oplon®
SECURE ACCESS

La piattaforma che supera la gestione frammentata. Centralizza e controlla ogni accesso, dal meno privilegiato al più critico

Oplon Secure Access è la soluzione Zero Trust che protegge ogni accesso a sistemi e applicazioni aziendali, consentendo a utenti interni ed esterni di operare in sicurezza **direttamente dal browser e in totale conformità alla direttiva NIS2.**
Negli ultimi anni, questo modello si sta affermando come nuovo standard per l'accesso alle applicazioni aziendali.
Una direzione che abbiamo intrapreso fin dalle prime fasi di sviluppo, **anticipando un'evoluzione oggi sempre più diffusa.**

- Accesso basato sull'identità
- Nessuna esposizione alla rete
- MFA per applicazioni legacy
- Accesso remoto senza VPN

Un unico workspace, **su architettura browser-based**, per l'accesso sicuro e il controllo delle identità

Centralizza l'autenticazione, l'autorizzazione e la connessione alle risorse aziendali, applicando un modello Zero Trust: **ogni accesso viene verificato, autorizzato e monitorato.**
Anziché una serie di strumenti scollegati tra loro, la piattaforma offre:

- Un unico livello di policy che regola l'accesso alle risorse da parte di utenti e macchine.
- Un browser come vettore di accesso, che riduce al minimo l'impatto sul lato client.
- Telemetria e log di audit che alimentano i sistemi di valutazione del rischio e i processi di compliance.

PAM
PRIVILEGED ACCESS MANAGEMENT

Controllo degli accessi privilegiati con monitoraggio e tracciabilità delle attività.

ZTNA
ZERO TRUST NETWORK ACCESS

Zero Trust per una connettività sicura ovunque.

IAM
IDENTITY & ACCESS MANAGEMENT

Gestione delle identità e degli accessi con autenticazione e policy centralizzate.

Contesti di accesso

Dalla rete alle risorse: controllo puntuale e sicurezza continua

Oplon Secure Access supporta i requisiti di controllo degli accessi in diversi contesti operativi, consentendo una connettività sicura a sistemi e applicazioni senza affidarsi a un'ampia esposizione di rete.

Accesso a macchine e servizi

Gestisci l'accesso per macchine, servizi e carichi di lavoro automatizzati.
Sostituisci i segreti condivisi con un'autenticazione basata sull'identità e guidata da criteri.

Accesso di appaltatori e terze parti

Concedi agli utenti esterni e ai fornitori un accesso controllato e limitato nel tempo. Diminuisce l'esposizione con autorizzazioni circoscritte e scadenza automatica dell'accesso.

Accesso per i dipendenti

Accesso semplice a tutte le applicazioni tramite un'unica identità e con la semplicità di un browser.

Modernizza l'accesso legacy

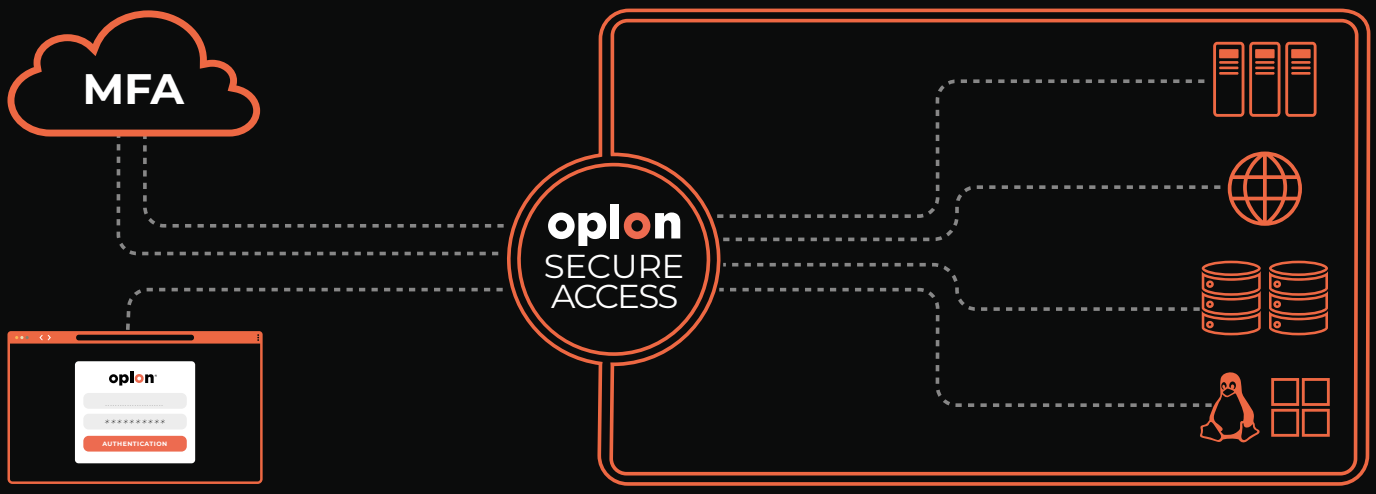
Proteggi le applicazioni legacy senza doverle riscrivere o sostituire.
Centralizza il controllo degli accessi e modernizza la fiducia in ambienti frammentati.

Accesso sicuro ai sistemi critici

Proteggi qualsiasi ambiente, database e sistema operativo. L'accesso è costantemente regolato da politiche rigorose.

Operazioni privilegiate sicure

Proteggi e gestisci l'accesso privilegiato ai sistemi critici. Ogni sessione è isolata, monitorata e completamente verificabile per impostazione predefinita.



Ambiti di applicazione

WEB APPLICATION

Accesso sicuro alle applicazioni web aziendali tramite MFA senza modifiche o integrazioni; OSA si interpone e gestisce tutto in modo trasparente.

REMOTE DESKTOP SERVICE ACCESS

Accesso via browser a desktop o applicazioni remote attraverso MFA integrato con sistemi esistenti (es. Active Directory) e basato su permessi utente.

REMOTE SHELL SERVICE ACCESS

Accesso SSH via browser con MFA senza inserire credenziali; gestione sicura delle password, funzionalità avanzate (file, copia/incolla) e logging completo delle attività.

Compliance

La soluzione Oplon Secure Access si distingue per la sua eccellenza nel garantire la conformità alle principali normative sulla sicurezza e protezione dei dati, come GDPR, NIST e NIS2.
Assicura la protezione dei dati personali, adotta le migliori pratiche di sicurezza e gestisce efficacemente i rischi, proteggendo le infrastrutture critiche e garantendo la continuità operativa.

Accesso sicuro per ogni caso d'uso

L'evoluzione dall'accesso di rete all'accesso alle risorse

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

Accesso remoto direttamente dal browser

Permette di accedere a sistemi, applicazioni e desktop direttamente dal browser, senza installazioni e senza VPN. Le risorse sono esposte in modo controllato e le sessioni sono protette, profilate e tracciate, semplificando la gestione degli accessi.

MFA for Legacy Applications

Autenticazione multifattoriale senza cambiare l'app

Estende l'autenticazione multifattore anche ad applicazioni legacy, senza interventi sul codice. Il secondo fattore viene applicato a livello di accesso, migliorando la sicurezza e riducendo i rischi legati alle credenziali statiche.

Remote Browser Isolation

Accesso web sicuro senza esporre le applicazioni

Le sessioni web vengono eseguite in un ambiente remoto isolato, con contenuti trasmessi all'utente senza rischio di codice malevolo. Questo approccio protegge da malware, ransomware e phishing, mantenendo applicazioni e sistemi non esposti verso l'esterno.

Identity Federation

Un unico livello di controllo per più fonti di identità

Consente di integrare sistemi di autenticazione esterni e utilizzare identità già esistenti. L'autenticazione federata è abilitata senza modifiche alle applicazioni, semplificando la gestione e garantendo accessi sicuri e coerenti.

Trusted Connection (no VPNs)

Connessioni sicure per applicazioni desktop

Consente di collegarsi a sistemi e servizi senza esporli direttamente, attivando connessioni solo quando necessario e verso risorse specifiche. Il modello è centralizzato, controllato e applicabile anche in ambienti IT/OT, integrandosi con strumenti esistenti.

Perché non usare le VPN?

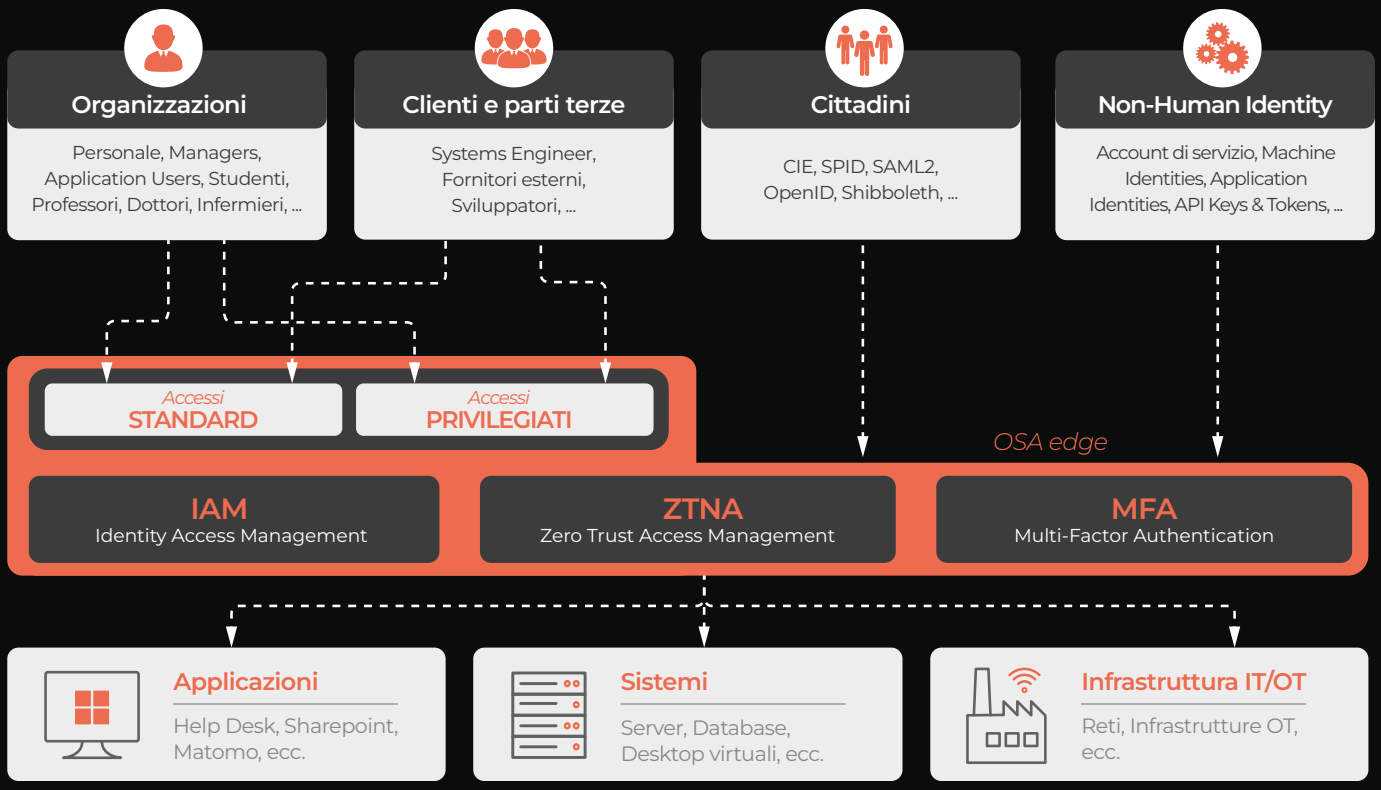
La sicurezza non è più nella rete. È nell'accesso.

Un modello di accesso a livello di risorsa consente al dispositivo di rimanere esterno alla rete aziendale, autorizzando l'accesso esclusivamente alle risorse necessarie e permettendo l'applicazione di politiche di sicurezza più granulari e precise.
Nei tradizionali modelli di accesso basati sulla rete, invece, la connessione tramite VPN comporta generalmente l'inserimento del dispositivo all'interno della rete aziendale, implicando criticità legate all'estensione della superficie di attacco, nonché una maggiore complessità operativa in termini di configurazione, gestione e manutenzione.

VPN / ACCESSI TRADIZIONALI	OPLON SECURE ACCESS
⊗ Accesso a livello di rete	✓ Accesso a livello di risorse
⊗ Ampia superficie di attacco	✓ Superficie di attacco minima
⊗ Fiducia statica	✓ Verifica continua
⊗ Visibilità limitata	✓ Tracciabilità completa

Livelli di sicurezza dell'accesso

Un'unica piattaforma per gestire identità, accessi e risorse



oplon®

Per saperne di più, visita il nostro sito
https://www.oplon.net
o scrivici a **info@oplon.net**

Oplon Networks è una società di ingegneria informatica nata nel 2010.
La mission è creare prodotti e servizi per garantire alta affidabilità e sicurezza a livello infrastrutturale nell'erogazione dei servizi, con standard qualitativi straordinari.
Realizziamo soluzioni per proteggere accessi, infrastrutture e servizi critici.
Per questo sviluppiamo strumenti di cybersecurity e soluzioni integrate per presidiare i moderni Data Center, Network, Cloud e Hybrid Cloud.

Sistema di gestione qualità certificato ISO/IEC 27001:2022 e UNI EN ISO 9001:2015
Dati e caratteristiche possono variare in qualsiasi momento senza alcun obbligo di preavviso.