

DATASHEET



U-ZTNA

Universal Zero Trust Network Access

Are you aware that your remote access has become your greatest vulnerability?

Today, nearly 65% of organizations open their information systems to external users. Every connection is an entry point. And every entry point is an opportunity for an attacker.

Yet most of this remote access still relies on technologies that may seem proven—but were designed more than 25 years ago.

VPN, DMZ, gateways: legacy solutions from another era—costly, complex to maintain, and above all dangerously permissive.

Because once connected, everything becomes accessible. The principle of implicit trust turns every compromised credential into a critical threat for any enterprise or organization.

While system administrators may be able to manage the exploitation of these vulnerabilities, the major risks of information system compromise are tied to the illegitimate use of authentication data.

In the face of these threats, the **Zero Trust Network Access (ZTNA)** model is emerging as a more suitable alternative. Based on the principle of 'zero trust', ZTNA involves systematically verifying every attempt to access the company's applications. No trust is granted by default: each access request is assessed based on the user's identity and the context of the request.



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY



Remote work has become mainstream, as have mobility, BYOD, and the use of external providers such as freelancers, consultants, and specialized agencies. These new practices have expanded the attack surface and made traditional security models based on the network perimeter obsolete. In this rapidly evolving usage environment, ZTNA provides an effective response by securing user access in a granular, dynamic way that is aligned with current and future threats.

Ekinops is a global provider of innovative and reliable connectivity solutions, listed on Euronext Paris. Ekinops has been serving telecoms operators and businesses worldwide since 2001. In 2026, Ekinops acquired Chimere, a French leader in cybersecurity within the ZTNA solutions market since 2019. Together, they have created a European leader in SASE that unifies connectivity, network security and application control.

Ekinops U-ZTNA : secure, simple, and universal access to all applications

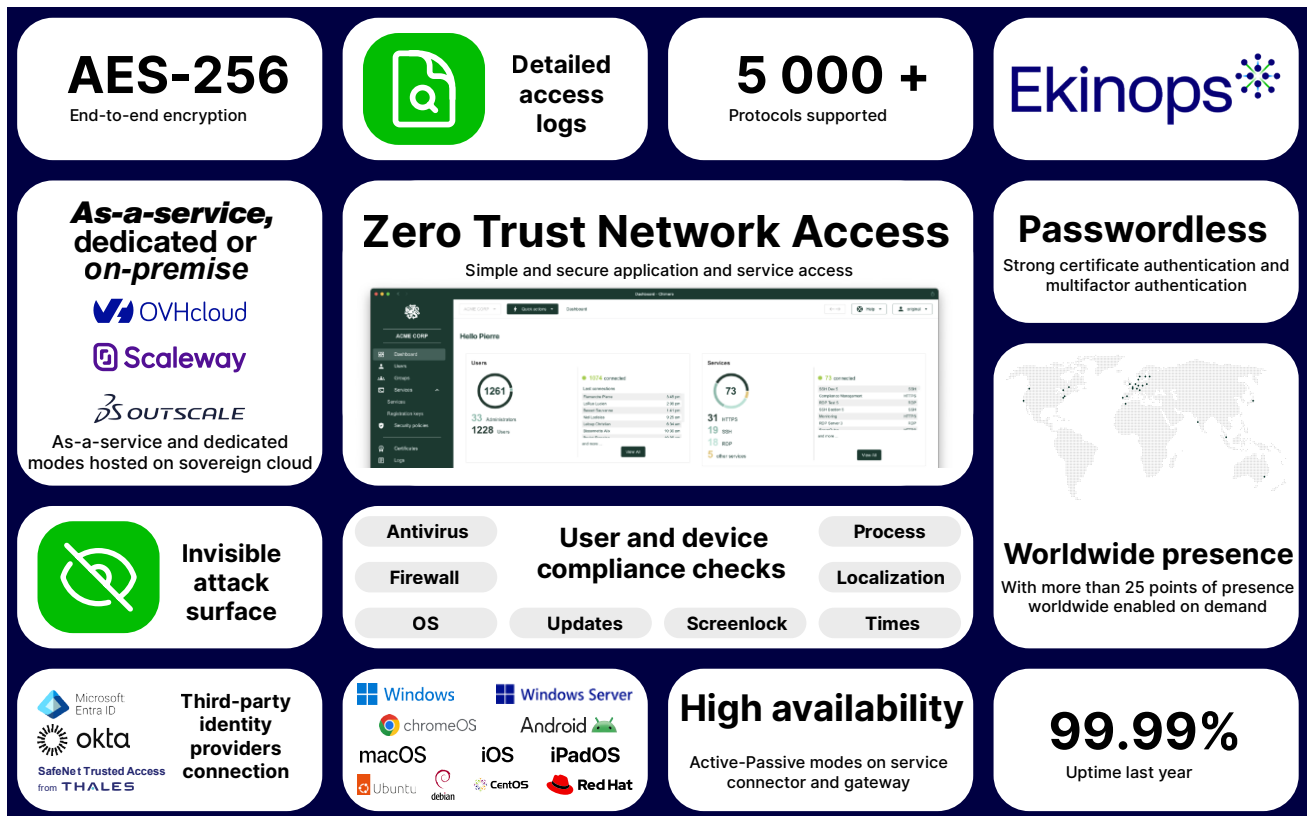
Developed, built, and hosted in Europe, Ekinops Universal ZTNA secures all access to hybrid environments (on-premise and cloud). With Ekinops U-ZTNA, authenticated users—wherever they are located—receive per-application access based on their identity, without requiring a persistent tunnel.

With Ekinops Universal ZTNA, the user never enters the network. The system verifies identity, device, and context, and grants access only to the authorized application. As a result, the attack perimeter is minimized because access is tightly constrained.

The application access experience remains unchanged, without depending on workstation configuration, while strictly enforcing the security policy defined by the organization.

Access therefore becomes fully independent of the underlying infrastructure. For example, a user can continue accessing an application after it has been migrated to the cloud, without any complex reconfiguration of firewalls or network flows by IT teams. This infrastructure-agnostic approach removes network dependency and makes operations more flexible and faster.

Why is Ekinops ZTNA “Universal”? Because a single secure access model is used for all applications (web applications, client-server applications, SSH/RDP, Clouds, Datacenters, etc.), regardless of where the user is located (from the local network or on the move).



Key benefits of our Ekinops U-ZTNA solution

■ Greater control over the information system and stronger cybersecurity

- Provides effective control over who can access what across the network
- Applies equally to on-site users and to users on the move, working remotely, or located anywhere in the world
- Eliminates the need for complex network micro-segmentation
- Improves management of personal devices used to access business data (BYOD)
- Removes dependency on the network infrastructure
- Secures all access to multi-cloud environments through **passwordless**, user-level granularity

■ Eliminating exposure

- No more internet-exposed ports, even for VPN access points and bastions.
- Immediate reduction in intrusion risk from indiscriminate scanning or the reuse of stolen credentials.
- Continuous evaluation of user “context” security (which access, from which location, and on which device) based on predefined and customizable policies
- Continuous verification of workstation compliance (antivirus, EDR, firewall, screen lock status, etc.)

■ Stronger application security

- End-to-end encryption
- High availability
- Least privilege access
- Uniform, standardized access levels and exchange security across the entire information system

■ Integration flexibility

- Fully managed turnkey deployment from public cloud, private cloud, or on-premise. SecNumCloud is also possible
- Strong compatibility with existing environments
- No substitution of application authentication
- Managed-service ready

■ Simplified regulatory compliance

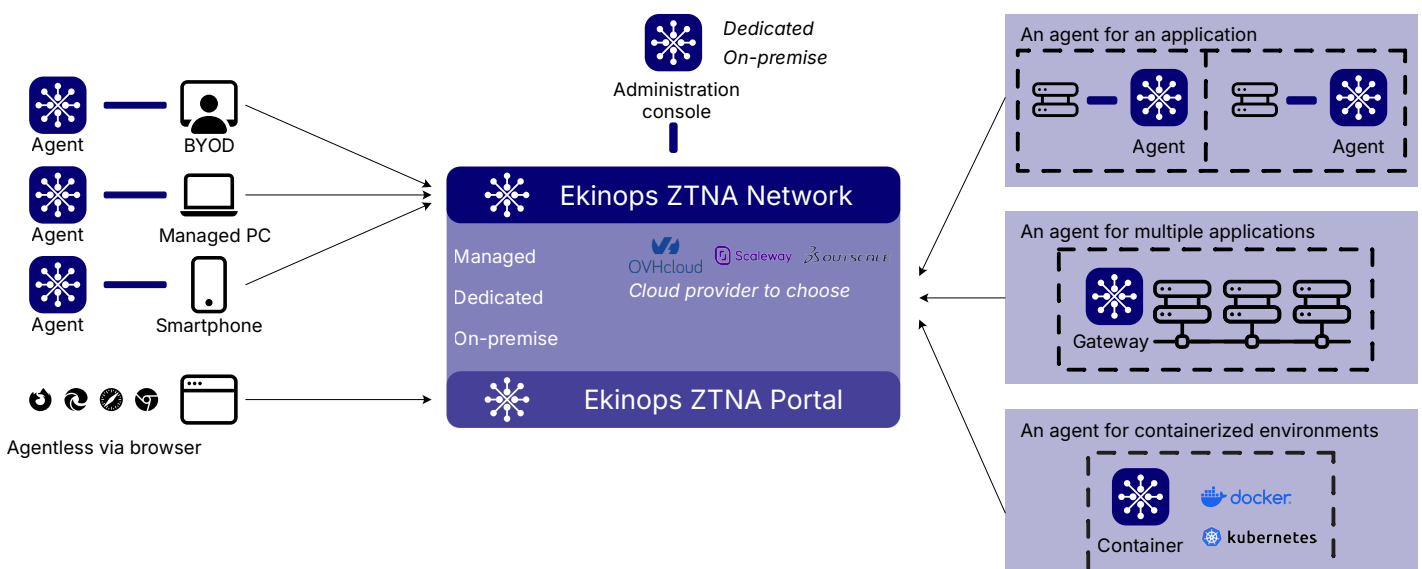
- **Standardized access controls** aligned with regulatory requirements (GDPR, NIS2)
- **Clear traceability of access** to applications and data (NIS2, DORA)
- **Centralized application repository**, useful for audits (GDPR)
- **Simplified justification of implemented security measures**

A more secure, flexible architecture aligned with today's usage patterns

Against a backdrop of accelerating digital transformation, the Ekinops U-ZTNA solution forms part of a modern security approach based on the **Software-Defined Perimeter (SDP)**, enabling traditional models to be replaced by an architecture that is more secure, flexible and suited to today's needs.

Ekinops U-ZTNA is built on four key components:

- A **central controller** that acts as the orchestration hub, authenticates users, enforces access policies, and authorizes or rejects connections
- A **user-side agent** and a **server-side agent** that provide precise flow control, full access traceability, and easier security audits
- A **secure intermediate network between the client agent and the server agent**, creating a fully secure, end-to-end encrypted transport layer



This architectural choice makes **private applications completely invisible from the Internet**. Unlike a traditional VPN solution or a DMZ, no enterprise resource is directly exposed. Ekinops U-ZTNA therefore delivers stronger control over user access and **reduces intrusion risk by 80%**.

Agentless: ZTNA access model and unified bastion

Ekinops U-ZTNA also offers an agentless version designed to meet security requirements in environments where installing an agent is not possible or not desired.

This version secures all remote access to internal corporate resources **without any software deployment on user endpoints**.

It relies on a **cloud bastion** (or **on-premise**) combined with a web portal acting as a single entry point for sensitive flows such as:

- HTTPS internal web applications (web portal only)
- SSH server administration (bastion)
- RDP remote desktops (bastion)

With **contextual access control** and deep integration with an **identity provider** (OIDC such as Azure AD, Entra ID, Okta, etc.), the organization retains full control over authorizations while ensuring **end-to-end traceability** of connections. The bastion also includes an **SSH and RDP session recording mechanism**, enabling **precise monitoring of actions performed** for supervision or audit purposes. These recordings fully support organizations' compliance efforts with European and industry-specific security requirements.

Key security use cases for our agentless version:

- External service providers requiring occasional access to critical systems
- Regulated or locked-down environments (DMZ, OT, IoT, industrial IT systems, etc.)
- Pilot/ PoC projects or rapid deployments, with no constraints on user endpoints
- Privileged access (PAM) through a centralized access point
- Compliance with European regulations (NIS2)

Users never connect directly to the target.

*No vendor lock-in with
Cloud providers*

*No restrictions on the type
of device to protect*

*Independence from the underlying
network infrastructure*

Deployment simplicity

*SASE-ready solution
combining bastion and ZTNA*

*Made in EU, built for today and
tomorrow*

Why trust us?

- Deep networking heritage: a CPE manufacturer that also produces indoor and outdoor cellular devices (MRU-5G)
- 100% compatible with the Ekinops SASE security stack
- Performance, resilience, and ROI: delivers a high level of traffic security for all user access at an optimal cost
- Simplicity: requires five times less time to maintain and operate
- Scalable: designed for today and tomorrow; deployment-ready for any managed service model (on-premise or cloud)
- Private data protection: delivers a high level of encryption for sensitive data and is not subject to the U.S. Cloud Act
- Open and easily integrated with any existing solution across the information system
- Built for European compliance: ideal for organizations focused on data sovereignty and alignment with regional regulations (GDPR, NIS2, DORA)
- No lock-in to a single cloud solution provider