SECLORE™

CHECKLIST

Evaluation Checklist For Enterprise Digital Rights Management Solutions

A comprehensive checklist for choosing the right EDRM solution

Purpose of this document

This document is a comprehensive checklist designed to enable enterprise security teams to compare the capabilities of various enterprise digital rights management (EDRM) solutions and choose the most appropriate solution for their enterprise.

What is Enterprise Digital Rights Management?

Enterprise Digital Rights Management (EDRM) is technology specifically developed to safeguard and efficiently manage digital assets, such as files and emails, both within and beyond an organization's boundaries. Its primary focus lies in controlling access to and governing the usage of sensitive information across diverse digital platforms commonly utilized in modern workplaces. EDRM empowers organizations to exercise granular control over their digital content, ensuring secure and authorized access while mitigating the risk of unauthorized distribution or misuse. By implementing EDRM solutions, businesses can effectively protect their valuable intellectual property and confidential data in today's rapidly evolving digital landscape.

THIS EVALUATION CHECKLIST COVERS THE FOLLOWING PRODUCT CAPABILITIES:

- Granular EDRM controls
- Advanced and Dynamic EDRM controls
- Dynamic watermarking
- End-user driven and automated protection
- Email security
- Authentication
- End-user experience with EDRM files and emails
- Administration
- Tracking
- Reporting and dashboards
- File and email decryption
- Operating system support
- File formats and applications support
- Deployment and customer support
- Total cost of ownership
- Key management
- Integration with:
  - Microsoft 365
  - Sharepoint Server (on-premises)
  - Data Classification tools (e.g., Spirion,
  - Microsoft Purview, GetVisibility, etc)
  - DLP Solutions (e.g., Broadcom (Symantec), Forcepoint)
  - CASB solutions (e.g., SkyHigh CASB)
  - Other integrations

Granular EDRM Controls	SECLORE	Vendor
Restrict file access and usage to specific users and/or user groups		
Ability to provide read-only permission		
Restrict editing of files by unauthorized users		
Restrict printing of files by unauthorized users		
Restrict soft copy printing e.g., Print to PDF/Save as PDF		
Restrict copying content from a file to an external location		
Ability to provide full controls on files to specific users and/or user groups		
Restrict sharing of permissions by unauthorized users		
Restrict running macro on files by unauthorized users		
Block screen capture via PrtScr key or third party tools like SnagIt, Camtasia		
Block screen sharing via conferencing tools (e.g., Webex, GoToMeeting, etc.)		
Block file access via remote connections (e.g., Windows RDP)		
Block file access on virtual environments (e.g., VDI, Citrix environments, virtual machines)		
Allow file access while offline		
Restrict file access while offline		
Allow for different set of permissions for a user when he/she is accessing the file online vs offline.		
Restrict saving unprotected copy with 'Save As' and other similar options		
Ability to save file in PDF format without the need to have full control permissions		
Enforce same set of controls when files accessed in native application vis-à-vis accessed online via browser		

Advanced EDRM Controls	SECLORE	Vendor
Restrict file access to a specific computer		
Restrict file access to a specific mobile device		
Restrict file access and usage based on date, time		
Restrict file access and usage based on number of days		
Expire all copies of a file remotely at any time		
Restrict file access to a particular IP address		
Restrict file access to a range of IP addresses		
Same level of security in collaboration with internal and external users		

Dynamic EDRM Controls	SECLORE	Vendor
Change permissions on a file after delivery		
Revoke access of users instantly and remotely		
Revoke access in real-time as soon as user gets online even though user has offline permissions on the file		
Replicate access of users instantly and remotely		
Replace access of users instantly and remotely		

Dynamic Watermarking	SECLORE	Vendor
Enforce watermarked viewing of protected files		
Enforce watermarked viewing of protected files even when the file is accessed in the native applications		
Enforce watermarked printing of protected files		
Ability to configure dynamic watermark content (Classification, date, time, username, etc.)		
Enforce watermark printing of protected files in browser		
Enforce watermarked viewing of protected files in a browser		
Display a combination of static and dynamic content in the watermark		
Display watermark on files accessed on mobile devices (iOS and Android)		
Customize the font and color of watermark content		

End-user Driven Protection	SECLORE	Vendor
Protect one or multiple files simultaneously		
Ease of use - Right Click on a file/multiple files and enable protection		
Protect email attachments of any file format		
Enable different policies for individual users or user groups for the same file		
Allow usage controls to be saved as 'Policy templates'		
Ability to protect a file with one/multiple policy templates		
Enable protection on a file from within a native Office application		
Enable domain based protection/access for recipients		
Protect email body and attachments while sending emails via Outlook client on the desktop		
Set ad-hoc usage controls on email message and attachment in context to the email recipients i.e. users outside of the email recipient list should not gain access to the protected email and attachments.		
Protect attachments while sending emails via OWA		

Automated Protection	SECLORE	Vendor
Automatically protect files by moving them to a network location folder (folder watcher)		
Ability for a child folder to have the same or different permissions from the parent folder		
Ability to configure protection for certain formats or all formats within a monitored folder		
Automatically protect files in Microsoft 365 (SharePoint Online/ OneDrive/Teams)		
Automatically protect office files on close		
Automatically protect files on download from an ECM or ERP systems (integration required)		
Automatically protect email body and attachments (from the server side) without any user intervention based on certain parameters like Sender, Recipient, Subject, metadata (x-header) tags		
Automatically protect files based on discovery of sensitive content by systems like DLP, Classification, Discovery or CASB systems (integration required)		
Protect incoming emails and attachments from particular senders automatically without any user intervention		
Protect incoming emails and attachments from all senders to a particular email address without any user intervention		

Email Security	SECLORE	Vendor
Send protected emails from Windows Outlook client		
Send protected emails from Mac Outlook client		
Send protected attachments from Windows Outlook client		
Send protected attachments from Mac Outlook client		
Send protected attachments from OWA		
Support for any email client on any OS by allowing for protection of emails on server side		
Support for any email client on any mobile OS by allowing for protection of emails on server side		
Give permissions to distribution lists to access protected emails and attachments		
Ability for the recipients to automatically extend permissions on protected email and attachments to additional users		
Ability to set ad hoc security on emails and attachments for the recipient list only		
Track protected emails and attachments from within Outlook itself		
Revoke access to protected emails and attachments from within Outlook itself		
Set expiry date for protected emails		
Protect incoming emails and attachments automatically without any user intervention		
Encrypt and Decrypt .pst files		
Track audit logs for decrypted .pst files		
Automatic rule-based protection of emails and attachments based on dynamic criterion e.g., sender, receiver, subject line, metadata (X-header) tags		
Automatic protection of emails based on custom metadata/tag/label fields tagged by 3rd party systems e.g., Discovery, Classification, and DLP systems		
View protected emails (body and attachment) from the browser on your desktop – without the need for a particular email client or software		
Reply to protected emails from the browser on your desktop or mobile – without the need for a particular email client or software		

Authentication	SECLORE	Vendor
Ability to authenticate users via Windows Active Directory		
Ability to authenticate users via Microsoft Azure Directory		
Ability to authenticate external users with their personal or work account		
Single sign-on (SSO) capabilities with Google		
Single sign-on (SSO) capabilities with Microsoft Azure		
Works with other identity/SSO solutions like Ping, Okta		
Ability for external users to access a file with a temporary one-time password (OTP) without creating an account		
Support for 2FA with time based OTP (TOTP)		
Support any authentication providers with OpenID Connect protocol		

End-user experience with EDRM Files and Emails	SECLORE	Vendor
View protected files online on Windows and Mac desktop platforms without installing any software		
Edit protected files online on Windows and Mac desktop platforms without installing any software		
View protected emails online without installing any software or depending on any particular email client		
Reply to protected emails online without installing any software or depending on any particular email client		
Open protected files in native applications		
Access to files according to permissions set by the file owner		
Unprotect files on desktop for users will permissions		
Open protected files online directly from SharePoint Online, OneDrive, and Teams		
Open protected files in native applications from SharePoint Online, OneDrive and Teams		
Access protected files on any browser		
Access protected files on any device (Windows OS, MacOS, iOS, Android)		
No dependency on OS to access protected files/emails on desktop or mobile devices		
No dependency on application license to access protected files/ emails on desktop or mobile devices		
External users can access protected common non-office formats like PDF, png, jpeg, txt, etc. without installing any specific tool or software		
Support for Dynamic Watermark viewing		
Ability to extend permission on protected files/emails		
Ability to automatically extend permissions on email and its attachments on 'Email Forward/Reply/Reply All' to any new recipient added without the need to do anything outside of the context of sending the email		
Ability to request for permissions on protected files/emails		
Access protected files with Save-back functionality from within the integrated app to avoid/reduce the need for file download		
Seamless and consistent external user experience with protected emails and/or files		
Security widget within the file to display the usage permissions for a user on the protected file		

Administration - General	SECLORE	Vendor
Segregation of duties: Support for different administrator roles based on scope of work		
Ability to create security admin user profiles		
Ability to create power users (business users) for managing groups		
Ability to view installation report detailing agent installations throughout the organization		
Centralized license management for admins		
Ability to auto-assign license based on usage		
Customized user interface with your company's logo		

Administration	SECLORE	Vendor
Must offer an Admin GUI for EDRM policy administration		
Ability to configure default EDRM permissions for email		
Ability to configure EDRM policies for users, user groups and domains		
Ability to configure EDRM controls differently for different users, group and domains		
Ability to transfer file ownership instantly for EDRM protected files		
Ability to replace users on EDRM protected files		
Ability to replicate user permissions on EDRM protected files		

Tracking	SECLORE	Vendor
Instant email alerts to file owners for unauthorized file activities performed by users on EDRM protected files		
Daily digest email sent to file owners summarizing all the day's activities on protected files		
Ability to track and revoke access to EDRM protected files, emails for internal users		
Ability to track and revoke access to EDRM protected files, emails for external users		
Ability to revoke access for a specific user/user group		

Reporting	SECLORE	Vendor
A web-based audit trail and dashboard for all EDRM activities performed on all files by all users		
Report builder tool for easy custom reporting based on user needs		
Ability to log forensic details - Name, Email id, IP Address, Device, Machine name, file location on users device, Allowed and disallowed operations		
Ability to log date/time on which the activity was performed by the user		
Ability to export activity logs for monitoring purposes		
Ability to export audit logs for regulatory compliance reporting		
Ability to provide unified view of major risk and usage parameters		
Monitor license utilization		
Ability to provide overall system health and utilization/adoption analytics		
Ability to import/publish logs into SIEM tools		
Report builder tool for easy custom reporting based on user needs		
Ability to log date/time on which the activity was performed by the user		

Dashboards	SECLORE	Vendor
Solution must offer a centralized dashboard for executive reporting via Insights into Risks - Present and Averted		
Solution must offer a centralized dashboard for executive reporting on EDRM protected data		
Solution must be able to show trends over a period of time for Risks		
Solution must be able to show trends over a period of time for EDRM protected data		
Solution must be able to show a map-based view for risky activities performed		
Solution must be able to show a map-based view for risky activities prevented		
Solution must be able to show unauthorized activities performed based on domain of users		
Dashboard for EDRM protected data with filters on time-period		
Solution must be able to show trends over a period of time for Risks		

Integration with Microsoft 365	SECLORE	Vendor
Connector for Microsoft 365 collaboration apps SharePoint Online/ OneDrive/Teams		
Enable protection on particular or multiple SharePoint Online document libraries		
File shall remain protected when moved/copied from an IRM-enabled document library to another library		
Automatically protect files of any format after upload to SharePoint Online/OneDrive/Teams		
Access protected files of any format from SharePoint Online/ OneDrive/Teams		
Edit and Save back files from SharePoint Online/OneDrive/Teams		
Enforce application permissions even when the file is outside the application		
Enforce dynamic policy federation - changing permissions as permissions within the application changes for all copies of protected files (even when the file is outside the application)		
Support for dynamic watermark on files for both Office and non-Office formats when protected from within SharePoint Online/OneDrive/Teams		
Watermarked viewing of files for both Office and non-Office formats when accessed from within SharePoint Online/OneDrive/Teams		

Support for opening protected files of both Office and non-Office formats online on any browser (no need of an agent)		
Support for editing and saving protected files of both Office and non-Office formats online on any browser (no need of an agent)		
Integration with MS Sensitivity labels for automatic protection of files and emails		

Integration with SharePoint server (On-Premises)	SECLORE	**Vendor**
Connector for SharePoint server (On-Premises)		
Enable protection on particular or multiple SharePoint On-Premises document libraries		
Automatically protect Office, PDF, images, txt files when downloaded from SharePoint On-Premises		
Support for Edit and Save back of files in Sharepoint application		
Enforce dynamic policy federation - changing permissions on the application changes permissions on all copies of protected files (even when the file is outside the application)		
Support for dynamic watermark on Office, PDF, images, txt files when protected via SharePoint On-Premises		
Watermarked viewing of Office, PDF, images, txt files when accessed from within SharePoint On-Premises		
Support for opening protected Office, PDF, images, txt files online on any browser (no need of an agent)		
Support for editing protected Office, PDF, images, txt files online on any browser (no need of an agent) and downloading the edited copy		

Integration with data classification tools (Spirion, Microsoft Sensitivity labels, GetVisibility etc.)	SECLORE	**Vendor**
Automatic protection of files/emails based on classification labels selected by data classification tools		
Automatic protection of files/emails based on classification labels selected by end users		

Integration with Broadcomm (Symantec DLP)	SECLORE	Vendor
Connector for Symantec DLP		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) on endpoint devices		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) on the network file shares		
Automatic protection of emails and attachment based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) within email message or attachments		
Automatic protection of files/emails based on classification labels after they are discovered by Symantec		
Allow for inspection of protected files/emails on the network		

Integration with SkyHigh CASB	SECLORE	Vendor
Connector for SkyHigh CASB		
Automatic protection of emails and attachment based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) within email message or attachments		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) in cloud		

Integration with Forcepoint DLP	SECLORE	Vendor
Connector for Forcepoint DLP		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) on endpoint devices		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) on the network file shares		
Automatic protection of emails and attachment based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) within email message or attachments		
Automatic protection of files/emails based on classification labels after they are discovered by Forcepoint		
Allow for inspection of protected emails and its attachments on the network		
Map protection policies to rules configured in Forcepoint email security		

Other integrations	SECLORE	Vendor
Compatibility with MDM/EMM systems		
APIs available for custom integrations		
Availability of integration package in Java and .NET		

File and Email Decryption	SECLORE	Vendor
Automatic decryption of protected emails and attachments for Discovery, Classification, and DLP systems to inspect, followed by automatic re-protection		
Support for file and email (.PST) decryption via a decryption tool		

Operating System Support	SECLORE	Vendor
All major Windows versions		
All major MacOS versions		
iOS devices		
Android devices		

File Formats and Applications Support	SECLORE	Vendor
Microsoft Office files: doc, docx, xls, xlsx, ppt, pptx, docm, pptm, xlsm		
PDF files		
txt and other ASCII-based files		
OpenOffice formats: odt, ods, odp, odf, odg		
Image files: jpg, jpeg, bmp, png, gif, tiff		
All major Microsoft Office versions: 2016, 2019, and Microsoft 365		
All major OpenOffice versions: 4.x		
All major Adobe Reader versions: XI, DC		
All major LibreOffice versions: 6.x		
All major Windows versions: 8.1, 10		

Deployment and Customer Support	SECLORE	Vendor
Availability as a hosted service in cloud		
Availability to deploy on-premises		
Ability to deploy in hybrid mode		
Silent installation of agent via central deployment tools for Windows and MAC		
Support for cloud-based system in a private cloud		
Support for seamless migration from cloud-hosted to on-premises deployment		
Support for automated patching of apps using app stores		
Support for automatic and silent client upgrades		
Availability of different modes of agent i.e. Protection mode and Receiver mode		
Availability of 24×7, SLA-bound support		
Access to delivery and on-going account management team for successful roll-out and on-going adoption of the technology		

Total cost of ownership	SECLORE	Vendor
No need to move infrastructure to cloud e.g., On-Premises AD to Azure AD, On-Premises exchange to exchange online, etc.		
No need to upgrade infrastructure to latest versions e.g., Windows 10, Microsoft O365, etc.		

Key Management	SECLORE	Vendor
Protected content and keys are kept separate for hack-proof security		
Pluggable encryption: Bring your Own Encryption		
Keys are never embedded within the protected file		
HSM Support: Bring your own master key		

About Seclore

Seclore is the Data Security Intelligence company for the era of enterprise AI. As AI systems increasingly read, generate, and act on data without direct human oversight, organizations need more than visibility—they need intelligence, control, and proof. Seclore ARMOR brings together data discovery, contextual intelligence, persistent protection, continuous enforcement, and usage insight within a single control model. By securing the data itself and ensuring protection travels with it, Seclore enables organizations to adopt AI confidently, demonstrate compliance continuously, and maintain trust across people, partners, and AI systems.

www.seclore.com