OPEN SYSTEMS
MANAGED SASE

SASE was step one. We run security.

OPEN-SYSTEMS.COM

Modern IT is distributed. Making it work reliably is the real challenge today.

Modern enterprises are distributed. Locations, users, partners and resources are no longer tied to a central place; they are global and cloud-based. Work and access happen everywhere.

This has fundamentally changed traffic flows, dependencies and operational complexity. What used to be predictable is now dynamic; what used to be local is now global. The bottleneck is rarely architecture; the bottleneck is operation.

If you are responsible for such an environment, the challenge is no longer architectural. It is operational. Running network and security across global, hybrid environments requires specialized expertise and continuous coordination across providers, platforms, and teams. Ensuring performance, maintaining security, and resolving incidents quickly becomes increasingly complex as scale increases.

Those who are accountable
Your Operational Questions

?

Do we have enough skilled staff to run networking and security across global hybrid environments at enterprise level?

?

Is 24×7 coverage with senior expertise realistically achievable?

?

How fast can incidents be resolved when multiple parties are involved (ISPs, security tools, cloud/SaaS providers, internal teams)?

This is where complexity shifts from architecture to execution.

You don’t need another layer of technology. You need a model that brings connectivity, security, and operations together and takes responsibility for how they perform in reality.

That’s exactly where Open Systems comes in.

Open Systems delivers **Unified Managed SASE**, combining connectivity, security, and 24×7 operations into one accountable model. So that security is not just implemented, but continuously operated and optimized.

One platform.
One network.
One operating model.

Modern SASE environments operate across three tightly connected layers:
Network, Security, and Operations.

The network layer determines how traffic moves. The security layer determines how access is controlled. The operations layer determines whether everything works, continuously.

Managing these layers separately creates fragmentation, leading to inconsistent policies, limited visibility and operational gaps.

They need to be designed and run as one system.

Networking
Global Connectivity (Backbone + Last Mile)
- 500+ PoPs
- 180+ countries
- SLAs (latency, jitter, packet loss)
- ISP sourcing & lifecycle

SD-WAN
- Application-aware routing
- Dynamic path selection
- Integrated failover

Security
Cloud Security (SSE)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS)

Zero Trust Architecture
- Identity-first access
- Continuous verification
- Granular segmentation

Managed Services – "Mission Control"
24×7 Mission Control ï Real-time monitoring ï Incident- & Change-Management ï Policy enforcement ï Continuous optimization

SD-WAN optimizes traffic. Connectivity determines performance. Operations make it reliable.

If the underlying network suffers latency, packet loss and/or instability, application performance degrades, regardless of architecture.

The Open Systems Network Layer

Global Backbone Connectivity (Open Systems)
Private backbone connectivity with 500+ PoPs; SLAs for availability and traffic quality (e.g., latency, jitter, packet loss), plus automatic healing and intelligent routing.

Result: *More stable application performance globally – less "internet randomness" on critical paths.*

Last Mile Connectivity
ISP sourcing and lifecycle management as a service, including centralized control and simplified provider coordination.

Business impact: *Less operational effort per site; reduced vendor friction.*

Line Operations Service (LOS)
24×7 monitoring of access lines including triage, ISP ticket handling, tracking until resolution, and bandwidth analytics in the portal.

Faster remediation *– internal teams don't have to act as an "ISP call center".*

The Open Systems Security Layer

ZTNA:
Identity and context based access to applications as a modern alternative to wide open VPN access.

Reduces attack surface and simplifies secure access for employees and partners.

SWG:
Secure web access through policy enforcement and threat protection for web traffic.

Protects users everywhere – in the office, on the road, or remote.

CASB:
Governance and control over SaaS usage (visibility, policies, risk management).

Reduces shadow IT risk and supports compliance.

Firewall Services:
Centralized firewall functionality as a service, consistent across users and locations.

Standardizes security baselines and reduces appliance overhead.

Reporting & Compliance Support:
Transparency, reporting, and processes that enable audits.

Eases proof and reduces operational friction.

Architecture defines potential. Operations define reality.

The Open Systems Managed Service

What used to be a design problem has become an execution problem. Today's reality: Day-to-day operations dominate with tickets, changes, escalations and provider coordination.

As a result, strategic initiatives are pushed aside, and IT becomes reactive instead of driving the business forward.

Enter Mission Control:
24×7 End-to-End Operations

- Follow-the-sun operational model
- Global team of expert level3-engineers
- Real-time monitoring across network + security layers
- Proactive issue resolution

What We Run for You

Connectivity Operations

- ISP sourcing and lifecycle management
- Single point of contact
- Unified billing and vendor abstraction
- 24×7 monitoring and incident handling

Security Operations

- Policy management and optimization
- Threat detection and response
- Change management and configuration
- Compliance support and reporting

Why This Matters

Most environments don't fail by design, they fail in execution: Performance degrades, incidents take longer to resolve, and responsibility becomes unclear across providers and tools. Not because the architecture is wrong, but because it is not operated as one system.

SASE doesn't remove these dependencies; it makes them visible and critical.

From complexity to control

The Open Systems Approach

Platform + Connectivity + Operations

- Architecture defines how traffic should flow
- Connectivity determines how it can flow
- Operations ensure it actually works

Proof Point: Over 10,000+ globally managed deployments, continuously optimized across backbone and edge.

Strategic Positioning

The industry focused on what to deploy. The real challenge is how security runs:

- Across networks
- Across clouds
- Across regions

What customers gain

End-to-end accountability
One provider across connectivity, security, and operations with clear ownership and consistent execution.

Performance and reliability
Optimized traffic paths, stable connectivity, and consistent user experience, globally.

Faster response
Incidents are resolved faster through standardized processes and 24×7 operations.

Operational focus
Less time spent on coordination and maintenance - more capacity for strategic initiatives.

Full visibility
End-to-end observability across users, traffic, and security, in real time.

Regulatory alignment
Built to support evolving requirements such as NIS2, DORA, ISO 27001, and SOC 2.

SASE was step one. **Now it has to work.**

We make sure it does.

LET'S TURN YOUR IT INFRASTRUCTURE INTO REAL SECURITY, END-TO-END.

About Open Systems

Open Systems is the leading European provider of co-managed SASE and Zero Trust operating models, helping enterprises and organizations securely operate complex hybrid and multi-cloud environments. Founded in 1990 and headquartered in Switzerland, the company generates over USD 100 million in annual revenue and protects global enterprise customers with more than 100,000 employees across operations globally.

Open Systems combines cloud-native networking and security with transparent, co-managed 24×7 operations to close the execution gap many organizations face when deploying modern architectures. As a European alternative to US- and Israel-based security providers, Open Systems places strong emphasis on regulatory alignment, operational visibility and shared responsibility, enabling secure, reliable and scalable network and security operations in an increasingly distributed IT landscape.