Pulse Secure®

Pulse Zero Trust Access

Service Secure Access sur le Cloud pour les environnements informatiques hybrides

Points Forts

Visibilité holistique, conformité et application pour les utilisateurs, les appareils, les applications et les passerelles

Accès direct et fiable de l'appareil à l'application avec support Dark Cloud en utilisant l'architecture Software Defined Perimeter

Accès fluide et sécurisé aux applications d'entreprise dans le Datacenter et sur le cloud

Subscription licensing par utilisateur flexible et gestion du cycle de vie pour les déploiements à l'échelle de l'entreprise

Valeur pour le Client

Zero Trust Access intégral avec surface d'attaque réduite

Visibilité depuis un écran unique (« single pane of glass »), gestion de la stratégie et analyse

Meilleure gouvernance et plus grande conformité

Réduction du coût total de possession et augmentation de la productivité

Solution

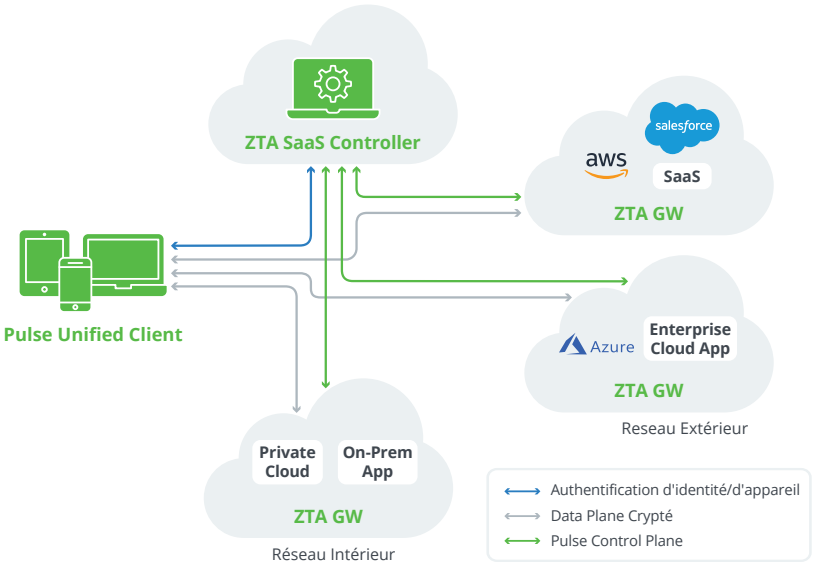
Le service PZTA basé sur le cloud (aligné sur l'architecture de réseau Zero Trust) permet un accès défini par logiciel, une authentification continue et un support Dark Cloud. Il se compose de ZTA Controller qui est hébergé et géré par Pulse Secure, de ZTA Gateway qui peut être déployée dans le cloud ou sur site par le client, et de ZTA Client installé sur les appareils des utilisateurs.

- Zero Trust Access en tant que service
- Visibilité et application end-to-end
- Client unifié : Windows, macOS, iOS et Android
- Intégration de l'écosystème au sens large
- Analyses et rapports complets
- Déploiement rapide, licensing flexibles

Zero Trust Access pour un monde hyper-connecté

La transformation numérique a déclenché une nouvelle ère d'hyper-connectivité entre les utilisateurs, les appareils, les applications et les infrastructures. Les entreprises doivent permettre un accès sécurisé, protéger les utilisateurs et les applications, et gérer les risques en matière de cybersécurité sur des réseaux de plus en plus distribués, avec peu ou pas de frontières. Aujourd'hui, les points d'extrémité, les applications et les services fonctionnent en dehors du périmètre traditionnel, ce qui met davantage en avant les approches Zero Trust. Les entreprises recherchent des solutions d'accès sécurisé intégrales qui répondent à ces nouveaux défis, plutôt que de continuer à ajouter de multiples produits ponctuels pour combler les lacunes. Cette approche fragmentaire est lourde et coûteuse à gérer, introduit des problèmes de sécurité supplémentaires et ajoute à un large éventail d'inefficacités et de risques.

Pulse Zero Trust Access (PZTA) relève le défi de l'accès sécurisé à l'ère de l'hyper connectivité en fournissant un accès direct et fiable aux applications et aux ressources dans des environnements informatiques hybrides. Il offre une visibilité holistique, une analyse intégrale, la conformité des points d'extrémité et une application adaptative. Grâce à l'authentification continue des entités et à l'intégration robuste de l'écosystème, PZTA propose un service d'accès qui offre une connectivité facile et protégée, une administration efficace et une flexibilité de déploiement pour répondre à vos besoins sur site ou dans le Cloud.



Pulse Secure®

Aperçu des cas d'utilisation

La plateforme PZTA (Pulse Zero Trust Access) de Pulse Secure permet à divers utilisateurs, où qu'ils se trouvent, d'accéder en toute sécurité à toutes les applications sur les clouds publics, privés et hybrides, ainsi qu'aux ressources des centres de données. Alors que les entreprises continuent d'évoluer avec une main-d'œuvre mobile et l'adoption de technologies informatiques hybrides, PZTA améliore la sécurité et la productivité, accroît la visibilité et améliore considérablement l'expérience des administrateurs et des utilisateurs dans le cadre d'une plateforme extensible Zero Trust.

Zero Trust Access pour les applications On-prem, SaaS et Hybrid Cloud

Pulse Zero Trust Access permet un accès sécurisé Zero Trust aux applications de votre entreprise dans le datacenter, le cloud privé et les clouds publics. ZTA Client offre une authentification continue de l'utilisateur et de l'appareil et un accès toujours protégé aux applications d'entreprise grâce à un canal de données crypté entre le ZTA Client sur l'appareil de l'utilisateur et la ZTA Gateway la plus proche de l'application. Les serveurs d'applications sont protégés et cachés, ce qui réduit les risques en matière de sécurité, ce qui est connu sous le nom de « support Dark Cloud ».

Défis	PULSE ZERO TRUST ACCESS
Difficile de gérer les ressources dans le cloud	Avec PZTA, la gestion et l'accès aux ressources dans le cloud fonctionnent exactement de la même manière que sur site, avec le même niveau de visibilité, de conformité, d'application et d'analyse. L'utilisateur n'accède jamais directement au serveur d'application. Lorsqu'une application est déplacée depuis un emplacement sur site vers le cloud, la prochaine fois que l'utilisateur tentera d'accéder à cette application, le ZTA Contrôlera le ZTA Client de l'utilisateur vers la ZTA Gateway la plus proche de cette application.
Maintenir le trafic des utilisateurs et des applications au sein du réseau de mon entreprise	PZTA sépare le flux de contrôle et le flux de données sur la base de l'architecture SDP. Tout le trafic des utilisateurs et des applications passe uniquement par la ZTA Gateway, qui est déployée dans le Virtual Private Cloud ou le datacenter du client, et le trafic de données ne passe jamais par le ZTA Controller.
Augmenter la productivité	Pour les administrateurs, le ZTA Controller permet de configurer de manière centralisée des stratégies intégrales Zero Trust Access qui lient les utilisateurs, les appareils, les passerelles et les applications, quel que soit le type d'application ou d'appareil, ou l'emplacement de l'utilisateur. Pour les utilisateurs finaux, quel que soit le type d'applications auxquelles ils essaient d'accéder ou le lieu depuis lequel ils y accèdent, le mécanisme d'accès reste le même. Cela simplifie, tout en l'unifiant, l'expérience des utilisateurs et des administrateurs, ce qui augmente la productivité de l'entreprise.
Assurer la sécurité d'accès lors de l'intégration des entreprises acquises	Au lieu de permettre un accès complet au réseau à différents endroits, PZTA permet aux administrateurs de spécifier quelles ressources seront partagées entre différents groupes d'utilisateurs à différents endroits en les ajoutant à la politique d'accès sécurisé centralisé. Si un niveau de séparation plus élevé est souhaité, les administrateurs peuvent choisir de configurer une passerelle distincte ou de mettre en place les différentes unités commerciales en tant qu'autres locataires dans une configuration partagée.

Visibilité, mise en œuvre et rapports de conformité

Pulse Zero Trust Access offre une visibilité centralisée de tous les utilisateurs se connectant à partir de n'importe lequel de leurs appareils, quel que soit leur emplacement, et de l'emplacement des applications et des ressources. Les administrateurs et les responsables de l'informatique et de la sécurité peuvent consulter en temps réel l'état et les tendances historiques à partir des différents tableaux de bord interactifs fournis dans le portail PZTA et recevoir des rapports prédéfinis et personnalisés à leur convenance.

Défis	SOLUTION PULSE ZERO TRUST ACCESS
Lacunes en matière de visibilité	PZTA offre une visibilité globale des utilisateurs, des appareils, des infrastructures et des applications. Tout accès est authentifié et autorisé par ZTA Controller. Toutes les activités d'accès sont saisies dans le tableau de bord Pulse ZTA et enregistrées à des fins de rapport et d'audit.
Il est nécessaire d'autoriser le programme BYOD mais cela pose un risque en matière de sécurité	Grâce à PZTA, les appareils BYOD peuvent bénéficier du même niveau d'accès Zero Trust que les appareils appartenant à une entreprise. Chaque fois que des utilisateurs tentent d'accéder à une application d'entreprise depuis un appareil personnel, le statut de conformité de l'appareil ainsi que d'autres contrôles de sécurité, tels que l'emplacement, l'heure de la journée, le comportement de l'utilisateur, seront évalués avant que l'accès ne soit accordé.
Garantir la conformité des accès des utilisateurs et des points d'extrémité	PZTA authentifie dynamiquement l'utilisateur, l'appareil et le profil de sécurité par rapport aux politiques d'accès granulaire avant et pendant la connexion. PZTA informera l'utilisateur de la violation ou pourra exécuter la restauration prédéfinie des points d'extrémité pour les utilisateurs qui se voient refuser l'accès ou qui n'ont le droit qu'à un accès réduit aux applications et aux ressources.

Détection et atténuation automatisées des anomalies

Ce qui est considéré comme sûr et normal varie d'une entreprise à l'autre. Pulse Zero Trust Access apprend et s'adapte en permanence en observant d'où les utilisateurs se connectent, quels appareils ils utilisent normalement et à quelles applications ils accèdent habituellement. Les administrateurs sont avertis lorsqu'il y a une anomalie par rapport au comportement normal des utilisateurs, et peuvent sélectionner une réponse prédéfinie ou une action d'atténuation suggérée à la volée.

Défis	SERVICE PULSE ZERO TRUST ACCESS
Détecter et prévenir le vol d'identifiants par des initiés malveillants dans le but de voler des données précieuses	Les défenses de périmètre traditionnelles rendent difficiles la détection et la localisation des vols d'identifiants commis par des initiés malveillants. PZTA peut alerter les administrateurs de la sécurité que l'employé en question utilise un appareil différent et se connecte depuis un autre endroit. Ensuite, l'administrateur peut soit prendre des mesures d'exécution prédéfinies, comme exiger une AMF, soit suspendre manuellement l'accès temporairement jusqu'à ce que la situation soit résolue.
Les administrateurs souhaitent restreindre l'accès lorsque les employés se rendent dans des lieux à haut risque	Ceci est facilement mis en œuvre avec PZTA. Lorsque l'emplacement de l'utilisateur change, la liste des applications accessibles est mise à jour dynamiquement. L'accès aux applications sensibles peut être temporairement supprimé lorsque l'employé voyage dans des endroits à haut risque ou lorsqu'il utilise des appareils qui ne répondent pas à toutes les exigences de conformité.

Analyse des comportements des utilisateurs

Chaque tentative d'accès d'un utilisateur à une application est envoyée au ZTA Controller pour authentification et autorisation. Dans ce processus, PZTA applique des informations détaillées sur l'utilisation et le comportement pour améliorer l'expérience de l'utilisateur, accroître la visibilité et prendre des mesures préventives pour minimiser les risques de sécurité potentiels.

Défis	SOLUTION PULSE ZERO TRUST ACCESS
Mesurer les facteurs de risque des salariés	PZTA attribue un « niveau de risque » à chaque utilisateur en fonction de son comportement et de son utilisation actuels et passés. Cette note est évaluée de manière dynamique et reflète à la fois l'action de l'utilisateur et le facteur de risque potentiel. Sur la base de cette note, les administrateurs peuvent adopter une approche différenciée vis-à-vis des utilisateurs.
Le CIO souhaite connaître le taux d'utilisation des ressources déployées	PZTA peut fournir des tendances d'utilisation complètes et des rapports d'utilisation détaillés pour aider le CIO et les cadres supérieurs à comprendre quelles sont les applications les plus utilisées. La solution prend en charge diverses requêtes en temps réel en utilisant l'interface graphique d'analyse ZTA pour zoomer sur un groupe d'utilisateurs, un lieu, des ressources, des passerelles ou même des utilisateurs individuels. Ces informations peuvent ensuite être appliquées à la planification des ressources et du budget.
L'administrateur veut savoir où déployer les ressources du réseau	À partir du rapport d'utilisation de PZTA, les administrateurs peuvent obtenir des informations détaillées sur le lieu physique où se rendent les utilisateurs et sur les ZTA Gateways auxquelles ils accèdent (jusqu'au niveau du groupe d'utilisateurs ou de l'utilisateur individuel). L'administrateur peut utiliser ces informations pour adapter au mieux la bande passante afin d'optimiser l'expérience de l'utilisateur et de réduire la charge opérationnelle.
Rendre les employés plus productifs	En obtenant une vue à 360 degrés sur la manière, le lieu et le moment où les utilisateurs accèdent aux ressources et aux applications, les équipes informatiques peuvent définir les meilleures pratiques telles que le moment de programmer la maintenance afin de minimiser les perturbations, et la priorité à accorder à la mise à niveau des appareils et des applications, etc. Cela permettra d'améliorer encore l'expérience et la productivité des utilisateurs.

Zero Trust as a Service

Pulse ZTA est un service fourni par Pulse Secure. Le contrôleur ZTA est hébergé et géré globalement par Pulse Secure.

Disponible sur place et dans le cloud

Les ZTA Gateways peuvent être déployées dans le Virtual Private Cloud du client dans le cloud public ou dans un environnement privé.

SDP et Dark Cloud

Adhésion à l'architecture SDP avec des applications invisibles accessibles uniquement après que l'utilisateur et le dispositif ont été authentifiés et autorisés.

Intégration poussée

Un vaste ensemble d'API permet une intégration facile avec la solution du partenaire de l'écosystème.

Architecture des micro-services

Microservices conteneurisés composés de petits processus indépendants pour une évolutivité et des performances maximales.

CARACTÉRISTIQUE	AVANTAGE
Politique d'accès end-to-end	Pour chaque ressource ou groupe de ressources, les administrateurs peuvent définir un ensemble de politiques d'accès end-to-end. Cela élimine la distinction entre les utilisateurs distants et ceux qui se trouvent sur le réseau de l'entreprise, le BYOD et les appareils appartenant à l'entreprise, et la question de savoir si les applications ou les ressources résident dans le Datacenter ou dans le cloud.
Dark Cloud	Le ZTA Client demandera toujours l'accès par l'intermédiaire de ZTA Controller sans savoir où résident le serveur d'application et les ressources protégées. Une fois l'accès accordé, la passerelle sans tête établit un tunnel de données crypté vers le client pour accéder à l'application. Cette fonctionnalité Dark Cloud réduit drastiquement la surface d'attaque.
Visibilité centralisée et conformité	Fournit aux administrateurs un écran unique pour une visibilité globale et des rapports de conformité sur les utilisateurs, les appareils, les applications et l'infrastructure pour tous les groupes d'utilisateurs, les emplacements, les types d'appareils, les ressources sur site et dans le cloud.
Séparation du flux de contrôle et du flux de données	Le plan de contrôle est limité à l'authentification et à l'autorisation entre le ZTA Client et le ZTA Controller. Le trafic des utilisateurs et des applications est envoyé directement entre l'utilisateur et la passerelle désignée après avoir été autorisé par le contrôleur. Cette séparation réduit le risque de perte de données et optimise l'expérience de l'utilisateur.
SSO adaptatif	Grâce à SAML 2.0, PZTA s'intègre aux solutions et services d'identité populaires pour fournir un SSO aux applications SaaS et tierces prises en charge. Les administrateurs ont également la possibilité d'activer le SSO adaptatif en fonction de profils de sécurité supplémentaires tels que le lieu, l'heure de la journée, le comportement des utilisateurs, etc.
Conformité du point d'extrémité	PZTA garantit la conformité des accès et réduit les menaces posées à la sécurité des points d'extrémité telles que les logiciels malveillants en authentifiant la position de sécurité de l'utilisateur et de son appareil par rapport aux politiques d'accès granulaire avant d'accorder l'accès. Les contrôles de conformité de la sécurité des points d'extrémité réduisent la possibilité d'introduire des logiciels malveillants ou d'autres menaces à la sécurité des appareils.
Analyse des comportements des utilisateurs	Les comportements des utilisateurs et les informations sur l'utilisation sont dynamiques et en constante évolution. PZTA exploite les données analytiques pour réduire les risques de sécurité, détecter les anomalies, optimiser l'expérience des utilisateurs et s'adapter aux besoins d'une main-d'œuvre de plus en plus mobile.
Protection des données et souveraineté	Toutes les données relatives aux utilisateurs et aux applications sont entièrement cryptées entre le client et la passerelle. Les données des applications ne sont jamais partagées dans le Data Plane hébergé par Pulse Secure.
GW On-prem et Hybrid Cloud	Les passerelles peuvent être déployées dans le cloud public, le cloud privé ou les centres de données des clients. Cette flexibilité informatique hybride permet aux entreprises de tirer parti des conditions de trafic et de bande passante les plus optimales pour réduire la latence et maintenir autant que possible les données dans le domaine de confiance.

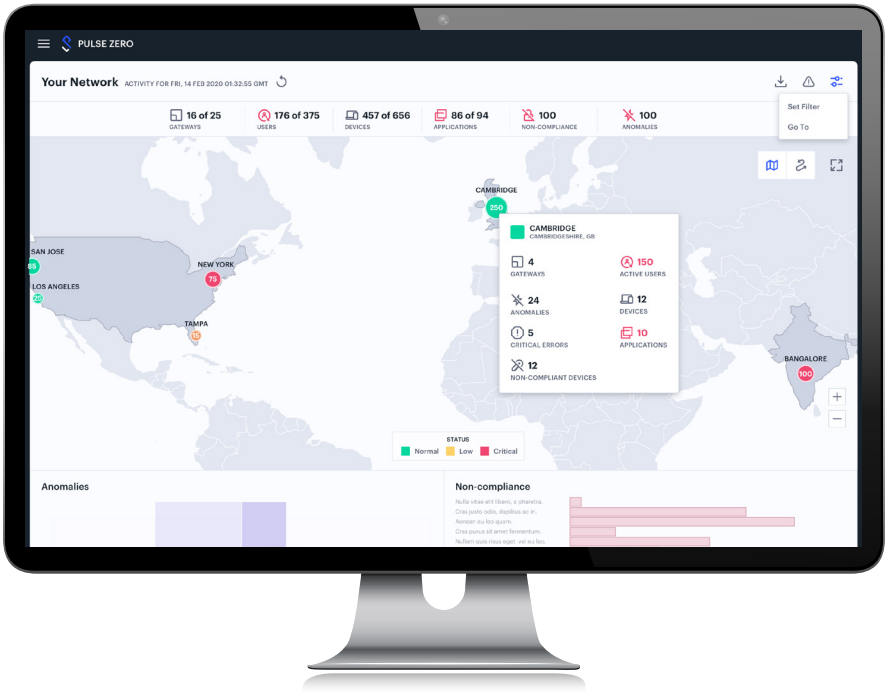
Pulse Secure®

Comment fonctionne Pulse Zero Trust Access

PZTA est basée sur l'architecture SDP qui adopte une approche Zero Trust pour l'accès sécurisé. Il se compose du ZTA Controller qui est hébergé et géré par Pulse Secure, de la ZTA Gateway qui peut être déployée dans un Virtual Private Cloud (cloud public AWS/Azure cloud, cloud privé hébergé ou sur site) et du ZTA Client qui est le même client unifié que Pulse VPN/NAC Client.

Chaque fois qu'un utilisateur souhaite accéder à une application ou une ressource protégée depuis son appareil, le ZTA Client ouvre une session avec le ZTA Controller pour demander l'accès. Le ZTA Controller, après avoir validé les informations d'identification de l'utilisateur, la conformité de l'appareil et les autres mesures de sécurité (telles que l'emplacement ou le comportement), autorisera la ZTA Gateway la plus proche de l'application ou de la ressource demandée, permettant ainsi la communication de données cryptées avec le ZTA Client. Tout au long de la communication, le profil de sécurité des points d'extrémité est continuellement évalué pour s'assurer que la session est sécurisée.

Ce flux d'accès Zero Trust est le même, que l'utilisateur se trouve à l'intérieur ou à l'extérieur du réseau d'entreprise, qu'il utilise un appareil appartenant à l'entreprise ou un appareil personnel (BYOD), ou qu'il accède à une application SaaS ou à une ressource sur site.



Le portail de l'administrateur PZTA offre une vue d'ensemble des utilisateurs, des lieux, des anomalies, etc.

Principaux avantages de Pulse Zero Trust Access

Expérience utilisateur simplifiée

Le ZTA Client est le même client unifié Pulse VPN/NAC éprouvé qui est utilisé par plus de 20 millions de clients Pulse aujourd'hui. Il prend en charge les systèmes d'exploitation courants tels que Windows, macOS, iOS et Android, et permet l'authentification à facteurs multiples (AFM), l'authentification unique (SSO) et les services VPN afin de simplifier l'expérience des utilisateurs lorsque les organisations mettent en œuvre PZTA ou migrent de VPN vers PZTA.

Politique d'accès sécurisé end-to-end

Avec PZTA, les administrateurs publient simplement une politique d'accès sécurisé end-to-end qui définit quel utilisateur/groupe d'utilisateurs peut accéder à l'application/la ressource. Que les utilisateurs soient à distance ou sur site, qu'ils utilisent leurs propres appareils ou des appareils appartenant à l'entreprise, ou qu'ils accèdent à des applications dans le datacenter ou dans le cloud, chaque fois que l'utilisateur choisit d'accéder à une ressource à partir de l'appareil du point d'extrémité, il sera authentifié et autorisé sur la base non seulement des références de l'utilisateur et de la conformité de l'appareil, mais aussi d'autres profils de sécurité telles que l'emplacement, le comportement de l'utilisateur, etc. C'est l'accès Zero Trust au travail.

Réduction de la surfacee

Tirant parti de l'architecture SDP (Software Defined Perimeter), le service PZTA offre une surface d'attaque beaucoup plus réduite. L'appareil de l'utilisateur final ne se connecte jamais directement à l'application ou aux ressources ; il ne peut lancer toutes les demandes d'accès que par une connexion sécurisée avec le ZTA Controller. Le ZTA Controller tient à jour la liste et la correspondance entre la passerelle et les applications protégées. Ce n'est qu'après une authentification et une autorisation réussies que le ZTA Client pourra établir un tunnel de données crypté avec la ZTA Gateway correspondante. Une fois l'accès terminé, le tunnel de données est fermé. Lorsque l'utilisateur final souhaite rétablir la connexion, il devra à nouveau être authentifié et autorisé par le ZTA Controller. Cela réduit considérablement la surface d'attaque et les vulnérabilités potentielles en protégeant la ZTA Gateway et les serveurs d'applications contre les hôtes et les appareils non fiables.

Visibilité holistique et confirmité

Pulse ZTA offre aux CIO, CSO et administrateurs informatiques un écran unique pour la visibilité et la conformité. À partir du tableau de bord PZTA, les administrateurs ont une vue globale des utilisateurs, des appareils, des passerelles, des applications et de leur statut, ainsi que des statistiques générales. D'un simple clic, les administrateurs peuvent zoomer sur n'importe quelle zone d'intérêt pour voir ce qui a causé une alerte ou un manquement. Les administrateurs, superviseurs et cadres peuvent commencer leur journée de travail en parcourant un rapport prédéfini avec un filtre et un format personnalisés à partir du tableau de bord PZTA.

Analyse des comportements des utilisateurs

Dans la mesure où tous les accès passent par le ZTA Controller, une multitude d'informations sur le comportement des utilisateurs, tant au niveau macro que micro, peuvent être collectées et apprises automatiquement. Il existe de nombreuses applications pratiques de l'analyse approfondie du comportement, comme la détection automatique d'anomalies lorsqu'il y a un changement de comportement par rapport à la routine normale, ou lorsqu'il y a une suspicion basée sur l'emplacement, l'appareil ou les activités. En fait, PZTA attribuera un « niveau de risque » unique à chaque utilisateur en fonction de son mode d'utilisation et de ses antécédents. Les administrateurs peuvent restreindre certaines applications en fonction des indices de menace ou limiter l'accès en fonction de l'emplacement, du type d'appareil et du profil de sécurité.

Users
- Employés
- Entrepreneurs
- Guests

Devices
- Mobiles
- PC/Mac
- Entreprise
- Personnels

Applications
- SaaS & Cloud Natif
- Sur Site
- 3rd Party
- Personnalisées

Infrastructure
- Sur site
- Cloud

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure, LLC offre des solutions d'accès sécurisé définies par logiciel qui fournissent de la visibilité et une connectivité aisée et protégée entre les utilisateurs, les périphériques, les choses et les services. L'entreprise propose des suites et une plateforme SaaS qui intègrent de manière unique le contrôle d'accès au cloud, au mobile, aux applications et au réseau pour un système d'information hybride. Plus de 24 000 entreprises et fournisseurs de services font confiance à Pulse Secure pour permettre à leurs équipes mobiles d'accéder en toute sécurité aux applications et aux informations dans le datacenter et le cloud tout en veillant à respecter les normes commerciales. Pour en savoir plus : www.pulsesecure.net.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

VERSION 07272020