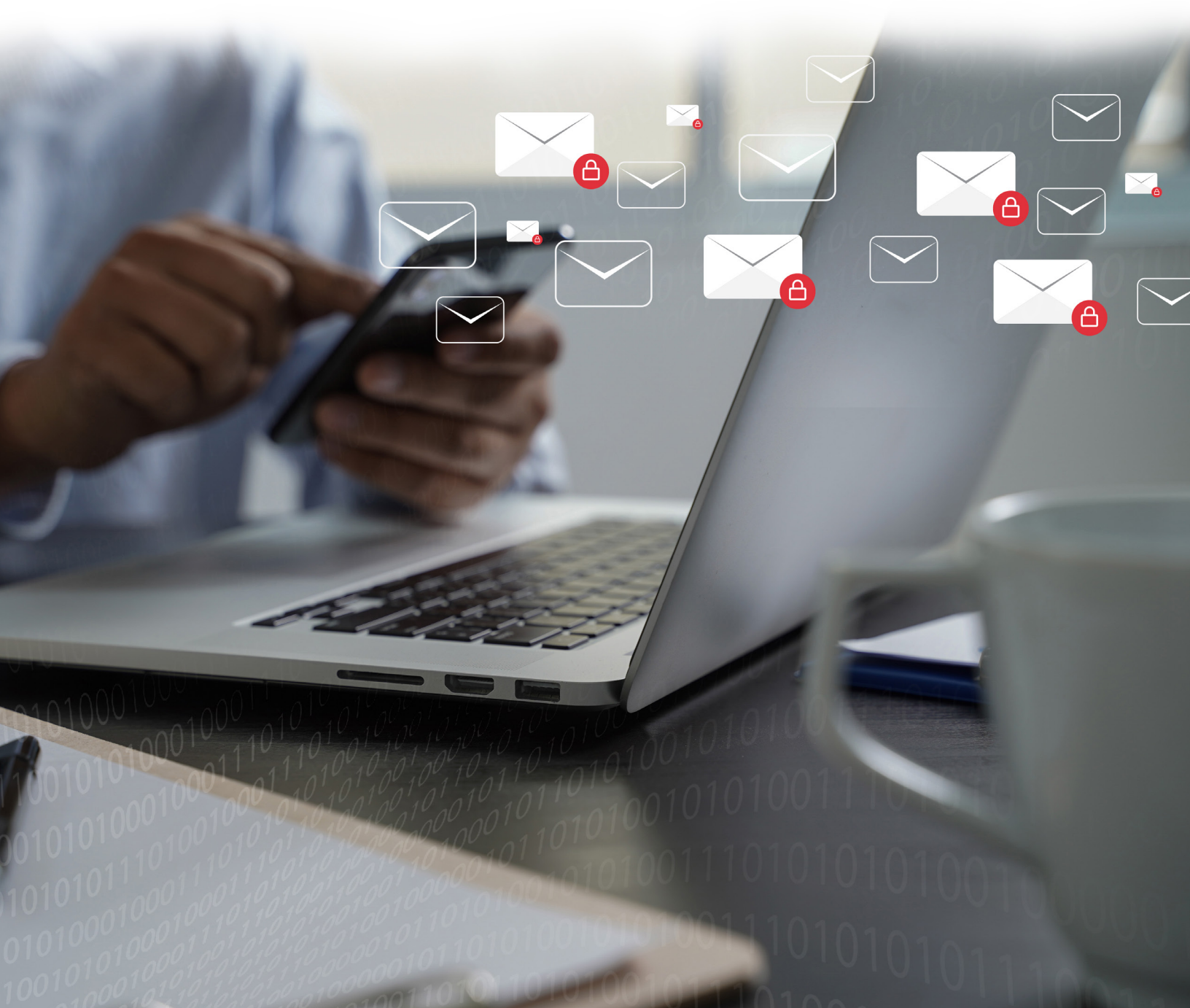
SECLORE

Seclore Email Encryption Plus



Emails are the easiest, most scalable, and most common way to communicate. However, they are also most common sources of data breaches – and often the most embarrassing. Leaked emails – whether about business strategy or office gossip – can drastically erode corporate reputation and competitive advantage.

Are Email Gateways and Traditional Encryption Solutions Enough?

Email Gateways or DLP (Data Loss Prevention) systems are often the preferred solutions to secure emails, however they have limitations. Firstly, they are restricted to your own email domain. These systems are unable to extend their governance and security capabilities to other domains. For example, an Email Gateway cannot restrict a board member, contractor, or partner from forwarding your emails and attachments to third parties.

Traditional email encryption, another common solution, cannot restrict authorized recipients from misusing the information. Once the email content and the attachment are decrypted, it is completely vulnerable to leakage and misuse.

In today's flat, hyper-connected world, such traditional solutions fail to protect emails beyond the enterprise perimeter.

How Seclore Extends Your Email Protection

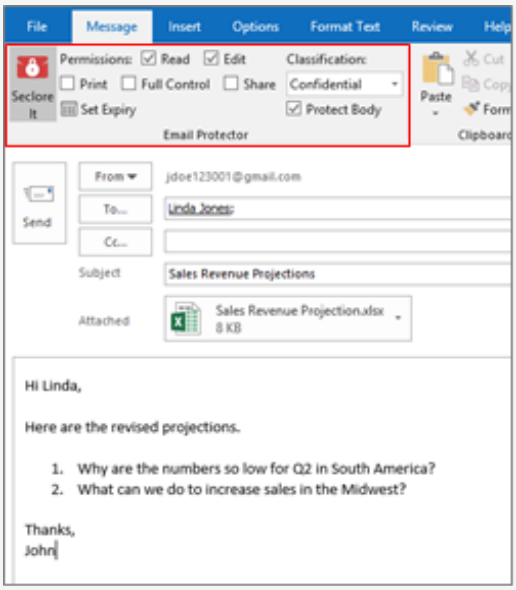
Seclore Email Encryption Plus, a key part of Seclore Rights Management technology, allows you to:

- Secure and track your emails – even when sent to other domains
- Control how the authorized recipient can use the attachment (view, edit, cut/paste, print)
- Track the use of emails and individual attachments
- Expire or revoke emails sent or forwarded to the wrong recipient by mistake or malice
- Automatically add protection to emails and attachments being sent or received without relying on the end user
- Integrate with leading DLP, Classification and Enterprise Applications to increase security

With Seclore Email Encryption Plus, granular usage controls travel with your email and remain in control even when the email and attachments are open and in use. Now you can be confident that your sensitive data remains protected and tracked wherever it resides.

Granular Usage Controls for Email

Protection is not black-and-white but granular and can be customized depending on your use case. For example, you can ensure that users cannot print, screen share or forward information that they're not supposed to, even accidentally. Also, you can automatically attach granular usage controls to emails through Exchange Online and Google mail within 24 hours. Seclore's Security24 in the cloud speeds up the provisioning process with automation so you can get started protecting data in the cloud within one business day.



Seclore Email Encryption Plus for Outlook

One-Click Email Protection

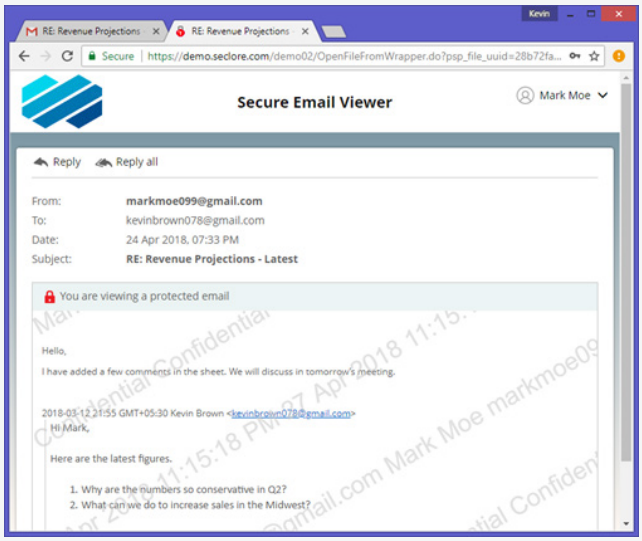
Security options in the ribbon allow the sender to control in just one click what each recipient can do with the email attachments. The sender can control:

- Reading, editing, printing, sharing
- The date and time of when the usage of the email and attachments will expire

Activity logs of all access and usage of the email content and attachments are available and updated in real time. You can also easily track and revoke access to your emails within the email itself for each individual recipient.

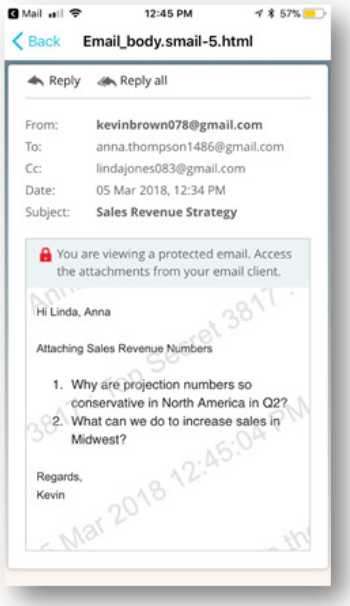
Accessing Protected Emails in a Browser without an Agent

Users without access to the agent – or not using Outlook - can simply open the extra attachment (with extension.smail.html) to open the email body directly in the Secure Email Viewer within the browser. Users can also reply to the email from the browser by clicking Reply or Reply All.



Accessing Emails on Mobile

The Seclore Email Encryption Plus extends security to the mobile world as well. With Seclore, your data is as safe on your mobile as on your desktop or laptop. This means that you can now work on your most confidential emails and documents while you're on the go. Moreover, you can view and reply to protected emails right from your iOS or Android phone!



Automatically protect emails by leveraging the 'subject', 'to' and 'from' data to protect emails with the appropriate usage controls without user intervention.

Automatically Protect Your Emails and Attachments

The Seclore Email Auto-Protector acts as an MTA (Mail Transfer Agent) and allows an organization to set up protection rules to automatically apply usage controls to emails and attachments in the background without human intervention. The process is completely transparent to the email sender. Usage control rules can also be applied to both outgoing and incoming emails. For outgoing emails, a rule can protect all attachments sent to a particular Gmail or Yahoo ID with view-only usage controls, while another rule can set view, edit and print usage controls with an expiration date for email attachments sent to a bidder for a new project. With incoming emails, if an email is from a sensitive client, the email can be automatically protected before it lands in your users' inbox.

1 Email is sent from internal user unprotected

2 Email Server or Cloud Service receives email

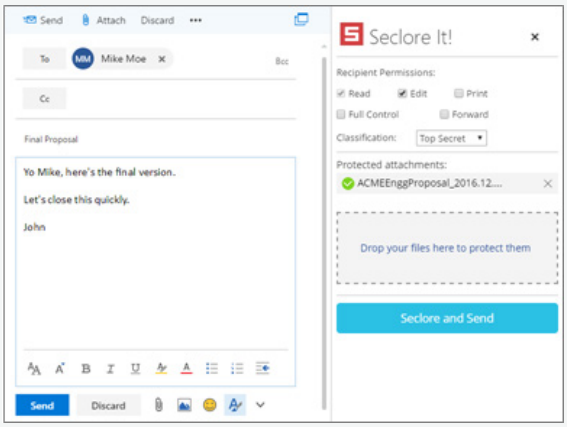
3 Email Auto-Protector scans if any rules are met, and applies usage rights automatically

4 External recipients receive a protected email that is protected and trackable

Seclore Email Encryption Plus in action. Protection happens entirely in the background, AFTER the user clicks 'send', so the user workflow remains untouched.

Email Encryption Plus Microsoft Email

Seclore Email Encryption plus integrates with any variation of Microsoft email (Outlook, Outlook Web Access, Exchange, Exchange Online) in the Cloud or on-prem to deliver a seamless email protection experience. Seclore Email Encryption Plus for Microsoft Email also integrates and automates with other best-of-breed data-centric security solutions such as Rights Management, Data Classification, and DLP.



Seclore Email Encryption Plus for OWA

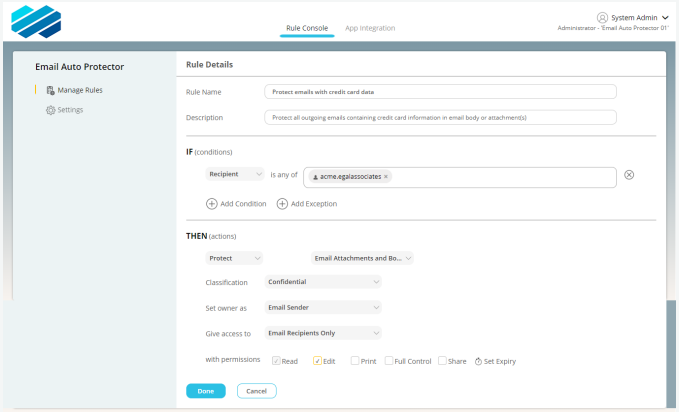
Seclore Email Encryption Plus DLP

DLP systems typically generate volumes of logs that require manpower and time to analyze. Moreover, since DLP is most often run in discovery mode (due to the risk of false positives and need for unhindered collaboration), any discovery of anomalous user behavior occurs only after the fact. For emails that need to be shared with external parties to support collaboration, there is no choice but to allow the emails and attachments to go completely unsecured.

Seclore offers an easy, streamlined solution to these DLP challenges with Seclore Email Encryption Plus for DLP. Once emails are processed by the DLP's email content inspection engine, Seclore can automatically map the appropriate access and usage policy to the email and its attachments. This ensures that recipients cannot misuse or leak the email after they receive and read it. An "allow" policy with DLP becomes an "allow, but prevent misuse" policy with Seclore.

Seclore Email Encryption Plus Classification

Data Classification enables organizations to better identify what information is sensitive - by applying visual markings and metadata labels to emails and documents. But Data Classification is unable to control when, where or how the information can be accessed and used. Further, Data Classification tools cannot track, control or revoke access to emails or documents once they are shared.



Setting up rules in the Email Auto-Protector

With Seclore Email Encryption Plus for Classification, persistent, granular access and usage controls are automatically attached to emails and attachments based on the email classification level selected by the user. Once the user classifies and sends the email, Seclore Email Encryption Plus for Classification reads the metadata to apply the appropriate usage controls to the email and attachment to protect and track it wherever it travels.

Seclore Email Encryption Plus Enterprise Applications

Seclore Email Encryption Plus for Enterprise Applications can also be used to protect email content sent automatically from applications such as SAP, CRM, or HRM systems. Business reports, customer statements, and other confidential information can be protected automatically before being emailed - with zero user intervention.

By applying persistent, granular usage controls to automatically generated information, Seclore Email Encryption Plus for Enterprise Applications ensures that data always remains secure – without affecting business workflows. Organizations can be confident that convenience and efficiency of automation do not compromise security.

Seclore Email Encryption Plus for Email Archival

Email Archiving solutions are also fully supported. Organizations have the option to automatically unprotect emails before being archived for long term retention and discovery.

SUPPORTED VERSIONS

Seclore for Outlook:

- Windows: Outlook 2007, 2010, 2013, 2016
- Mac: Outlook 2016 (64 bit)
- Office 365

Seclore for Outlook on the web:

- Office 365 Enterprise
- Microsoft Exchange Server 2016

Seclore Decrypter for Email

Various email security solutions cannot discover sensitive content in encrypted emails and hence fail to decide whether emails should be shared or blocked.

Seclore Decrypter for Email enables secure access to Seclore protected emails and attachments. Decrypting emails and attachments allow email security solutions like DLP, CASB, SEG, and other email content inspection solutions to inspect content and patterns to make appropriate decisions (Allow / Block / Protect) before sending. The Seclore decrypter is universal and works with any email security solution.

Once the Seclore Decrypter for Email is deployed in your email infrastructure, you control the encrypted content exchanged between employees and with external partners. The decrypter does not require any end-user dependency or enablement and is independent of the user device or email client installed on their device.

Seclore Decrypter for Email also works with Seclore Email Auto-Protector to automatically decrypt and re-encrypt Seclore protected emails and attachments before sending them outside the organization.

KEY FEATURES

- **Accelerated Provisioning in the Cloud:** The entire provisioning process from installation to testing and verification is automated, providing data protection of emails and documents in the cloud within 24 hours.
- **One-Click Email Protection:** Protect emails and attachments with just one-click to ensure they always remain private and confidential.
- **Automatically Protect Emails:** Leverage the 'subject', 'to' and 'from' data to automatically protect emails with the appropriate usage controls without user intervention.
- **Extend Email Protection with DLP and Classification:** Automatically add granular usage controls to sensitive data that is classified or discovered in emails and attachments, allowing sensitive information to be shared without interruption or increased security risk.
- **Persistent Security:** The security controls stay with the content regardless of where the email is sent, respective of email client or device. Protection does not depend on the Email Server or Service.
- **Granular Protection:** Protection is not black-and-white but granular and can be customized depending on your use case.
- **Seamless Workflow Integration:** The security options seamlessly fit into the normal email composition workflow. Permissions can be assigned from a simple interface that is part of the Microsoft Outlook Ribbon.
- **'Smart' Sharing:** If protected emails are forwarded, any additional content will get protected automatically and new recipients can get access to the email content immediately.
- **On-the-Fly User Registration:** New external users are automatically registered in Seclore. User registration and onboarding happens via automatic workflows when the email is sent.
- **Email Body Protection:** The message body can also be protected to restrict unauthorized email forwards. Inline responses and email threads are fully supported – right inside Outlook.
- **Access Protected Email without Any Agent Installation:** Protected email body content and attachments can be accessed seamlessly in the browser without any agent installation.
- **Comprehensive Activity Tracking:** Details on how protected emails and attachments are being tracked in real time wherever they go – even to other email domains over public networks or on mobile devices.
- **Email Expiry and Remote Control:** Access to protected emails and attachments can be revoked at any time – even after they are sent. You can also schedule your emails and attachments to expire at any time – regardless of whose inbox they reside in.

About Seclore

Seclore offers the market's first fully browser-based Data-Centric Security Platform, which gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and audit the usage of data wherever it goes, both within and outside of the organization's boundaries. The ability to automate the data-centric security process enables organizations to fully protect information with minimal friction and cost. Over 2000 companies in 29 countries are using Seclore to achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.
Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

Global Headquarters
USA
691 S. Milpitas Blvd
Suite 217
Milpitas, CA 95035
+1-844-473-2567

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49-7621-5500-350

India
Excom House Second Floor
Plot No. 7 & 8
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91-22-6130-4200
+91-22-6143-4800

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City
PO Box 73030
Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

SECLORE