

SECLORE

Seclore Classification-Driven Data Protection



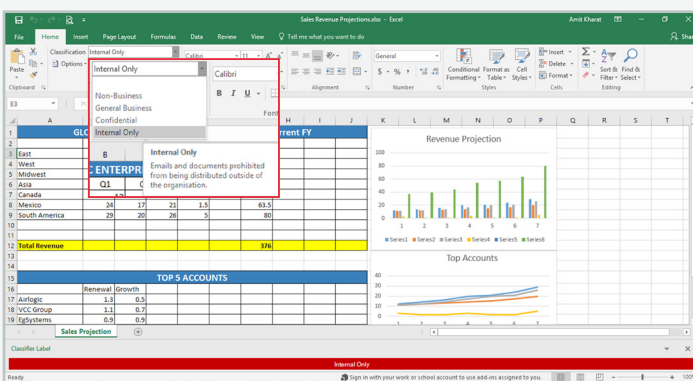


Seclore Classification-Driven Data Protection enables organizations to easily define and apply classification to their documents and emails when users create, modify or send them. Seclore Classification-Driven Data Protection, works seamlessly with Seclore Rights Management, allowing organizations to classify and automatically protect and track their sensitive information in one-click - wherever it travels to close security gaps and address regulatory compliance.

Other key features include:

- Easy-to-define classification policies that reflect the organization's unique data security and regulatory requirements
- Extensive classification configuration options including how much input the user should have and how a classified document should be treated
- Metadata classification labels attached to files via Windows File Explorer to control who can see or share content
- Identity-based classification rules can be defined using Active Directory attributes
- Adaptable visual markings on documents ensure awareness of the data classification and safeguarding responsibilities
- Policy violations are flagged to assist security administrators with remediation

Users can easily select a classification policy from a drop-down menu



One-Click Classification and Protection

Seclore automatically adds the appropriate usage controls and tracking to the file when a user selects a classification label. Now you can be confident that your sensitive information remains fully under your control no matter where it travels. All that is required of your users is a single click!

Put Your Users in the Driver Seat

Granting users the self-governance to select the appropriate level of classification for their documents and emails helps build their awareness and engagement in protecting the sensitive data that they are creating, modifying, or sending. When they deem a document or email as sensitive by adding the appropriate classification label, protection and tracking are added seamlessly without any additional steps on their part.

Keyword-Based Classification

With Keyword-Based Classification you never have to worry that a sensitive document or email is shared without being classified and protected. When a sensitive keyword is detected in a document, email or email attachment, an automatic notification

How Seclore Classification-Driven Data Protection Works

Seclore Classification-Driven Data Protection empowers an organization's users to apply relevant visual and metadata labels to emails, attachments and files to better identify what information is sensitive and requires protection. As documents are created or shared, the sender can easily select the appropriate classification from a user-friendly menu.

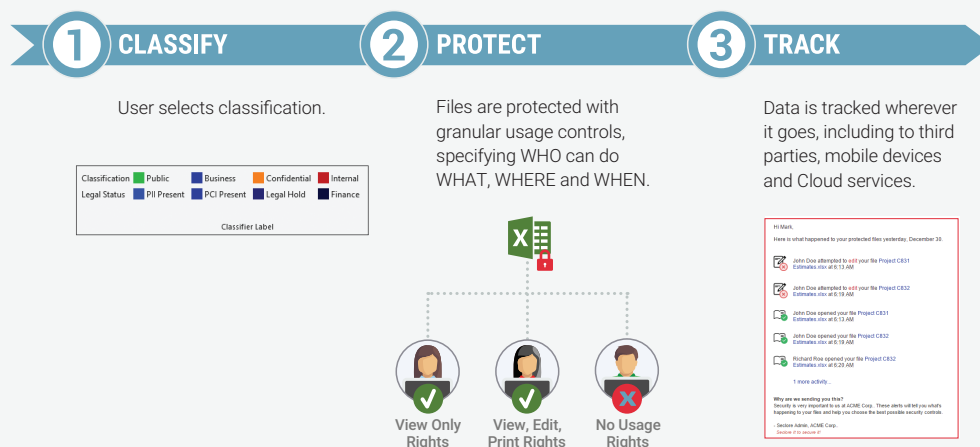
prompts the user to either select a classification label or upgrade the classification label that was selected. Depending on the configuration, you can allow users to modify the classification label or require them to change to the recommended classification level before closing a document or sending an email.

No File or Email Left Unprotected

Seclore also provides you the option to make classification mandatory for all documents and emails which ensures all sensitive documents have protection policies when shared. Requiring classification on all documents and emails is especially important when sharing files with third-parties as many companies are required by compliance regulations to protect personal data even when it's not in their possession.

Simplify Audit and Compliance Reporting

Seclore provides visibility into classified and protected documents. Seclore features automatic tracking of classified file access and usage such as who viewed it, what they did with it, what device/IP address was used to access it, and when. Knowing how sensitive a document is and what actions have occurred on the document makes it easy to address regulatory compliance and audit reporting requirements.



The ability to remotely revoke access is also essential to addressing the proliferation of compliance regulations that require organizations to protect IP and Personally Identifiable Information (PII) data wherever it resides.

By automating the protection of documents and not relying on users to add usage controls, organizations can ensure sensitive information remains fully protected and rapidly reduce security gaps.

An Integrated, Automated Approach to Data-Centric Security

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

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



About Seclore

Seclore offers the market's first open, browser-based Data-Centric Security Platform, which gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and track 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.

www.seclore.com

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

Singapore

Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

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

