

ZERO TRUST NETWORK ACCESS (ZTNA)

Sicherer Zugriff auf alle Unternehmens-Ressourcen: Für jeden Benutzer, auf jedem Gerät und an jedem Ort.

Sicherer Zugriff für alle – überall

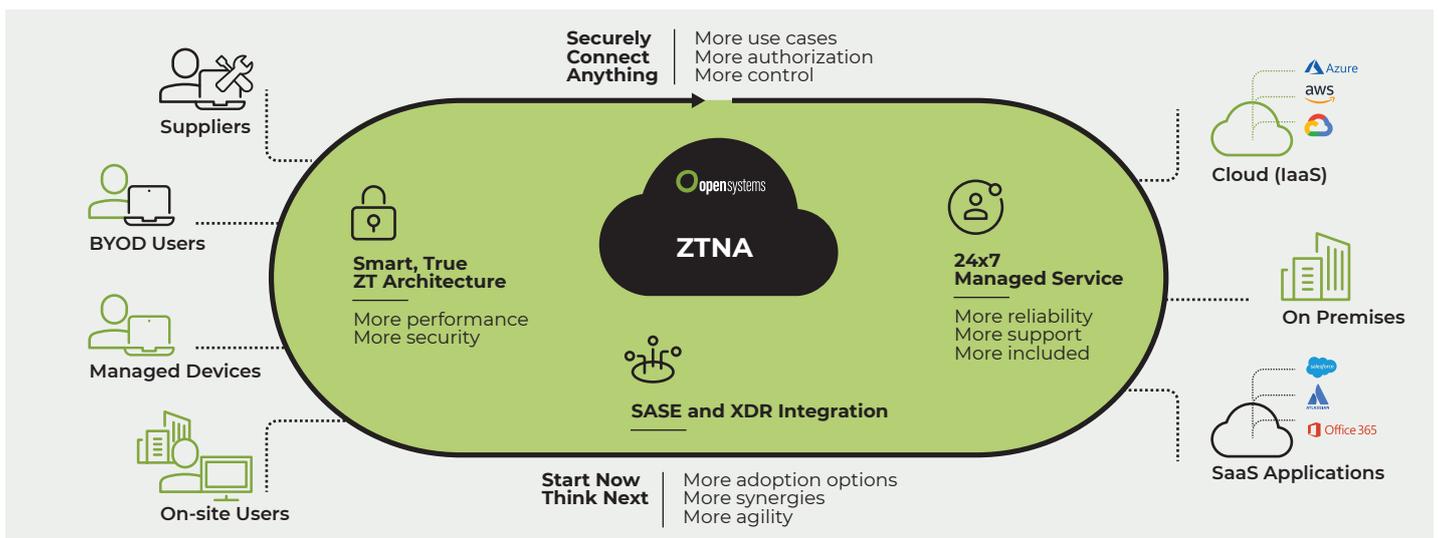
Zugangskontrolle hinkt den Anforderungen hinterher

Die Angriffsfläche ist mit dem Wechsel in die Cloud und den neuen Arbeitsweisen deutlich grösser geworden. Hürden zur Authentifizierung von Benutzern und Partnern beeinträchtigen die Produktivität und schaffen Sicherheitslücken. Gleichzeitig ist die Zugangs-Verwaltung komplex und die Bereitstellung träge.

ZTNA macht die Zugriffskontrolle sicher, flexibel und einfach zu verwalten

Die ZTNA-Architektur folgt einem flexiblen Vertrauensmodell. Benutzer, Endpunkte und Anwendungen müssen authentifiziert und autorisiert sein, um Zugriff zu erhalten. Die zentrale Verwaltung ist richtlinienbasiert und granular, was Flexibilität und Sicherheit gewährleistet.

Never trust, always verify



Ermöglichen Sie einen sicheren Zugriff auf Unternehmens-Ressourcen – für jeden Benutzer mit jedem Gerät an jedem Ort.

Warum ZTNA von Open Systems?

ALLES SICHER VERBINDEN



Open Systems ZTNA (agentless oder agent-based) ermöglicht allen Benutzern und Partnern, von allen Standorten einen flexiblen und sicheren Ressourcen Zugang – egal welches Gerät verwendet wird. Der Zugriff auf Anwendungen wird über ein gesamtheitliches Interface verwaltet.

ZERO TRUST ARCHITEKTUR – CLEVER UND SICHER



Open Systems bietet integriertes Smart-Routing über cloudbasierte ZTNA PoPs für schnellere Verbindungen. Identitätsprovider (IDP) und ZTNA Enforcement-Punkte werden getrennt, um die Auswirkungen einer ZTNA-Cloud-Kompromittierung zu minimieren.

24X7 VOLLSTÄNDIGER MANAGED SERVICE



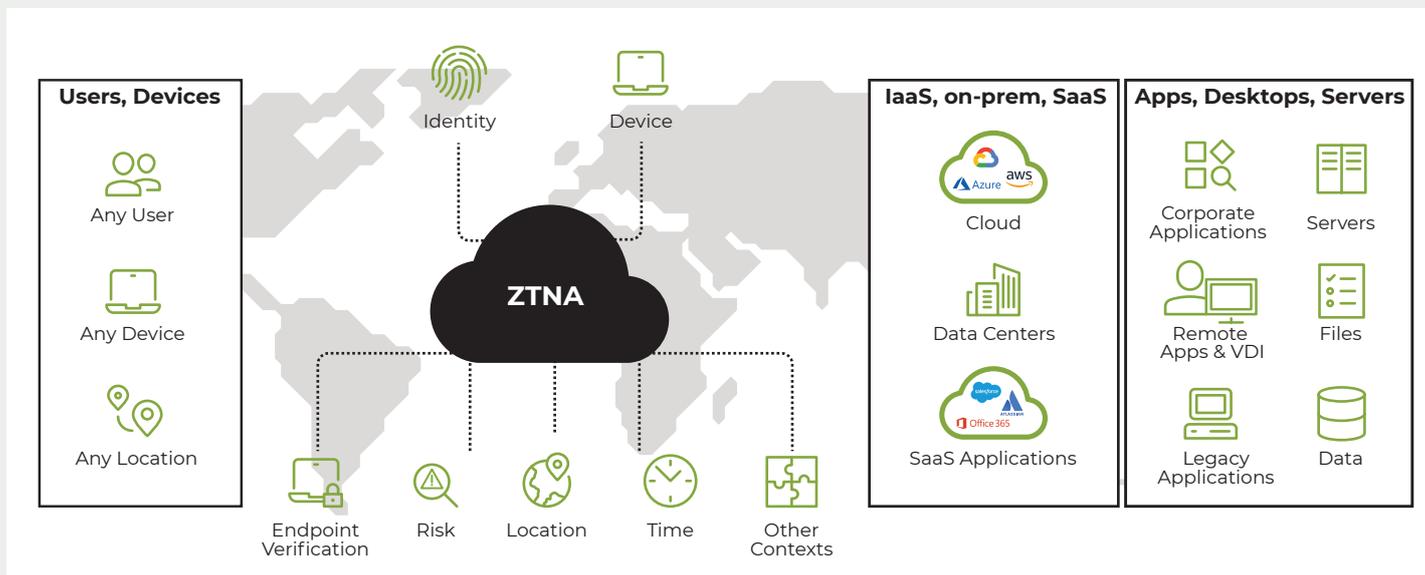
Open Systems ZTNA wird fixfertig geliefert, mit allen erforderlichen Fähigkeiten und Betriebsfunktionen, für den sofortigen Einsatz. Zudem liefert das Kundenportal Status, Zugriffskontrolle und ständige Überwachung für zuverlässigen Betrieb.

Zero Trust Network Access (ZTNA)

Open Systems

ZTNA Roadmap

- Agentless Cloud Lösung
- HTTP(S), RDP, SSH
- Self-Service
- Agent-based Lösung verfügbar
- Cloud oder On-Prem, jede Applikation
- Vollständiger Managed Service verfügbar



FÜR JEDEN BENUTZER



- Agentless oder Agent-based, um all Ihre Benutzer abzudecken
- Agent-based: Verschlüsselung des Datenverkehrs via ZTNA erzwingen und ein Secure Web Gateway hinzufügen

VIelfÄLTIGE POLICY OPTIONEN



- Erweitern Sie die Authentifizierung mit Anmeldedaten, Zertifikaten und MFA
- Richtlinien nach Benutzergruppe, Gerätestatus und NDR-Risikoeinstufung

ZUGRIFF AUF JEDE APPLIKATION



- Kurze Wege indem Enforcement-Punkte nahe an Ihren Anwendungen sind
- Kontrolle über Zugriff auf unternehmenseigene SaaS-, cloudbasierte und lokale Anwendungen

Neu definiert: Netzwerk und Sicherheit als vollständiger Service aus der Cloud

Integrieren Sie Open Systems ZTNA mit unserem cloudbasierten SASE-Service (Secure Access Service Edge). Starten Sie Ihren Weg zu SASE mit ZTNA und fügen Sie weitere Services von Open Systems (SWG, SEG, MEP, Firewalls, CASB) unkompliziert hinzu. Sie können alles über ein gesamtheitliches Interface verwalten. Zudem können Sie NDR-Risikodaten (Network Detection and Response) für eine verbesserte Zugriffskontrolle, Authentifizierung und Sicherheit nutzen.



Open Systems verbindet und schützt Nutzer, Apps und Daten mit einer umfassenden, einheitlichen und benutzerfreundlichen Technologieplattform sowie einem ausgezeichneten 24x7 Managed SASE Service.