

Comparison of Seclore & Microsoft Information Protection

DATASHEET

Look at these numbers...



30K

U.S.

Organizations

Newly Hacked Via Holes in Microsoft's Email Software

Source: [KrebsonSecurity.com](https://krebsonsecurity.com)

Before 2021 Breach



Microsoft Exchange Was Used to Hack Diplomats

Source: [Bloomberg.com](https://www.bloomberg.com)

Microsoft Spills
38 Million

Sensitive Data Records Via Careless Power App Configurations

Source: [Upguard.com](https://www.upguard.com)

Microsoft Security Shocker

250 Million

Customer Records Exposed Online

Source: [Forbes.com](https://www.forbes.com)



Your Data Can Be Easily Hacked with Microsoft Information Protection

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.

Data protection capabilities in Microsoft 365 are either lacking or fail to deliver secure collaboration, or both. Using an M365 enterprise offering like Microsoft Information Protection (MIP) may provide data security for your organization for free. But it may not be the best-of-breed solution that meets your organization's data security needs. The "free" offering may work in favor of Microsoft, but it does not necessarily help you achieve your enterprise security goals.

Why Seclore's Data-Centric Security Platform Is Better?

Parameter	Challenges with Microsoft	Benefits of Seclore
 Data Security	The file is unprotected when uploaded to the cloud applications. For example, opening a file in Office Online from cloud applications allows easy copying of content.	Provides consistent protection for all file formats across all channels of communication and collaboration.
 Granular Security Control	Security does not extend universally to non-MS Office formats. Non-Microsoft files like PDF documents do not get protected when shared via Outlook on the desktop.	Data always remains protected, whether on users' devices or in the cloud, regardless of the format.
 Data-centric Audits	No way to revoke a document for specific users. Revoking a document means killing all recipients' access to the files and resending a new copy to the intended recipients making it impractical.	Granular controls – time expiry, device lock, location lock, set differentially for different user/user groups. Revocation can be done contextually to provide flexibility.
 Visibility	Easy to bypass the security. For example, users can copy content and create unprotected copies by converting a Word file to PDF with copy permission.	Secure even when accessed in online mode with dynamic watermark overlay.



Security gaps lead to a false sense of security



Parameter	Challenges with Microsoft	Benefits of Seclore
 Ease of Use	High-end user friction because of pre-requisites, incomplete and inconsistent experience, e.g., viewer and MIP plugin requirements for non-office formats, Office license and Outlook a pre-requisite for access on mobile, tracking user activities for office files only, revoke for all or none.	Agentless access makes it easy for end-users to access protected documents, making security in external collaboration with third parties simple. End users can easily track their protected emails and documents, gain visibility via real-time alerts, daily digest, and revoke if needed, without going through an admin.
	Predefined sensitivity label-based policies make the MIP framework impossible to adopt for ad-hoc collaboration making it less flexible, admin dependent, and introducing delays. Every time a new partner is onboarded and needs to access MIP-protected documents, they will first need to be added to the sensitivity label policies. This activity needs admin intervention.	Policies are built at runtime to accommodate real-world ad-hoc collaboration needs. Inbuilt features like Smart share to extend permissions and Requesting access from data owners allow users can send emails and share documents via cloud applications on the go.



<i>Parameter</i>	<i>Challenges with Microsoft</i>	<i>Benefits of Seclore</i>
 Administrative and End User Overheads	It is essential to set up permissions beforehand via sensitivity labels, as security policies are not in sync with collaboration apps' permissions. For example, every time there is a change in permissions on SharePoint Online or MS Teams, the MIP admin needs to make the relevant changes in the sensitivity label policies. Imagine the administrative nightmare to keep policies in sync! This heavy dependence on administrators makes the MIP framework impossible to adopt at a large scale.	Policies are built dynamically on the fly and federated from the collaboration apps, removing the need for admin intervention.
	There is a severe need for end-user, admin training, and awareness. The users need to understand labels and policies, different experiences for office and non-office formats, license requirements, etc.	Dynamic policies, policy federation, low touch administration, and agentless access reduce the need for end-user and admin training and awareness.
	Difficult to handle business changes (Transfers, terminations, role change, and new hires) that require regular admin intervention and policy updates	It is a security tool that adjusts and provisions for business changes, making it easy to adapt and scale.



Higher administration needs, policy creation, and maintenance overheads make it challenging to adopt the solution at scale, increasing the data security risk for an enterprise.



Reduced Admin and Policy overheads allow for a faster rollout at scale within an enterprise.

About Seclore

Seclore offers the market's first entirely browser-based data-centric security solution, enabling organizations to use files wherever they go, both within and outside their boundaries. The ability to remotely enforce and audit who can view, edit, copy, screen share, and redistribute files empowers organizations to embrace mobility, file-sharing, and external collaboration with confidence. With over 2000 companies in 29 countries using Seclore to protect 10 petabytes of data, Seclore is helping organizations achieve their data security, governance, and compliance objectives.

Learn how easy it is to keep your most sensitive data safe and compliant.

Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

