FICHE TECHNIQUE

Zscaler Private Access™

Une solution ZTNA optimisée 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 équipes hybrides ni à ceux de votre entreprise.
Les pare-feu et VPN classiques créent une surface d'attaque considérable, facilement exploitable par les hackers. Ils placent également les utilisateurs directement sur votre réseau, favorisant ainsi le déplacement latéral des menaces. Si les identifiants de vos utilisateurs sont compromis, les hackers peuvent accéder aisément à vos données sensibles. L'utilisation d'un VPN pour permettre l'accès à vos équipes hybrides et aux tiers accroît les cyber-risques, dégrade l'expérience utilisateur et alourdit la charge administrative. Pour garantir un accès sécurisé aux utilisateurs, quel que soit leur appareil ou leur lieu de travail, une solution plus efficace est indispensable.

Selon le rapport Zscaler ThreatLabz 2025 sur les risques liés aux VPN, 92 % des personnes interrogées craignent que les vulnérabilités des VPN non corrigées entraînent directement des incidents de ransomware, soulignant la difficulté de corriger les VPN en permanence et en temps opportun.

Avantages :

- **Remplacer les solutions VPN vulnérables**
  Réduisez la surface d'attaque et éliminez les déplacements latéraux en connectant les utilisateurs directement aux applications, et non au réseau, ce qui renforcera votre posture de sécurité.
- **Prévenir les cyberattaques**
  Minimisez les risques de violation grâce à la protection des applications privées contre les menaces liées au Web et à l'identité, à une protection avancée contre les menaces avec inspection inline complète et à une protection contre la perte de données.
- **Autonomiser votre personnel hybride**
  Étendez en toute transparence un accès ultra-rapide aux applications privées aux utilisateurs, au siège social, aux filiales et aux tiers.
- **Réduire la complexité opérationnelle**
  Offrez un accès sécurisé et optimisé, sans produits ponctuels coûteux et complexes, grâce à une plateforme ZTNA unifiée et cloud native pour les utilisateurs, les workloads et l'IoT/OT.

© 2025 Zscaler, Inc. Tous droits réservés.

Les hackers peuvent facilement contourner les outils traditionnels 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, de la complexité et 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 transparente aux applications qui leur sont nécessaires, et de faire appel à une solution ZTNA (Zero Trust Network Access) pour redéfinir la sécurité des applications privées.

Zscaler Private Access™ (ZPA)

Première solution ZTNA du marché à être optimisé par IA, 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 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 majeurs 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.

92 % des personnes interrogées craignent que les vulnérabilités des VPN non corrigées entraînent directement des incidents de ransomware, soulignant la difficulté de corriger les VPN en permanence et en temps opportun

— Rapport Zscaler ThreatLabz 2025 sur les risques liés aux VPN

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

©2025 Zscaler, Inc. Tous droits réservés.

Principaux cas d'utilisation

Accès distant sécurisé (alternative au VPN)
Les VPN cloud ou basés sur les appliances vous exposent aux cyberattaques. Ils sont truffés de vulnérabilités et régulièrement exploités par les hackers. Leur conception centrée sur le réseau achemine le trafic vers les serveurs distants, élargit la surface d'attaque et permet les déplacements latéraux en plaçant les utilisateurs directement sur le réseau, ce qui favorise les attaques par ransomware. Les VPN sont peu sécurisés, lents et complexes à gérer.

La solution ZPA répond aux défis liés aux VPN en proposant un accès Zero Trust à tous les utilisateurs, ainsi qu'une connectivité directe aux applications privées. Résultat : la surface d'attaque est restreinte puisque les applications sont masquées par Zero Trust Exchange. La segmentation utilisateur–application optimisée par l'IA permet également de prévenir les déplacements latéraux. Enfin, la protection contre les attaques sophistiquées est assurée grâce à une inspection intégrée du trafic et des fonctions de sécurité des applications et données. ZPA offre 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 aux VPN. La conception 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), sans avoir besoin de déployer d'infrastructure supplémentaire telle que des App Connectors.

Accès sécurisé aux applications pour les utilisateurs au bureau et à distance
Dans le monde du travail actuel, les utilisateurs travaillent depuis leur domicile, d'autres sites distants, des filiales et le siège social, ce qui remet en question les modèles de sécurité traditionnels. Les entreprises ont besoin d'un accès continu aux applications, sans compromettre la sécurité Zero Trust en cas de sinistre ou de dégradation de l'infrastructure. La conformité aux normes réglementaires est également essentielle à la continuité d'activité.

ZPA Private Service Edge vous permet de déployer la puissance du cloud dans vos locaux, en appliquant les mêmes fonctions de sécurité que celles dont bénéficient 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.

Appareils BYOD et accès utilisateur tiers
L'accès tiers traditionnel reposait sur des solutions coûteuses, complexes et risquées (VDI, RDP, SSH ou VNC) qui plaçaient les utilisateurs directement sur le réseau et exposaient les systèmes internes à des appareils 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 leur propre appareil pour se connecter aux sites Web intranet, aux systèmes internes et aux équipements, sans devoir déployer un logiciel client spécifique. Les utilisateurs tiers et les appareils non gérés sont ainsi séparés de votre réseau et de vos applications, ce qui garantit la protection des données sensibles contre les opérations non autorisées de copier/coller, d'impression et de chargement/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 de sécurité 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 transparent aux applications privées, ce qui élimine le besoin de convergence des réseaux ou d'équipement supplémentaire.

©2025 Zscaler, Inc. Tous droits réservés.

Accès distant privilégié pour OT/IT
Les employés et les fournisseurs tiers doivent accéder aux actifs OT/IT régulièrement afin de maximiser la disponibilité de la production et d'éviter les interruptions dues aux pannes d'équipement et de processus. ZPA permet un accès rapide, sécurisé et fiable aux environnements OT/IT depuis les sites sur le terrain, l'usine ou de tout autre emplacement. ZPA pour OT/IT offre un accès de bureau à distance entièrement isolé et sans client aux systèmes cibles internes RDP, SSH et VNC, sans exiger des utilisateurs qu'ils installent un client sur leur appareil en utilisant des serveurs intermédiaires et des VPN traditionnels.

Alternative à la VDI
Les équipes informatiques et de sécurité manquent de contrôle sur les appareils non gérés, ce qui engendre des risques pour l'entreprise. Traditionnellement, les entreprises ont recours à la VDI pour permettre l'accès aux applications sur ces appareils. Or, la VDI place les utilisateurs directement sur le réseau, exposant ainsi les applications internes à des terminaux non gérés. De plus, la VDI est coûteuse, complexe à gérer et difficilement évolutive. Dans le contexte de la transformation numérique, les applications modernes sont généralement basées sur le Web ou un navigateur, et la diffusion d'un bureau complet via une VDI n'offre pas une expérience utilisateur optimale.

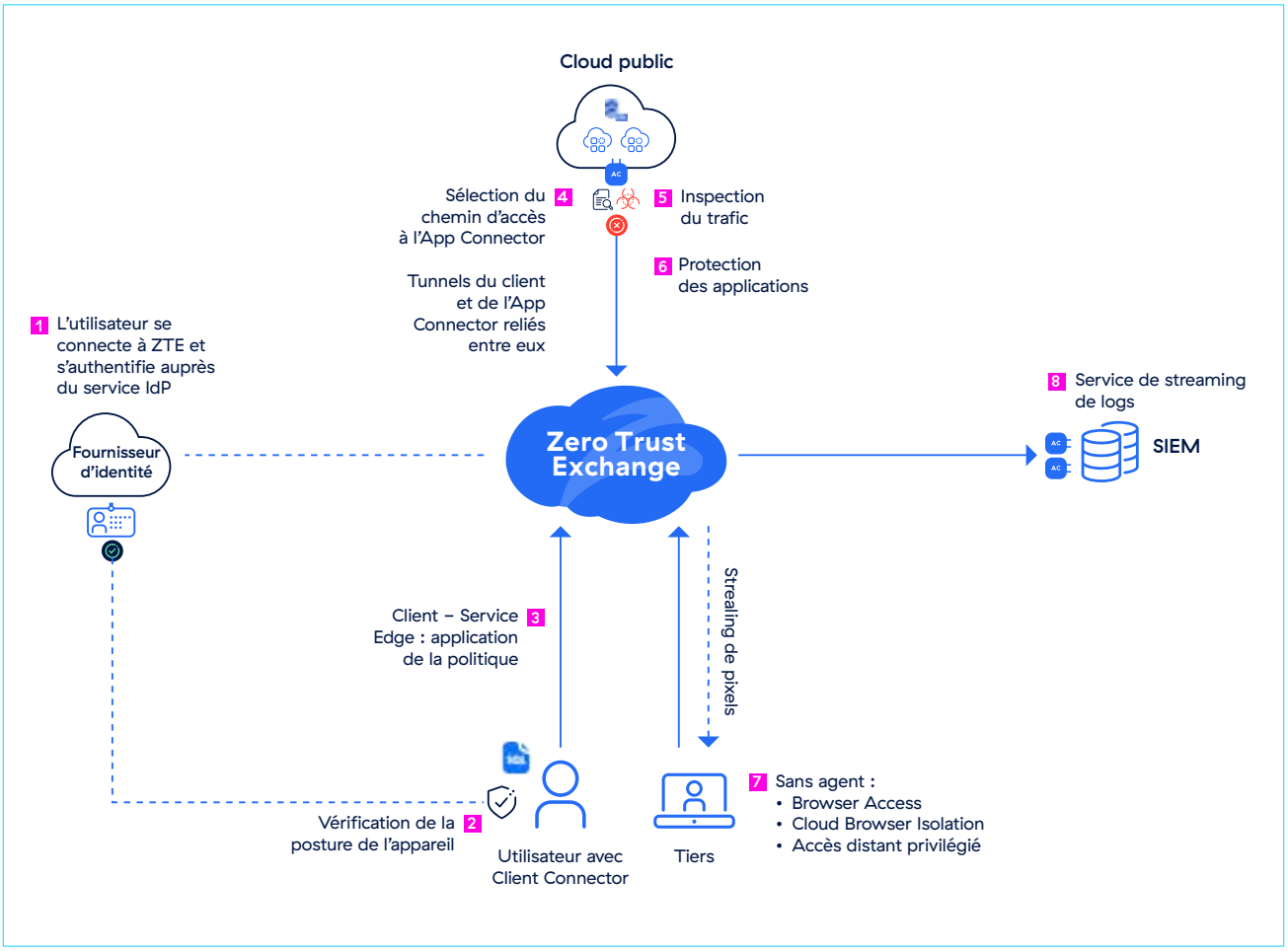
Alternative efficace à la VDI, la solution ZPA offre un accès sécurisé sans agent, basé sur un navigateur et conçu pour les appareils non gérés. Les utilisateurs bénéficient d'un accès rapide et transparent aux applications privées via le Service Edge le plus proche. L'architecture ZPA permet un accès 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 en restituant des pixels/images sur l'appareil de l'utilisateur final, au lieu d'un contenu réel : les données présentes au sein des applications demeurent ainsi sécurisées. ZPA permet aux administrateurs de créer des politiques d'isolation qui définissent la manière dont un utilisateur peut interagir dans un environnement cloisonné.

Microsegmentation (segmentation utilisateur–application)
Les solutions d'accès à distance comme les VPN offrent un accès complet au réseau, et exposent donc les adresses IP et les applications sur Internet. Les VPN étendent le réseau interne aux appareils distants et, de par leur conception, nécessitent du trafic entrant, créant ainsi une surface d'attaque publique. Sans une segmentation réseau adéquate, une vulnérabilité dans un segment peut compromettre l'ensemble du réseau de l'entreprise. Cependant, la mise en œuvre de la segmentation requiert des règles de pare–feu complexes, difficiles à maintenir, qui perturbent souvent les applications et peuvent compliquer l'accès pour les utilisateurs de VPN. Au sein des grandes entreprises, cela implique souvent une haute disponibilité, un routage complexe et des liaisons privées coûteuses.

La segmentation autonome utilisateur–application de Zscaler fournit une segmentation utilisateur–application précise, en faisant une solution robuste pour un déploiement de politiques cohérentes à grande échelle et l'élimination du déplacement latéral des menaces. Elle automatise l'intégralité du cycle de vie de la segmentation en visualisant chaque application depuis la phase de découverte, en procédant à une segmentation plus rapide grâce à des recommandations basées sur l'IA et en renforçant votre posture de sécurité grâce à des informations en temps réel.

©2025 Zscaler, Inc. Tous droits réservés.

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 le 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.

©2025 Zscaler, Inc. Tous droits réservés.

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

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 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 autonome utilisateur-application	Automatisez l'intégralité du cycle de vie de la segmentation en visualisant chaque application depuis la phase de découverte, en procédant à une segmentation plus rapide grâce à des recommandations basées sur l'IA et en renforçant votre posture de sécurité grâce à des informations en temps réel. Optimisée par des modèles d'apprentissage automatique continuellement entraînés sur des millions de signaux clients et sur vos propres profils d'accès uniques aux applications, la segmentation autonome utilisateur-application peut vous aider à éliminer les déplacements latéraux des menaces, à accélérer votre transition vers une approche ZTNA, et à simplifier et à faire évoluer les opérations Zero Trust.
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.
Protection des données et contre les menaces	Maîtrisez le risque de menaces grâce à une inspection complète du contenu. Repérez et contrôlez les données sensibles au travers de la connexion de l'utilisateur vers l'application.
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).
Accès sécurisé aux applications S2C existantes	Activez cette fonctionnalité pour sécuriser l'accès aux applications existantes connectées au réseau telles que les applications VoIP, Follow Me Printer et serveur-client.
Accès aux applications B2B	Activez l'accès bidirectionnel sécurisé aux applications et aux workloads hébergés sur le réseau (extranet) de votre partenaire commercial.

©2025 Zscaler, Inc. Tous droits réservés.

Accès 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 offre aux sous-traitants et aux utilisateurs BYOD un accès fluide aux applications depuis n'importe quel appareil et navigateur Web.
ZTNA au bureau	Mettez en œuvre la solution ZTNA pour les utilisateurs au bureau utilisant les ZPA Private Service Edges, garantissant ainsi un accès rapide et transparent aux applications. 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 ininterrompu aux applications critiques, même en cas d'événement catastrophique, grâce à une solution de continuité d'activité hébergée ou entièrement gérée par le client.

Avantages

Réduire la surface d'attaque
En éliminant les VPN vulnérables et en rendant les applications invisibles sur Internet, les utilisateurs non autorisés ne peuvent pas les trouver et les attaquer. ZPA crée un segment unique entre un utilisateur autorisé et une application privée spécifique, bloquant toute connectivité entrante et n'autorisant que les connexions sortantes via des microtunnels chiffrés vers les appareils des utilisateurs. Les administrateurs peuvent détecter et isoler automatiquement les applications, services et workloads malveillants grâce à la découverte d'applications, réduisant ainsi davantage la surface d'attaque.

Éliminer les déplacements latéraux
La connectivité basée sur le principe du moindre privilège garantit que l'accès aux applications est accordé individuellement à un utilisateur autorisé à accéder à des applications spécifiques, et non à l'ensemble du réseau. Ainsi, les déplacements latéraux entre applications ou sur le réseau sont impossibles. Comme ZPA ne repose pas sur les adresses IP, il n'est plus nécessaire de configurer ni de gérer une segmentation réseau complexe, des listes de contrôle d'accès (ACL), des règles de pare-feu ou des traductions d'adresses réseau.

Bloquer les utilisateurs compromis, les menaces internes et les attaques sophistiquées
Grâce à ses fonctionnalités intégrées d'inspection inline et de DLP, ZPA minimise les risques liés aux utilisateurs compromis et aux attaques actives. ZPA bloque automatiquement les attaques provenant du Web et offre une couverture complète des techniques les plus courantes, notamment le Top 10 de l'OWASP.

ZPA assure également une prise en charge complète des signatures personnalisées pour une application immédiate des correctifs virtuels contre les vulnérabilités de type « zero-day ». ZPA minimise les risques liés aux tiers et aux appareils personnels (BYOD) grâce à un accès totalement isolé aux applications, protégeant ainsi les données sensibles des appareils non gérés grâce à l'isolation du navigateur cloud intégrée.

Offrir une expérience utilisateur exceptionnelle
Une connectivité rapide et constante, qui ne nécessite pas de connexion et de déconnexion d'un client VPN, permet aux utilisateurs distants de bénéficier d'un accès plus sécurisé et plus efficace. Les prestataires, fournisseurs et partenaires tiers profitent d'un accès fluide depuis n'importe quel appareil et navigateur Web, sans installation de client. Les utilisateurs s'inscrivent avec leurs identifiants SSO existants (Azure AD, Okta, Ping, etc.). De plus, les administrateurs peuvent optimiser la productivité des utilisateurs en détectant et en résolvant de manière proactive les problèmes de performances liés aux difficultés d'accès aux applications privées, aux interruptions de réseau ou à la congestion du réseau.

Bénéficier d'une plateforme unifiée pour un accès sécurisé aux applications, aux workloads et aux appareils
Étendez le modèle Zero Trust aux applications privées et aux appareils OT/IT afin de simplifier et d'intégrer de multiples outils d'accès à distance disparates. En unifiant les politiques de sécurité et d'accès, vous êtes en mesure de stopper les violations et de réduire la complexité opérationnelle.

©2025 Zscaler, Inc. Tous droits réservés.

Zscaler Private Access (ZPA) : plusieurs options pour démarrer

	Plateforme Zscaler Essentials (ZS-ESS-PLATFORM)	Plateforme sans client ZPA (ZPA-CLIENTLESS-PLATFORM)	Plateforme Zscaler Private Access (ZS-ZPA-PLATFORM)	Plateforme Zscaler (ZS-PLATFORM)
Services de la plateforme d'accès privé				
Contrôle d'accès granulaire par utilisateur, groupe et ports	✓ 1 utilisateur pour 20 utilisateurs abonnés (min : 500 utilisateurs abonnés)	✓	✓	✓
Service de streaming de logs				
Surveillance permanente de l'intégrité de toutes les applications				
Ancrage IP source : redirection sélective du trafic de l'application vers les serveurs de destination appropriés				
App Connector : machine virtuelle légère permettant les connexions sortantes à Zscaler ZTE	Autant que nécessaire, jusqu'à la capacité maximale du système	Autant que nécessaire, jusqu'à la capacité maximale du système	Autant que nécessaire, jusqu'à la capacité maximale du système	Autant que nécessaire, jusqu'à la capacité maximale du système
ZPA Private Service Edge : ZTNA pour les utilisateurs distants et au bureau	–	–		
ZPA pour les applications traditionnelles (VoIP, S2C, etc.)	–	–	Services Edges VPN complémentaires (minimum : 50 utilisateurs)	Services Edges VPN complémentaires (minimum : 50 utilisateurs)
ZPA Business Continuity Cloud	–	–	Module complémentaire (minimum : 500 utilisateurs)	Module complémentaire (minimum : 500 utilisateurs)
Segmentation utilisateur vers application	10 segments d'applications	20 segments d'applications	20 segments d'applications	20 segments d'applications
Segmentation autonome utilisateur-application et renseignements	–	–	**Module complémentaire**	**Module complémentaire**
Accès par des tiers			Module complémentaire (minimum : 500 utilisateurs)	Module complémentaire (minimum : 500 utilisateurs)
Accès basé sur un navigateur pour les appareils non gérés	–	✓	✓ Possibilité d'acheter des licences supplémentaires pour utilisateurs invités avec ZPA-CLIENTLESS-PLATFORM	✓ Possibilité d'acheter des licences supplémentaires pour utilisateurs invités avec ZPA-CLIENTLESS-PLATFORM
Portail utilisateur : portail Web unique permettant aux utilisateurs d'accéder aux applications autorisées et aux consoles privilégiées				
Norme d'accès distant privilégié Privileged Remote Access : PRA sans client vers les systèmes OT (jusqu'à 10) (RDP/SSH/VNC)				
Browser Isolation pour les applications privées et SaaS		**Module complémentaire**	**Module complémentaire**	**Module complémentaire**
Monitoring de l'expérience numérique	–	–	✓	✓
Norme ZDX : visibilité sur les données télémétriques des utilisateurs, de la connectivité et des applications				
Protection des applications privées et des données	**Module complémentaire**			
Protection des données pour les applications privées, gestion des incidents et classification des données		–	**Module complémentaire**	✓
Zscaler Deception : leurres intégrés pour détecter les utilisateurs compromis		–	✓ (minimum : 500 utilisateurs)	✓ (minimum : 500 utilisateurs)
AppProtection pour protéger les applications privées contre les menaces du Top 10 de l'OWASP et inspection du trafic Web		**Module complémentaire**	**Module complémentaire**	**Module complémentaire**

©2025 Zscaler, Inc. Tous droits réservés.

Principaux facteurs de différenciation

Première solution ZTNA optimisée par l'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 et accéder aux applications :** prévenez le piratage applicatif, le piratage 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.
- **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 sécurisé via navigateur :** exploitez l'accès basé sur un navigateur pour les tiers grâce à une solution DLP intégrée.
- **Élimination des déplacements latéraux grâce à la segmentation autonome utilisateur–application :** cette solution offre une segmentation utilisateur–application précise, visualise les accès et affine les politiques grâce à l'apprentissage automatique afin de minimiser la surface d'attaque et de prévenir les menaces latérales.
- **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

Zscaler a été désigné parmi les leaders 2025 du Gartner® Magic Quadrant™ pour le Security Service Edge (SSE) **

En savoir plus

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

Gartner n'approuve aucun fournisseur, produit ou service décrit dans ses publications de recherche, et ne conseille pas aux utilisateurs de technologie de sélectionner uniquement les fournisseurs ayant les cotes les plus élevées ou toute autre désignation. 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. Gartner décline toutes les garanties, exprimées ou implicites, à l'égard de cette recherche, y compris toute garantie de valeur marchande ou d'aptitude à un but particulier.

GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États–Unis et dans le monde, et MAGIC QUADRANT est une marque déposée de Gartner, Inc. et/ou de ses filiales. Ces marques sont utilisées dans ce document avec l'autorisation de leurs détenteurs. 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. En redirigeant automatiquement le trafic utilisateur vers le serveur Zscaler Service Edge le plus proche, ce service garantit l'application des politiques de sécurité et d'accès sur tous les appareils, sites et applications.

Accès sans client Zscaler
Les utilisateurs peuvent se connecter en toute sécurité aux applications, aux workloads et aux appareils OT via un accès intégré basé sur un navigateur (Web, RDP, SSH, VNC) ou via Zscaler Browser Isolation pour un accès sans client sur les appareils non gérés.

ZPA App Connector
Les App Connectors sont des machines virtuelles légères qui se placent devant les applications privées déployées dans le data center ou le cloud public, négociant une connectivité de sécurité entre un utilisateur autorisé et une application nommée grâce à une connexion sortante qui n'expose pas les applications à Internet.

ZPA Network Connector
Les Network Connectors sont des machines virtuelles légères déployées devant les serveurs d'applications du data center et qui se connectent aux Services Edges VPN de Zscaler Cloud via un tunnel sortant.

ZPA Service Edges
Les Service Edges appliquent les politiques de sécurité et d'accès, en établissant la connexion sortante entre un utilisateur autorisé (via Client Connector et Browser Access) et une application privée spécifique (via App Connector). La plupart de nos clients utilisent nos Public Service Edges, hébergés dans plus de 160 points de présence (PoP) à travers le monde et capables de gérer des millions d'utilisateurs simultanés pour les plus grandes organisations internationales. Les Private Service Edges, gérés par Zscaler, peuvent également être hébergés sur site afin d'offrir aux utilisateurs locaux un accès direct à leurs applications sans quitter leur réseau local. Ils garantissent ainsi la continuité d'activité grâce à un accès ininterrompu aux applications critiques, même en cas d'événement catastrophique.

ZPA Private Cloud Controller
Les Private Cloud Controllers sont des contrôleurs par entité que les utilisateurs, les ZPA Private Service Edges et les App Connectors peuvent utiliser lorsque Zscaler Cloud n'est pas disponible ou accessible.

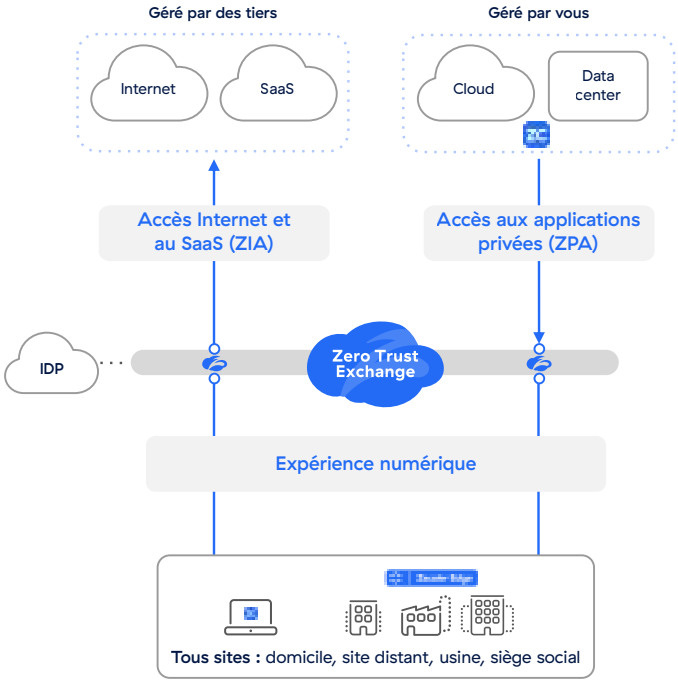
ZPA est une composante de la solution globale Zero Trust Exchange

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.

©2025 Zscaler, Inc. Tous droits réservés.

Zscaler sécurise le personnel : accès sécurisé, rapide et fiable aux applications,

déployable en quelques jours pour une cybersécurité et une expérience utilisateur améliorées.



Protection supérieure contre les menaces et des données,
expérience utilisateur optimale, réduction de la complexité et des coûts

Spécifications techniques

Composants Zscaler	Plateformes et systèmes compatibles	
Client Connector	iOS 17 ou versions ultérieures	ChromeOS version 137 ou versions ultérieures
	Android 9 ou versions ultérieures	Linux
	Windows 8 ou versions ultérieures	macOS 14 ou versions ultérieures
Accès sans client	Navigateurs Web modernes : (compatibles HTML5), Chrome, Edge, Firefox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Private Service Edge	AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat	
Private Cloud Controller	AWS, Microsoft Azure, VMware, Red Hat	

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

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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