

Email Security

Stop what reaches the inbox, known or not.

Email Security from TrustLayer provides protection from known, unknown and emerging email threats, including phishing and Business Email Compromise (impersonation) attacks.

DETECTION

Layered detection, near-zero false positives.

Traditional engines catch the volume. Algorithmic and behavioural analysis catch what is built to slip past them.



SPAM, VIRUSES,
PHISHING

Traditional threats

- Comprehensive protection from traditional email threats including spam, viruses, large-scale phishing attacks and malicious URLs.
- Multiple signature and behaviour-based antivirus engines offer protection from all forms of malware including zero day variants.



IMPERSONATION &
BEC

Targeted attacks

- A unique combination of advanced technologies addresses modern targeted threats including impersonation attacks (business email compromise or CEO fraud) and unknown malware.
- Executive Tracking Lists use details synced from Azure AD to detect users' real names within header and envelope address fields.



10,000+
ALGORITHMS

Algorithmic analysis

- Traditional pattern, message attribute and characteristic matching are complemented with algorithmic analysis for ultimate threat detection without impacting accuracy.
- Behavioural analysis alone includes over 10,000 algorithms analysing more than 130 variables extracted from each email message.

99.999% spam detection with near zero false positives, and 100% virus protection.

POLICY ENGINE

Control exactly how email flows.

At the core of Email Security is a sophisticated policy engine that allows the IT administrator to customise exactly how email flows in and out of the organisation. The engine can inspect all aspects of email and take appropriate action: deliver, quarantine, company quarantine, re-route, notify or reject. Conditions include:

Size

Content

Attachments

Headers

Sender

Recipients

Spam score

Time

Source

Destination

SECURITY AND ROUTING

Detect. Route. Manage.

Email Security is both an advanced email security solution and a full cloud-based email routing engine.



Policy engine

- ✓ Over 20 conditional triggers control email delivery and filter messages
- ✓ Inspects size, content, attachments, headers, sender and recipients
- ✓ Actions include deliver, quarantine, company quarantine, re-route, notify and reject



Routing & quarantine

- ✓ A full cloud-based email routing engine as well as an advanced security solution
- ✓ Fully featured company and personal quarantines for message management
- ✓ Unlimited quarantines, for example Spam, Malware and Advertising



Deep categorisation

- ✓ Distinguishes professional marketing from suspect mass email campaign messages
- ✓ Flexible policies detail precisely how different message types are processed and tagged
- ✓ Add tags such as [EXTERNAL] or [MARKETING] to subject lines

99.999%

spam detection

100%

virus protection

10,000+

behavioural algorithms

130+

variables per message

MULTIMODE DEPLOYMENT

Deploy your way.

100% cloud based and easy to deploy with a simple MX record change, or use M365 Connector Mode.

DNS-based mode

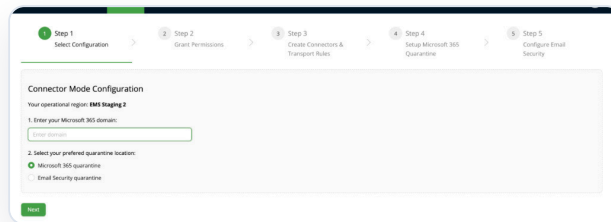
Requires a simple MX record change to route email traffic via the TrustLayer MTA clusters. Mail is scanned, rules applied, then delivered to the destination SMTP server.

Connector Mode

Uses Microsoft Transport Rules and Connectors via Azure, integrating directly with M365. Choose either Microsoft's 'Junk' folder or TrustLayer's comprehensive quarantine for delivery of suspicious or unknown emails.

API features

Available using Microsoft Graph API, such as the ability to retract and delete messages after they have been delivered, including forwarded threads.



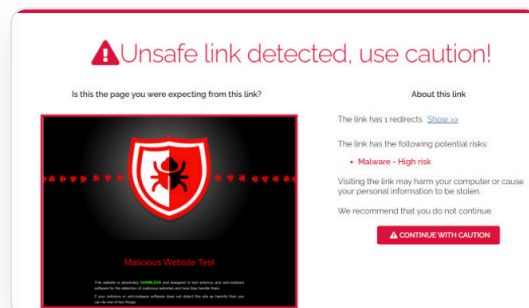
Choose Connector Mode or DNS Mode at setup.

ADDON SERVICES

Extend the mailbox.

SecureMail. Provides an end-to-end encrypted messaging service via Outlook or web portal. Messages delivered over a TLS encrypted channel.

Compliant Email Archive. Unlimited email backup for fully compliant journalling of messages. Includes user and admin search for audit compliance and legal hold events.



LinkScan rewrites embedded URLs and shows destination content prior to click.

KEY FEATURES

What you get out of the box.



Anti-Spam

Multiple engines use a combination of technologies to detect spam as well as more sophisticated targeted phishing and impersonation attacks.



Anti-Malware

Multiple layers of traditional signature and behaviour-based AV engines for detection of malware, including static sandboxing of file attachments.



TrustLayer LinkScan™

Rewrites URLs embedded in email messages and provides point-of-click protection using multiple reputation engines and 3rd party services. Options to auto-redirect, prompt to continue, block on threat, and show or hide target URLs. Option to scan at time of delivery as well as time of click, including messages with embedded QR codes.



Safe & Deny Lists

Create company-wide and/or individual user Safe & Deny Lists, supported by the Outlook Addin.



Executive Tracking Lists

Use details synced from Azure AD to automatically detect users' real names within header and envelope address fields to protect against impersonation attacks and CEO fraud.



Nearby (Cousin) Domains

Compares sender domain to legitimate domain names to identify nearby domains that vary from the actual domain name by one or two characters.



Keyword Lists

Create unlimited keyword and regex lists. Use rules to analyse messages and take action based on confidential or sensitive content.



Subject Tags & Headers

Add tags such as [EXTERNAL] or [MARKETING] to message subject lines. Add HTML or plain text headers to inbound messages alerting users to potential risks.

REPORTING

Evidence on demand

Real-time Visibility	Charts provide detailed visibility of inbound and outbound mail flow as well as triggered rules and actions taken.
Curated Reports	Build reports from available fields and criteria and export via PDF. Search audit reports by time, user, sender address, sender IP, subject, recipient, final action and more.
Scheduling & Alerting	Link curated reports to a delivery schedule so analytics reach email inboxes on a regular cadence.
Interactive Reports	Fully interactive charts and tables take admins from high-level trends to forensic detail in a few clicks for prompt incident response.
Top Trend Reports	A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and emailed to recipients.
Multiple Views	Analyse and report by time, user, sender address, subject, sender IP, recipient, direction, final action and rule name.
Detailed Audit	Granular view and analysis of individual messages with the exact reason an email was delivered or rejected. Includes full email headers and the SMTP conversation with the remote email server.



TLS / Opportunistic TLS

Enforce TLS encryption and restrict communication with email servers that do not support TLS. Option to enable opportunistic TLS with fall-back to plain text if TLS is not supported by the receiving mail server.



File Attachments

MIME type checking of file attachments with the ability to block dangerous file types. Detect password-protected archives.



Sending Limit Monitoring

Automatic protection from attempts to send large volumes of messages outbound, preventing domain blacklisting.



Mail Queuing

Email is automatically queued for up to 6 days (144 hours) in the event of a failure or outage of the primary email service or server(s).



DHA Protection & Authentication

Drop email destined for an invalid or fake email address. Support for SPF, DKIM and DMARC.

MANAGEMENT

Central control

Policy Engine	Over 20 conditional triggers to control email delivery and filter messages based on size, keyword, spam score, time, source, destination, attachments, headers and more.
Quarantine	Option to move messages to Company (Admin) and/or User Quarantine (Outlook). Daily Digest emails list all messages within the user's quarantine, allowing them to be safely previewed, released or blocked. Unlimited quarantines.
Authentication & Sync	AD Kerberos, SSO, Captive Portal and RADIUS accounting. AD sync service ensures changes are replicated seamlessly.
Web Portal	Fully integrated with TrustLayer's other modules, the CloudUSS dashboard offers a single pane of glass for management and reporting.
Delegated Admin	Full Role-Based Access Control (RBAC) enables a range of access profiles and control/visibility permissions.
Disclaimers	Append an HTML or plain text disclaimer to all outbound email. Set different disclaimers for different domains or groups.

PART OF THE TRUSTLAYER PLATFORM

This service is part of the Mail layer. Eight solutions, four layers, one platform.



Browse

Web

CASB

AI Exposure



Posture

CSPM

SSPM



Mail

Email

Archiving



Users

SAT