

OPEN SYSTEMS SASE EXPERIENCE

The Open Systems SASE Experience Advantage:

- Improved user experience.
- Simplified network access.
- Increased availability.
- Enhanced security.
- Enabled remote workforces.
- Higher end-user productivity.
- Better visibility and control across hybrid environments and teams.
- Faster incident response.
- Lower cost and complexity.

Secure Access Today and Tomorrow

Open Systems SASE Experience eliminates complexity of secure global access and network management, while providing easy and comprehensive global support. Simply put, Open Systems provides a better user experience while enabling secure global access to anyone, anywhere so customers can focus on other business priorities.

Balance Security and Performance

Today's challenges include remote and hybrid workforces, applications and data in the cloud and on premises, shadow IT, branch offices, as well as global threats and malware.

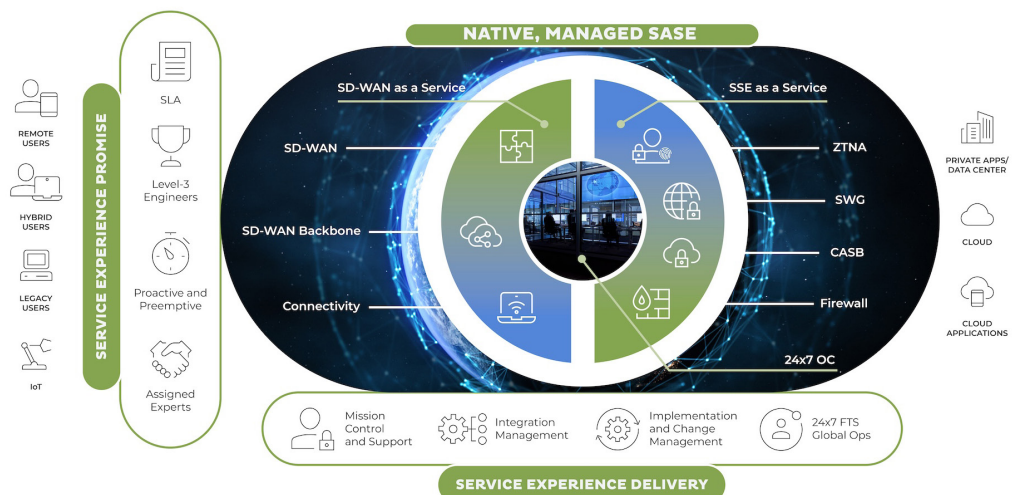
In this complex business environment, it's difficult to ensure secure remote and onsite access from anywhere at any time. Modern organizations are under pressure. Often with small teams and limited budgets, network and security teams are struggling to secure the IT environment without slowing down productivity.

Move to the Service Edge

Converging network management and security into a single architecture is one proven way to enhance visibility and control, enable dynamic management, and secure access to data and applications anywhere. Secure Access Service Edge (SASE) – a category defined by [Gartner](#) – is a comprehensive network security and connectivity solution. It combines network security (e.g., secure web gateway, firewall, zero trust network access) and wide-area networking (SD-WAN) into a single cloud-based platform. But for some CIOs, it may still be out of reach because of its complexity.

Improve your SASE Experience

Open Systems takes a revolutionary approach to secure network access: Open Systems SASE Experience. It delivers all the benefits of SASE, but with an exceptional service delivery experience. SASE Experience is ideal for enterprises globally who are struggling with the resources to do it all. It simplifies the acquisition, implementation and management of a comprehensive, unified platform that enables consistent, resilient, and secure access to users, applications, and data across IT and OT cloud, on-premises and hybrid environments.



This approach empowers businesses to navigate today's secure access challenges with confidence, supercharging their secure access success and leading them toward a transformative and safer future.

Open Systems SASE Experience is more than a managed solution; it's a comprehensive and unified approach that provides unparalleled ease of use and a great experience, backed by 24x7 expert operations and support. It frees you from the operational overhead of appliance purchases, installation, and maintenance, to minimize staffing costs, and provide a fast ROI.

Simply put, Open Systems provides a better user experience while enabling secure global access to anyone, anywhere so customers can focus on other business priorities.

Our Promise

Open Systems provides peace of mind with 24x7 monitoring, incident handling and change management provided by expert engineers. Open Systems SASE Experience delivers a dependable, tailored, and secure offering that goes beyond mere promises to tangible, measurable results.



SASE Experience is designed to deliver reliable, secure access globally. It enables organizations to remain agile, resilient and secure to maintain operational continuity and security as businesses (and threats) evolve. It ensures customers have full visibility and a full overview of the entire hybrid IT environment to ensure escalations are kept to a minimum. This offering is comprised of:

- Personalized services and support from level-3 analysts.
- **SD-WAN**: Simplify network and security operations with edge-to-edge software-defined network.
- Connectivity Services: Backbone services ensure application performance no matter where the users and apps are located.
- **ZTNA**: Provide flexible, secure access to anyone, anywhere – from global offices to remote workforce.
- **Secure Web Gateway**: Protect yourself from web threats, enforce business policies, and confidently control web traffic globally.
- **CASB**: Gain visibility and control across cloud applications – even Shadow IT with continuous discovery and monitoring of cloud applications.
- **Firewall**: Stop external threats and prevent unauthorized lateral movement with a firewall service tailored to your needs.
- **Advanced Threat Protection**: Protect data and block malicious URLs, domains and IPs with high quality and zero-hour threat intelligence feeds and active IOC feed management.

“Open Systems helped GEA transition from MPLS to SASE, and they’ve been a valuable, collaborative partner during our move to the cloud.”

Request a Demo

For organizations who need to connect and protect users, apps, and data everywhere, Open Systems SASE Experience combines a security and networking technology platform with an award-winning 24x7 managed service to deliver a comprehensive, unified, easy-to-use solution that meets you where you are on your cloud journey.



Open Systems simply connects and secures hybrid environments so companies can focus on meeting their business goals. The Open Systems SASE Experience helps reduce risk, improve efficiency, and accelerate innovation with a comprehensive, easy-to-implement and use combination of SD-WAN and Security Service Edge delivered as a Service with a superior user experience. That’s our Service Experience Promise.

Provide reliable connectivity
anywhere, even in difficult
locations for cloud
and WAN traffic

Connectivity hurdles of global organizations

Private backbones bring stability and performance

100 Cities

The map displays 100 cities, each represented by a green dot and a label box. The cities are distributed across the world, with a high density in North America and Europe. The following table lists the cities shown on the map:

City	City	City	City	City
Council Bluffs	Des Moines	Milan	Oshawa	Berlin
Cheyenne	Chicago	Toronto	Montreal	Frankfurt
Vancouver	Seattle	The Dalles	Portland	Phoenix
Salt Lake City	San Francisco	Palo Alto	Santa Clara	San Jose
Los Angeles	East Los Angeles	Las Vegas	Querétaro	Monterrey
Mexico City	Dallas	Miami	Bogotá	Santiago
São Paulo	Vinhedo	Atlanta	Berkeley County	Richmond
Virginia	Ashburn	Hampton	Washington DC	Columbus
NewPort	New York City	New York East	Jersey City	Manchester
Dublin	Amsterdam	Utrecht	Cardiff	London
Gent	Saint-Ghislain	Paris	Madrid	Marseille
Milano	Turin	Jeddah	Riyadh	Dubai
Doha	Mumbai	Pune	Begaluru	Chennai
Bangalore Urban	Kuala Lumpur	Singapore	Jakarta	Manila
Sydney	Canberra	Melbourne	Hong Kong	Guangzhou
Shenzhen	Shanwei	Changhua	Hangzhou	Shanghai
Tokyo	Osaka	Busan	Chuncheon	Seoul
Qingdao	Beijing	Hebei	Novosibirsk	Moscow
Saint Petersburg	Hamina	Helsinki	Gävle	Oslo
Stockholm	Warsaw	Zurich	Petah Tikva	Alexandria
Manama	Nanjing	Chongqing	Chengdu	Abu Dhabi
Tel Aviv	Jerusalem	West Jerusalem	Rosh Haayin	Novosibirsk

Global Backbone Connectivity, Product Brief by Open Systems ©2025, proprietary

Why choose Global Backbone Connectivity by Open Systems?

500+ PoPs



Open Systems is the only SASE provider capable of leveraging more than 500 PoPs around the world. This gives unprecedented coverage for better WAN performance. Also, because the PoPs are strategically located near SaaS providers, it offers reliable connections to cloud apps worldwide.

HIGHLY RESILIENT



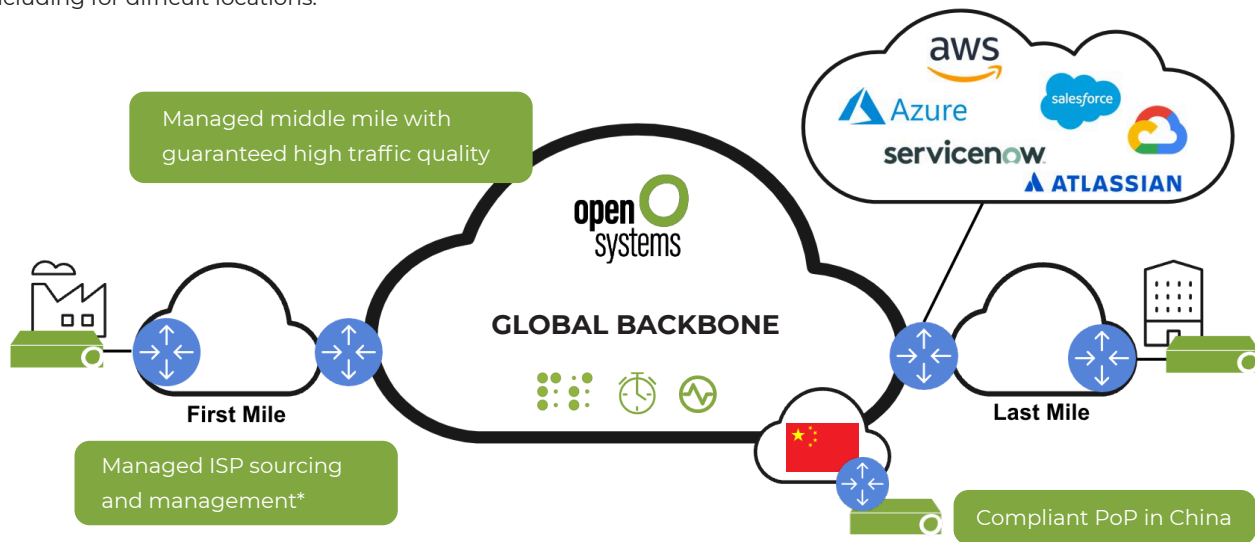
Open Systems' platform features automatic healing, intelligent routing and end-to-end SLAs so that organizations can benefit from guaranteed traffic quality anywhere in the world.

VERSATILE



Global Backbone Connectivity offers flexible settings for controlling how much bandwidth you need, and which applications can leverage it. And it works in difficult locations.

Open Systems ensures excellent **traffic quality** in the backbone, minimizing **packet loss, latency and jitter**, and provides end-to-end SLAs including for difficult locations.



*Available through Open Systems Last-Mile Connectivity service

MANAGED ISP SOURCING & MANAGEMENT



In conjunction with Open Systems Last-Mile Connectivity service, customers profit from end-to-end SLAs. Open Systems sources and manages first- and last-mile ISP lines, offering the best mix of connectivity that optimizes performance and costs depending on customers' requirements.

GUARANTEED TRAFFIC QUALITY



In addition to availability SLAs, Global Backbone Connectivity guarantees traffic quality SLAs. This is to ensure that traffic passing the backbone has the lowest possible latency, packet loss and jitter, providing the best performance to WAN and cloud applications in the world.

DIFFICULT LOCATIONS



The Global Backbone Connectivity service is operational and meets regulatory standards in 32 countries, including China, ensuring high-speed connections, even in difficult areas.



Open Systems is a leading provider of native, managed SASE solutions that enable organizations to simply connect and secure hybrid environments to meet their business goals. 24x7. Around the globe. Open Systems SASE Experience helps reduce risk, improve efficiency, and accelerate innovation with a comprehensive, easy-to-use combination of SD-WAN and Security Service Edge delivered as a service with a superior user experience.

ZERO TRUST NETWORK ACCESS (ZTNA)

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

Provide secure access to anyone anywhere

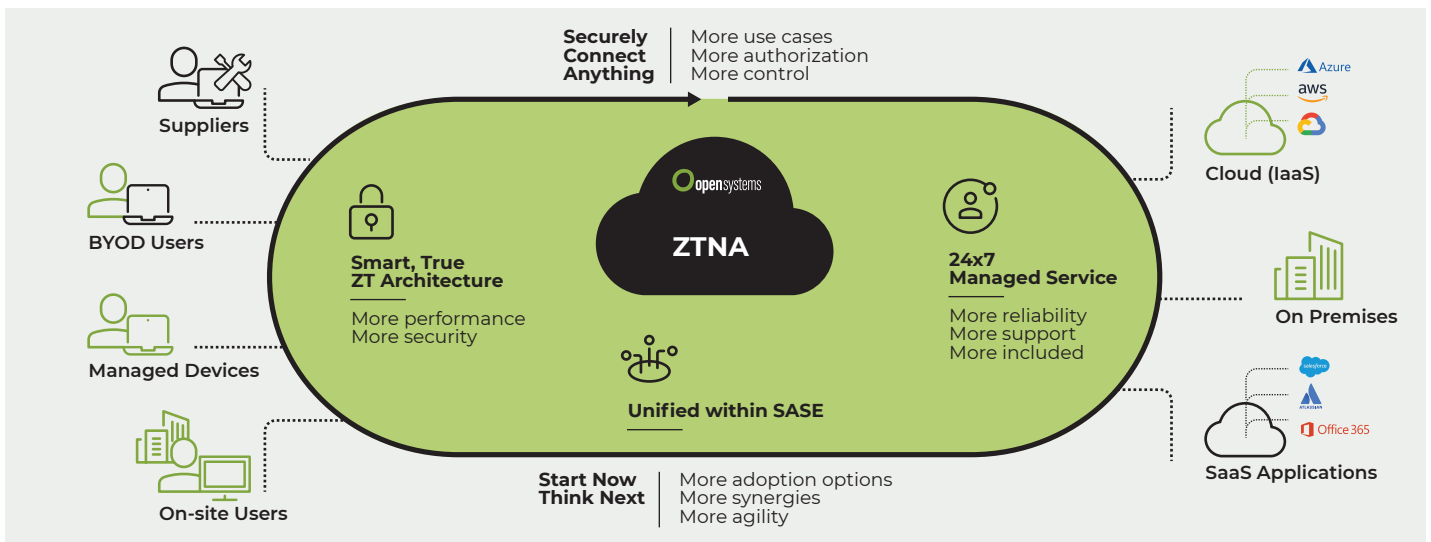
Access control lags behind today's business and security needs

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



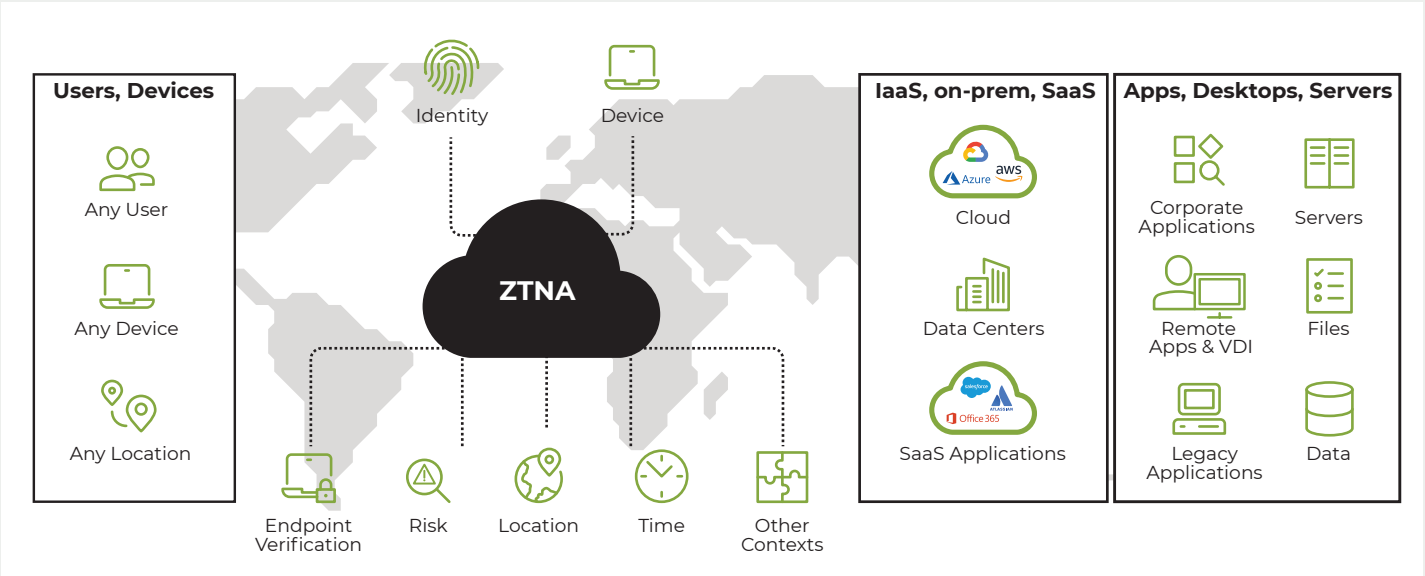
Open Systems ZTNA is delivered ready to go, with all the required capabilities and operational functionalities to start using it today. The customer portal provides insights into status, policy controls, and the monitoring you need for reliable operations.

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



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, Email Security, 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.



Open Systems is a leading provider of native, managed SASE solutions that enable organizations to simply connect and secure hybrid environments to meet their business goals. 24x7. Around the globe. Open Systems SASE Experience helps reduce risk, improve efficiency, and accelerate innovation with a comprehensive, easy-to-use combination of SD-WAN and Security Service Edge delivered as a service with a superior user experience.

EMAIL SECURITY

Protect business communication and user productivity.

Fully managed, adaptable, and intelligent defense

Email remains the #1 attack vector for cyber threats – now supercharged by AI, impersonation tactics, and business email compromise (BEC). From phishing to thread hijacks, legacy filters can't keep up. Organizations today need more than basic protection; they need a fully managed, adaptable, and intelligent defense.

Open Systems Email Security combines best-in-class Secure Email Gateway (SEG) capabilities with adaptive AI detection. Whether you need foundational sender authentication and encryption, or advanced behavior-based filtering, our layered service secures every email touchpoint – while reducing complexity for IT and compliance teams.

What Sets Our Solution Apart

MULTI-LAYERED THREAT DEFENSE



Combines SEG control with ICES-level detection to block malware, phishing, BEC, and emerging threats – before they hit the inbox.

FLEXIBLE, INTEGRATED CONTROL



Granular sender authentication policy-based encryption, and self-service visibility tools – all integrated with your IT and SASE infrastructure.

CONTINUOUSLY LEARNING & IMPROVING



Built-in prevention and ongoing tuning create a security fabric that evolves with threats – minimizing false positives and maximizing resilience.

Three Service Levels

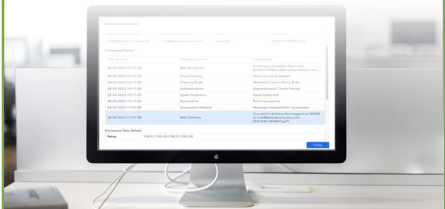
CUSTOMER PORTAL

Visibility & Control

Use Case: Security teams need real-time insight into email flows and threats.

Benefits: Role-based access and drill-down analytics deliver fast, secure control.

Open Systems Difference: Self-service tools reduce reliance on support while maintaining governance and audit readiness.



EXPERT SUPPORT

Execution & Optimization

Use Case: New sender configuration, encryption with partners, or resolving misclassifications.

Benefits: 24/7 expert support ensures issues are resolved accurately and fast.

Open Systems Difference: Threat escalations and tuning are handled by email security pros – minimizing false positives and policy errors.



DESIGNATED ACCOUNT MANAGEMENT

Execution & Optimization

Use Case: Organizations with custom routing or phased DMARC rollouts.

Benefits: Tailored policy designs that align to business needs.

Open Systems Difference: TAMs provide hands-on, proactive consulting – especially for exec-level protection and domain reputation defense.



Service Benefits

COMPLETE THREAT PROTECTION



Blocks phishing, malware, spam, and zero-day threats using real-time AI-powered detection layered with proven SEG defenses.

OPERATIONAL COMPLIANCE



Focus Encryption, policy enforcement, and logging are seamlessly built into daily workflows, helping to meet evolving standards like DORA, NIS2, and GDPR.

EXPERT-MANAGED SECURITY



From SPF/DKIM configuration to BEC mitigation, our experts handle setup, tuning, and escalation – ensuring secure, scalable performance.

Service Components

STANDARD EMAIL SECURITY



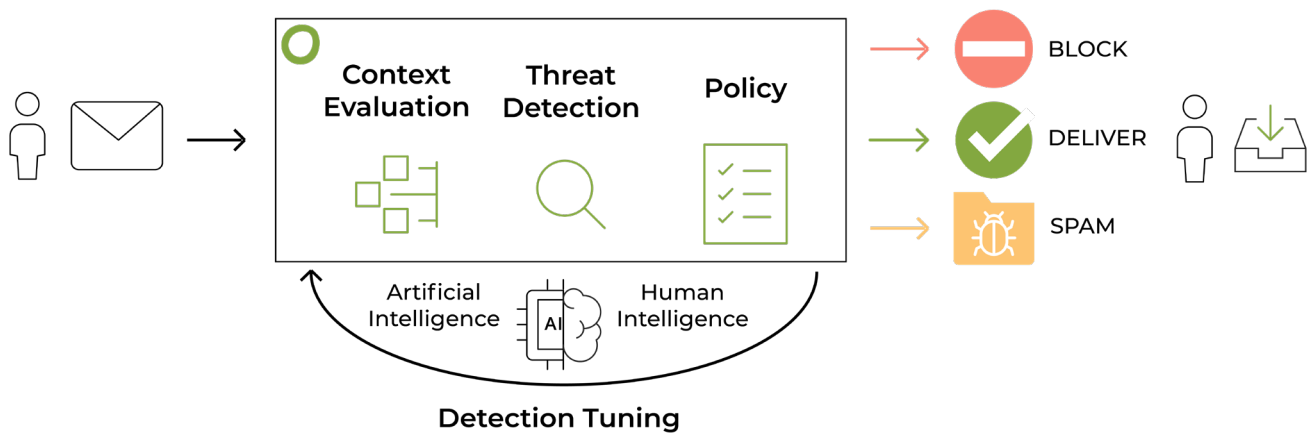
- Sender Verification:** SPF, DKIM, and DMARC to block spoofing and domain abuse.
- Content Analysis:** Signature-based and heuristic filtering with threat intel and phishing detection.
- Policy Enforcement:** Customizable rules for routing, tagging, encryption and quarantine.

ADVANCED EMAIL SECURITY



- Context Evaluation:** Analyzes sender behavior, message tone, and history for anomalies.
- Threat Detection:** Stops zero-hour phishing, AI-generated content, QR-based malware, and impersonation.
- Detection Tuning:** Real-time escalation feedback loop refines detection and improves accuracy over time.

How it Works



Context Evaluation & Policies:

- SPF, DKIM, and DMARC protect brand reputation and block forged senders
- TLS encryption ensures compliant transmission
- Admins apply block/allow lists and policies at both connection and content levels

Layered Filtering & Threat Detection:

- Emails are analyzed using multi-engine content inspection: signature-based AV, behavioral spam detection, URL scanning, and ATP modules
- Advanced AI adds a layer of contextual detection to identify deep-fake messages and thread hijacks before delivery

Adaptive Model Tuning:

- Detection rules are continuously optimized based on real-world outcomes
- Support escalations feed into the learning loop, enhancing performance with every incident
- Custom configurations are guided by designated TAMs



Open Systems provides Managed SASE solutions that combine networking and security functions on a cloud-native platform, securely connecting hybrid IT environments for greater efficiency, enhanced security, and maximum scalability.