

DATASHEET



SSE

Security Service Edge

Sécuriser l'environnement informatique hybride : un impératif stratégique

Nos entreprises et l'ensemble de nos métiers sont aujourd'hui hyperconnectés, et les cyberattaques sont chaque jour plus nombreuses et destructrices. Les organisations de toutes tailles doivent renforcer leurs défenses. Les entreprises dépendant de plus en plus de l'accès à Internet pour accéder à des applications critiques hébergées dans des clouds publics, des clouds privés et des centres de données, il est devenu essentiel de sécuriser ces points d'accès.

L'expansion rapide des infrastructures cloud hybrides a non seulement **multiplié la surface d'attaque**, mais aussi mis **à rude épreuve les performances du réseau**, compromettant la qualité de service (QoS) et la qualité d'expérience (QoE) des applications. Toute panne, utilisation abusive ou violation peut avoir un impact immédiat sur le chiffre d'affaires, la réputation de la marque et la continuité opérationnelle.

Ekinops est un fournisseur mondial de solutions de connectivité innovantes et fiables, coté sur Euronext Paris. Ekinops est au service des opérateurs télécoms et des entreprises du monde entier depuis 2001. En 2025, Ekinops a renforcé son expertise en cybersécurité dans le domaine de l'accès Internet sécurisé, créant un leader européen du SASE qui unifie la connectivité, la sécurité des réseaux et le contrôle d'accès.

Développée, fabriquée et hébergée en France, la plateforme **Security Access Service Edge (SASE) d'Ekinops** concentre 25 ans d'expertise en matière de réseaux et 20 ans d'analyse et de classification du trafic web.

Ekinops SSE : simplicité, sécurité et souveraineté

Le **Security Service Edge (SSE) d'Ekinops** est crucial pour les entreprises qui adoptent des environnements de travail cloud et hybrides. Il intègre des solutions de sécurité telles que le **Secure Web Gateway (SWG)** incluant nativement la technologie **Zero Trust Internet Access (ZTIA)**, le **Cloud Access Security Broker (CASB)** et le **Data Loss Prevention (DLP)** pour offrir une protection complète des utilisateurs et des données, qu'ils se trouvent sur site ou à distance.

Le SSE permet de centraliser et de renforcer la sécurité en offrant une protection continue et adaptative contre les menaces, tout en assurant une gestion simplifiée des accès cloud et une prévention efficace des pertes de données. Le SWG est disponible en mode SaaS comme en mode On-Premise ; le CASB et le DLP sont proposés en SaaS.

Face à l'augmentation des cyberattaques et à la complexité croissante des infrastructures réseau modernes, le SSE apporte une réponse adaptée aux nouvelles exigences en matière de sécurité. En appliquant le principe Zero Trust, basé sur la technologie exclusive **Zero Trust Internet Access (ZTIA)**, Ekinops SSE garantit que chaque demande d'accès à un contenu web est vérifiée et sécurisée, réduisant ainsi les risques d'intrusion.

Ekinops SSE contribue à prévenir les risques civils et pénaux, favorise le respect du droit du travail et permet le déploiement et la reconnaissance formelle des politiques informatiques. Il contribue activement à votre conformité avec les réglementations RGPD, NIS2 et DORA.



Des clients dans tous les secteurs

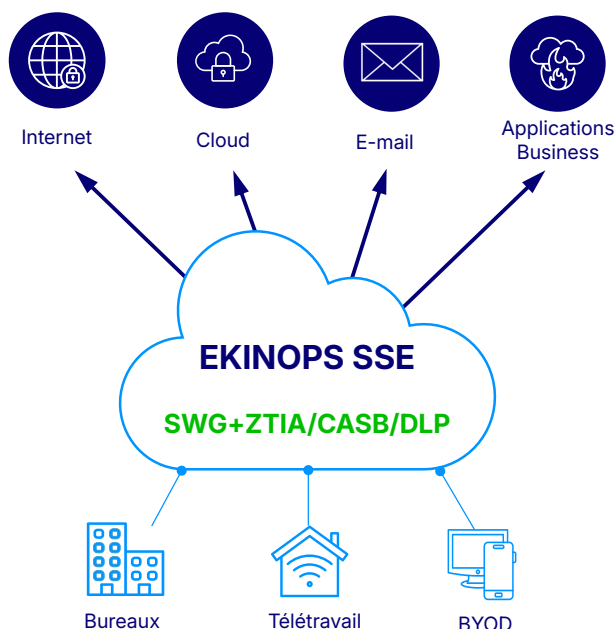
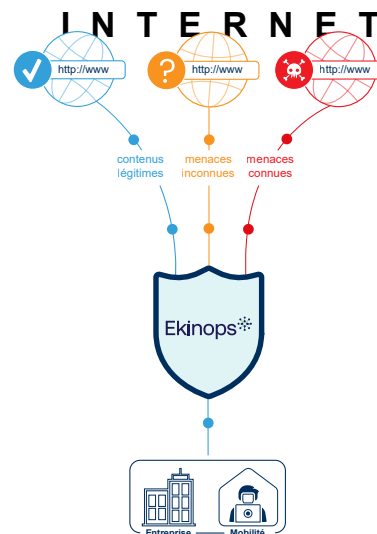
JULES



La technologie Zero Trust Internet Access (ZTIA) d'Ekinops

La majorité des solutions de cybersécurité sont basées sur la reconnaissance de la menace pour pouvoir la bloquer. Or, on assiste à une explosion du nombre de menaces : sur environ 330.000 nouveaux domaines recensés chaque jour, 25% d'entre eux sont identifiés comme étant des domaines malveillants en 2026. Ces technologies ne peuvent plus suivre et deviennent obsolètes.

La posture **Trust-Centric** d'Ekinops renverse ce paradigme : elle n'autorise l'accès des utilisateurs qu'à des sites de confiance préalablement vérifiés. Ainsi, toutes les attaques éphémères non référencées sont bloquées par défaut. Cette approche est rendue possible par l'exhaustivité et la qualité de la base de connaissance Ekinops, qui contient plus d'un milliard d'URLs classifiées (25 millions de domaines et adresses IP) et identifie 99 % du trafic Internet des entreprises françaises.



Fonctions de sécurité intégrées

Ekinops SSE réunit le filtrage web Trust-Centric, le CASB et le DLP dans une console unique, avec une architecture flexible adaptée aux ressources distribuées.

Sécurise les collaborateurs distants

Ekinops SSE répond efficacement aux enjeux d'accès des utilisateurs nomades et en télétravail, et assure la sécurité où qu'ils se trouvent.

Protège les usages des applications SaaS

Ekinops SSE garantit une sécurité robuste pour les applications SaaS et renforce la protection des données de l'entreprise.

Déploiement SaaS ou On-Premise

Le SWG s'adapte à votre politique de confidentialité des données et peut également être déployé On-Premise.

Pourquoi nous faire confiance

- **Une approche Trust-Centric unique sur le marché** : là où les autres solutions autorisent le trafic par défaut puis cherchent à reconnaître la menace, le ZTIA n'autorise que les domaines préalablement vérifiés — les attaques éphémères et les menaces inconnues sont bloquées par construction. Le ZTIA est inclus par défaut dans le SWG, sans option ni surcoût.
- **La meilleure connaissance du web français** : 20 ans à répertorier et classer les usages du web français. 99 % du trafic Internet des entreprises françaises est correctement identifié (99,5 % sur les catégories de sites critiques), sur une base de plus d'un milliard d'URLs classifiées — également proposée en marque blanche aux éditeurs de logiciels et aux fournisseurs de services afin d'améliorer leurs propres solutions.
- **Souveraineté et conformité européenne** : solution conçue, fabriquée et hébergée en France, sur une chaîne de valeur 100 % européenne. Les clés de chiffrement ne sont jamais stockées hors d'Europe et aucun fichier n'est conservé. Idéal pour les organisations soucieuses de la souveraineté de leurs données et de l'alignement réglementaire régional (RGPD, NIS2, DORA).
- **Simplicité et rapidité de mise en œuvre** : le SWG est opérationnel en moins d'une heure en mode SaaS, sans tunnel à créer ni à maintenir et sans matériel à dimensionner. Une console unique pour le SWG, le CASB et le DLP.
- **Ouverture et flexibilité** : interopérabilité avec tout SI existant, logs temps réel exportables vers tout SIEM (Sekoia, Splunk...) et solutions NDR. Adapté aux PME comme aux marchés de taille moyenne.
- **Performance et maîtrise du budget** : prise en charge d'un niveau élevé de trafic en toute sécurité pour tous les points d'extrémité, avec un abonnement simple au nombre d'utilisateurs à protéger — sans coût supplémentaire caché.
- **Références multiples** : institutions publiques et gouvernementales, télécommunications, santé, éducation, transports, logistique, banque et finance.