Secure Email Gateway

PRODUCT BRIEF

Protect your users from spam, phishing attacks and malware coming in via malicious emails.

Prevent security breaches through solid email protection

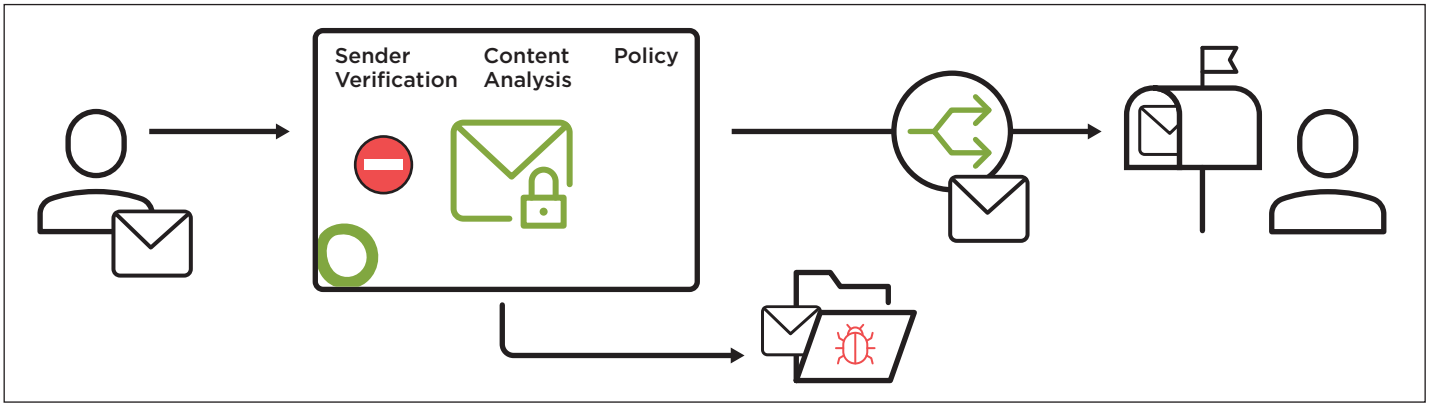
Malicious emails are a prime attack vector

Most successful cyberattacks start with a phishing link in an email or with a compromised attachment. 96% of malware delivery happens via email. The traditional, single-layer defense approach is no longer enough.

Protect users from harm and ensure the integrity of email communications

The Secure Email Gateway serves as the entry point for emails coming from outside the organization, shielding the email infrastructure and users from unsolicited emails using multilayer protection. Custom policies, such as those against unsafe attachments, are applied to protect users. Policies to ensure message integrity, such as DKIM, are also easily enforced.

Sender and content verification powered with policy enforcement



Sender verification, content analysis, and policy come together to deliver a secure email experience.

Why choose Secure Email Gateway by Open Systems?

Multilayer protection with M365

Various layers of defense act to filter all unsolicited emails. They range from lightweight tests, such as header checks, to deep message analysis. The Microsoft 365 integration offers two-tier protection, leveraging what's provided out-of-the-box while adding additional protection and policy enforcement options on top.

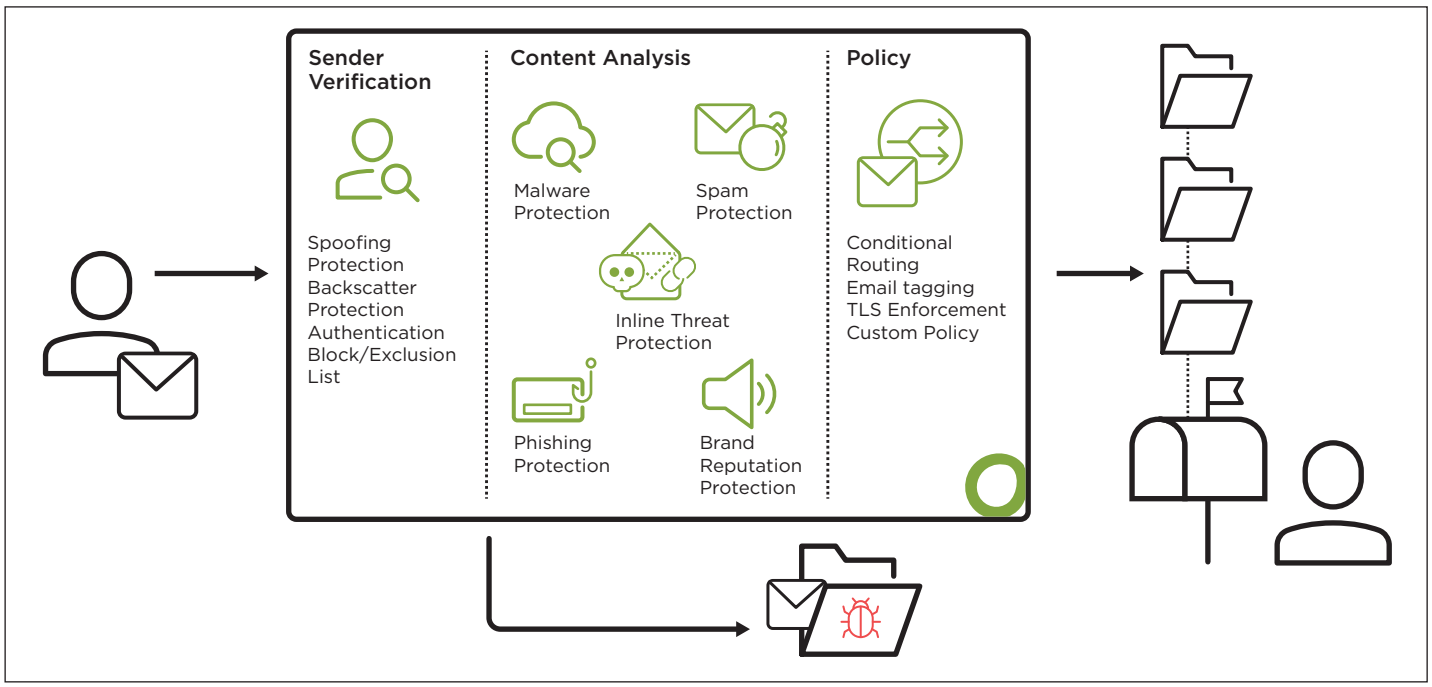
Customization

Organization-specific needs are implemented through customized rules and filter actions, which are selectively configurable. Right from the installation, the Secure Email Gateway is fine-tuned to your organization's environment.

Ease of use

The Secure Email Gateway provides an assortment of self-service tools and APIs that serve to protect against threats contained in email links. Moreover, a message tracker allows for easy investigation of unsuccessful email correspondence, and a DMARC reporting page provides detailed insights into who is sending emails using your name.

How is sender and content verification powered with policy enforcement?



Sender verification

- Customize through exclusion and block lists – at SMTP or policy level
- Protect brand reputation through SPF, DKIM, and DMARC
- Prevent backscatter spam attacks
- Authenticate via message security (TLS)

Content analysis

- Use multi-layer protection against malware
- Protect against spam through heuristic analysis and by using real-time intelligence data
- Detect and warn users of potential phishing URLs
- Protect brand reputation by avoiding abuse of your domain by others

Policy

- Route emails based on conditions (including to quarantine)
- Set per-user exclusion and block lists
- Tag messages for the email backend
- Enforce encryption and authentication based on custom policies

Additional Benefits

- Advanced Threat Protection: defend against zero-day threats contained in email links
- Cloud Sandbox: get even better protection against malware which has never been seen before
- Phishing Protection: add user awareness screens if used with Open Systems Secure Web Gateway

opensystems

Open Systems is a secure access service edge (SASE) pioneer that enables organizations to connect to themselves, to the cloud, and to the rest of the world. With cloud-native architecture, secure intelligent edge, hybrid cloud support, 24x7 operations by level-3 engineers, and predictive analytics, the Open Systems SASE delivers a complete solution to network and security.

Learn more at **open-systems.com** |