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

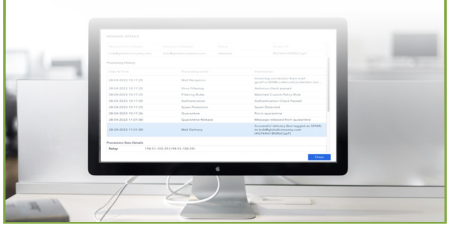
CUSTOMER PORTAL

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.

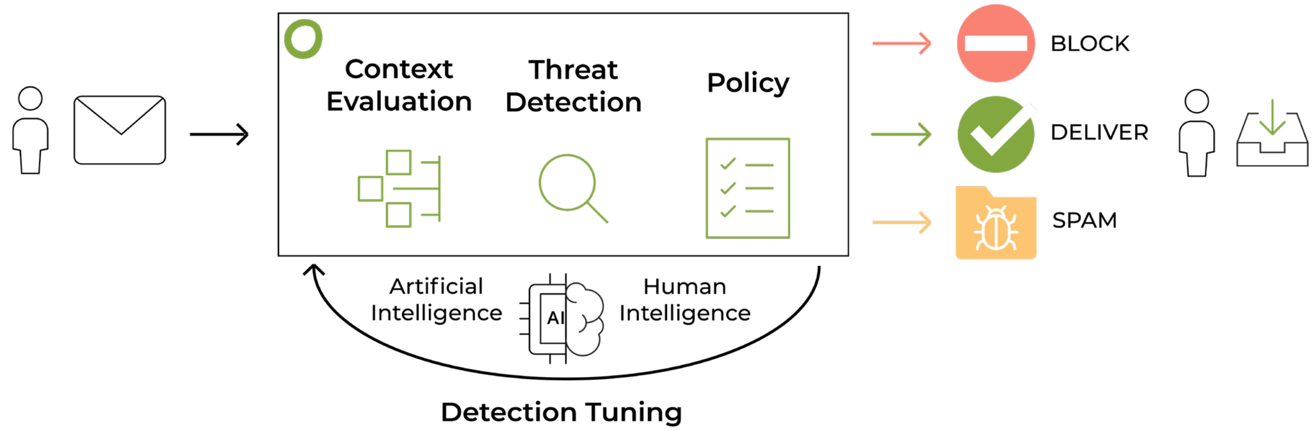
ADVANCED EMAIL SECURITY

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.