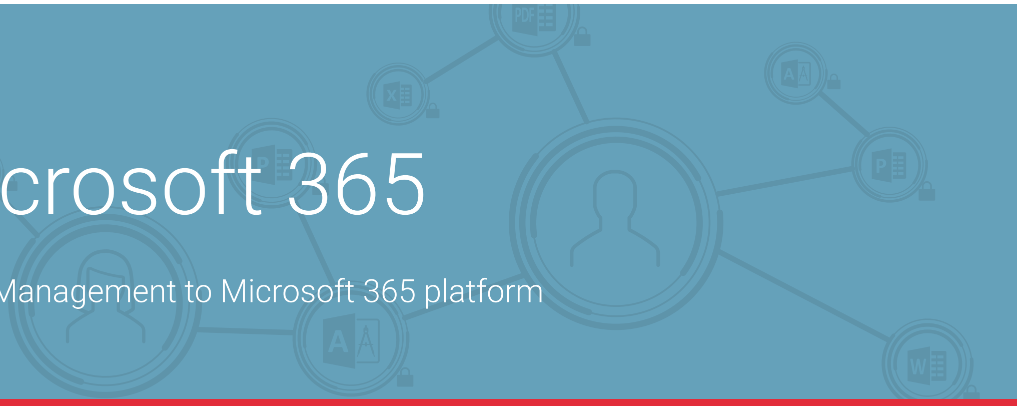
Seclore for Microsoft 365

Seamlessly add best-in-class Rights Management to Microsoft 365 platform



KEY FEATURES

- Automatic protection as soon as documents are uploaded
- Federation of policies from Microsoft 365, even after document is downloaded
- Enterprise ID federation for Azure with SSO
- One-click access of protected documents in native application and in Seclore Online browser
- Edit and save back content automatically in Microsoft 365
- Instantly revoke access to emails and documents, even after download
- Automatically add data security to sensitivity labels on emails and documents

As your organization moves to the cloud and embraces Microsoft 365, the most immediate concern you need to overcome is the security of your sensitive data and intellectual property. Today, data protection capabilities available in Microsoft 365 are either lacking, or fail to deliver secure collaboration, or both.

Seclore Rights Management for Microsoft 365

Seclore Rights Management provides persistent, granular usage controls on sensitive documents created on Office desktop applications, emailed through Exchange Online and Outlook Web, classified by sensitivity labels, and uploaded to Microsoft Teams, SharePoint Online and OneDrive in Microsoft 365.

Once users create, classify, or upload their protected documents, authorized users and recipients can open, utilize, and edit the document securely through their browser. In addition, users who have synced Seclore protected files on their desktop using OneDrive can open and edit them in native applications and automatically save them back to Microsoft Teams, SharePoint Online and OneDrive. By attaching usage controls to sensitive or classified emails and documents in Microsoft 365, users can confidently collaborate on the cloud with minimal impact to their productivity.

Key Features and Benefits

Industry-leading Rights Management for Microsoft 365

Your organization can start using best-in-class Seclore Rights Management technology on Microsoft 365 platform. Your employees can securely collaborate with internal and external users without worrying about accidental or deliberate data leakage.

Automatic protection of uploaded documents to Microsoft Teams and SharePoint Online

Enforce automatic protection in Microsoft 365 as soon as documents are uploaded into Microsoft Teams channels or SharePoint Online. The user does not need to worry about manually protecting documents or deciding which security policy to apply.

Policy federation and instant revocation

Minimize administrative overhead by federating permissions directly from SharePoint Online, instead of defining policies in the Seclore Unified Policy Server separately. Changes in SharePoint permissions automatically and instantaneously get reflected on the protected document anywhere in the world. Access to the protected document in Microsoft Teams, SharePoint and on the downloaded document are both automatically revoked.

Full support for native desktop apps on Windows and Mac

Users can access Seclore protected documents in native office applications on their Windows or Mac. By installing the Seclore agent on a user's machine, data protection on documents is enforced as per the organization's policies as well as all authorized activities and unauthorized attempts are tracked.

Seamless access for both internal and external users

Accessing Seclore protected documents from Microsoft 365 applications like Microsoft Teams, SharePoint and OneDrive is simple. With one click, the protected document opens in a feature rich and secure Seclore Online Editor.

Enterprise ID Federation with Azure

Seamless identity federation with Azure allow employees and external users to authenticate using Enterprise Azure Identity solution before accessing Seclore protected files. Seclore agent's 'one-time authentication' feature allows users to sign-in only once on any device for seamless access.

Secure agentless access within the browser itself

Your Microsoft 365 users can open Seclore protected documents with a single-click from Microsoft Teams, SharePoint Online and OneDrive once their authentication is federated from Microsoft 365 through SSO. Users can open and edit the protected document in the browser without downloading the document. The edited documents are automatically saved back.

Seamless access in native application from Microsoft Teams

Users can select usage controls (view, edit, print, share) in the Outlook ribbon and then click the 'Seclore it' button to add persistent, granular usage control to sensitive emails sent across and outside the organization.

Users can also edit and automatically re-save the protected file in Microsoft 365 through OneDrive sync client or they can edit documents directly from the desktop's OneDrive Sync through the native application. Edited documents are automatically synchronized back to Microsoft 365.

Automatic email protection with Exchange/Exchange Online

Seclore Email Auto-Protector for Exchange Online in Microsoft 365 provides automatic protection of incoming and outgoing emails and attachments.

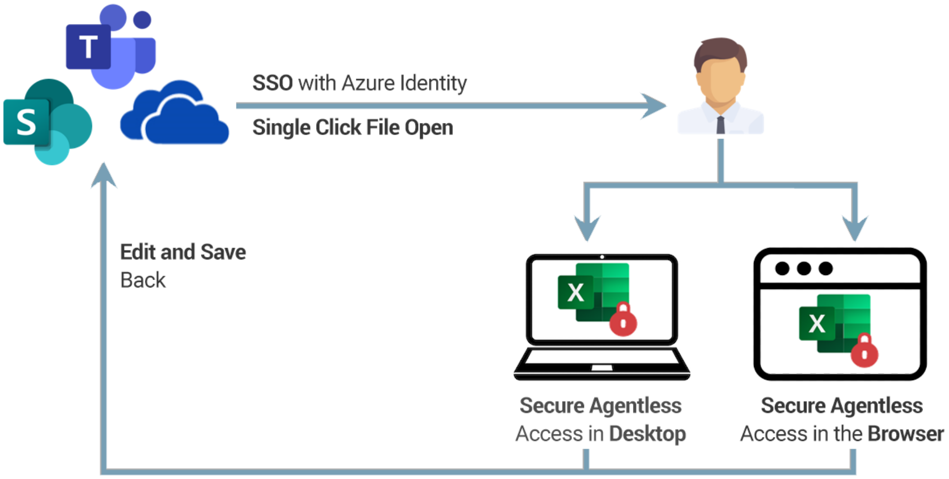
Automatic data protection added to sensitivity labels

Whether Microsoft's sensitivity labels are manually or automatically applied, Seclore automatically attaches a predefined security policy to the document or email, based on the sensitivity of the label. Without security on highly classified data, the data is at risk, rendering the label meaningless.

An Open Approach to Data-Centric Security

Seclore's open Data-Centric Security Platform enables organizations to seamlessly integrate leading DLP, Data Classification, Rights Management and SIEM systems with Microsoft 365 for iron-clad data protection and tracking. The open framework leverages metadata to automate processes between the various systems, ensuring sensitive information is automatically protected without user intervention as documents are discovered, classified, downloaded, or emailed.

The tight integration provides the flexibility to connect existing best-of-breed data protection solutions with Microsoft 365 collaboration and content management solutions, while allowing you to future-proof your infrastructure for new, innovative data- centric security technologies.


SSO with Azure Identity
Single Click File Open
Edit and Save Back
Secure Agentless Access in Desktop
Secure Agentless Access in the Browser

Seclore extends best-in-class Rights Management to the Microsoft 365 platform -- Automatic protection in Microsoft Teams and SharePoint Online, allowing users to seamlessly authenticate using Microsoft Azure identity, experience one-click opening of protected documents in a browser or native application, seamless editing, and automatic save-back into SharePoint Online.

Microsoft 365 Solutions Supported by Seclore

Protection on Desktop and Access in Native Apps

&

User Driven Email Protection

Automated Email Protection

Automatic Data Protection for Sensitivity Labels

Securing Collaboration and Productivity Apps

Identity Federation