opensystems

ZERO TRUST NETWORK ACCESS (ZTNA)

Provide users on any device, anywhere, secure access to any application or resource.

## Provide secure access to anyone anywhere

Access control lags behind today's business and security needs
The cyberattack surface of organizations has grown significantly with the shift to the cloud, the dispersion of work locations and new access scenarios. User authentication hurdles for remote users and partners limits their productivity and creates security gaps, while being complex to manage and slow to provide.

ZTNA makes access control secure, flexible, and simple to manage
ZTNA architecture follows an adaptive trust model, operating on a need-to-know, least-privilege basis. Only authenticated and authorized users, endpoints, and applications are granted access to resources. Access is managed centrally, and is policy-based and granular, ensuring flexibility and security.

Never trust, always verify
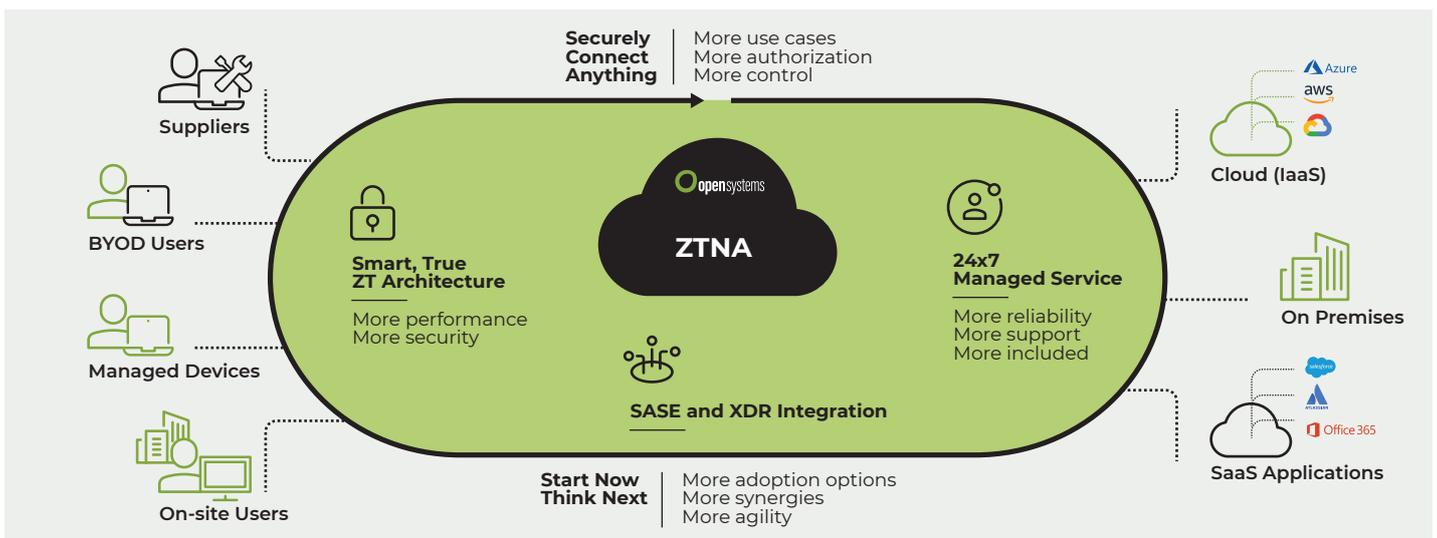
Enable any user using any device in any location to securely access corporate applications

Why choose ZTNA by Open Systems?

CONNECT EVERYTHING SECURELY

Open Systems ZTNA can be agentless or agent-based to provide flexible and secure access to new users, sites, and partners using any device, anywhere in the world. A single interface manages access to any type of corporate application anywhere.

SMART, TRUE ZERO TRUST ARCHITECTURE

Open Systems offers integrated smart routing via cloud-based ZTNA PoPs, ensuring higher performance. By separating the identity provider (IDP) and ZTNA enforcement points, available on-prem or in the cloud, the impact of a compromised ZTNA cloud can be minimized.

24X7 FULLY MANAGED SERVICE

Open Systems ZTNA is delivered ready to go, with all the required capabilities and operational functionalities to start using it today. The customer portal provides insights into status, policy controls, and the monitoring you need for reliable operations.

Zero Trust Network Access (ZTNA)

Open Systems ZTNA features

- Agentless cloud solution
- HTTP(S), RDP, SSH
- Self-Service

- Agent-based solution also available
- Cloud and on-prem, any application
- Fully managed service available

Users, Devices

Any User

Any Device

Any Location

Identity

Device

ZTNA

Endpoint Verification

Risk

Location

Time

Other Contexts

IaaS, on-prem, SaaS

Azure aws
Cloud

Data Centers

Office 365
SaaS Applications

Apps, Desktops, Servers

Corporate Applications

Servers

Remote Apps & VDI

Files

Legacy Applications

Data
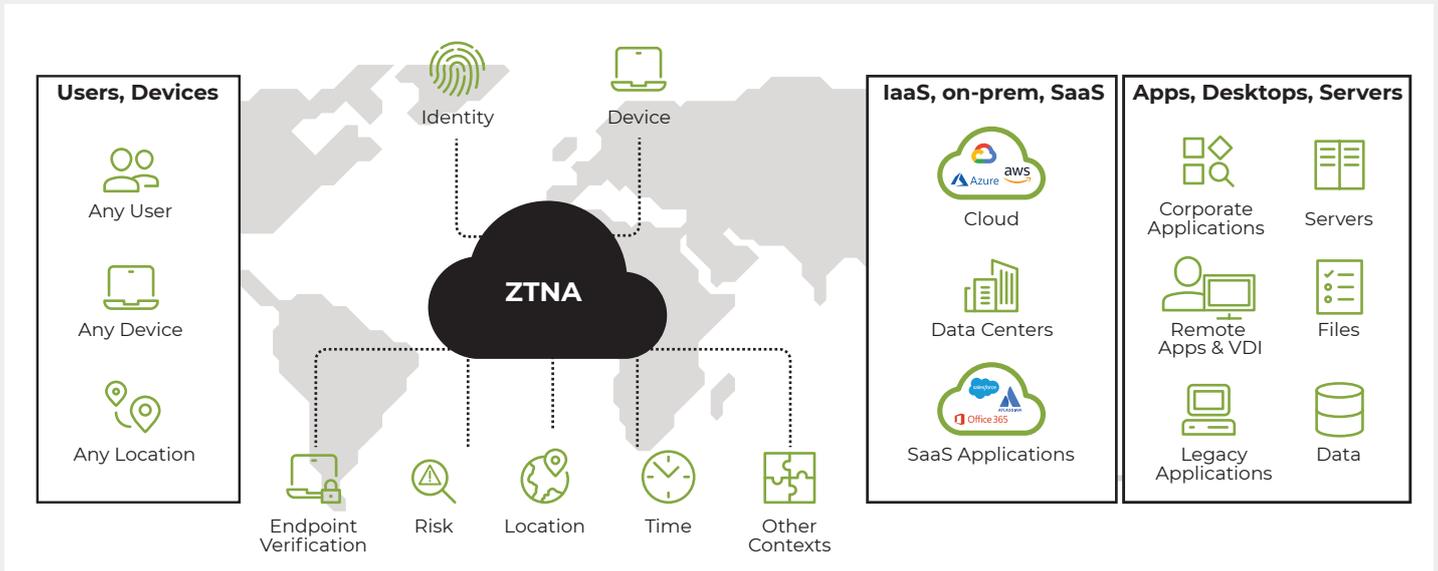
SERVE EVERY USER

- Agentless or agent-based to include all your users
- For agent-based: enforce encryption on all traffic going via ZTNA and add a Secure Web Gateway

RANGE OF POLICY OPTIONS

- Enrich authentication using credentials, certificates, and MFA
- Set policy by factors including user group, device posture, and NDR-provided risk score

ACCESS ALL APPLICATIONS

- Ensure short paths and place enforcement points near your apps
- Control access to corporate SaaS, cloud-based and on-premises applications

---

Start reinventing how you deliver network and security as a complete service from the cloud

Integrate Open Systems ZTNA with our cloud-based SASE (Secure Access Service Edge) services. Begin your SASE journey with ZTNA and add other Open Systems services, such as SWG, SEG, MEP, Firewalls, and CASB, as needed. You can conveniently manage all these services from a unified interface. Additionally, leverage NDR (network detection and response) risk data to enrich access control, authentication and security.

Oopen systems

Open Systems connects and protects users, apps, and data everywhere they live with a comprehensive, unified easy-to-use technology platform combined with an excellent 24x7 Managed SASE service.