

Comparison of Enterprise Rights Management Solutions

Seclore

VS

Microsoft AIP

(Azure Information Protection)

Overview...

Open vs Locked In

SECLORE

- Seclore has an **open architecture** that fits in with your existing IT infrastructure, and still keeps you **future-ready**
- No change to your existing:
 - Identity and Access Management (IAM) tools
 - File Servers and ECM systems
 - Transaction systems and Reporting tools
 - Email and Collaboration tools
 - DLP and other security tools

MICROSOFT AIP

- Microsoft restricts you to its ecosystem and forces you to use Azure AD, SharePoint, Outlook etc.
 - You must have an Azure AD directory to use Azure Information Protection.

Security and Compliance

SECLORE

- **Military grade security** which is tested by governments and defence agencies globally
 - Option to keep Identity Management system on-premise and not use a Cloud service
 - **IP Address controls** provide compliance with geographic data residency norms
 - **Bring Your Own Encryption (BYOE)** to ensure tamper-proof custom encryption
 - **Granular controls** in terms of blocking Copy/Paste, Print to PDF, Offline access

MICROSOFT AIP

- Microsoft is vulnerable to man-in-the-middle attacks and has been cracked publicly.
 - It is possible for a user with (at least) VIEW permissions to decrypt the data with a publicly available open-source tool.
- With rights to edit, user can copy secure content out, even post revocation user can access for 30 days

Automation vs Manual

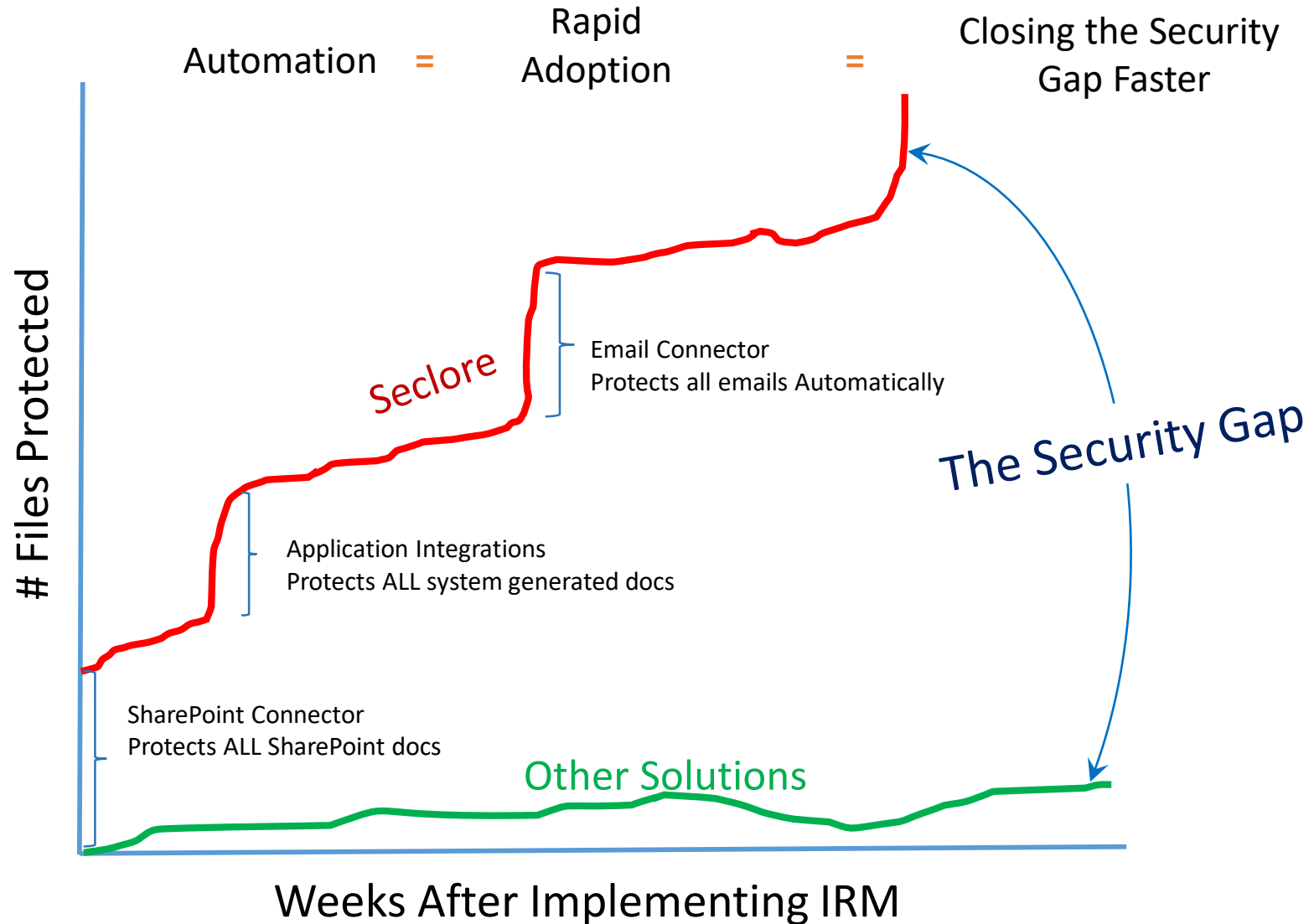
SECLORE

- Seclore **automates protection** to ensure adoption is quick and predictable
 - Connectors make file protection automatic
 - Policy federation makes policy management automatic
 - Connects into enterprise DLP, Classification, CASB, Discovery, SIEM solutions
 - Protecting data at its source accelerates adoption
 - Little to No dependency on the end user
 - Low overheads on IT team for extensive user enablement and training

MICROSOFT AIP

- Microsoft depends on manual protection with dependency on the end user.
- Over dependency on the end user to control enterprise risk.
- User enablement and training overheads

Why Automation Matters?



Usability and Security in External Collaboration

SECLORE

- Higher **focus on usability** for larger enterprise rollout and adoption
 - Removing user from the context with automated protection
 - Same level of security in external collaboration
 - **OTP based access**, with automated external user on-boarding
 - **Track and Revoke** from within Email app
 - **Agentless**, browser based editing of protected files
 - **Smart sharing**, enabling users to extend permissions on protected files
 - **Request for access** in case one does not have access

MICROSOFT AIP

- Difficult when it comes to providing security in external collaboration
 - Differential ways to protect MS-Office and non-office formats
 - Format change for non-office formats
 - Online viewing only (office formats)
 - Only office formats protection from within email
 - Requires admin intervention for changing controls

Admin Overheads

SECLORE

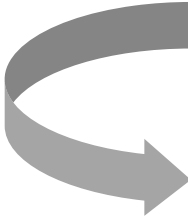
- Simplified Policy management with options for predefined and custom policies
- **Policy federation** from integrated applications reduces policy management overheads
- Managing protected content is easier with following bulk actions
 - **Transferring ownership** of protected documents from one employee to another (e.g. Employee transfer / Termination)
 - **Revoke access** to all documents (in case of termination)
 - **Replace user** with same permissions (in case of role change / transfers)
 - **Replicate user** with same permissions (in case of addition)

MICROSOFT AIP

- Heavy reliance on admin for policy management.
- Higher admin efforts to handle scenarios like Terminations, Transfers, role change

Why Policy Federation Matters?

Microsoft SharePoint Access Policy -Example



<input type="checkbox"/> kevinbrown078@gmail.com	User	Full Control
<input type="checkbox"/> lindajones087@gmail.com	User	Contribute
<input type="checkbox"/> mikemorgan380@gmail.com	User	Edit

SharePoint Controls	Seclore Usage Control Policies
View Only	View on internal IP addresses
Edit	View + Edit on internal IP addresses
Contribute	View + Edit + Screen Share on Linda's device only
Full Control	View + Edit + Print + Screen Share + Offline anywhere until <i>Date</i>

- Enterprise Application controls extend to information downloaded from the application too
- All user additions/Deletions reflect automatically on all old/new downloads.
- Eliminates Policy management overheads for administrators

Dynamic Rights Management

SECLORE

- Dynamic permissions management based on document workflow provides seamless and transparent user experience
 - **Smart sharing**, enabling users to extend permissions on protected files
 - **Request for access**, approval workflow built-in
 - **Instant Revocation** on documents once rights revoked

MICROSOFT AIP

- Dependency on administrator and / or user to make policy / permission changes
 - Requires admin / user intervention for changing controls
 - No built in request approval workflow
 - On revocation, user continues to have access by default for 30 days

Key Management

SECLORE

- Clear separation of keys and encrypted content.
- Seclore does not store the protected files anywhere on its servers.
- Enables complete dynamic rights management without the need to reshare / resend the document.
- Key Management server can be On-Premise / On-Cloud.

MICROSOFT AIP

- When protected with custom permissions, keys are stored with the encrypted document.
- No dynamic rights management. Document needs to be updated with new permissions and needs to be resend / reshared.
- Key Management server is On-Cloud.

Request Access

SECLORE

- Users can request for access with the click of a button.

MICROSOFT AIP

- There is no auto-generated request for access functionality, which makes it difficult for a recipient to access the document even though sender wants to give him/her permission to access the document.

Track and Revoke

SECLORE

- Access can be revoked for specific users remotely. This is real-time and the user will no longer be able to open the protected document.
 - Access to protected emails and protected attachments can be revoked.

MICROSOFT AIP

- If access is revoked, it will be revoked for all users.
 - It is not possible for the user to revoke access to protected emails and protected attachments.

Super User Privileges

SECLORE

- Seclore administrators' span of control is limited when it comes to the protected content. They can never unprotect a Seclore protected file.

MICROSOFT AIP

- Users who are assigned super user permissions can automatically remove protection from documents or emails that were protected by AIP.
 - A user with administrative permissions can assign anyone as a super user, including their own account. There is a high risk of super user accessing business-critical documents and misusing information.

More details...

Product (Feature Richness and Usability)

Feature	Seclore	Microsoft AIP
Classification based protection	✓	✓
Folder based protection	✓	✓
Any File Protection (Generic Protection)	✓	✓
Email Protection (Body and Attachments)	✓	Partial (Only office formats)
Agentless browser based access (Office formats)	✓	Partial (Only email body)
Agentless browser based access for other formats (PDF, Images, TXT..etc)	✓	X
Agentless browser based editing of protected MS Office files	✓	X
Identity Federation	✓	✓
Policy Federation	✓	X
Track and Revoke of emails and attachments from within MS Outlook	✓	X
Smart Sharing from within MS Outlook (User with share permissions can forward the protected email and provide access to new users)	✓	X

Product (Feature Richness and Usability)

Feature	Seclore	Microsoft AIP
Expire content for a particular user and / or user group	✓	X
Permissions can be revoked for a particular user or group after a file/email is shared	✓	X
Assigning different permissions to different users (While using custom permissions)	✓	X
Support Open Office for odt, ods, odp and Office formats	✓	X
Automated DRM protection for formats other than MS-Office	✓	X
Email notifications and Activity Alerts	✓	✓
View Audit log information for protected emails	✓	X

Security Control

Feature	Seclore	Microsoft AIP
Block: Print, Print to PDF	✓	✓
Block: Screen Capture	✓	✓
Block: Copy Paste to Unprotected document	✓	X
Block: Secure Copy Paste to Protected document with higher privileges	✓	X
Excel Cell Referencing using Secure Copy Data	✓	X
Lock file to a Device	✓	X
Lock file to an IP Address range	✓	X
Display of a dynamic watermark (MS AIP shows watermark in Office files only)	✓	Partial
Pluggable Encryption (BYOE)	✓	X
Safe from Man-in-the-middle attacks	✓	X
Offline Access (Apply real time permissions whenever user comes online)	✓	Partial
Security from Super users (No Super user concept)	✓	X

Automation (Integration Friendliness)

Feature	Seclore	Microsoft AIP
Support for leading DLP solutions: Symantec, Forcepoint, McAfee, GTB	✓	Partial
Support for leading classification solutions: Boldon James	✓	X
Support 3 rd party Identity Management System including cloud identity brokers : Ping, Okta, CA Siteminder	✓	X
Support for SIEM, Risk and Compliance tools: Splunk, ArcSight	✓	X
Support for leading ECM, EFSS other than Sharepoint E.g. IBM ECM	✓	One Drive Only
Policy Federation from integrated application	✓	X
Watermark Federation from integrated application	✓	X

Minimum Administrative Overheads

Feature	Seclore	Microsoft AIP
Segregation of Duties (Segregation based on various administrative tasks, Power Users, End Users)	✓	X
Bulk Operations like Transfer Ownership, Revoke Access, Replace/Replicate users	✓	X
Request Access workflow for a user who doesn't have access to a file (Automated approval workflow)	✓	X
Smart Sharing for protected emails and files (Extend permissions on protected emails and attachments)	✓	X

Thank You!