DATASHEET

U-ZTNA

Universal Zero Trust Network Access

Etes-vous conscients que vos accès distants sont devenus votre plus grande vulnérabilité?

Aujourd'hui, près de 65% des entreprises ouvrent leur système d'information à des utilisateurs externes. Chaque connexion est une porte d'entrée. Et chaque porte est une opportunité pour un attaquant.

Pourtant, la majorité de ces accès distants s'appuient sur des technologies qui semblent éprouvées... mais conçues il y a plus de 25 ans.
VPN, DMZ, passerelles : des solutions héritées d'un autre temps, coûteuses, complexes à maintenir... et surtout dangereusement permissives.

Car une fois connecté, tout devient accessible. Le principe de confiance implicite transforme chaque identifiant compromis en menace critique pour toute entreprise ou organisation.

Malgré la possibilité pour les administrateurs systèmes de maîtriser l'exploitation de ces vulnérabilités, les risques majeurs de compromission des systèmes d'information des entreprises sont liés à l'utilisation illégitime d'informations d'authentification, notamment les identifiants et mots de passe, par des acteurs malveillants (anciens collaborateurs, revente d'identifiants sur le darknet, etc.).

Face à ces menaces, le modèle du **Zero Trust Network Access (ZTNA)** s'impose comme une alternative plus adaptée. Basé sur le principe de «confiance zéro», le **ZTNA** consiste à vérifier systématiquement chaque tentative d'accès aux applications de l'entreprise. Aucune confiance n'est accordée par défaut : chaque accès est évalué en fonction de l'identité de l'utilisateur et du contexte de la demande.

Le télétravail s'est généralisé, tout comme la mobilité, le BYOD et le recours à des prestataires externes tels que freelances, consultants ou agences spécialisées. Ces nouvelles pratiques ont élargi la surface d'attaque et rendu obsolètes les modèles de sécurité traditionnels fondés sur le périmètre réseau. Dans ce contexte d'évolution drastique des usages, le ZTNA apporte une réponse efficace en sécurisant les accès des utilisateurs de manière granulaire, dynamique et adaptée aux menaces actuelles et futures.

Ekinops est un fournisseur mondial de solutions de connectivité innovantes et fiables, cotée sur Euronext Paris. Ekinops sert les opérateurs télécoms et les entreprises dans le monde entier depuis 2001. En 2026, Ekinops a acquis Chimere, un leader français de la cybersécurité dans la plateforme de solutions ZTNA depuis 2019. Ensemble, ils ont créé un leader européen du SASE qui unifie connectivité, sécurité réseau et contrôle des applications.

Ekinops U-ZTNA : un accès sécurisé, simple et universel à toutes les applications

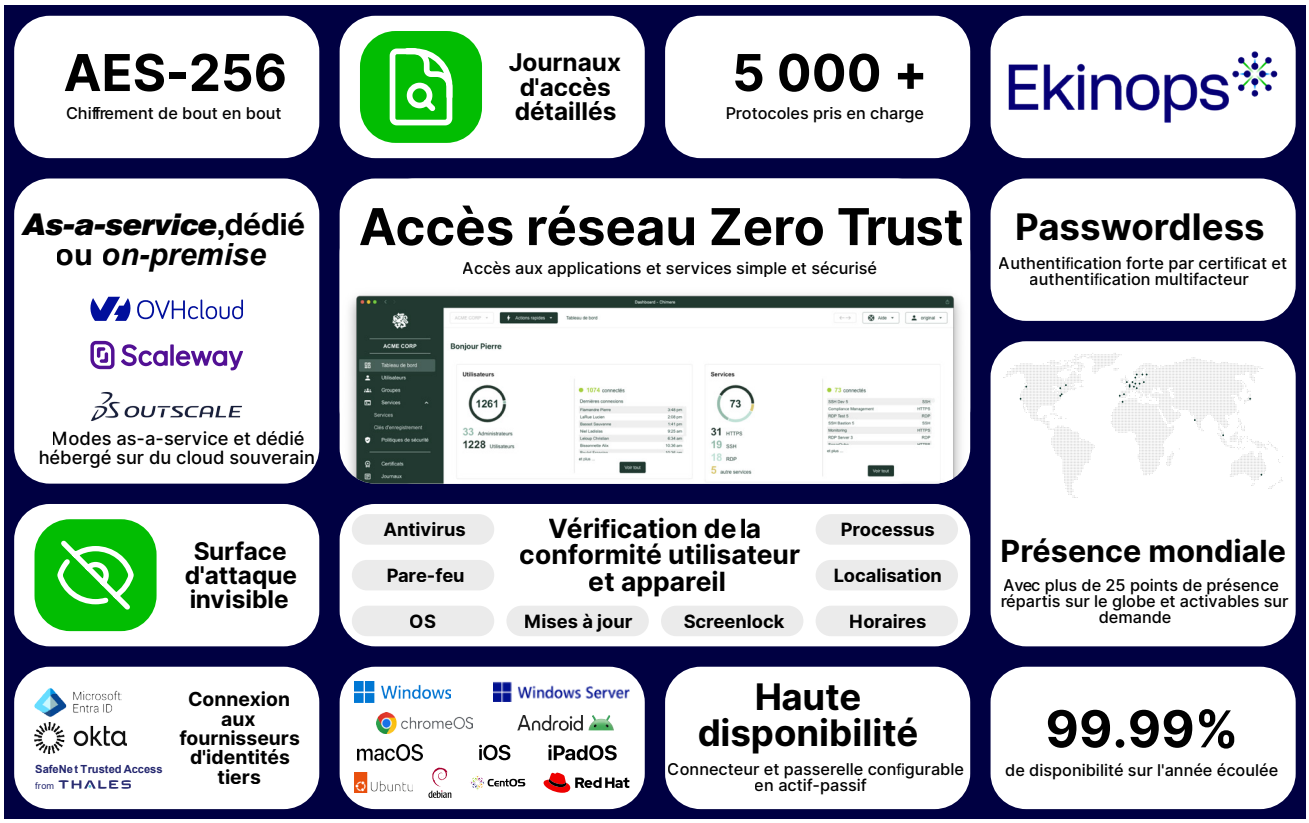
Développé, fabriqué et hébergé en Europe, Ekinops Universal ZTNA assure tout accès aux environnements hybrides (on-premise et cloud). Grâce à Ekinops U-ZTNA, les utilisateurs authentifiés, quel que soit leur emplacement, reçoivent un accès par application d'entreprise en fonction de leur identité sans nécessiter un tunnel persistant.

Avec Ekinops Universal ZTNA, l'utilisateur n'entre jamais dans le réseau. Le système vérifie l'identité, le device, le contexte et donne accès uniquement à l'application autorisée. Le périmètre d'attaque est ainsi limité car contraint.

L'expérience d'accès aux applications reste identique, sans dépendre de la configuration du poste de travail, tout en respectant strictement la politique de sécurité définie par l'entreprise.

Les accès deviennent ainsi totalement indépendants de l'infrastructure sous-jacente. Par exemple, un utilisateur peut continuer à accéder à une application après sa migration vers le cloud sans aucune reconfiguration complexe des pare-feux ou des flux réseau par les équipes IT. Cette agnosticité vis-à-vis de l'infrastructure supprime la dépendance au réseau et rend les opérations plus flexibles et plus rapides.

En quoi Ekinops ZTNA est-il « Universel » ? : parce qu'un seul modèle d'accès sécurisé est utilisé pour toutes les applications (applications web, applications client-serveur, SSH/RDP, SaaS, Clouds, Datacenters, ...)et ce quelque soit l'emplacement de l'utilisateur (depuis le réseau local ou en mobilité).



Principaux bénéfices de notre solution Ekinops U-ZTNA

■ *Meilleures maîtrises du SI et renforcement de la cybersécurité*

- Assure un contrôle efficace sur qui a accés à quoi sur le réseau
- S'applique aussi bien aux utilisateurs sur site qu'aux utilisateurs en mobilité, en télétravail ou à l'autre bout du monde
- Evite de réaliser une micro-segmentation réseau complexe
- Améliore la gestion des dispositifs personnels pour accéder à des données professionnelles (BYOD)
- Suppression de la dépendance en l'infrastructure réseau
- Sécurise tout accès aux environnements multi-cloud grâce à une granularité utilisateur **sans mot de passe**

■ *Suppression de l'exposition*

- Fin des ports exposés sur internet, même pour les points d'accès VPN et Bastions.
- Réduction immédiate du risque d'intrusion par scan sauvage ou par réutilisation d'identifiants dérobés.
- Recherche permanente de la sécurité du « contexte » de l'utilisateur (quels accès, depuis quelle localisation et quel device...) selon des politiques prédéfinies et customisables
- Vérifications permanentes et continues de la conformité du poste de travail (antivirus, EDR, firewall, désactivation de l'écran de verrouillage, ...)

■ *Augmentation de la sécurité applicative*

- Chiffrement de bout en bout
- Haute disponibilité
- Accès moindre privilège (*Least Privilege*)
- Niveaux d'accès et de sécurité des échanges uniformes et standardisés à travers tout le SI

■ *Souplesse d'intégration*

- Utilisation managée clé en main à partir d'un cloud public ou privé ou « on-premise ». SecNumCloud est également possible
- Forte compatibilité avec l'existant
- Pas de substitution à l'authentification des applications
- Prêt pour le Service Managé

■ *Facilité de conformité réglementaire*

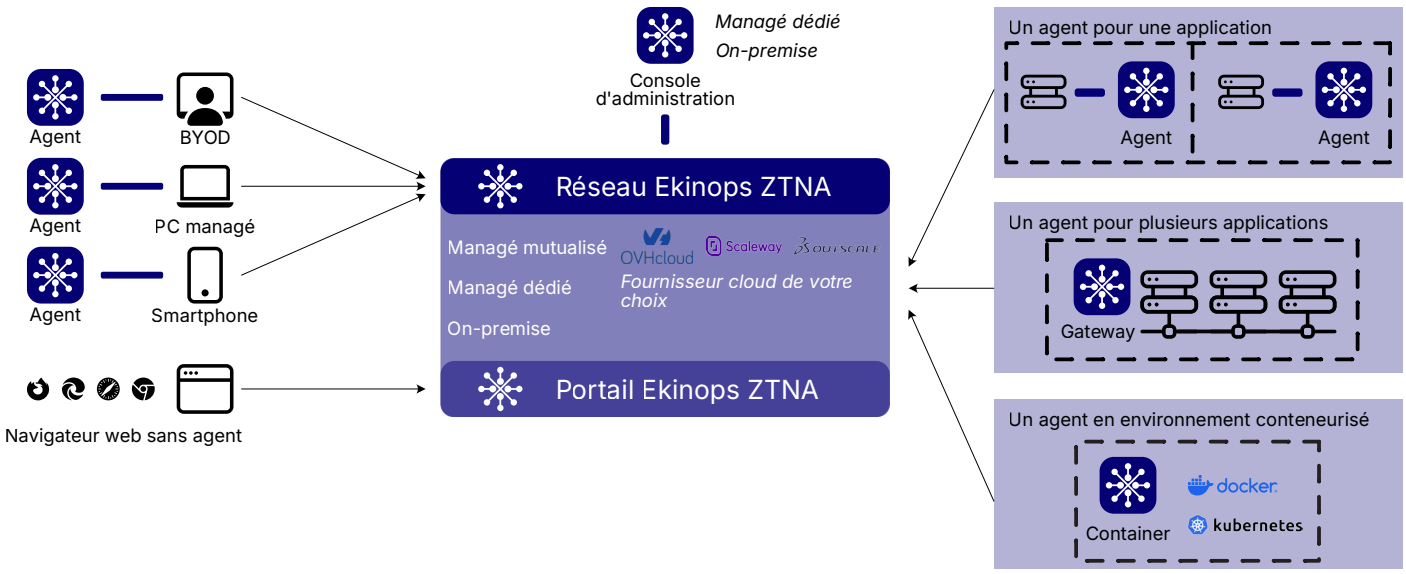
- **Contrôles d'accès standardisés**, alignés avec les exigences réglementaires (RGPD, NIS2)
- **Traçabilité claire des accès** aux applications et aux données (NIS2, DORA)
- **Référentiel centralisé des applications**, utile pour les audits (RGPD)
- **Justification simplifiée des mesures de sécurité** mises en place

Une architecture pensée pour la sécurité moderne

Dans un contexte de transformation numérique accélérée, la solution Ekinops U-ZTNA s'inscrit dans une approche moderne de sécurité basée sur le **Software Defined Perimeter (SDP)**, permettant de remplacer les modèles traditionnels par une architecture plus sécurisée, flexible et adaptée aux usages actuels.

Ekinops U-ZTNA repose sur quatre composants clés :

- Un **contrôleur central** qui agit comme un point central d'orchestration, authentifie les utilisateurs, applique les politiques d'accès et autorise ou non les connexions
- Un **agent côté utilisateur** et un agent **côté serveur** qui délivrent un contrôle précis des flux, une traçabilité complète des accès et facilitent les audits de sécurité
- Un **réseau sécurisé intermédiaire entre l'agent client et l'agent serveur**, créant une couche de transport totalement sécurisée et chiffrée de bout-en-bout



Ce choix architectural permet de rendre les **applications privées totalement invisibles depuis Internet**. Contrairement à une solution VPN classique ou à une DMZ, aucune ressource de l'entreprise n'est directement exposée. Ekinops U-ZTNA garantit ainsi une meilleure maîtrise des accès utilisateurs et **réduit de 80% les risques d'intrusion**.

Déclinaison « agentless » : modèle d'accès ZTNA et bastion unifié

Ekinops U-ZTNA propose également une déclinaison « agentless » conçue pour répondre aux besoins de sécurité pour les environnements où l'installation d'un agent n'est pas possible ou n'est pas souhaitée.

Cette version permet de sécuriser tout accès distants aux ressources internes des Entreprises **sans aucun déploiement logiciel sur les postes utilisateurs**.

Elle repose sur un **bastion cloud** (ou **on-premise**) plus un portail web agissant comme points d'entrée uniques pour les flux sensibles comme :

- HTTPS applications web internes (portail web uniquement)
- SSH administration de serveurs (bastion)
- RDP bureaux à distance(bastion)

Avec un **contrôle d'accès contextuel** et via une intégration fine avec un **fournisseur d'identités** (OIDC tels que Azure AD, Entra ID, Okta, ...), l'entreprise reste maître des autorisations, tout en assurant une **traçabilité complète** des connexions. Le bastion intègre également un **mécanisme d'enregistrement des sessions SSH et RDP**, permettant un **suivi précis des actions menées**, à des fins de supervision ou d'audit. Ces enregistrements s'inscrivent complètement dans les démarches de conformité des entreprises aux exigences de sécurité européennes et sectorielles.

Principaux cas d'usages de sécurisation de notre version « agentless » :

- Les prestataires externes devant accéder ponctuellement à des systèmes critiques
- Les environnements réglementés ou verrouillés (DMZ, OT, IoT, SI industriels, ...)
- Les projets pilotes ou déploiements rapides, sans contrainte sur les postes utilisateurs
- Les accès à privilèges (PAM) à travers un point d'accès central
- La mise en conformité aux règlements européens (NIS2)

Les utilisateurs ne se connectent jamais directement à la cible.

Aucun verrouillage aux fournisseurs de Cloud	*Aucune restriction sur le type d'appareil à protéger*	*Indépendance des infrastructures réseaux sous-jacentes*
Simplicité des déploiements	*Solution «SASE-Ready» englobant «Bastion & ZTNA»*	*Fabriquée en UE et conçue pour aujourd'hui et pour demain*

Pourquoi nous faire confiance ?

- Fortes racines réseau : fabriquant de CPE, produit également des dispositifs cellulaires extérieurs et intérieurs (MRU-5G)
- 100% compatible avec la stack de sécurité Ekinops SASE)
- Performance, résilience et retour sur investissement : assure un niveau élevé de sécurisation du trafic pour tous les accès utilisateurs à un coût optimal
- Simplicité : 5 fois moins de temps nécessaire pour maintenir et opérer
- Evolutive : conçue pour aujourd'hui et pour demain ; prête à l'emploi pour tout service managé (on-prem ou cloud)
- Protection des données privées : délivre un niveau élevé de chiffrement des données privées- non assujetti au Cloud Act américain
- Ouvert et intégrable facilement avec toute solution existante au sein d'un SI
- Orientée conformités Européennes : convient parfaitement aux organisations concernées par la souveraineté des données et l'alignement avec les réglementations régionales (RGPD, NIS2, DORA)
- Aucun verrouillage à un fournisseur de solutions en Cloud

© 2026 Ekinops France SA « all rights reserved » - Ekinops se réserve de modifier sans préavis les caractéristiques techniques dans le présent document sans préavis-ds_U-ZTNA--FR_0526