SECLORE

Seclore Rights Management

Automated. Integrated. Data-Centric Security.

Easily Define, Enforce, and Remotely Control Granular Usage Polices

Seclore Rights Management protects sensitive information regardless of device or location. Whether a file is on a server, in an email, on a mobile device, or copied to a USB memory stick unintentionally left behind in an airport, unauthorized users will not be able to access the information. Since usage policies stay with the file, Seclore enables organizations to securely adopt the Cloud, BYOD, and external collaboration.

Seclore makes it easy to centrally define, associate, enforce, modify and audit granular file usage permissions including:

WHO can access the file?
User or Groups Within or Outside the Organization

WHAT can they do with it?
View, Edit, Print, Copy Content, Take Screen Grabs, Work Offline

WHEN can they do it?
Automatic File Expiry, Date and Time Ranges, Number of Days from First Access

WHERE can they do it?
Specific Computers or Devices, Specific IP Address

Ease of Use Means Greater Adoption

Policy Federation

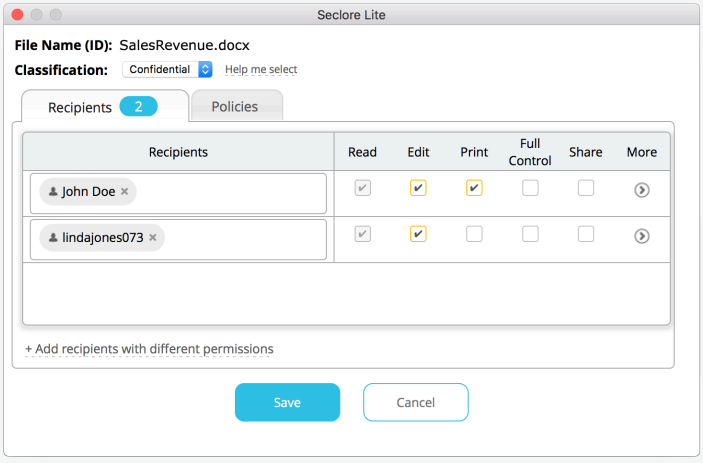
You can automatically apply rights to a file by inheriting policies and mapping them to Seclore using Seclore's Policy Federation capability. Policy Federation provides common policy administration across ERP, ECM and File-Sharing services and Seclore Rights Management.

Bulk Updates

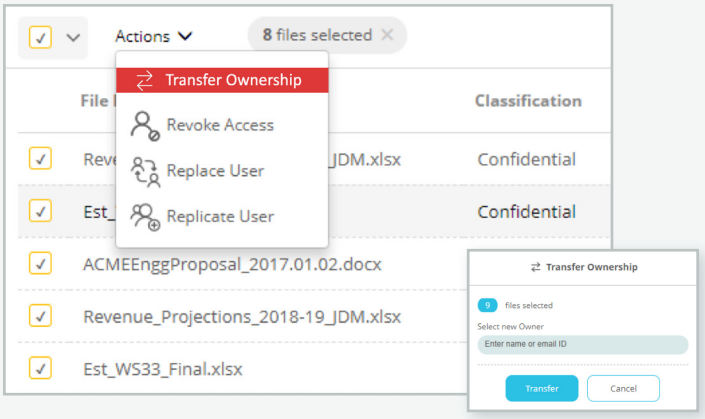
Because employees join, leave and transfer to new teams within an organization on a regular basis, Seclore has removed the onerous task of updating user permissions one at a time. With bulk updates, IT can perform a mass transfer of ownership or revocation of users' rights on protected files, and replicate a user's permissions to another user. These time saving bulk update features reduce the management of protected documents to just one step.

Protect Any File on Any Device and OS

Seclore allows users to protect and utilize any type of file from any device using native applications. The ability to openly utilize Rights Management across all types of documents and devices ensures full adoption while minimizing interruption to work processes.



Granular Control:
Define and attach granular information-centric usage controls to a folder, file or document



Bulk Updates
Replace, replicate or remove access of a user or multiple users at one time.

Here are ways the access and usage policies can be attached to a file:

When a file is closed or saved

When it leaves the network

When the file is attached to an email

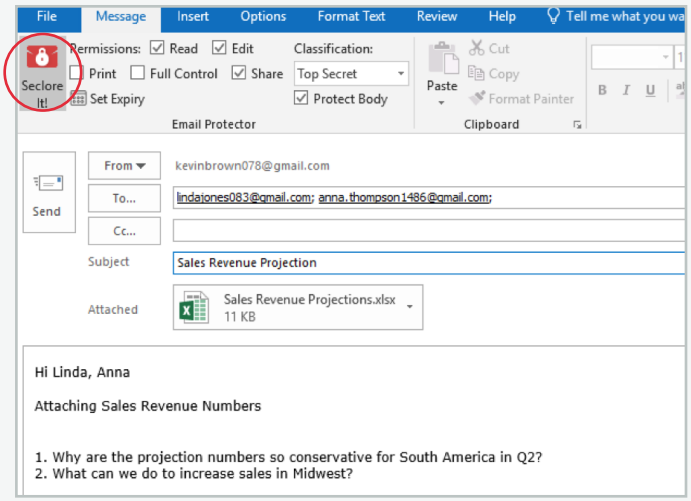
When a file is placed in specially configured 'hot folder'

When a file is downloaded from a document management system

When it is uploaded to Box or other file sharing systems

When the file is created based on user-defined prompts

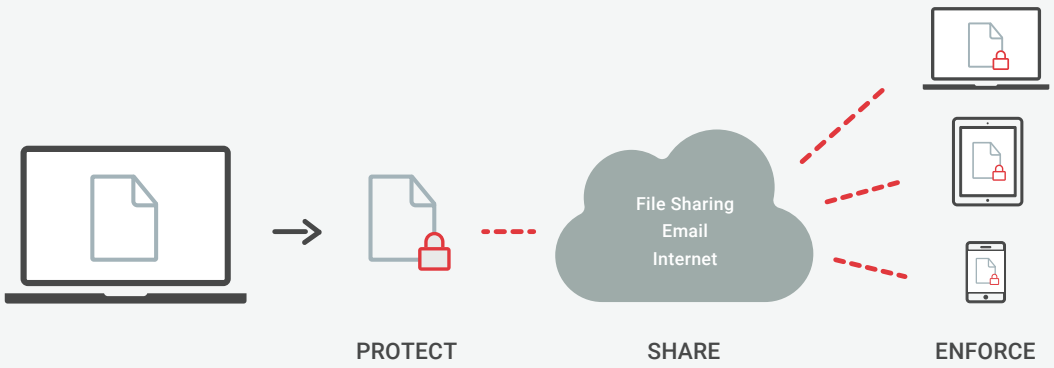
When discovered by a DLP (Data Loss Prevention) system



Easily protect documents and email content within Outlook

Manual and Automated Protection Methods

Here is how Seclore works to protect information. First, you protect a file on your computer. Then you can share the protected file any way you like: email, file-sharing service, USB drives, or using a CD or DVD including placing a file in a 'hot folder' where the file automatically adopts the rights assigned to the folder. You can also connect Seclore Rights Management to your enterprise systems and automatically protect documents as they are downloaded, discovered and shared. The granular usage controls are permanently enforced, regardless of what device or platform the recipient uses to access the file.



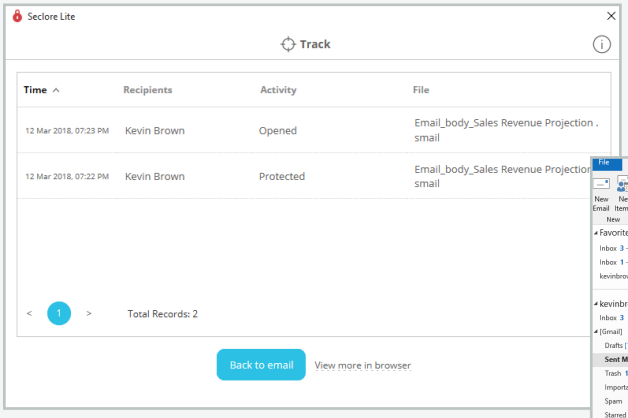
Seclore also allows a user to create and send a protected email from their mobile device or MDM application. Usage enforced policies are based on the 'To,' 'From,' and 'Subject Line,' and are automatically attached to email and documents to safeguard incoming data.

Easily Utilize Protected Documents

Difficulty in using protected documents can bring an entire Rights Management deployment down to its knees. A well-designed Rights Management system should maintain security without hindering the ability of recipients to utilize protected content.

Extend the Security of ECM, DLP, ERP, CRM, Email, and File Sharing Solutions

Seclore offers a rich suite of pre-built connectors that enable organizations to persistently control documents and data as they are downloaded from an ECM system, discovered by a DLP system, shared via EFSS, or attached to an email.



Securely Collaborate on Mobile Devices

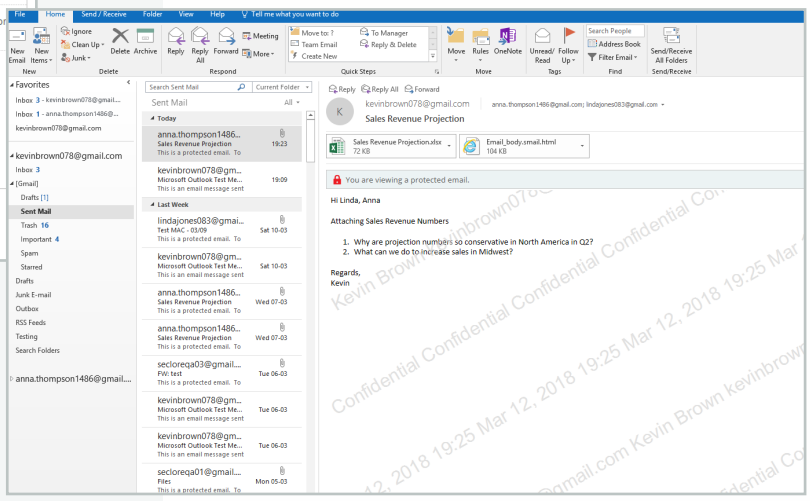
Collaboration on mobile devices has rapidly increased due to technological advancements which creates a nightmare for IT professionals and a dream scenario for cybercriminals.

Seclore offers multiple ways organizations can secure sensitive emails and documents on an employee-owned device. Seclore Lite for Mobiles can automatically protect documents shared to a mobile device or MDM-enabled device with persistent, granular usage controls that enforce who can access the document, what they can do with the document (view, edit, and reply) and for how long.

Browser-Based Rights Management

In addition to the Seclore Rights Management full-fledged client that offers all capabilities, Seclore also provides a light client that can be installed **without administrative privileges.**

Native apps are available for Windows, Mac, iOS, and Android. For the ultimate ease-of-use, Seclore enables organizations to view, edit and print protected files from their browser **without any agent download.** As well, administrators and other users can protect files and track usage within their browser.



Comprehensive Email Protection

In the modern world, email is the most widely utilized form of communication. Seclore Rights Management offers the richest set of email security capabilities in Outlook, and is easy for users to add security and usage policies to sensitive email messages and attachments. Recipients see the protected emails within the Outlook window itself, and any forwards or replies will also stay protected with the same security controls.

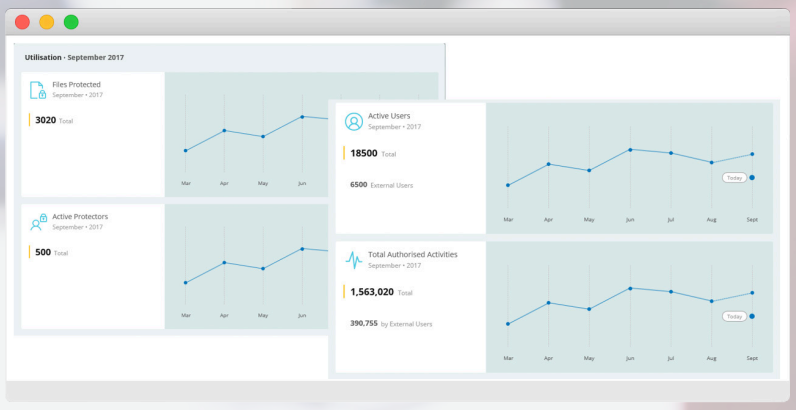
External recipients can collaborate on the same email thread using the browser-based Secure Email Viewer, without any agent. Protectors can track each of their emails, to see who has accessed it, what they've done (edit, print, etc.) and when, from within Outlook itself. Protectors also have the power to revoke access for any user at any time, to ensure that sensitive content is no longer accessible. This is the true 'Undo Send' button that you've always wanted but never really had, until now.

Frictionless Authentication

Seclore also features a rich Identity Federation capability, enabling users to authenticate using a variety of SSO, social media, and directory sources.

Simplify Audit and Compliance Reporting

Seclore features automatic tracking and monitoring of files access and usage wherever they travel or reside. Ready access to consolidated data about who viewed the file, what they did with it, what device was used to access the file, and when, makes it easy to address regulatory compliance and audit reporting requirements.



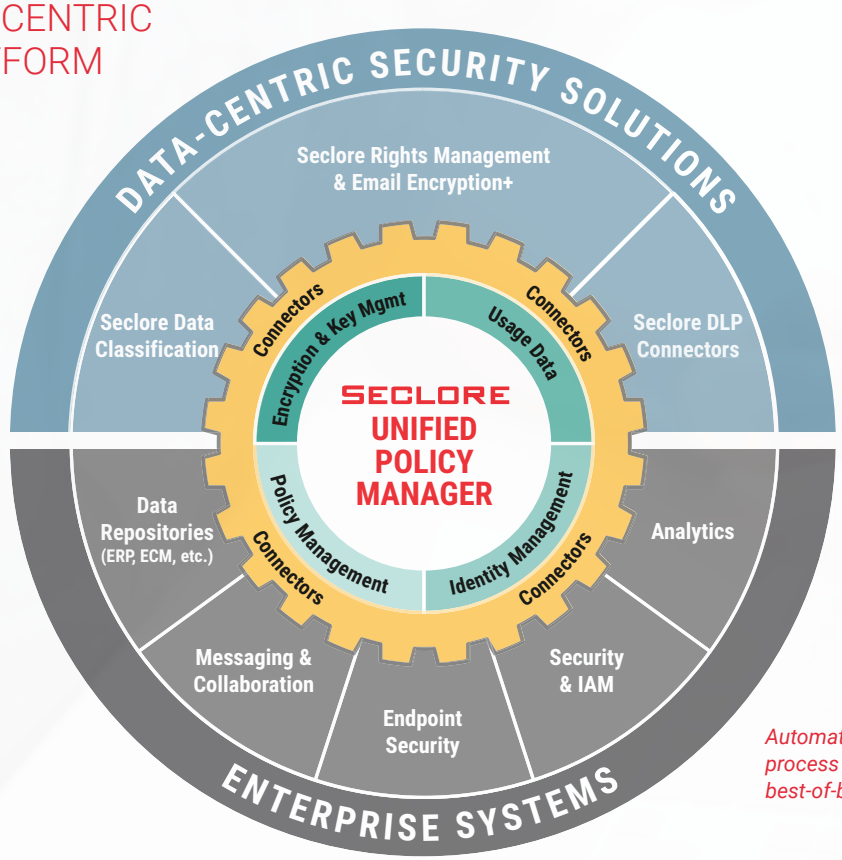
Audit Usage of Information: WHO accessed the file, WHAT did the user do, WHEN & WHERE is all captured from distributed usage environments and reported centrally to simplify audit and compliance reporting

An Integrated, Automated Approach to Data-Centric Security

Seclore Rights Management in combination with Seclore Data Classification enables organizations to seamlessly integrate other best-of-breed data-centric security solutions (such as DLP, CASB and eDiscovery) to automate the end-to-end data-centric security process, from discovery to classification to protection and usage tracking.

The rich library of connectors and policy federation also makes it easy for organizations to integrate existing enterprise content management and collaboration solutions (such as email, EFSS, ERP, and ECM) into the data-centric framework so that documents are automatically classified and protected as they are downloaded and shared.

SECLORE DATA-CENTRIC SECURITY PLATFORM



Automate the data-centric security process with the flexibility of using best-of-breed security solutions

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 analyze 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