DATASHEET

TrustLayer Compliant Email Archive

Reduce email data risks, meet regulatory frameworks, and optimize storage costs. TrustLayer's Compliant Email Archive provides a centralized and secure email repository for eDiscovery, ensuring preservation, retrieval and integrity of all emails and their metadata.

TrustLayer Compliant Email Archive (CEA) enables organizations to meet compliance requirements and respond to internal and external requests for information.

The Compliant Email Archive from captures and stores every message sent or received securely in a separate, secure, tamper-proof database in the cloud. Archived messages are de-duplicated, compressed, indexed and encrypted.

An intuitive search interface – accessible from any device – allows IT, HR, and end users themselves, to quickly find emails using multiple search criteria. Privileged users can rapidly search all mailboxes, or selected mailboxes, to respond quickly to internal or regulatory requests.

Enterprise class Archive
A Compliant Email Archive enables organizations of all sizes to respond quickly and efficiently whenever the inevitable internal investigation or regulatory disclosure request comes in.

Without an archiving solution the only way to respond is by slowly and painfully going through each mailbox separately to find messages that are 'in scope'. Even worse, fully complying with a request may involve the drawn-out process of restoring old mailboxes.

Having an archive makes message retrieval straightforward and effortless. Full indexing and a powerful search interface supporting multiple criteria – including sender or destination addresses, keywords, dates and even attachment content – reduces search times to seconds or minutes rather than days.

COMPLIANT EMAIL ARCHIVE

- Keep a secure, tamper-resistant copy of every email sent and received
- Encrypted message store hosted in a high-availability cloud
- Easy to deploy using the journal function available on most email platforms
- Cost-effective: licenses only required for active mailboxes sending/receiving a minimum number of messages
- Managed, predictable storage costs: saving messages to a separate server can reduce premium mail server costs by up to 75%
- Message and attachments fully indexed when archiving for lightning fast search
- User's can search/restore lost or deleted emails using multiple search criteria, including via an Outlook addin - without calling the IT team.
- Enables efficient response to internal or regulatory search requests across all (or a selection of) mailboxes
- Retention policies automatically delete messages as they age, with the option to store emails indefinitely.
- In the event of a primary Email service outage users have access to historic emails via a web interface.
- Immutable audit log of all search activity to demonstrate governance and data protection.

Improved User Productivity

Users interact with the archive using an intuitive search interface, supporting a wide range of search criteria to rapidly retrieve messages. Search is available via a web interface from any device with a browser and can also be integrated within Outlook.

Once search results are returned users can read and review message contact or perform a range of actions. Messages can be downloaded and opened in their email client, forwarded to their inbox, printed, exported to PDF or for larger messages, forwarded to their mailbox as a ZIP file.

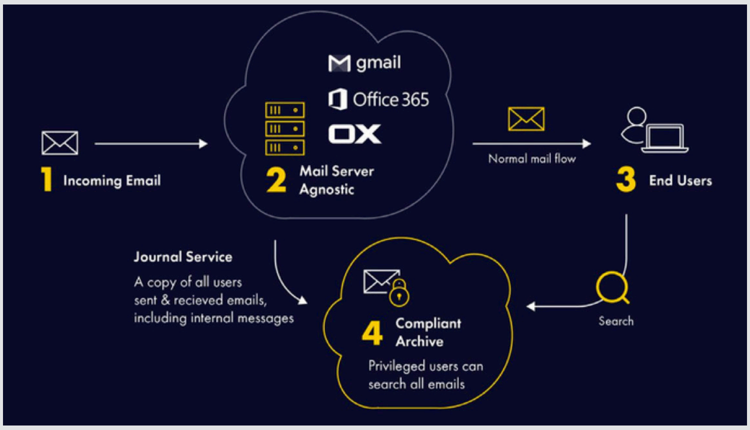
Users are fully empowered to manage their own email stores without the need to call the helpdesk - reducing support overhead and directly driving user productivity. Search history enables rapid repetition of recent searches and the option to save search criteria simplifies replication of complex searches. Privileged Search allows authorized users to search across multiple mailboxes – or the entire organization.

Access to Privileged Search is carefully controlled and audited to ensure appropriate use.

How It Works

TrustLayer's Compliant Email Archive can be set up in minutes. Most primary email services – including Exchange and Exchange Online (O365) – support email journaling as a service. This service sends the archive a copy of all emails sent and received. As messages are archived they are also de-duplicated, compressed, encrypted and indexed.

Once the journal service is configured the archive is available to use immediately and requires very little day-to-day administration. An optional service is available to ingest historic email messages from mailboxes - or other sources such as .PST files.



Regulatory and Internal Investigations

In a world where the regulatory and legislative compliance landscape is ever expanding - combined with an increasing amount of sector-specific requirements and guidelines - the need to retain business records and electronic communications is no longer optional for most organizations.

The ability to respond to requests for information, defend against litigation, or conduct internal investigations, is critical. Being able to react effectively is even more essential once a regulator is involved.

Being able to demonstrate that specialized tools are in place, along with relevant processes, clearly shows a responsible approach to data management.

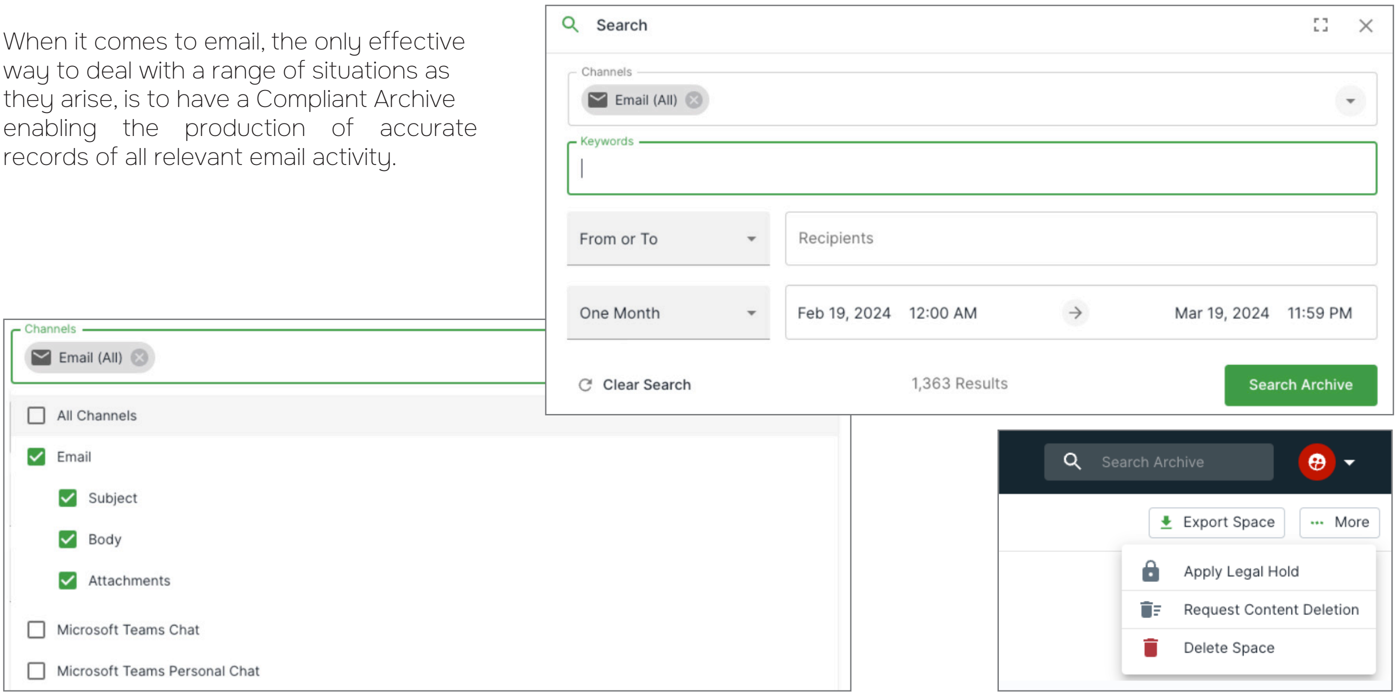
When it comes to email, the only effective way to deal with a range of situations as they arise, is to have a Compliant Archive enabling the production of accurate records of all relevant email activity.

Archiving and GDPR

With the introduction of GDPR email is frequently at the center of Subject Access Requests. Organizations without an easy way of searching historic emails will not be positioned to respond to GDPR-related requests within the required time limits, or worse, may not be able to respond at all. Furthermore, TrustLayer's Compliant Email Archive also supports the 'Right to Be Forgotten' with a well-defined and audited method of deleting a message or messages from the archive, facilitating GDPR compliance.

Governance

Over time an email archive will inevitably contain large amounts of sensitive content. Audit and control features are therefore essential, and all search and administrator actions need to be monitored. The Compliant Email Archive provides all the necessary controls to monitor how the system is being used and what search activity takes place. Users can be authenticated using Single Sign-On (SSO) to provide access convenience but with appropriate levels of security.



Search

Channels: Email (All)

Keywords:

From or To | Recipients

One Month | Feb 19, 2024 12:00 AM → Mar 19, 2024 11:59 PM

Clear Search — 1,363 Results — Search Archive

Channels: Email (All)

□ All Channels
☑ Email
☑ Subject
☑ Body
☑ Attachments
□ Microsoft Teams Chat
□ Microsoft Teams Personal Chat

KEY FEATURES

Access Levels	• **Standard / Basic (LDAP) Users** – access to their own nominated email addresses • **Privileged Users** – eDiscovery users who can access all/subset of the archived emails within a single tenant, with comprehensive audit trails showing which emails have been searched for and opened • **Data Guardian Users** – Data Guardian users have access to audit trails within a single tenant and are able to review Privileged User searches • **Privileged & Delete Users** – similar to Privileged Users, with the extended functionality to be able to delete emails from the archive in an audited manner (for example within a 'Right To Be Forgotten' process) • **Administrators** – no access to search the archive but can administer accounts and basic settings.
Audit & Reporting	Access and search activity by Privileged accounts is audited and can be automatically emailed to designated mailboxes to ensure governance of the archive
Authentication	AD and SSO supported, including Multi-Factor Authentication
Deletion of Messages	A privileged delete option to allow controlled deletions to support GDPR right to be forgotten requirements as part of an audited and controlled process.
Data Migration Options	PST import / Mailbox Import via IMAP
Data Guardian	Configure your Data Protection Officer or other executives to act as Data Guardian, receiving alerts and summaries whenever an archive search is executed.
Encryption	Data at Rest using AES-256 Data in Transit using TLS (supported via SMTP) Browser/IMAP access using SSL/TLS
Journalling	Recommended via standard SMTP journal feature but can also support collection via EWS or IMAP
Licensing	Only active users require a license - old mailboxes/ex-employees are not chargeable
Data Storage	Email Archive is hosted on Amazon's AWS platform, with datacentres located in London (UK) and Frankfurt (EU) - customers choose location at time of tenant provisioning
PST/EML Ingestion	Optional service to import legacy PST or EML files from incumbent archive
Retention	Automatically delete emails when they reach a specific age or retain messages indefinitely
Search UI	Simple or Advanced search UI using key words / wild cards or granular search criteria to refine Dates, To, From, Subject, Message, Body, Attachment type/content. User search UI can also be integrated into Outlook using the Home Folder feature
User Actions	Users can take further action with search results such as Open within native email client (e.g. Outlook) or Forward, Restore (to mailbox), Print or Save to PDF
Outlook Add-in	Allows users to browse their personal Archive witout leaving the Outlook interface
Platforms Supported	Includes Exchange (all versions) including Office 365 Exchange Online, G Suite, Domino, GroupWise