SECLORE

Seclore for Microsoft Sensitivity Labels

Automatically add best-in-class data-centric security to sensitive documents and emails classified by Microsoft's sensitivity labels

KEY FEATURES

- Automatic protection for classified documents
- Automatic and agentless protection for classified emails
- Persistent, granular usage controls
- Seamless integration with discovery solutions like DLPs, CASBs, SEGs to automate data security
- One-click access of protected documents in the native application or Seclore Online browser
- Security dashboard to meet compliance, audit, and risks objectives
- Real-time revocation of access to protected documents and emails regardless of where they reside

More than ever before, users are working outside the corporate network, pushing more organizations to adopt the cloud. With this significant paradigm shift to the new virtual workplace, the volume of data is exploding everywhere.

Data classification is often the first line of defense in knowing what data is sensitive, the level of sensitivity, and where it resides. However, classifying data alone is meaningless when it comes to security. Without adding data protection to a classified document or email, the data is defenseless and at risk. The visual label may determine the level of sensitivity, but it also alerts nefarious insiders and hackers which data is most valuable to steal or misuse.

Also, employees need to collaborate externally with partners, contractors, vendors, and suppliers; however, trusted third parties could share sensitive information with unauthorized users. And employees can unknowingly share classified data with bad actors. Once data classified as highly sensitive is outside the organization, there is no tracking or revoking access to recover the data.

Also, the growth of data protection laws and regulations like GDPR, NYDFS, HIPAA, ISMS-ISO27001 require organizations to effectively label and track regulated data such as PII, shared within and outside the organization. Classified data by itself, though, has no real protection without the appropriate security permissions attached to it based on the classification label.

Another challenge is the data protection capabilities available in Microsoft 365. They are either lacking or fail to deliver secure collaboration or both. Because of these data protection challenges, Data Protection Officers cannot meet compliance objectives with classification labels alone. The label does its job by identifying the level of sensitivity but does not make it "actionable" by protecting it from loss.

So, how can your organization keep control of your sensitive data even after classified by Microsoft's sensitivity labels?

Adding Data-Centric Security for Microsoft Sensitivity Labels

Seclore for Microsoft Sensitivity Labels provides automatic data protection with persistent, granular usage controls on sensitive documents classified in Office desktop applications, and emailed through Outlook on desktop, Outlook on the Web, and Outlook on Mobile (Android or iOS).

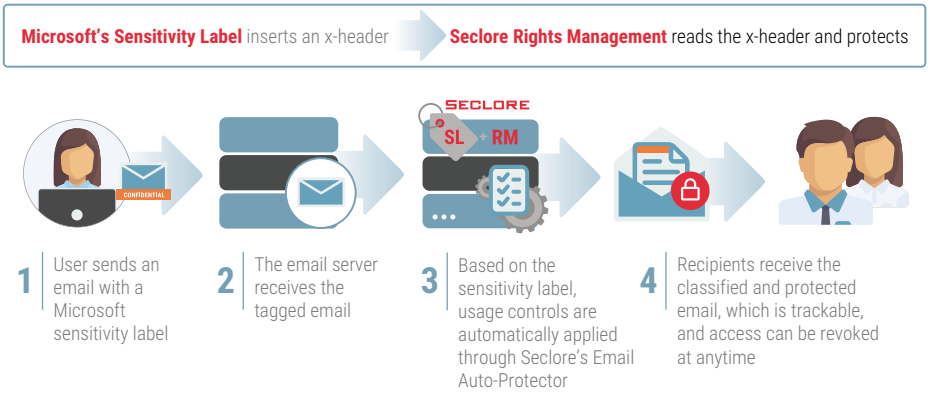
Once users classify documents using MS Office applications, automatic data protection from Seclore is triggered based on the applied label's security policies. Also, classified emails and attachments sent on any device through any Outlook email client are also automatically protected through Seclore's Email Auto-Protector. Seclore's granular usage controls (view, edit, print, share, screen share), ensures only authorized users and recipients can open, utilize, and edit the document or email.

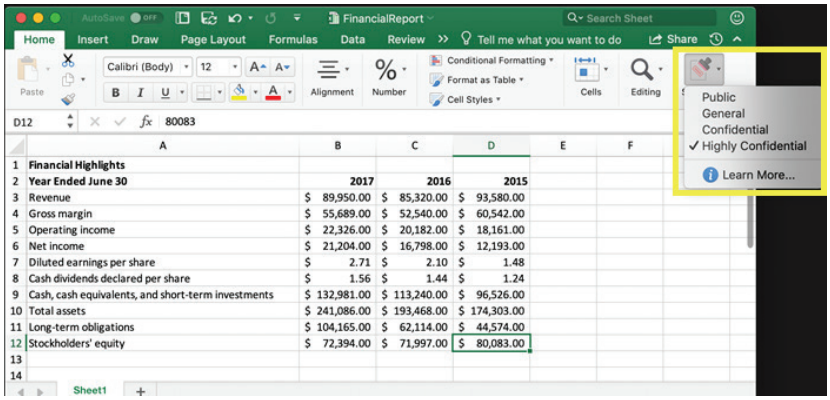
In addition, users who sync files on the desktop using OneDrive can automatically protect sensitive files classified with Microsoft's sensitivity labels within the MS Office desktop application. By attaching usage controls to classified emails and documents in OneDrive, users can securely collaborate with minimal impact on their productivity.

Seamless integration with Discovery solutions

Besides automatic protection and secure collaboration of classified data, Seclore also provides seamless integration with Discovery solutions like DLPs, CASBs, and SEGs. Seclore allows the Discovery solutions to read the sensitivity label on a protected document or email and take the appropriate action (allow/block) based on the sensitivity of the information.

Automatically protecting classified data that is sensitive improves your organization's overall security posture to protect against data breaches, prevent sensitive data fall into the wrong hands, and meet compliance regulations.





1 The user selects a sensitivity label

2 If the document is sensitive, it gets automatically protected when the file is closed

3 Discovery solutions can read the classification metadata to take action

How it Works

Classification-Driven Protection for Office documents

When users open a document in Office applications like Word, Excel, and PowerPoint, they can manually apply a Microsoft sensitivity label. The sensitivity label also can be applied automatically based on pre-defined policies. Once the document or email is marked with a sensitivity label, Seclore's persistent, granular usage controls are automatically attached to it and remain with it wherever it travels. As a result, the protected classified data is now trackable, whether it resides inside or outside the organization's network.

Classification-Driven Protection for emails and attachments

When a sensitivity label is detected on an email, access and usage controls are automatically attached to the email and attachments by Seclore's Email Auto-Protector.

The Email Auto-Protector acts as an MTA (Mail Transfer Agent) and allows an organization to set up data protection rules to automatically apply usage controls to emails and attachments. As a result, the process is entirely transparent to the email sender, and access to the email and attachments can be modified or revoked at any time for secure collaboration.

Key Benefits

Seclore Data-Centric Security Platform combined with Microsoft's sensitivity labels

Seclore's best-in-class data-centric security technology is integrated seamlessly with Microsoft's sensitivity labels. The combined solution allows employees to securely collaborate with internal and external users without your organization worrying about accidental or deliberate data leakage.

Automatic protection of classified documents

As soon as a document is classified with a Microsoft sensitivity label by a user or automatically applied by a policy, Seclore automatically applies the appropriate data protection rule. Thus, the user does not need to worry about manually protecting documents or deciding which security policy to apply.

Automatic and agentless protection of classified emails

Seclore automatically adds granular usage controls to sensitive data classified or discovered in emails and attachments from any device, or any email client, allowing sensitive information to be shared without interruption or security risk.

Close security gaps

Seclore for Microsoft Sensitivity Labels provides true value to classified data, enabling organizations to close security gaps.

Data-Centric Governance

Seclore provides a dashboard with real-time tracking and visibility on authorized and unauthorized attempts performed on protected data regardless of the location of the documents. In addition, the dashboard helps organizations meet compliance regulations by centralizing data-centric audits in a single view.

Lower administrative cost, higher ROI

Automation of data protection eliminates the dependency on users to manually protect sensitive emails and documents, requiring less administrative resources for user training and support. Plus, automation accelerates the adoption of data security along with minimal deployment and reduced ongoing administrative costs to maximize your ROI.

Persistent security

Seclore's granular usage controls stay with the protected content wherever the document or email is sent, regardless of the email client or device.

Integrated approach to data-centric security

Seclore's open Data-Centric Security Platform integrates and automates the discovery, classification, and rights management process. Seclore allows discovery solutions like DLPs, CASBs, SEGs, etc., to read Microsoft's sensitivity labels' metadata on emails to automatically apply the appropriate action and security policy.

Seamless access to both internal and external users

Users can seamlessly access protected files in the native application or Seclore's secure browser-based Online Editor for secure collaboration.

Email expiry and remote control

Access to protected documents and emails and attachments can be revoked at any time – even after they are shared. And while defining usage policies, you can also schedule your emails and attachments to expire at any time – regardless of whose inbox they reside in.

Edit and automatically re-save classified and protected files through OneDrive Sync client

Users can apply sensitivity labels to documents directly from the desktop's OneDrive Sync through the native application. Edited documents are automatically synchronized back as classified and protected to Microsoft 365.

SECLORE