau sont par conséquent impossibles. ZPA ne ne base pas sur les adresses IP et il n'est donc plus nécessaire de mettre en place et de gérer une segmentation complexe du réseau, des listes de contrôle d'accès (ACL), des politiques de pare–feu ou des translations d'adresses réseau (NAT).

Éviter les utilisateurs compromis, les menaces internes et les hackers
Les fonctions intégrées d'inspection inline et de DLP minimisent le risque de compromission des utilisateurs et d'attaques. ZPA neutralise automatiquement les attaques Web en déjouant toutes les techniques des assaillants, y compris celles mentionnées dans le Top 10 OWASP. ZPA propose également des signatures personnalisées pour concevoir des correctifs virtuels actifs immédiatement contre les vulnérabilités de type « zero day ». ZPA minimise les risques liés aux tiers et au BYOD grâce à un accès totalement cloisonné aux applications qui maintient les données sensibles à l'écart des dispositifs non gérés, à l'aide d'une isolation intégrée du navigateur dans le cloud.

Offrir une expérience utilisateur optimale
Une connectivité toujours performante, qui n'exige pas de se connecter et de se déconnecter des VPN, offre aux utilisateurs distants un accès plus sécurisé et rapide. Les sous–traitants, fournisseurs et partenaires externes bénéficient d'un accès fluide depuis n'importe quel appareil et navigateur Web, sans devoir installer de client. Les utilisateurs s'enregistrent avec leurs informations d'identification SSO existantes (Azure AD, Okta, Ping, etc.). De plus, les administrateurs peuvent pérenniser la productivité des utilisateurs en détectant et en traitant de manière proactive les problématiques de performances des utilisateurs finaux causés par des difficultés d'accès aux applications privées, des dysfonctionnements du chemin réseau ou une congestion du réseau.

Plateforme unifiée pour un accès sécurisé aux applications, aux instances et aux dispositifs
Étendez le Zero Trust aux applications privées et aux dispositifs OT/IT pour simplifier et intégrer plusieurs outils d'accès à distance différents, en unifiant les politiques de sécurité et d'accès afin de déjouer les intrusions et de réduire la complexité opérationnelle.

Options de forfait de Zscaler Private Access

	Plateforme Zscaler Essentials (ZS-ESS-PLATFORM)	Plateforme Zscaler Private Access (ZS-ZPA-PLATFORM)	Plateforme Zscaler (ZS-PLATFORM)
Services de la plateforme d'accès privé	Oui 1 utilisateur pour 20 utilisateurs abonnés (min : 500 utilisateurs abonnés)	Oui	Oui
Contrôle d'accès granulaire par utilisateur, groupe et ports			
Service de streaming de logs			
Surveillance permanente de l'intégrité de toutes les applications			
Ancrage IP source			
App Connector	$	Autant que nécessaire, jusqu'à la capacité maximale du système	Autant que nécessaire, jusqu'à la capacité maximale du système
ZPA Private Service Edge			
Accès par des tiers	$	Oui PRA pour plus de 500 utilisateurs	Oui PRA pour plus de 500 utilisateurs
Accès par navigateur			
Portail utilisateur			
Privileged Remote Access (PRA) Standard			
Monitoring de l'expérience numérique	$	Oui	Oui
ZDX Standard			
Sécurité pour les applications privées	$	$	Oui Leurre pour plus de 500 utilisateurs
Protection des données pour les applications privées			
Gestion des risques : leurre			
Segmentation	20 segments d'applications (10 enregistrements/90 jours, période de visibilité historique limitée)	20 segments d'applications (10 enregistrements/90 jours, période de visibilité historique limitée)	20 segments d'applications (10 enregistrements/90 jours, période de visibilité historique limitée)
Aperçu des segments et de la segmentation des applications			
Module complémentaire de segmentation	Oui 100 enregistrements/14 jours Rapports hebdomadaires à la demande, téléchargement et analyse sur jusqu'à 30 jours de données Importation d'applications à partir d'un système interne ou de sources tierces (Qualys, Tenable, ServiceNow)	Oui 100 enregistrements/14 jours Rapports hebdomadaires à la demande, téléchargement et analyse sur jusqu'à 30 jours de données Importation d'applications à partir d'un système interne ou de sources tierces (Qualys, Tenable, ServiceNow)	Oui 100 enregistrements/14 jours Rapports hebdomadaires à la demande, téléchargement et analyse sur jusqu'à 30 jours de données Importation d'applications à partir d'un système interne ou de sources tierces (Qualys, Tenable, ServiceNow)
Nombre illimité de segments d'applications			
Segmentation optimisée par IA			
Informations sur la segmentation			
Importation de segments d'application (à partir de fichiers de données structurés)			
Module complémentaire : AppProtection	Module complémentaire	Module complémentaire	Module complémentaire
Visibilité sur les attaques sur les applications			
Protection contre le Top 10 OWASP : injection SQL, Cross-site scripting, scanners d'environnement et de ports			
Protection contre les menaces de type « zero day »			
Surveillance des utilisateurs à haut risque			

Principaux facteurs de différenciation

Première solution ZTNA optimisée par IA du secteur, ZPA offre une sécurité supérieure et une expérience utilisateur optimale :

- **Solution conçue nativement pour un accès basé sur le moindre privilège :** les utilisateurs autorisés ne peuvent se connecter qu'aux ressources approuvées, et non à votre réseau, ce que ne permettent pas les VPN traditionnels.
- **Les hackers ne peuvent plus identifier ni accéder aux applications :** empêchez la compromission des applications, le vol de données et les déplacements latéraux en dissimulant totalement les applications privées par rapport à l'Internet public.
- **Inspection inline complète :** protégez vos applications en identifiant et neutralisant tout exploit visant les applications privées. Vous déjouez ainsi automatiquement les attaques Web les plus répandues tout en protégeant vos données grâce à une DLP performante.
- **Continuité d'activité à l'échelle mondiale sans impacter la sécurité :** minimisez l'impact des perturbations et appliquez un accès Zero Trust qui répond aux exigences strictes de conformité, même lorsque le cloud Zscaler est inaccessible
- **Accès sans client :** l'accès des tiers s'effectue via un simple navigateur et est protégé par une fonction DLP.
- **Suppression des déplacements latéraux grâce à une segmentation optimisée par IA :** bénéficiez d'une segmentation précise de chaque utilisateur connecté à une application, d'une visibilité sur les accès et de politiques qui s'affinent grâce à l'apprentissage automatique. Vous minimisez ainsi la surface d'attaque et empêchez le déplacement latéral des menaces
- **Présence mondiale de l'edge :** bénéficiez d'une sécurité et d'une expérience utilisateur optimales avec plus de 160 edges cloud dans le monde, ainsi qu'un Service Edge local en option pour étendre le Zero Trust sur votre campus d'entreprise.
- **Design cloud native :** tirez parti de l'évolutivité d'une plateforme fournie depuis le cloud, sans appliance coûteuse sur site ni infrastructure complexe, et qui s'adapte au développement de votre entreprise.
- **Plateforme ZTNA unifiée pour les utilisateurs, les instances et les appareils :** connectez-vous en toute sécurité aux applications privées, aux services et aux dispositifs OT grâce à la plateforme ZTNA la plus complète du secteur.
- **Fait partie d'une plateforme Zero Trust extensible :** protégez et dynamisez votre entreprise avec Zscaler Zero Trust Exchange qui s'adosse à un framework SSE (Security Service Edge) complet.

**Gartner, Magic Quadrant pour le Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15 avril 2024

Gartner ne cautionne aucun fournisseur, produit ou service mentionné dans ses études, ni ne recommande aux utilisateurs technologiques de limiter leur choix aux solutions des fournisseurs les mieux classés ou distingués de quelque autre forme que ce soit. Les publications de recherche de Gartner se composent des opinions de l'organisation de recherche de Gartner et ne doivent pas être interprétées comme des déclarations de fait. Les rapports d'étude de Gartner reflètent les avis des équipes d'analystes de Gartner et ne doivent en aucun cas être considérés comme des déclarations de fait. Gartner s'exonère de toute garantie, expresse ou tacite, concernant ces études, y compris toute garantie de qualité marchande et d'adéquation à un usage particulier.

GARTNER est une marque appartenant à Gartner et Magic Quadrant est une marque déposée par Gartner Inc. et/ou ses filiales aux États-Unis et à l'international. Ces marques sont utilisées dans ce document avec autorisation. Tous droits réservés.

Modules de la solution

Zscaler Client Connector
Client Connector est une application légère qui s'exécute sur les ordinateurs portables et les appareils mobiles des utilisateurs. Elle transmet automatiquement le trafic utilisateur au Service Edge Zscaler le plus proche, garantissant ainsi l'application des politiques de sécurité et d'accès à tous les appareils, sites et applications.

Accès sans agent de Zscaler
Les utilisateurs peuvent se connecter en toute sécurité aux applications, aux instances et aux dispositifs OT via un accès par navigateur (Web, RDP, SSH, VNC) ou via Zscaler Browser Isolation pour un accès sans client à partir des appareils non gérés.

ZPA App Connector
Les App Connectors sont des machines virtuelles légères installées en amont des applications privées déployées dans le data center ou le cloud public. Elles assurent une connectivité sécurisée entre un utilisateur légitime et une application spécifique, via une connexion sortante qui ne rend pas les applications visibles depuis Internet.

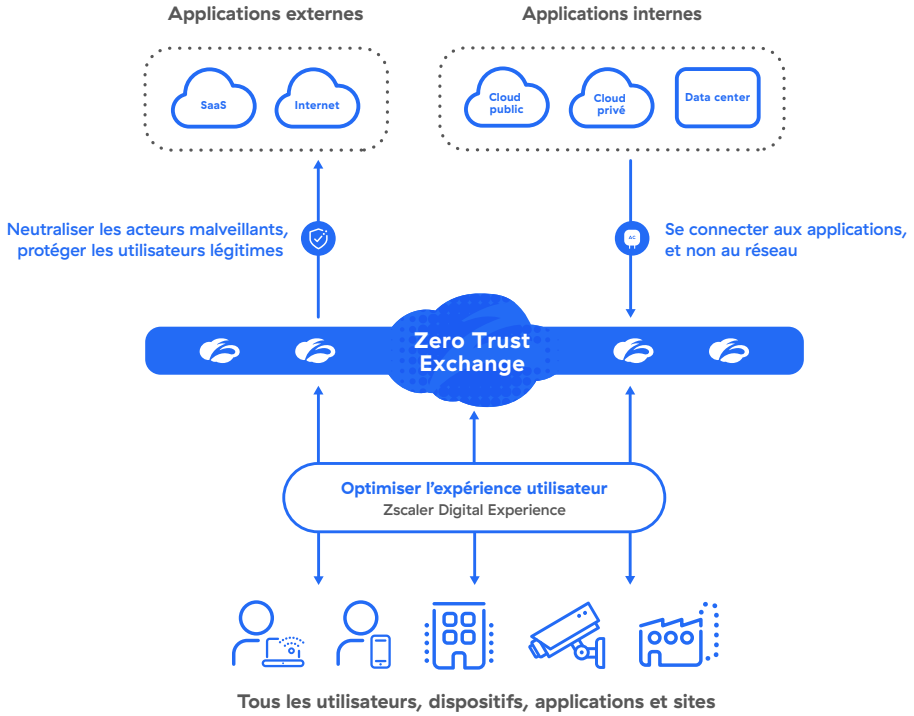
ZPA Service Edges
Les Service Edges appliquent des politiques de sécurité et d'accès, en connectant la connexion sortante d'un utilisateur autorisé (via Client Connector et Browser Access) à une application privée spécifique (via App Connector). La plupart des clients utilisent nos Public Services Edges, hébergés dans plus de 160 points de présence (PoP) dans le monde et capables de gérer des millions d'utilisateurs en simultané. Les Private Service Edges, gérés par Zscaler, peuvent également être hébergés sur site afin de fournir aux utilisateurs sur site le chemin le plus court vers les applications sur site, sans quitter le réseau local. Cela permet d'assurer la continuité d'activité grâce à un accès ininterrompu aux applications critiques, même en cas de sinistre.

ZPA, une composante de la solution globale Zero Trust Exchange

Zscaler Zero Trust Exchange est une plateforme cloud native au service d'un SSE (Security Service Edge) complet afin d'interconnecter les utilisateurs, les instances et les dispositifs, sans jamais les positionner sur le réseau d'entreprise. La solution permet de maîtriser les risques de sécurité et la complexité associés aux outils de sécurité périmétrique qui étendent le réseau, élargissent la surface d'attaque, accentuent le risque de déplacement latéral des menaces et peinent à prévenir les pertes de données.

Comment Zscaler fournit une politique Zero Trust aux utilisateurs, aux instances et à l'OT/IT

Déploiement en quelques semaines pour renforcer la cybersécurité et l'expérience utilisateur



Spécifications techniques

Composants Zscaler	Plateformes et systèmes compatibles	
Client Connector	iOS 9 ou versions ultérieures	macOSX 10.10 ou versions ultérieures
	Android 5 ou versions ultérieures	CentOS 8
	Windows 7 ou versions ultérieures	Ubuntu 20.04
Accès sans client	Navigateurs Web modernes :	Chrome
	(compatible HTML 5)	Edge
		Firefox
App Connector	AWS	Microsoft Hyper-V
	Centos, Oracle et Red Hat	VMware vCenter ou vSphere Hypervisor
	Microsoft Azure	Hôte Docker

zscaler™ | Experience your world, secured.™

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 les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur un SSE, constitue la plus grande plateforme inline de sécurité cloud au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter **@zscaler**.

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