

DATASHEET



SSE

Security Service Edge

Securing the hybrid IT environment: a strategic imperative

Our companies and all our business lines are now hyperconnected, and cyberattacks are growing more numerous and destructive by the day. Organizations of every size must strengthen their defenses. As businesses rely increasingly on Internet access to reach critical applications hosted in public clouds, private clouds and data centers, securing these access points has become essential.

The rapid expansion of hybrid cloud infrastructures has not only **multiplied the attack surface**, it has also **placed network performance under severe strain**, compromising the quality of service (QoS) and quality of experience (QoE) of applications. Any outage, misuse or breach can have an immediate impact on revenue, brand reputation and business continuity.

Ekinops is a global provider of innovative, reliable connectivity solutions, listed on Euronext Paris. Ekinops has served telecom operators and enterprises worldwide since 2001. In 2025, Ekinops strengthened its cybersecurity expertise in secure Internet access, creating a European SASE leader that unifies connectivity, network security and access control.

Developed, manufactured and hosted in France, the **Ekinops Security Access Service Edge (SASE) solution suite** brings together 25 years of networking expertise and 20 years of web traffic analysis and classification.



**Customers in
every sector**

Ekinops SSE: simplicity, security and sovereignty

The **Ekinops Security Service Edge (SSE)** is essential for companies adopting cloud and hybrid working environments. It integrates security solutions such as the **Secure Web Gateway (SWG)**, the **Cloud Access Security Broker (CASB)** and **Data Loss Prevention (DLP)** to deliver complete protection for users and data, whether on site or remote.

SSE centralizes and strengthens security by providing continuous, adaptive protection against threats, while ensuring simplified cloud access management and effective prevention of data loss. The SWG is available both as SaaS and On-Premise; CASB and DLP are delivered as SaaS.

Faced with the rise in cyberattacks and the growing complexity of modern network infrastructures, SSE delivers a response tailored to new security requirements. It applies the Zero Trust principle, based on the exclusive **Zero Trust Internet Access (ZTIA)** technology, guaranteeing that every request to access web content is verified and secured, reducing the risk of intrusion.

Ekinops SSE helps prevent civil and criminal risks, supports compliance with employment law and enables the deployment and formal acknowledgement of IT policies. It actively contributes to your compliance with the GDPR, NIS2 and DORA regulations.

JULES



VILLE DE
MARSEILLE



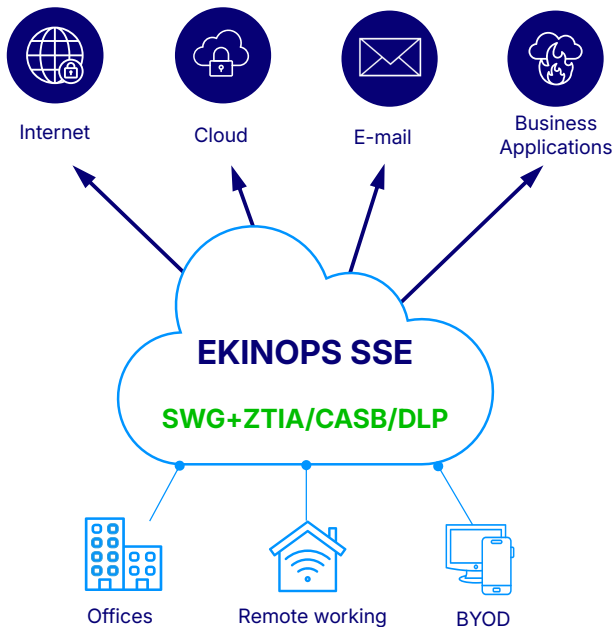
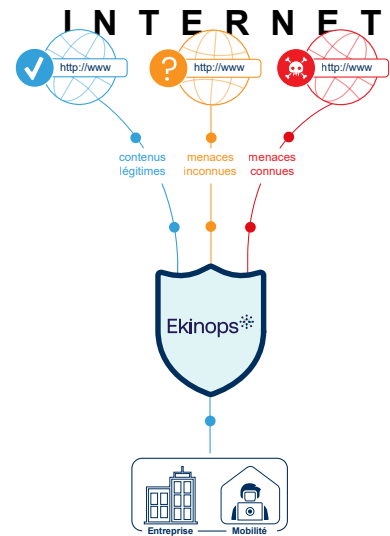
CHU
Poitiers

CENTRE HOSPITALIER UNIVERSITAIRE

Zero Trust Internet Access (ZTIA) technology by Ekinops

Most cyber defense solutions are based on recognizing a threat in order to block it. Yet the number of threats is exploding: from nearly 330,000 new domains recorded every day, 25% of them are identified as malicious domains in 2026. These technologies can no longer keep pace and are becoming obsolete.

Ekinops' **Trust-Centric** posture reverses this paradigm: it grants users access only to trusted sites that have been verified beforehand, so every unlisted, short-lived attack is blocked by default. This approach is made possible by the completeness and quality of the Ekinops knowledge base, which contains more than one billion classified URLs (25 million domains and IP addresses) and correctly identifies 99% of French business Internet traffic.



▪ Integrated security functions

Ekinops SSE brings Trust-Centric web filtering, CASB and DLP together in a single console, with a flexible architecture adapted to distributed resources.

▪ Secures remote employees

Ekinops SSE efficiently addresses security issues for nomad and remote workers and ensures security from anywhere.

▪ Protects SaaS application usage

Ekinops SSE guarantees robust security for SaaS applications and enhances enterprise data protection.

▪ SaaS or On-premises deployment

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

Why trust us

- **A Trust-Centric approach that is unique on the market:** where other solutions allow traffic by default and then try to recognize the threat, ZTIA grants access only to domains that have been verified beforehand — short-lived attacks and unknown threats are blocked by design. ZTIA is included in the SWG by default, with no option or extra cost.
- **Recognized Industrial actor:** 20 years spent cataloguing and classifying web usage in a database of more than one billion classified URLs — also offered on a white-label basis to software vendors and service providers to enhance their own solutions.
- **Sovereignty and European compliance:** a solution designed, manufactured and hosted in Europe on a 100% European value chain. Encryption keys are never stored outside Europe and no files are retained. Ideal for organizations concerned with data sovereignty and regional regulatory alignment (GDPR, NIS2, DORA).
- **Simplicity and speed of deployment:** the SWG is operational in under an hour as SaaS, with no tunnels to build or maintain and no hardware to size. A single console for SWG, CASB and DLP.
- **Openness and flexibility:** interoperability with any existing IT system, real-time logs exportable to any SIEM (Sekoia, Splunk, etc.) and NDR solutions. Suited to SMEs and mid-sized markets.
- **Performance and budget control:** securely supports a high level of traffic for all endpoints, with simple per-user subscription pricing — no hidden additional costs.
- **Multiple references:** public and government institutions, telecommunications, healthcare, education, transport, logistics, banking and finance.