DATASHEET

TrustLayer Email Security

Email Security from TrustLayer provides protection from known, unknown and emerging Email threats, including Phishing and Business Email Compromise (Impersonation) attacks.

Email Security (EMS) from TrustLayer provides comprehensive protection from traditional email threats including spam, viruses, large-scale phishing attacks and malicious URLs.

EMS also includes a unique combination of advanced innovative technologies to address modern targeted and sophisticated email threats including impersonation attacks (business email compromise or CEO fraud) and unknown malware.

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.

Multiple signature and behaviour-based antivirus engines offer protection from all forms of malware including zero day variants.

- 99.999 % spam detection with near zero false positives
- 100% virus protection

At the core of EMS is a sophisticated policy engine that allows the IT administrator to customize exactly how email flows in and out of the organization. The engine can inspect all aspects of email, including size, content, attachments, headers, sender, recipients and take appropriate action, such as deliver, quarantine, company quarantine, re-route, notify, reject.

EMS is both an advanced email security solution and a full cloud-based email routing engine with fully featured company and personal quarantines for message management.

Deep categorization – distinguishing between professional marketing and suspect mass email campaign messages for example – enables flexible policies that detail precisely how different types of messages are processed and tagged.

EMS is fully managed by and delivered through the TrustLayer Platform that also includes Web Security, Cloud Application Security, Posture Management, and Multi-Factor Authentication. The TrustLayer Platform provides a single web interface for central policy configuration and management, as well as data visualization and reporting.

EMAIL SECURITY

- 100% cloud based and easy to deploy with a simple MX record change or use M365 Connector Mode.
- Incorporates many advanced technologies to ensure enterprise level threat detection rates with very high accuracy
- Manipulate messages inline by adding custom tags, html branded content, or routing, including post-delivery message deletion via API.
- Multiple traditional signature and behaviour based AV engines including static sandboxing of file attachments
- TrustLayer LinkScan™ provides time-of-click protection from malicious URLs in emails with the option to scan links at time of delivery, including messages with embedded QR codes.
- Empower users with Personal Quarantine and daily digest of messages, safe sender list and report spam all via integrated Outlook Addin.

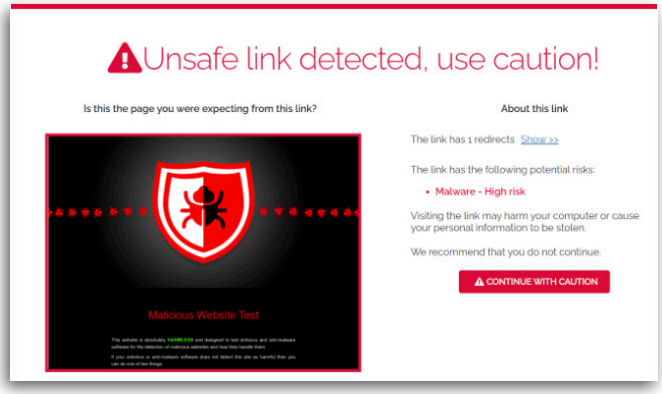
ADDON SERVICES

SecureMail

Provides end-to-end encrypted messaging service via Outlook or web portal. Messages delivered over 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.



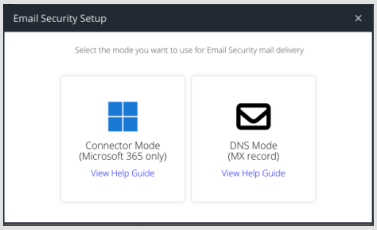
LinkScan engine rewrites embedded URL's and provides overview of destination content prior to click.

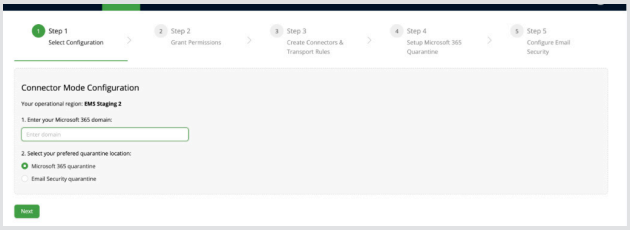
MULTIMODE DEPLOYMENT

1. **DNS-based** mode requires a simple MX record change to route email traffic via the TrustLayer MTA clusters. Mail is scanned, rule applied and then delivered to the destination SMTP server.

2. **Connector Mode** uses Microsoft Transport Rules & 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.

3. **API** features are also available using Microsoft Graph API, such as the ability to retract and delete messages after they have been delivered (inluding forwarded threads).





KEY FEATURES

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.
TrustLayer LinkScan	• LinkScan rewrites URL's 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/hide target URLs • Option to scan at time of delivery as well as time of click
Safe & Deny Lists	• Create company-wide and/or individual user Safe & Deny Lists (supports 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/CEO Fraud.
Nearby (Cousin) Domains	• Compares sender domain to legitimate domain names to identify nearby domains (that vary from actual domain name by one or two characters)
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
Keyword Lists	• Create unlimited keyword and regex lists. Use rules to analyse messages and take action based on confidential or sensitive content.
DHA Protection	• Drop email that is destined for an invalid or fake email address
Email Authentication	• Support for SPF, DKIM, and DMARC

MANAGEMENT

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 delivered listing all messages within the user's Quarantine allowing them to be safely previewed, released or blocked (Supports Outlook Addin) • Unlimited Quarantines (e.g. Spam, Malware, Advertising)
User Authentication and Synchronisation	• Multiple authentication methods supported including 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 interface 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.

REPORTING

Real-time Visibility	• Charts provide detailed visibility of inbound and outbound mail flow as well as triggered rules and actions taken.
Curated Reports	• Admins can build their own reports based on available fields and criteria, and can then export via PDF. • Audit reports can be searched using multiple criteria including time, user, sender address, sender IP, subject, recipient, final action and more.
Shceduling and Alerting	• Link curated reports to a delivery schedule so analytics can be delivered to email inboxes on a regular cadence.
Interactive Reports	• Charts and Tables in the portal are fully interactive enabling admins to go from high-level trends to forensic-level detail with just a few clicks enabling prompt incident response.
Detailed Audit	• Granular view and analysis of individual messages with the exact reason an email was delivered or rejected. Includes full Email headers and SMTP conversation with the remote email server