Ivanti Neurons for Zero Trust Access

Accès sécurisé pour l'Everywhere Workplace

Grâce à Ivanti Neurons for Zero Trust Access (nZTA), une connexion sécurisée est établie entre le périphérique et les applications Web sur site et dans le Cloud pour renforcer la sécurité, la productivité et la conformité, tout en améliorant de façon significative l'administration et l'expérience utilisateur.

L'accès Zero Trust partout

Mettez en place une authentification permanente des utilisateurs et des périphériques ainsi qu'un accès sécurisé toujours actif aux applications métier, qu'elles se trouvent sur site, dans le centre de données ou dans les Clouds privés et publics.

Authentifiez et autorisez automatiquement les utilisateurs, les périphériques et la connexion aux applications en fonction de contraintes granulaires flexibles pour garantir un contrôle adaptatif, une microsegmentation et une réduction de la surface d'attaque.

Une amélioration de la visibilité et des analyses

Consultez l'état en temps réel et les tendances historiques, et exploitez les informations d'utilisateur et de comportement apprises par nZTA, notamment l'emplacement depuis lequel l'utilisateur se connecte, les périphériques qu'il utilise le plus souvent et ceux auxquels il accède en général afin de réagir proactivement et de limiter les risques de sécurité.

Une amélioration de la productivité et de l'agilité d'entreprise

Implémentez en toute sécurité de nouveaux services et appliquez plus rapidement des changements de stratégies granulaires. nZTA évite les problèmes liés au fait d'« épingler » le trafic et améliore l'expérience utilisateur grâce à un accès direct aux applis. Et comme vous utilisez un seul client pour l'accès sur site, l'accès à distance et l'accès direct au Cloud, vous accélérez vos efforts de Zero Trust en toute tranquillité.

Le choix et la flexibilité : des stratégies granulaires et un positionnement des passerelles

Placez des passerelles où vous le souhaitez. Prenez en charge jusqu'à cinq périphériques pour chaque utilisateur nommé et ajoutez le nombre de passerelles de votre choix pour garantir une sécurité optimale dans votre environnement.

Aucune congestion du trafic réseau, pas de frais de données

Avec nZTA, vos données ne passent jamais par notre plateforme, ce qui réduit les besoins en bande passante d'entreprise et élimine les frais de données liés aux SWG et aux CASB.

L'intégration au VPN

Stimulez la productivité et évitez les retards d'implémentation des infrastructures ou des logiciels en intégrant nZTA à un VPN existant. Proposez

facilement et rapidement un accès sécurisé aux nouvelles applis, intégrez de nouvelles unités commerciales ou facilitez les opérations de fusions et acquisitions.

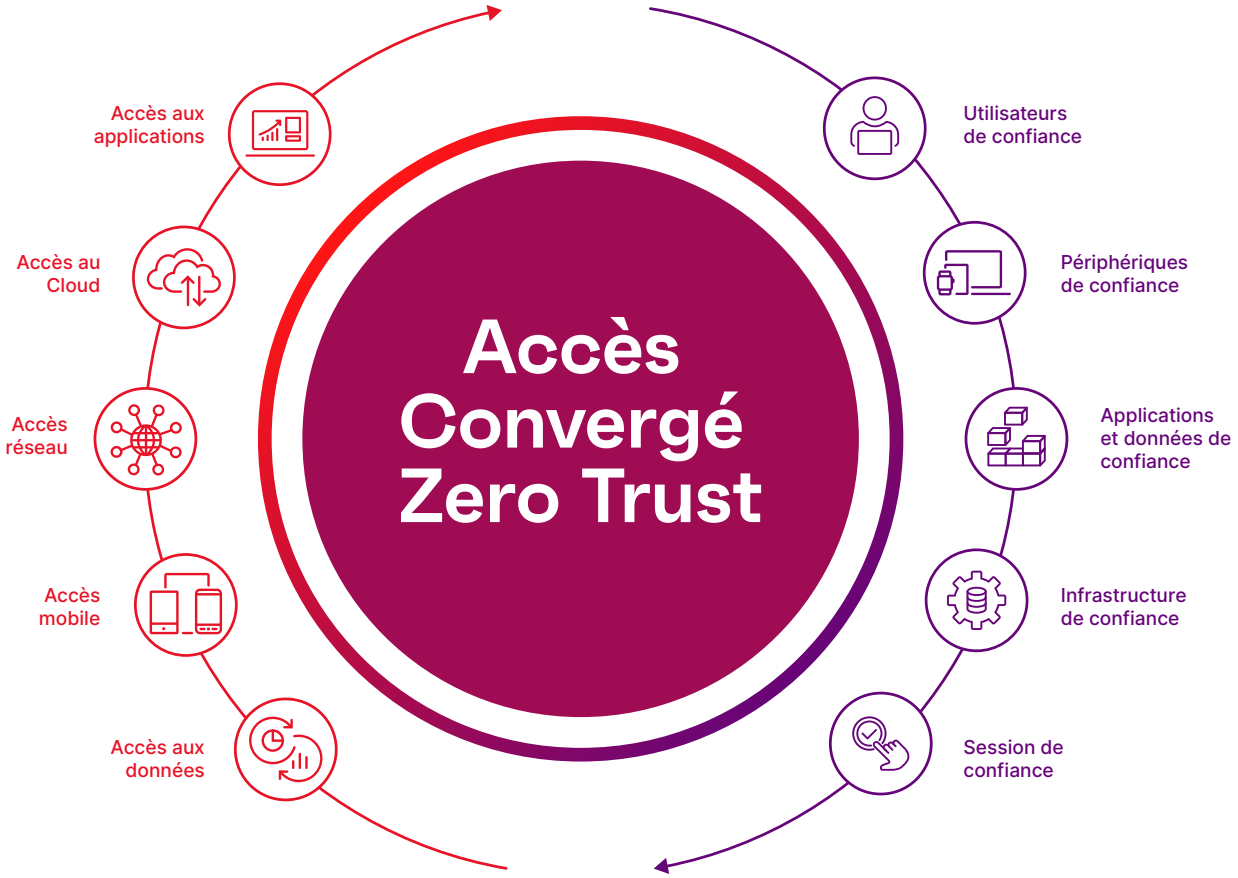
Le fonctionnement en détail

nZTA est une solution d'accès réseau Zero Trust en SaaS, conçue pour fonctionner avec votre solution de VPN ou dans les entreprises où tout se fait dans le Cloud.

nZTA authentifie et autorise les utilisateurs en vérifiant leur identité et la sécurité de leur périphérique avant d'ouvrir une session. nZTA gère chaque demande d'accès et chaque session via une stratégie déployée, gérée de façon centralisée et complétée par des fonctions UEBA (analyse du comportement des utilisateurs et des entités) prédéfinies, qui surveillent et évaluent les attributs de chaque session. Les scores de risque propriétaires permettent d'identifier les activités non conformes, malveillantes ou anormales, ce qui garantit une réaction plus rapide aux menaces.

Les passerelles nZTA sont déployées de manière flexible là où vous le souhaitez, soit sur site soit à côté de vos applis dans le Cloud. Cette proximité optimise l'expérience utilisateur, réduit la latence et permet un déploiement informatique hybride à grande échelle. Le contrôleur vérifie les stratégies d'accès sur le périphérique et la passerelle, créant un tunnel MTLS sécurisé et éliminant toute interaction des données avec le contrôleur nZTA.

nZTA assure une flexibilité des déploiements et une gestion cohérente des stratégies pour déployer des applications partout, tout en apportant des fonctions complètes d'accès sécurisé aux entreprises dotées d'un environnement de Cloud pur.



Fonction	Advantage
Stratégie d'accès de bout en bout	Définissez des stratégies d'accès de bout en bout pour chaque ressource, sans aucune distinction entre les utilisateurs distants et les utilisateurs sur site.
Dark Cloud	Les applications invisibles ne deviennent accessibles qu'une fois l'utilisateur et le périphérique authentifiés et autorisés.
Visibilité depuis une seule console	Visibilité holistique et rapports de conformité des utilisateurs, des périphériques, des applications et de l'infrastructure pour toute l'entreprise.
Séparation des outils de contrôle et de données	Le trafic des utilisateurs et des applications est transmis directement entre l'utilisateur et la passerelle concernée, ce qui limite les risques de perte de données et améliore l'expérience utilisateur.
SSO adaptatif	Intégration via SAML 2.0 pour fournir le SSO aux applications en SaaS et tierces prises en charge.
Conformité du poste client	L'utilisateur et les périphériques sont authentifiés par rapport à des stratégies granulaires avant que l'accès ne soit autorisé, ce qui limite les logiciels malveillants et autres menaces.
Analyse du comportement des utilisateurs	Exploitez les données d'analyse pour limiter les risques de sécurité, détecter les anomalies, optimiser l'expérience utilisateur et vous adapter aux collaborateurs mobiles.
Confidentialité et souveraineté des données	Toutes les données des utilisateurs et des applications sont entièrement cryptées entre le client et la passerelle, et nZTA n'interagit jamais avec les données des clients.
Sur site et dans le Cloud hybride	Vous pouvez déployer des passerelles dans le Cloud public, dans le Cloud privé ou dans le centre de données du client.

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr