Fiche technique

Zscaler Private Access™

ZTNA de nouvelle génération : un accès rapide, sécurisé et fiable des collaborateurs aux applications.

Zscaler redéfinit l'accès aux applications privées avec ses fonctionnalités avancées de connectivité, de segmentation et de sécurité : votre entreprise déjoue les menaces et assure une expérience utilisateur de tout premier rang.

Les approches traditionnelles de réseau et de sécurité ne répondent pas aux besoins des collaborateurs hybrides modernes.
La connexion des utilisateurs aux applications privées ne devrait pas être lente, complexe ou à risque. Le mode de travail hybride et la transformation du cloud ont bouleversé les modèles de sécurité réseau basés sur le périmètre. Les applications privées migrent vers le cloud et les utilisateurs accèdent aux applications via l'Internet public, à partir de tout appareil, à partir de tout lieu. Les approches traditionnelles qui s'appuient sur des VPN et des pare-feu pour contrôler l'accès aux applications perdent en efficacité dans un monde orienté cloud et mobilité.

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

Avantages :

- **Doper la productivité des collaborateurs hybrides**
  Garantissez un accès rapide et transparent aux applications privées, que vous soyez à domicile, au bureau ou ailleurs.
- **Maîtrisez les risques de piratage de données**
  Minimisez la surface d'attaque et déjouez les déplacements latéraux en rendant les applications invisibles depuis Internet et grâce à un accès à moindre privilège.
- **Neutraliser les attaques sophistiquées**
  La protection des applications privées, unique en son genre, et l'inspection complète du trafic en mode inline minimisent le risque de compromission des utilisateurs et d'attaques actives.
- **Étendre le Zero Trust à l'ensemble des applications, des instances et des appareils**
  La plateforme ZTNA la plus complète au monde fournit un accès sur la base du moindre privilège aux applications privées, aux instances et aux dispositifs OT/IIoT.
- **Simplifier l'opérationnel**
  Notre plateforme cloud native élimine les solutions traditionnelles d'accès à distance telles que les VPN difficiles à faire évoluer, à gérer et à configurer.

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 trop importante pour les télétravailleurs d'aujourd'hui.
- **Les pare-feu traditionnels, les VPN, les postes VDI et les applications privées créent une large surface d'attaque :** les hackers peuvent identifier et exploiter des ressources vulnérables et exposées.
- **L'accès à l'ensemble du réseau favorise un mouvement latéral sans entrave :** les VPN positionnent les utilisateurs sur votre réseau, ce qui permet aux hackers d'accéder sans peine aux données sensibles.
- **Les utilisateurs compromis et les menaces internes peuvent contourner la sécurité traditionnelle :** des hackers experts détournent ainsi des informations d'identification et des identités pour accéder à des applications privées, dans le cas où seuls des outils d'accès distants traditionnels ou un ZTNA de première génération sont déployés.

Il est temps de repenser la façon dont nous connectons les utilisateurs de manière sécurisée et transparente aux applications qui leur sont néces-saires et de redéfinir la sécurité des applications privées avec un ZTNA de nouvelle génération.

Zscaler Private Access™ (ZPA)

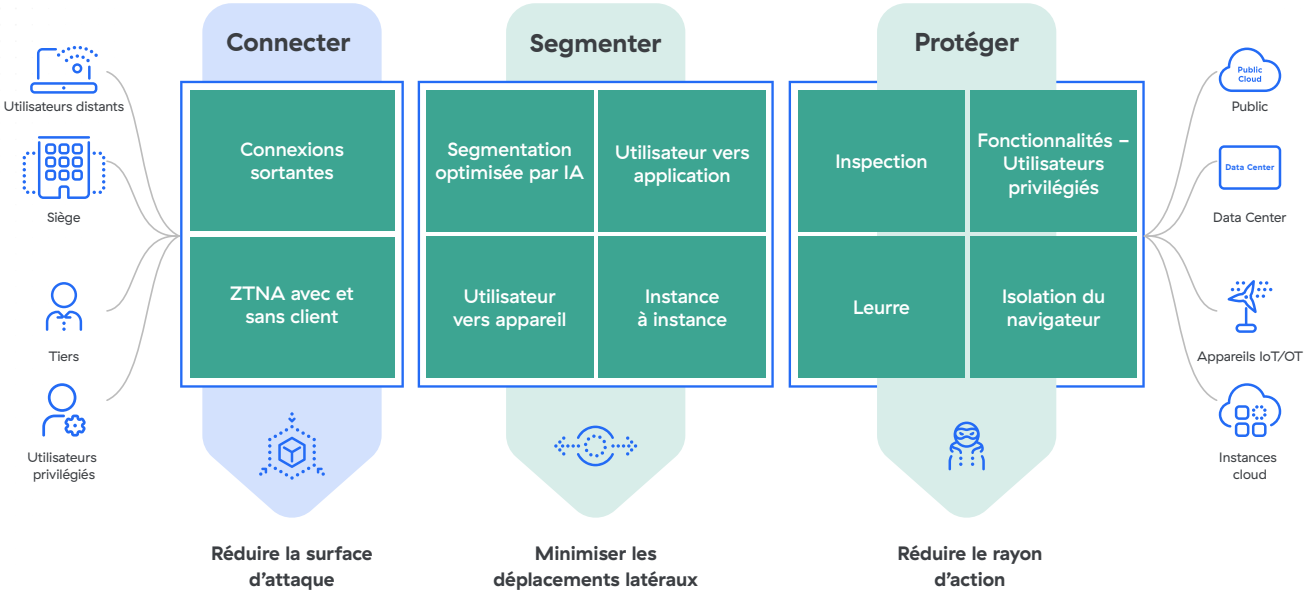
ZPA est la plateforme ZTNA la plus déployée au monde. Elle applique le principe du moindre privilège pour offrir aux utilisateurs une connectivité directe et sécurisée aux applications privées, actives sur site ou dans le cloud public, tout en supprimant les accès non autorisés et les déplacements latéraux. Service cloud natif basé sur un framework Security Service Edge (SSE) global, ZPA peut être déployé en quelques heures pour remplacer les VPN et les outils d'accès à distance traditionnels, avec les avantages suivants :

- **Offrir une expérience utilisateur optimale :** en connectant les utilisateurs directement aux applications privées, vous éliminez le backhauling lent et coûteux des VPN traditionnels et vous prenez en charge de manière proactive toute problématique liée à l'expérience utilisateur.
- **Minimiser la surface d'attaque :** les applications sont rendues invisibles depuis Internet, empêchant les utilisateurs et les appareils non autorisés de les identifier. Les connexions sortantes entre l'utilisateur et l'application garantissent qu'aucune application ou adresse IP n'est exposée.
- **Assurer un 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 transiter par le réseau.
- **Éliminer les déplacements latéraux :** les applications sont segmentées afin que les utilisateurs ne puissent accéder qu'à une application spécifique, ce qui limite 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 les plus précieuses.
- **Identifier les utilisateurs et les appareils compromis :** des leurres intégrés permettent d'identifier et de neutraliser rapidement les utilisateurs et appareils malveillants.

D'ici 2025, au moins 70 % des nouveaux environnements d'accès à distance feront principalement appel à un accès réseau Zero Trust (ZTNA).

— Gartner

ZPA et les nouveaux cas d'utilisation du ZTNA



Principaux cas d'utilisation

Alternative aux VPN
Les VPN n'ont pas été conçus dans un souci de sécurité, d'évolutivité ou d'expérience utilisateur. Traditionnellement, les VPN effectuent le backhauling de l'ensemble du trafic des utilisateurs distants vers des data centers qui peuvent se trouver à des milliers de kilomètres, ce qui est source de latence et de frustration des utilisateurs. Une fois connectés, les VPN tunnelisent les utilisateurs au-delà du pare-feu et les positionnent sur le même réseau que vos applications, ce qui permet des déplacements latéraux.

ZPA propose une alternative en fournissant un accès rapide et direct aux applications via plus de 150 points de présence (PoP) répartis dans le monde entier, sans les risques de sécurité associés au VPN. La connectivité sortante dissocie l'accès aux applications de l'accès au réseau, ce qui rend les applications invisibles depuis Internet. ZPA connecte les utilisateurs aux applications, non aux réseaux, et les utilisateurs n' accèdent qu'à des applications désignées, sans possibilité de déplacement latéral. Le design cloud native de ZPA implique que les équipes informatiques peuvent éliminer les appliances de passerelle entrante telles que les équilibreurs de charge, les concentrateurs VPN et autres dispositifs de sécurité, réduisant ainsi les coûts et la complexité.

Sécuriser les collaborateurs hybrides
Les utilisateurs travaillent désormais depuis leur domicile ou des sites distants, remettant en question les approches traditionnelles de sécurité. ZPA offre un accès transparent et sécurisé aux applications privées, où qu'elles soient et depuis n'importe quel appareil. Les utilisateurs présents au siège de leur entreprise bénéficient d'une expérience identique via ZPA Private Service Edge.

ZPA Private Service Edge vous permet de déployer la puissance du cloud sur site, en appliquant les mêmes fonctionnalités de sécurité que celles qui protègent vos utilisateurs distants, avec le même niveau de performances. ZPA est désormais en mesure de fournir des fonctionnalités d'Universal ZTNA pour une expérience utilisateur rapide

et cohérente. De plus, grâce au monitoring de l'expérience digitale, vous bénéficiez d'une visibilité en temps réel sur la dégradation des performances et les dysfonctionnements, encourageant ainsi la productivité du travail hybride. Dans le cadre de Zscaler Zero Trust Exchange™, les utilisateurs bénéficient d'une plateforme SSE intégrée pour un accès sûr, rapide et direct à Internet, aux applications SaaS, aux instances, aux dispositifs et aux applications privées.

Accès des tiers/alternative au VDI
Dans le passé, l'accès des tiers reposait sur une infrastructure VDI (postes de travail virtualisés) complexe et coûteuse ou sur d'autres clients/protocoles d'accès à distance au poste de travail (RDP, SSH ou VNC) qui positionnaient les utilisateurs directement sur votre réseau et exposaient les systèmes internes à des dispositifs non fiables. La fonction d'accès sans client de ZPA rendent l'accès des tiers aussi facile que d'accéder au Web, tout en réduisant les coûts et en maîtrisant les risques. Vos fournisseurs, sous-traitants et partenaires peuvent utiliser librement le navigateur de leur choix, à partir de leurs propres appareils, pour se connecter aux sites Web intranet, aux systèmes internes et aux équipements, sans requérir de client. Les utilisateurs tiers et les appareils non gérés sont isolés de votre réseau et de vos applications, ce qui garantit que les données sensibles n'échappent jamais à votre contrôle et sont protégées contre le copier/coller, l'impression et le téléversement/téléchargement non autorisés. Avec un accès sans client, vos équipes informatiques peuvent fournir une expérience améliorée et sécurisée aux utilisateurs sans devoir accuser les coûts liés à la gestion de l'infrastructure VDI traditionnelle.

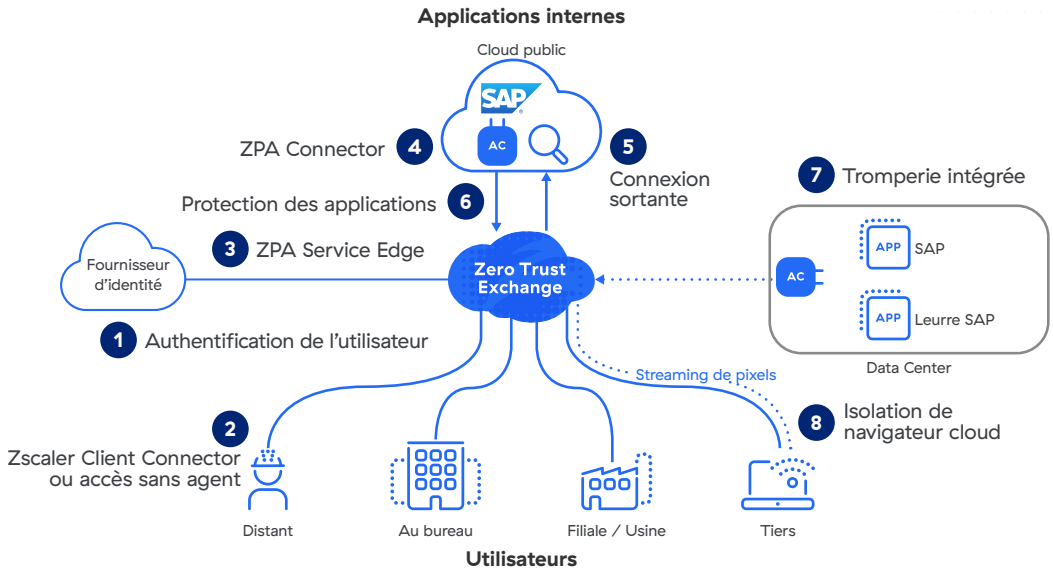
Fusions/acquisitions et cessions
Les fusions/acquisitions et les cessions imposent souvent d'associer des réseaux, ce qui peut s'avérer difficile en raison du chevauchement des plages IP et du déploiement de pare-feu entre les deux entités. ZPA accélère considérablement les tâches d'intégration suite à une fusion/acquisition, en ramenant le processus à quelques semaines au lieu de plusieurs mois. La solution offre un accès transparent aux applications privées, sans recourir à un VPN, et élimine la nécessité de faire converger plusieurs réseaux ou d'investir dans des équipements réseau supplémentaires, libérant ainsi des ressources qui peuvent être affectées à des missions à plus forte valeur ajoutée.

Accès sécurisé des opérateurs en environnement OT et IIoT
Les collaborateurs et des fournisseurs tiers doivent pouvoir accéder aux ressources OT et IIoT afin d'optimiser la disponibilité des environnements industriels et éviter les perturbations dues aux défaillances des équipements et des processus. ZPA permet un accès rapide, sécurisé et fiable aux environnements OT et IIoT depuis les sites sur le terrain, les usines ou tout autre lieu. ZPA for IoT/OT fournit un accès à distance totalement cloisonné aux systèmes cibles internes RDP, SSH et VNC sans devoir installer un client sur l'appareil des utilisateurs qui ferait appel à des serveurs jump ou des VPN traditionnels.

Connectivité sécurisée entre les instances
Les entreprises modernes ont besoin d'une connectivité rapide et sécurisée entre leurs instances présentes au sein d'environnements privés, hybrides et multicloud. ZPA for Workloads réduit la complexité et les coûts opérationnels tout en activant une connectivité basée sur le Zero Trust pour les instances présentes au sein de ces environnements. Les instances étant positionnées en aval de ZPA, elles sont invisibles depuis Internet et ne peuvent donc pas être ciblées par une attaque.

Zero Trust Branch Connectivity
Zero Trust Branch Connectivity connecte en toute sécurité les sites distants, les usines et les data centers sans la complexité des VPN, en garantissant un accès Zero Trust entre les utilisateurs, les appareils IoT/OT et les applications, en fonction des règles en vigueur. La solution élimine la surface d'attaque et empêche tout déplacement latéral des menaces en connectant les utilisateurs et les appareils IoT/OT aux applications via Zero Trust Exchange. Zero Trust Branch Connectivity simplifie considérablement les communications des sites distants en éliminant tout routage complexe, les VPN et les pare-feu. La solution permet également un forwarding flexible et une gestion simple des politiques grâce au framework éprouvé des politiques de ZIA et de ZPA.

ZPA étend l'accès sur la base du moindre privilège à l'ensemble de l'entreprise.



Mode opératoire

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 est authentifié auprès du fournisseur d'identité (IdP) à l'aide de ses informations d'identification SAML SSO.
2. La posture du dispositif d'un utilisateur est vérifiée avec Zscaler Client Connector, un agent logiciel léger installé sur l'ordinateur portable ou l'appareil mobile de l'utilisateur. ZPA peut également récupérer la posture du dispositif via une intégration avec les principaux fournisseurs de solutions EPP/EDR/XDR (par exemple, CrowdStrike, Microsoft Defender, SentinelOne).
3. L'application Zscaler transmet le trafic de l'utilisateur à l'instance 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. Ensuite, ZPA Service Edge détermine l'application la plus proche de l'utilisateur et établit une connexion sécurisée à un ZPA App Connector, une machine virtuelle légère installée dans l'environnement hébergeant les serveurs et les applications.
5. Deux tunnels sortants, l'un provenant du Client Connector sur l'appareil et l'autre de l'App Connector, sont associés par ZPA Service Edge.
6. Une fois qu'une connexion est 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.
7. La fonction intégrée Zscaler Deception détecte les utilisateurs compromis qui accèdent à des applications de leurre et peut ainsi neutraliser tout accès aux ressources internes de l'environnement Zero Trust Exchange.
8. En outre, les utilisateurs tiers peuvent se connecter à des applications privées grâce à un accès par navigateur ou à Zscaler Browser Isolation (isolation du navigateur) qui prend en charge les accès sans client à partir d'appareils non gérés.

Un ZPA Service Edge peut être soit hébergé par Zscaler dans le cloud (ZPA Public Service Edge), soit présent sur site au sein de votre infrastructure (ZPA Private Service Edge). Dans un cas comme dans l'autre, le Service Edge est géré par Zscaler sans devoir déployer une appliance.

Fonctionnalités clés

Moteur de politiques basées sur le risque	Validez en permanence les politiques d'accès en fonction de la posture de risque de l'utilisateur, de l'appareil, du contenu et 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 avoir besoin d'un 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. L'Universal ZTNA garantit un accès et des politiques cohérentes pour tous les utilisateurs, où qu'ils se trouvent et quelles que soient les applications impliquées.
Reprise après sinistre	Bénéficiez d'un accès permanent aux applications stratégiques, même lors d'un sinistre, grâce à une solution de continuité des activités contrôlée par le client. Cette solution déploie un chemin d'accès aux applications privées stratégiques par le biais d'une instance de ZPA Private Service Edge.
Identification des applications	Identifiez 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 une segmentation optimisée par AA (apprentissage automatique) qui vous est automatiquement recommandée dans ZPA. Vous identifiez ainsi rapidement et facilement les segments d'applications adéquats et élaborez des politiques d'accès pertinentes. Optimisée par des modèles AA entraînés sur des millions de signaux provenant de clients et sur vos propres profils d'accès aux applications, la segmentation optimisée par AA contribue à réduire votre surface d'attaque interne.
Segmentation 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.
Segmentation utilisateur vers appareil	Veillez à ce que tous les accès aux équipements et systèmes OT/IIoT soient accordés selon le principe du moindre privilège, avec une segmentation utilisateur vers appareil. Autorisez les fournisseurs tiers et les utilisateurs distants à se connecter aux équipements depuis n'importe quel emplacement grâce à ZPA for IoT/OT.
Segmentation des instances	Avec ZPA for Workloads, sécurisez la connectivité et les communications entre les instances au sein des environnements hybrides et multicloud.
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, capable de détecter les menaces. 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 ne sont pas identifiées par les fonctions traditionnelles de sécurité réseau.
Technologie de leurre intégrée	Détectez et contrez les hackers et les menaces internes les plus sophistiqués grâce à des applications fictives, avec une mise en quarantaine automatisée des utilisateurs compromis sur l'ensemble du périmètre de Zero Trust Exchange.
Isolation du navigateur Web	Fournissez un accès cloisonné et sans client vers les applications Web stratégiques pour les collaborateurs et le personnel externe qui utilisent leurs appareils personnels (BYOD). Veillez à ce que les terminaux non gérés vulnérables ou infectés par des malwares ne mettent ni votre réseau ni vos applications en péril. Contrôlez l'exfiltration des données (copier/coller, impression, chargement/téléchargement) pour éviter toute perte de données sensibles.
Accès distant privilégié	Permettez aux administrateurs et utilisateurs privilégiés de se connecter en toute sécurité aux sites intranet, aux systèmes internes et aux équipements sans avoir recours à un VPN, à une VDI ou à des clients desktop de type RDP, SSH et VNC.
Protection des données et contre les menaces	Maîtrisez les risques associés aux menaces grâce à une inspection complète des contenus. Repérez et contrôlez les données sensibles transitant sur une connexion entre un utilisateur et une application.
Zero Trust SD-WAN	Connectez en toute sécurité vos sites distants, usines et data centers sans la complexité des VPN, en garantissant un accès Zero Trust et basé sur les politiques d'entreprise entre les utilisateurs, les dispositifs IoT/OT et les applications.

Avantages

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

Minimiser les déplacements latéraux
La connectivité repose sur un accès basé sur le moindre privilège. L'accès aux applications est accordé sur une base individuelle : l'utilisateur autorisé accède à des applications spécifiques et non au réseau complet. Les déplacements latéraux entre les applications ou sur le réseau sont par conséquent impossibles. ZPA ne reposant pas sur les adresses IP, il n'est plus nécessaire de déployer et gérer une segmentation complexe du réseau, des listes de contrôle d'accès (ACL), des politiques de pare-feu ou des translations d'adresses NAT. Grâce à une fonction intégrée de leurre, ZPA permet aux équipes de sécurité de détecter et d'isoler immédiatement un utilisateur malveillant ou un appareil compromis qui tente de se déplacer latéralement sur le réseau d'entreprise.

Prévenir les utilisateurs compromis, les menaces internes et les hackers
Une protection des applications privées, unique en son genre, dotée de fonctions intégrées d'inspection inline, de leurre et de prévention des pertes de données, permet de minimiser le risque de compromission des utilisateurs et d'attaques actives. ZPA déjoue automatiquement les attaques Web avec une prise en compte des techniques les plus répandues, y compris celles du Top 10 des risques de sécurité de OWASP. D'autre part, les signatures personnalisées des vulnérabilités de type « zero day » permettent d'appliquer un correctif virtuel (virtual patching). ZPA minimise les risques liés aux tiers et au BYOD grâce à un accès cloisonné aux applications qui empêche les appareils non gérés d'accéder aux données sensibles, ceci étant possible grâce à un service cloud d'isolation de navigateur. Des applications factices déployées par la fonctionnalité de leurre permettent aux équipes de sécurité de contenir les menaces actives sur le réseau en empêchant les utilisateurs compromis d'accéder aux ressources.

Optimiser l'expérience utilisateur
Une connectivité toujours rapide, qui n'exige pas de se connecter et de se déconnecter de clients VPN, offre aux utilisateurs distants un accès plus sécurisé et plus performant. Les sous-traitants, fournisseurs et partenaires tiers bénéficient d'un accès fluide depuis n'importe quel appareil et navigateur Web sans devoir installer de client.
Les utilisateurs s'enregistrent avec leurs identifiants SSO existants (Azure AD, Okta, Ping, etc.). De plus, les administrateurs assurent la productivité des utilisateurs en détectant et en résolvant de manière proactive toute problématique de performances des utilisateurs finaux causée par des difficultés d'accès aux applications privées, des dysfonctionnements au niveau du chemin réseau ou une congestion du réseau.

Une plateforme unifiée pour un accès sécurisé aux applications, aux instances et aux appareils
Étendez Zero Trust aux applications privées, aux instances et aux dispositifs OT/IIoT pour simplifier et intégrer différents outils d'accès à distance, en unifiant les politiques de sécurité et d'accès, pour ainsi déjouer toute tentative de compromission et simplifier les opérations.

Versions de Zscaler Private Access

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Services de la plateforme	Ancrage des IP sources, fournisseurs d'identité (IdP) multiples, LSS	(+) Accès au data center étendu	(+) Environnement de test, PKI client	(+) Environnement de test, PKI client
Segmentation utilisateur vers application	10 segments d'applications	500 segments d'applications	Segments illimités d'applications	Segments illimités d'applications
App Connector	20 paires	50 paires	Nombre illimité de paires	Nombre illimité de paires
ZTNA sur site[1]	1 paire (virtuelle)	1 paire de Service Edges privés par 5 000 utilisateurs	1 paire de Service Edges privés par 2 000 utilisateurs	1ère paire de Service Edges privés incluse, paire supplémentaire par tranche de 1 000 utilisateurs
Accès sans client[2]	—	✓	✓	✓
Monitoring intégré de l'expérience digitale	—	Standard	Standard	Standard
Technologie de leurre intégrée	—	Standard	Advanced	Advanced Plus
Protection des applications	—	—	✓	✓
Isolation intégrée	—	—	Standard	Advanced Plus
Protection des données (applications privées)	—	—	—	✓
Support premium	—	—	—	✓

Principaux facteurs de différenciation

Seule plateforme ZTNA de nouvelle génération du secteur, Zscaler Private Access optimise la sécurité et l'expérience utilisateur :

- **Solution conçue nativement pour un accès à moindre privilège :** vos utilisateurs légitimes 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 et accéder aux applications :** prévenez le piratage applicatif, le vol de données et les déplacements latéraux en rendant les applications privées, les instances et les appareils totalement invisibles depuis 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.
- **Leurre intégré :** arrêtez les tentatives de déplacement latéral et la propagation des ransomwares avec la seule solution ZTNA dotée d'une fonction de leurre en natif.
- **Accès sans client :** l'accès des tiers s'effectue via un simple navigateur et est protégé par une DLP.
- **Amélioration de la productivité :** bénéficiez d'une visibilité complète sur l'accès aux applications privées afin de détecter les problématiques qui pèsent sur l'expérience utilisateur.
- **Présence mondiale des edges :** bénéficiez d'une sécurité et d'une expérience utilisateur optimales grâce à plus de 150 edges cloud dans le monde. Un Service Edge local est proposé en option pour déployer le Zero Trust sur votre siège social.
- **Design cloud native :** tirez parti de l'évolutivité d'une plateforme fournie depuis le cloud, sans appliances sur site coûteuses ni infrastructure complexe. La plateforme s'adapte ainsi à l'évolution de votre entreprise.

[1]La version ZPA Business Edition prend en charge jusqu'à 5 paires de Service Edges privés ; achat de paires supplémentaires requis à partir de 50 000 utilisateurs. La version ZPA Transformation Edition prend en charge jusqu'à 10 paires de Service Edges privés; achat de paires supplémentaires requis à partir de 50 000 utilisateurs. La version ZPA Unlimited Edition prend en charge jusqu'à 50 paires de Service Edges privés ; achat de paires supplémentaires requis à partir de 50 000 utilisateurs.

[2]L'accès sans client comprend l'accès par navigateur et l'accès distant privilégié (pour jusqu'à 10 systèmes).

- **Plateforme ZTNA unifiée pour les utilisateurs, les instances et les appareils :** connectez-vous en toute sécurité à des applications, des services et des dispositifs OT privés grâce à la plateforme ZTNA la plus complète du marché.
- **Une plateforme Zero Trust extensible :** protégez et dynamisez votre entreprise avec Zscaler Zero Trust Exchange, qui repose sur un framework SSE (Security Service Edge) complet.

Modules de la solution

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

Zscaler Branch Connector
Branch Connector, disponible sous forme d'appliance physique et virtuelle, améliore les performances des applications en éliminant le backhauling et en redirigeant tout le trafic des filiales et des data centers directement vers l'edge Zscaler le plus proche, minimisant ainsi la latence. Ce composant permet une communication bidirectionnelle entre les utilisateurs, les serveurs, les dispositifs IoT/OT (sur lesquels Client Connector ne peut pas être installé) et les applications, sur n'importe quel réseau, via Zero Trust Exchange.

Zscaler Clientless Access
Les utilisateurs peuvent se connecter en toute sécurité aux applications, aux instances et aux dispositifs OT via un accès intégré basé sur un navigateur (Web, RDP, SSH, VNC) ou via Zscaler Browser Isolation pour un accès sans client à partir d'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 autorisé et une application spécifique, via une connexion sortante qui n'expose pas les applications à Internet.

ZPA Service Edges
Les Service Edges appliquent les politiques de sécurité et d'accès, en établissant une connexion sortante entre un utilisateur autorisé (via Client Connector et Browser Access) et une application privée spécifique (via App Connector). Nos clients, parmi les plus grandes entreprises mondiales, font appel à nos Services Edges publics hébergés sur plus de 150 hubs dans le monde. Les Service Edges privés, gérés par Zscaler, peuvent également être hébergés sur site afin de fournir aux utilisateurs sur site le chemin le plus court vers leurs applications sur site, sans quitter le réseau local.

Gartner

Zscaler a été reconnu comme Leader dans le Magic Quadrant de Gartner dédié au SSE en 2022 et 2023.

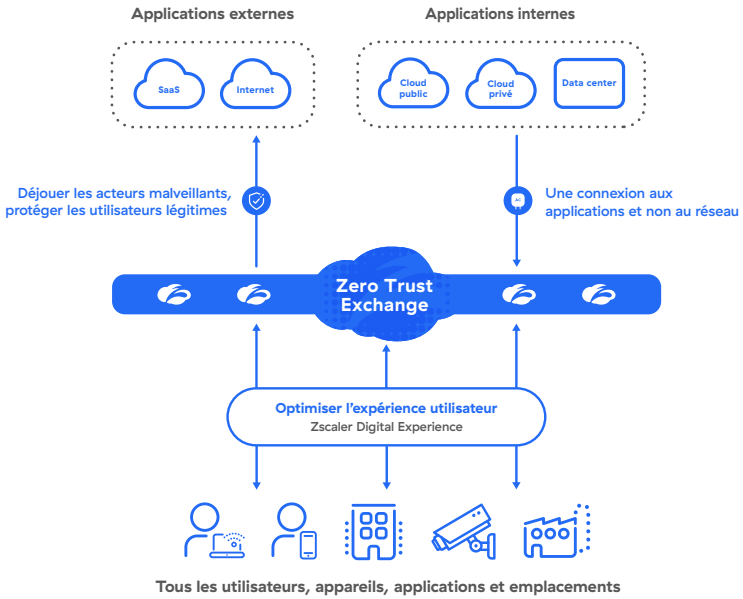
En savoir plus →

ZPA est une composante de la solution globale Zero Trust Exchange

Zscaler Zero Trust Exchange est une plateforme cloud native qui déploie un SSE (Security Service Edge) complet afin de connecter les utilisateurs, les instances et les appareils, 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 périmétriques. Ces derniers étendent le réseau, élargissent la surface d'attaque, accentuent le risque de déplacement latéral des menaces et échouent à prévenir les pertes de données.

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

Un déploiement en quelques semaines pour améliorer la cyberprotection et l'expérience utilisateur



Spécifications techniques

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

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, indépendamment de l'emplacement. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange, orientée SSE, constitue la plus vaste plateforme intégrée de sécurité cloud. 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