oplon®
SECURE ACCESS

The platform that replace the patchwork. Unify and control every access, from the least privileged to the most critical.

Oplon Networks Secure Access is the Zero Trust solution that protects every access to enterprise systems and applications, enabling both internal and external users to operate securely **directly from the browser and in full compliance with the NIS2 Directive.**
In recent years, this model has increasingly established itself as the new standard for enterprise application access. This is a direction we embraced from the earliest stages of development, **anticipating an evolution that is now becoming more and more widespread.**

- Identity-based access
- No network exposure
- MFA for legacy applications
- Remote access without VPNs

A single **browser-based workspace** for secure access and identity control.

Centralizes authentication, authorization, and connectivity to enterprise resources by applying a Zero Trust model: every access request is verified, authorized, and monitored. Instead of relying on a collection of disconnected tools, the platform provides:

- A unified policy layer governing access to resources for both users and machines.
- A browser-based access approach that minimizes client-side impact.
- Telemetry and audit logs that feed risk assessment systems and compliance processes.

PAM
PRIVILEGED ACCESS MANAGEMENT

Privileged access control with activity monitoring and full traceability.

ZTNA
ZERO TRUST NETWORK ACCESS

Zero Trust architecture for secure connectivity anywhere.

IAM
IDENTITY & ACCESS MANAGEMENT

Identity and access management with centralized authentication and policy enforcement.

Access Contexts

From network access to resource access: granular control and continuous security

Oplon Networks Secure Access supports access control requirements across multiple operational environments, enabling secure connectivity to systems and applications without relying on broad network exposure.

Machine and Service Access

Manage access for machines, services, and automated workloads.
Replace shared secrets with identity-based, policy-driven authentication.

Contractor and Third-Party Access

Provide external users and vendors with controlled, time-limited access. Reduce exposure through scoped permissions and automatic access expiration.

Employee Access

Simple access to all applications through a single identity with the convenience of a browser.

Modernize Legacy Access

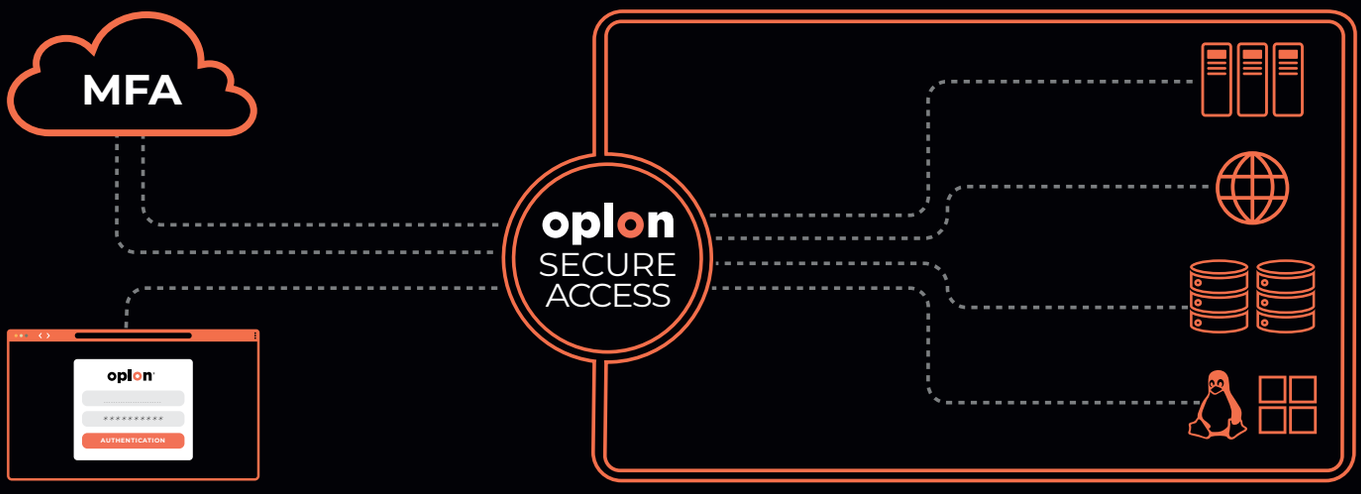
Protect legacy applications without rewriting or replacing them.
Centralize access control and modernize trust across fragmented environments.

Secure Access to Critical Systems

Protect any environment, database, and operating system.
Access is continuously governed by strict security policies.

Secure Privileged Operations

Protect and manage privileged access to critical systems.
Every session is isolated, monitored, and fully auditable by default.



Application Areas

WEB APPLICATION

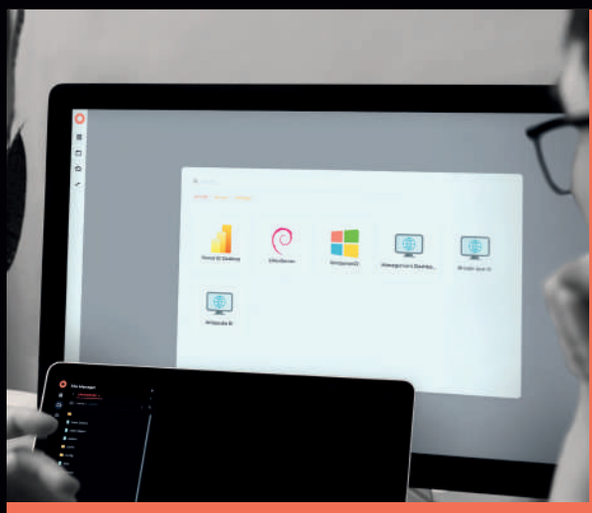
Secure access to enterprise web applications via MFA without requiring any modifications or integrations; OSA acts as an intermediary and manages the entire process transparently.

REMOTE DESKTOP SERVICE ACCESS

Browser-based access to remote desktops or applications via MFA, integrated with existing systems (e.g., Active Directory) and based on user permissions.

REMOTE SHELL SERVICE ACCESS

SSH access via browser with MFA without entering credentials; secure password management, advanced features (files, copy/paste), and comprehensive activity logging.



Compliance

The Oplon Secure Access solution stands out for its excellence in ensuring compliance with major security and data protection regulations, such as GDPR, NIST, and NIS2. It ensures the protection of personal data, adopts best security practices, and effectively manages risks, safeguarding critical infrastructures and ensuring business continuity.

Secure access for every use case

The evolution from network access to resource access

Oplon Secure Access offre un unico metodo di accesso per connettere in modo sicuro gli utenti alle molteplici applicazioni, servizi e sistemi senza esporre la rete. Questi metodi supportano casi d'uso comuni quali l'accesso remoto, la connettività di terze parti e la protezione delle applicazioni legacy.

Clientless Remote Access

Remote access directly from the browser.

It enables access to systems, applications, and desktops directly from the browser, without requiring installations or a VPN. Resources are exposed in a controlled manner, and sessions are secured, profiled, and tracked, simplifying access management.

MFA for Legacy Applications

Multi-factor authentication without modifying the application.

It extends multi-factor authentication to legacy applications without requiring any changes to the application code. The second factor is enforced at the access layer, improving security and reducing risks associated with static credentials.

Remote Browser Isolation

Secure web access without exposing applications.

Web sessions are executed in a remote isolated environment, with content streamed to the user without exposure to malicious code. This approach protects against malware, ransomware, and phishing, while keeping applications and systems unexposed to the external network.

Identity Federation

A single control layer for multiple identity sources.

It enables integration with external authentication systems and reuse of existing identities. Federated authentication is enabled without application changes, simplifying management and ensuring secure and consistent access.

Trusted Connection (no VPNs)

Secure connections for desktop applications.

It enables connections to systems and services without directly exposing them, activating connections only when needed and only to specific resources. The model is centralized, controlled, and applicable also in IT/OT environments, integrating with existing tools.

Why not use VPNs?

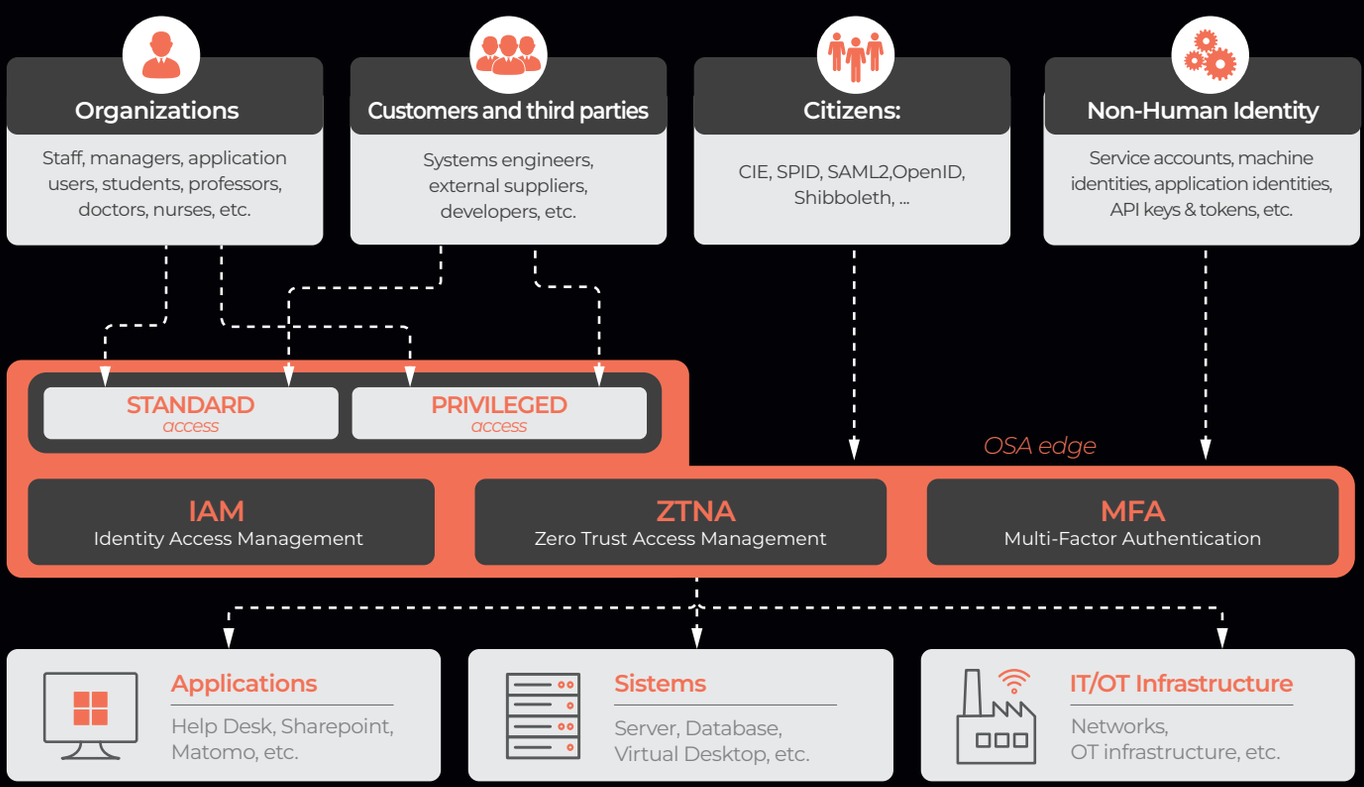
Security is no longer in the network. It is in access.

A resource-level access model allows the device to remain outside the corporate network, granting access only to the required resources and enabling more granular and precise security policies.
In traditional network-based access models, instead, VPN connectivity typically places the device inside the corporate network, introducing challenges related to an expanded attack surface as well as increased operational complexity in terms of configuration, management, and maintenance.

VPN / ACCESSI TRADIZIONALI	OPLON SECURE ACCESS
⊗ Resource-level access	✓ Network-level access
⊗ Minimal attack surface	✓ Large attack surface
⊗ Continuous verification	✓ Static trust
⊗ Full traceability	✓ Limited visibility

Access security layers

A single platform to manage identities, access, and resources.



oplon®

For more information, visit our website
https://www.oplon.net
or email us at **info@oplon.net**

Oplon Networks is an IT engineering company founded in 2010.
Its mission is to develop products and services that ensure high reliability and security at the infrastructure level in service delivery, maintaining exceptional quality standards. Excellence is the primary objective. For this reason, the company develops cybersecurity tools and integrated solutions to secure modern data centers, networks, cloud, and hybrid cloud environments.

Quality management system certified according to ISO/IEC 27001:2022 and UNI EN ISO 9001:2015.
Data and specifications may change at any time without prior notice.