ZERO TRUST NETWORK ACCESS (ZTNA)

Provide secure access to any corporate application for users on any device, anywhere.

Secure access. Anywhere. Anytime.

Open Systems ZTNA enables an adaptive trust model that operates on a need-to-know, least privilege basis to ensure that only authenticated and authorized users, endpoints, and applications are granted access to resources. Access is managed centrally, and is policy-based and granular, allowing for flexibility without sacrificing security.

Architecture

Delivered with the following architecture components:

- **ZTNA Cloud Points of Presence (PoPs)**: Smart, shortest path routing, where traffic is forwarded to the enforcement point closest to the requested app
- **ZTNA Enforcement Points (EPs)**: Access control points according to ZTNA policy, where the decision is made to provide access

Policies

Policies determine under which circumstances users get access based on user authentication and target application:

- **Authentication**:
  - Various identity Provider (IdP) connection options for user authentication (SAML, OIDC, LDAP, RADIUS)
  - Device authentication based on TLS client certificates
  - Multi-factor authentication (MFA)
- **Authorization based on context**:
  - Location
  - Time
  - Device posture[1]
  - Risk score[1] (from Open Systems NDR)

For authentication, Open Systems ZTNA can leverage any cloud IdPs that support SAML or OIDC protocols such as Azure AD and Okta as well as on-premises identity systems that support LDAP or RADIUS such as Active Directory. The service supports multi-factor authentication (MFA), and can check device certificates.

Once authenticated, users and devices are evaluated by authorization policies to see if they are allowed to access specific applications. It will be possible to enhance authorization policies with additional conditions and contexts such as location, time, device posture, etc. by integrating with external systems such as IdPs, MDMs, XDR, etc.).

1 Initial integration cost (via API) might apply

Applications
Access to any app, anywhere: • On-prem apps and resources • Apps in IaaS (e.g. Azure, AWS, GCP) • Corporate SaaS (for initial access control) The following prerequisites are necessary: • Wildcard certificate for customer domain • IdP integration (SAML, OIDC, LDAP, RADIUS)

ZTNA Packages

Two ZTNA packages are available:

- **ZTNA Entry:** Designed as a modern replacement for traditional VPN access.
- **ZTNA Full Access:** Delivers the complete set of advanced ZTNA capabilities for granular, identity- and context-aware access control.

Access Control

Feature	Description	ZTNA Entry	ZTNA Full Access
Identity-based access	Access is granted based on user identity from an identity provider.	✓	✓
Role- and group-based access control	Access decisions are tied to organizational roles or groups (e.g. HR, Finance).	✓	✓
Granular least-privilege access enforcement	Applies access enforcement to private apps, services and devices (per app/service or network/IP) using concept of least privilege.	✓	✓
Conditional access policies	Applies rules based on location, time, device health etc. to allow or block access.	✗	✓
Certificate-based conditional access	Uses device certificates to verify trusted endpoints (especially in high-security orgs).	✗	✓
Continuous conditions assessment	Monitors sessions in real time and can revoke access if conditions change.	✗	✓
Device posture checks	Evaluates device compliance (e.g. OS version, antivirus, EDR) before granting access.	✗	✓
Just-in-time (JIT) access	Grants temporary access for limited duration (e.g. contractors, support staff).	✗	ZTNA Audit Module
Supervisor mode	Provides live insights into active RDP, VNC and SSH sessions.	✗	ZTNA Audit Module
Session recording	Records RDP, VNC and SSH sessions for future review.	✗	ZTNA Audit Module

Identity and Authentication

Feature	Description	ZTNA Entry	ZTNA Full Access
Federated Single Sign-On (SSO)	Enables users to log in once and access multiple apps without repeated authentication.	✓	✓
Identity Federation/Integration with Major IdPs	Supports third-party identity providers (IdPs) like Entra ID, Okta, Ping, Google and other OIDC capable IdPs.	✓	✓
Multi-Factor Authentication (MFA)	Adds an extra layer of verification (e.g. phone prompt, token) to prevent unauthorized access.	✓	✓
Certificate-based Authentication	Allow users to access chosen applications seamlessly with device-certificate authentication (e.g. SWG).	✓	✓

Connectivity and Applications

Feature	Description	ZTNA Entry	ZTNA Full Access
Agent-based Access (Client)	Uses an installed agent on the enduser device or server to enable deeper control, device posture checks, and full app support. Allows access to web-based as well as any TCP-/UDP-based applications.	✓	✓
Agentless Access (Browser-based)	Lets users access apps via browser without installing a client, ideal for BYOD and third parties. Supports web-based access to SSH, RDP, VNC, HTTP, HTTPS, SMB or Telnet applications.	✗	✓
Private App Access	Provides secure access to internal (non-public) applications hosted on-prem or in the cloud.	✓	✓
SaaS App Integration	Extends policy and access control to cloud apps like Salesforce, Google Workspace, etc.	✓	✓
Trusted Network Detection	Automatically detects when a user is on a predefined trusted network (e.g. corporate LAN) and adapts access policies, bypassing ZTNA to allow direct access for certain traffic.	✓	✓
Custom Domain/Application Discovery	Automatically discovers new apps, IPs, or services requiring ZTNA policies.	✗	✓

Modules

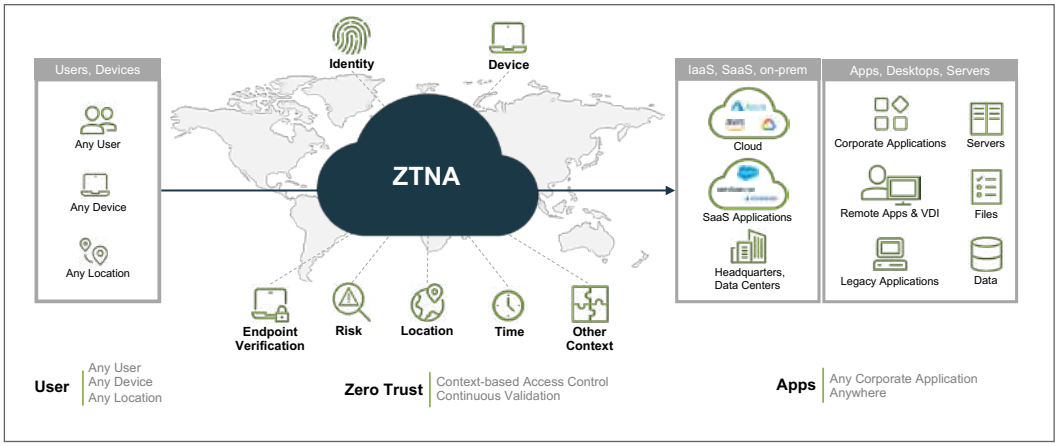
ZTNA Audit

- Just-in-time access provisioning: admit access to corporate apps based on request
- Supervisor mode: get live insights into active RDP, VNC and SSH sessions
- Session recording: record RDP, VNC and SSH sessions for future review

The retention time of the session recordings depends on the number and length of the recordings. Mission Control reserves the right to delete old recordings in case they affect the availability of the service.

Benefits of ZTNA

ZTNA is a security architecture where only authenticated and authorized users and endpoints are granted access to corporate applications.



Open Systems ZTNA: managed service, with central, identity-based access policies to connect any user, with any device to any app anywhere.

- **Connects everything securely**
  ZTNA provides secure conditional access to corporate applications anywhere to various users (employees, contractors, partners) using any device, anywhere in the world.
- **Smart architecture**
  Open Systems offers integrated smart routing via cloud-based ZTNA PoPs, ensuring higher performance.
- **Truly zero trust**
  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**
  ZTNA is delivered ready to go, with all the required capabilities and operational functionalities to start using it today. The Mission Control Portal provides insights into status, policy controls, and the monitoring companies need for reliable operations.

The Open Systems ZTNA Cloud is built to be highly available and resilient, ensuring seamless automated failover within and across cloud regions.

Service Management

For every service, Open Systems delivers flexible technology, maximum transparency, and around-the-clock network security and monitoring. It's an intrinsic part of a high-reliability organization. Service Management closes the gap between security policy and operations, and reduces complexity. The service fee includes the following.

ZTNA Cloud (PoPs)

- Global coverage
- Managed and monitored by Open Systems
- No traffic interception in the ZTNA Cloud

Deployment models

- Fully SaaS, VMs, on-prem hardware, or a hybrid combination
- Built-in redundancy and geo-distribution for reliable and performant access
- Deploy on-prem PoP (VM or hardware) to improve the user-to-application latency or for compliance reasons
- Deploy Enforcement Points (VM or hardware) on premises, in your data center or in the cloud close to your private applications to enforce a secure channel between the users and the apps

24x7 Operations

Highly skilled certified engineers in Mission Control monitor your systems proactively, ensure compliance with your security policy and work according to clearly defined processes in order to review and perform global changes that are driven by the dynamic needs of your organization.

After extensive testing procedures, all required security updates and patches are installed on a regular basis, always keeping the systems up to date. The device is capable of booting different releases, which facilitates an effective fallback and rapid recovery if required. All environment-specific configurations are automatically generated, based on the configuration database operated by Mission Control. This is an essential part of an efficient disaster recovery process because it makes it possible to generate and reinstall an identical configuration in a very short time.

Installation

- Definition of architecture and technical configuration
- Definition of the administrative contacts and escalation procedures
- Preconfiguration, delivery and functional verification tests of the Open Systems service with all required hardware and software components

24x7 monitoring

- 24x7 proactive monitoring, event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Mission Control Engineers

Change management

- Self-service tools in the Mission Control Portal empower administrators to configure policies and change requests themselves
- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures
- Review of change requests by Mission Control Engineers, clarifications and feedback in case of hidden risks
- Strong user authentication with audit trail

Troubleshooting and maintenance

- Real-time auditability with integrated ticketing system
- Debugging of incidents within the periods defined in the SLA
- Replacement of defective or outdated hardware and restoring of functionality
- Analysis, testing and installation of software patches and upgrades
- Predefined disaster recovery processes

Reporting and logging

- Dashboards provide extensive visualization of users, devices, applications and sessions
- Analytics tools give full visibility into all ZTNA session details through log exploring tools
- SIEM integration allows you to consume events via Logs API and feed into third-party tools for correlation, alerting, and response automation

Coverage of technology risk

- Hardware and software are replaced free of charge if defective, outdated or if the quality or availability of the implemented systems are no longer guaranteed by the manufacturer

Co-Management via Mission Control Portal

Configuration of new corporate applications and ZTNA policy management is done via the Mission Control Portal. Lightweight agent upgrade and rollout is included, as well as permission management of your admin users. Operations include monitoring, troubleshooting, configuration and certificate management. Reports and tools that support the implementation and management of global IT security and availability are part of the service.

- Configuration of new corporate applications
- Permission management of customer admin users
- ZTNA security policy management
- Real-time monitoring and reporting
- Operations: monitoring, troubleshooting and configuration management

The state-of-the-art web portal makes it easy to communicate with Mission Control. The portal provides transparency over your network and applications in real time, including reports and tools that support the implementation and management of global IT security and availability.

For more information, see the **Service Management** fact sheet.

Open Systems is certified for ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

HIPAA Compliance Verified by VanRein Compliance 2025

Note: Due to the licensing and export restrictions of our technology suppliers, we are not permitted to provide services in certain sanctioned countries. The specific countries affected depend on each supplier's compliance requirements. We therefore refer to the respective suppliers' license terms, which may also apply to end users.