



*BOOST EMAIL
SECURITY EFFICIENCY:*
**5 PROVEN
ROI DRIVERS**

*Enhancing Protection & ROI
Through Operational Excellence*

INTRODUCTION: The Hidden Costs of Email Security Operations

Email remains the most exploited communication channel. Despite significant investments in email security solutions and phishing awareness training, many organizations find themselves grappling with operational inefficiencies that erode the return on investment. These challenges often manifest as manual processes, persistent misconfigurations, delayed policy changes, and underutilized features, all of which contribute to increased risk and operational overhead.

5

**CRITICAL
OPERATIONAL
LEVERS**

This guide delves into five critical operational levers that organizations can activate to not only bolster their email security posture but also achieve greater efficiency and cost-effectiveness. By focusing on these areas, businesses can transform their email security operations from a reactive necessity into a proactive, strategic advantage.

5 Critical Operational Levers

To Bolster Email Security Posture and Achieve Greater Efficiency and Cost-Effectiveness

1

Automating Triage to Reduce Manual Overhead

2

Mitigating Configuration Debt with Expert Guidance

3

Accelerating Policy Adaptation Through Self-Service Tools

4

Aligning Policies with Business Needs

5

Enhancing Visibility for Proactive Threat Detection



1

AUTOMATING TRIAGE

to Reduce Manual Overhead

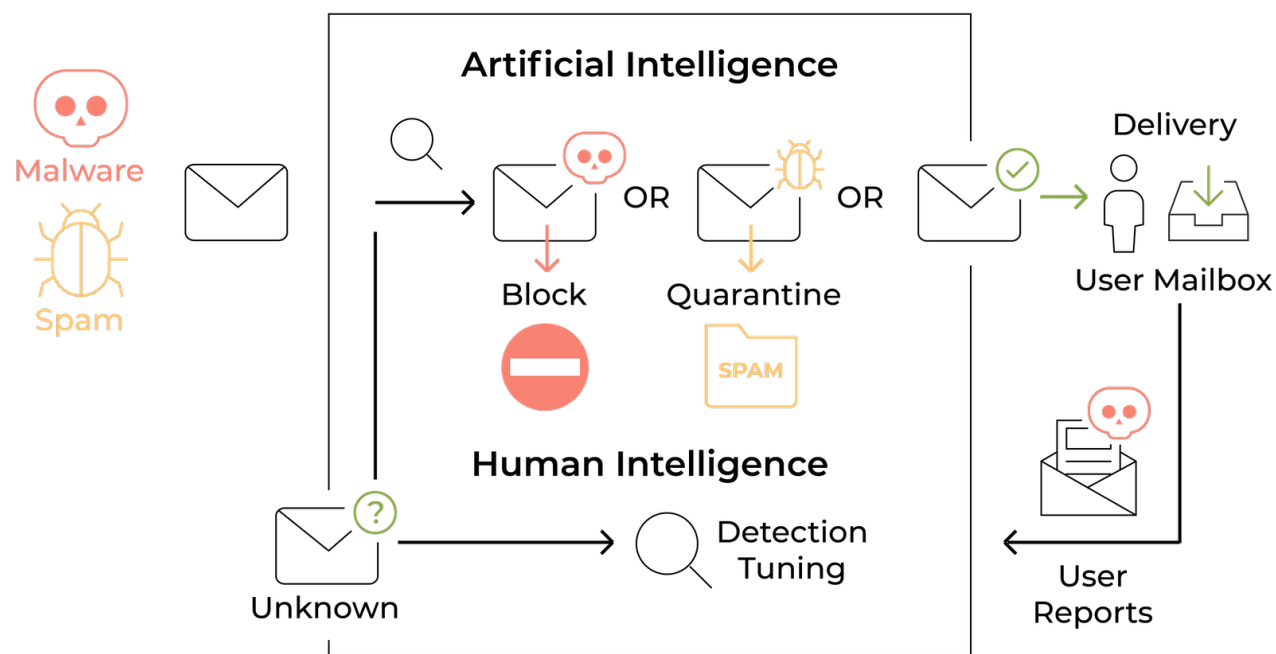
Phishing reports, spam releases, and threat escalations can flood small teams. Without automation, even well-meaning user reports become a bottleneck. For instance, if multiple employees report the same phishing email, manually reviewing each report can consume valuable time and resources.





Combining machine learning-driven detection tuning with analyst-supported triage workflows can alleviate this burden. AI algorithms can suppress false positives, identify anomalies, and continuously improve detection accuracy, while human oversight ensures that genuine threats are addressed promptly.

Sophisticated detection models that incorporate behavioral analysis and contextual threat scoring help improve threat detection of even sophisticated attacks like business email compromise or targeted phishing, while still maintaining a low level of false alarm. This combination of automation and expert support enables organizations to minimize manual overhead and respond to threats more effectively.





2

MITIGATING CONFIGURATION DEBT

with Expert Guidance

As email systems evolve – through mergers, cloud migrations, or the rollout of new tools – configuration complexity grows. Small missteps in settings like SPF, DKIM, or TLS encryption can lead to significant issues, including message delivery failures or domain spoofing vulnerabilities.

Consider a scenario where a marketing team integrates a new email campaign tool that requires specific DNS records to function correctly. Without the expertise to configure these records properly, emails may be marked as spam or fail to deliver altogether, impacting business operations and customer engagement.





Relying solely on internal teams to navigate these technical nuances often leads to delays, errors, or unnecessary overengineering. When configuration support is available around the clock, and backed by teams experienced in maintaining large, secure email infrastructures, even complex or time-sensitive updates become routine and low-risk.

Mitigate Configuration Gaps



**Ensure SPF
Alignment**



**Implement
DKIM Signing**



**Enforce
DMARC Policy**



**Verify TLS
Usage**

By offloading complex or sensitive changes to trusted experts, organizations can ensure timely and error-free implementation of configurations. This approach reduces operational strain and maintains a clean, compliant, and future-ready email posture.

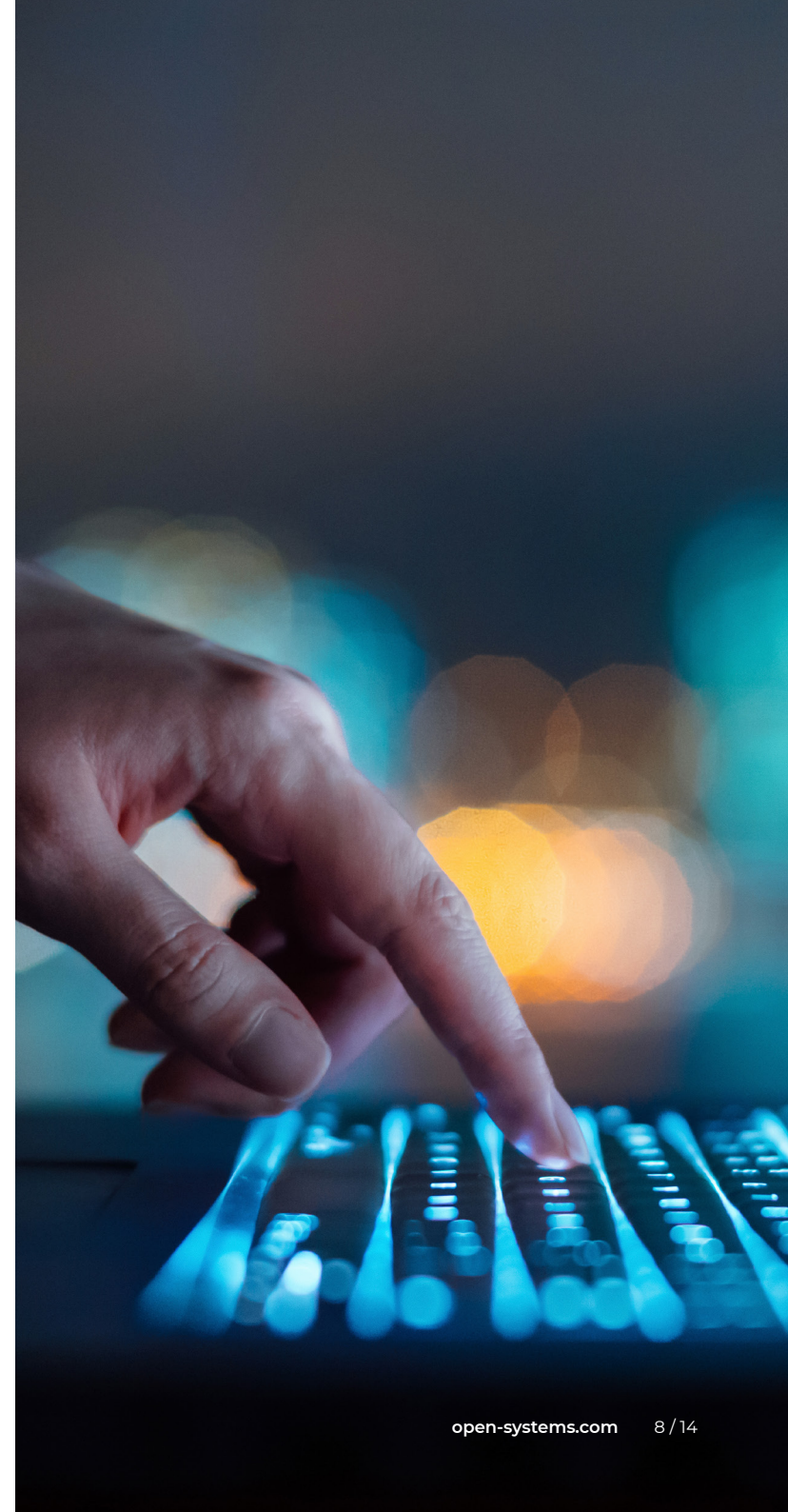
3

ACCELERATING POLICY ADAPTATION

Through Self-Service Tools

The dynamic nature of business operations necessitates frequent updates to email security policies. Trusted senders change, new marketing platforms are adopted, and emerging threats require swift action. Relying on lengthy change control processes or third-party ticketing systems for minor updates can introduce delays and expose the organization to unnecessary risk.

For example, if a new partner's email domain needs to be added to the allow list to ensure seamless communication, waiting for approval through traditional channels can result in missed opportunities and disrupted workflows. Empowering internal teams to make policy changes directly – while ensuring the integrity of those changes – creates a more agile and responsive security posture.





Intuitive self-service tools enable teams to safely adjust allow/block lists or sender verification settings without needing to file a ticket for every request. Built-in validation checks and optional manual oversight mechanisms by the support team ensure that changes are accurate and secure. This approach reduces turnaround times for common configuration changes, empowering users to respond to operational needs without delay.

Email Security Policy Settings



Attachment Protection

Block or sanitize malicious file types



URL Protection

Detect and rewrite suspicious links



Impersonation Protection

Identify spoofed or impersonated emails



Outbound Filtering

Scan outgoing emails for threats



4

ALIGNING POLICIES

with Business Needs

Policies should not impede business operations but rather support them. Generic policies often fail to account for specific business requirements, leading to inefficiencies and potential vulnerabilities. For example, if a C-level executive requires all incoming emails to be duplicated to their assistant for visibility and coverage, a generic routing policy may not accommodate this need without additional configuration.





Tailoring policies to align with business needs ensures that infrastructure configuration and security measures are both effective and conducive to operational efficiency. Working with experts who understand both business requirements and technical capabilities allows organizations to implement policies that protect without disrupting workflows.

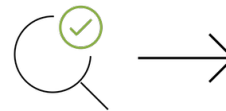
By translating unique business needs into secure, scalable technical policies, organizations can maintain a strong security posture while supporting business objectives. This alignment fosters a culture of security that is integrated into daily operations rather than being viewed as an obstacle.



Routing

Dual Delivery for
Executive Oversight

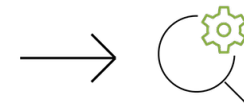
Department
Visibility



Outbound Checks

External
Communications

Legal/Compliance
Surveillance and DLP
(Keyword and
Pattern Matching)



Inbound Policies

Attachment Type
Filtering

Message Tags
(i.e. "External Sender")

VIP Protection
(High Profile Accounts)



5

ENHANCING VISIBILITY

for Proactive Threat Detection

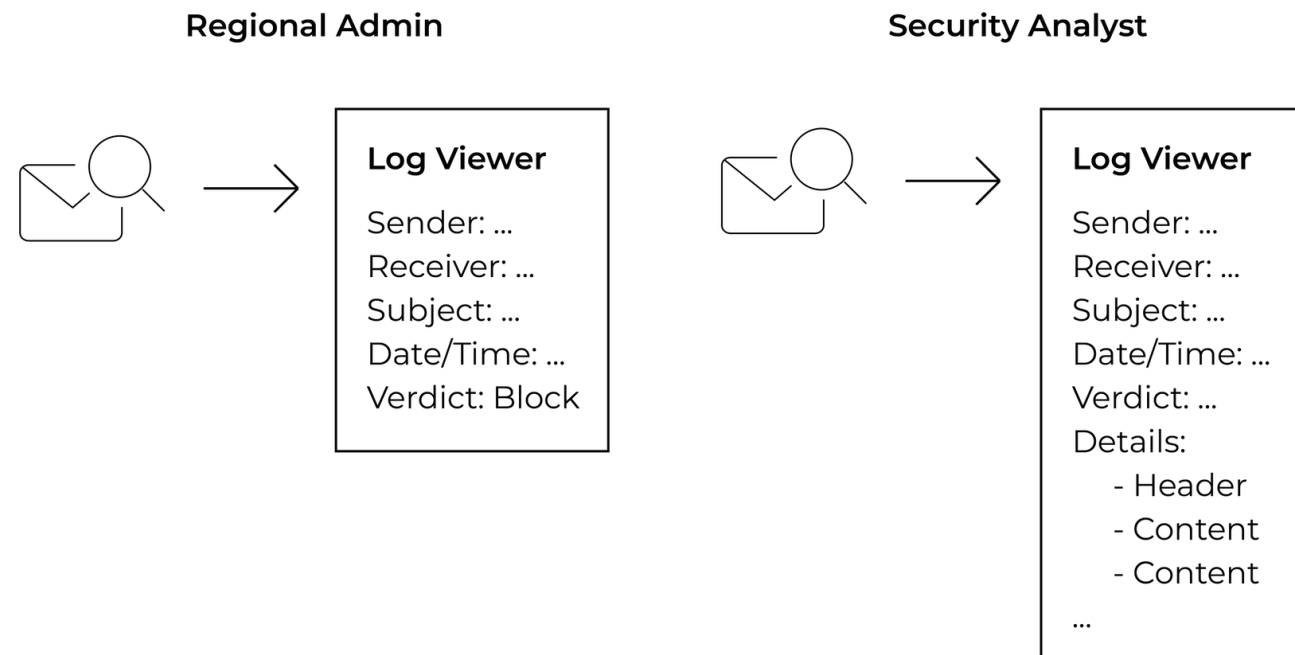
In many organizations, security teams lack real-time visibility into email traffic, making it challenging to detect and respond to threats promptly. Without comprehensive insights into inbound and outbound messages, administrators are often left reacting to user complaints or delayed alerts rather than identifying issues as they arise.





For instance, consider a scenario where an employee receives a phishing email that bypasses initial filters. Without the ability to trace the email's path or analyze its content in detail, the security team may struggle to determine the source and scope of the threat. This lack of visibility can lead to delayed responses, increased risk, and potential breaches.





By implementing centralized, role-based views that offer real-time and historical analysis of email traffic, organizations can empower their security teams to detect anomalies early. Granular access controls ensure that sensitive data is protected while enabling teams to act swiftly and confidently. Such visibility not only enhances threat detection but also supports compliance audits and long-term security tuning.



HOW OPEN SYSTEMS HELPS

Operationalizing Email Security Excellence

Maximizing the return on your email security investment requires more than just deploying tools – it involves optimizing the operations behind them. Open Systems delivers this operational edge through a fully managed, co-piloted approach:

-  **Real-Time, Role-Aware Customer Portal:** Provides deep visibility and self-service capabilities that empower teams to monitor and manage email traffic effectively.
-  **24x7 Expert Support:** Offers around-the-clock assistance for technical issues, configuration changes, or incident escalations, ensuring timely and accurate resolutions.
-  **Dedicated Technical Account Management:** Aligns security policies with business requirements, offering proactive guidance on best practices, compliance, and emerging threats.
-  **AI-Driven Automation:** Enhances detection accuracy and operational efficiency by integrating machine learning algorithms into detection and triage workflows.

By integrating expert support, intuitive tooling, and smart automation, Open Systems helps organizations reclaim time, reduce costs, and strengthen their security posture – without sacrificing flexibility or control. Would you like to assess how well your current email operations support your security goals? Let's explore where these five levers could move the needle for your organization.



Open Systems is a leading provider of native Managed SASE solutions, converging network and security functions on a cloud-native platform. Founded in 1990, the Swiss cybersecurity company, headquartered in Zurich, supports businesses and organizations in more than 180 countries with a holistic, customer-centric service model that guarantees 24x7 expert support. The combination of an innovative platform, integrated solutions, and excellent service ensures secure, reliable, and worry-free network operations – even within the complex IT infrastructures of global manufacturing companies and NGOs. Open Systems not only enhances security but also boosts operational efficiency and accelerates innovation.