SECLORE™

Seclore for Microsoft 365

Add Enterprise-Grade Security for Your Microsoft 365 Platform

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. Data protection capabilities available in Microsoft 365 are either lacking or fail to deliver secure collaboration or both.

1 in 5
Corporate Employees use a Microsoft 365 Cloud Service

Source: Teamshub

145 Mn users 2021

270 Mn users 2022

The number of daily active users of Microsoft Teams have **almost doubled** the past year.

Source: Statista

15% of organizations using Microsoft 365 have suffered over 500 data breaches in the last year.

26% of users reported that the inbuilt security controls in Microsoft 365 made collaboration very difficult.

43% reported these security tools part of Microsoft 365 required a high level of admin to maintain.

Source: Businesswire

Seclore Data-Centric Security for Microsoft 365

Your organization can leverage best-in-class Seclore data-centric security to securely collaborate using Microsoft 365.

Protection on desktop
Seamless access in native apps

Classification-driven protection
Drive protection

Email protection
User-driven and automated

Securing collaboration and productivity apps

Securing mobile data sharing

Identity federation

Enterprise-Grade Security: Seclore provides persistent, granular usage controls on sensitive documents created, edited, emailed, uploaded, or shared using Microsoft 365 Apps. Seclore's laser-sharp security focus adds the much-needed (and currently missing) enterprise-grade security to your Microsoft 365 application stack.

It Just Works: It fits right into your Microsoft 365 setup, even if you have subscribed to the base Microsoft 365 plans. Users can continue to create, collaborate on Microsoft 365. Seclore automatically secures this information in this workflow. Protected documents can be seamlessly accessed using the standard options in Microsoft 365. Single Sign-On with Azure AD and file access through agentless secure browser-based editors or desktop applications ensure zero impact on user

Absolute Security Through Automation: Automatic Protection at source, which includes Desktop, SharePoint, OneDrive, Teams, and Email, ensures consistent and scalable security, without depending on the administrators to define policies or end-user to take decisions. Seclore protects millions of documents everyday with no admin overhead.

Seclore offers best-in-class Data-centric security for Microsoft 365

- **ZERO** User **Dependency**
- **100%** Seamless User Experience
- **FULL** Interoperability with Sensitivity Labels
- **NO** Admin Overhead
- **SECURE** External Collaboration
- **FULL** Control over Security

SECLORE™

Value Proposition

ZERO User Dependency | Automatic Protection Microsoft Apps

Seclore automatically protects the sensitive data as soon as it is created, uploaded, shared on the Microsoft 365 cloud. There is zero dependency on the user to decide the type of security to be applied to the sensitive information. The user doesn't need to worry about manually protecting documents or deciding which security policy needs to be applied.

100% Seamless User Experience | Native

Seclore automatically authenticates users through Azure AD Single Sign-On, with no additional authentication-flows. Users can access secured documents in their Microsoft 365 Apps directly in their desktop applications or in Seclore's Agentless Secure Browser-based editor. Edited documents are automatically synchronized back. to

FULL Interoperability with Sensitivity Labels

Microsoft Sensitivity Labels may be suitable, but the MIP security that follows is not. Seclore's Sensitivity-label-driven-protection enforces Seclore protection as soon as your users or automation classifies your sensitive content.

NO Admin Overhead | Policy Federation and Security Workflows

Seclore federates user permissions directly from Microsoft 365 apps without any policy definition in Seclore's Policy Server. Changes in SharePoint permissions automatically and instantaneously get reflected on the protected document anywhere in the world, even if they are residing outside Microsoft 365 cloud apps. Seclore allows document owners to revoke access to information for a specific person and at any given time. Seclore's Security workflows like Smart Share and Request Access Rights prevent the user's productivity from getting impacted without waiting for Admin to create and roll out policies. Seclore starts giving value from day zero itself.

SECURE External Collaboration | Any Platform, Any Application

Seclore delivers a frictionless user experience no matter where your partners, vendors, customers access files and emails - across devices, platforms, and applications. Security travels with the file. Authentication is seamless through Seclore's inbuilt Identity Management system. External users don't even need Microsoft Application licenses to access Secure documents shared with them.

FULL Control over Security

Seclore offers the flexibility to host Seclore systems on the Seclore Cloud, any other public or private cloud, or on-your premises. If necessary, add an additional layer of security through your preferred choice of HSM. Gain complete controlover where the servers, keys, and metadata are stored and managed.

See How Seclore Gives You More

FEATURES	MIP	SECLORE
Security		
Dynamic watermarking	🟠	🟢
Secure data in Cloud applications	🔴	🟢
Revoke user's access at any point in time	🟠	🟢
User Experience		
Ease of access of desktop, Online, and mobile	🟠	🟢
Agentless access i.e. agent installation is not a prerequisite	🟠	🟢
Track user activities by data owners	🟠	🟢
Request for access and extend permissions	🟠	🟢
Administrative and User Overheads		
Policy federation	🔴	🟢
Support for business changes like transfers, terminations, role changes, and others	🟠	🟢

🔴 No Security 🟠 Limited Security 🟢 High Security

"We found Seclore to be the most secure and unbreakable tool to ensure the privacy of our data as we share it with governments and regulators all over the world."

Head – Dept. of Safeguards
International regulator of nuclear technology

"Seclore's depth of technology and expertise helped us address our customers' concerns when they share their most sensitive Intellectual Property with us."

Director – Operations
Large semiconductor equipment manufacturer

"The Seclore platform works seamlessly with our existing data sharing and access control tools, giving us even more value from our existing IT investments."

SVP – Retail Liabilities
Largest credit card services organization