A Seclore Whitepaper

SECLORE

An Evaluation Checklist for Enterprise Digital Rights Management (EDRM) Solutions

A comprehensive checklist for choosing the right EDRM solution

Enterprise Digital Rights Management (EDRM)[1] is a technology that controls the access and usage of information in stand-alone files and emails (known as 'unstructured' information).

EDRM solutions have been available in one form or another for more than a decade. However, new technology trends such as Cloud Computing and mobile device usage are raising expectations and pushing the boundaries of EDRM capabilities. The increased need to outsource and collaborate with third parties and temporary partners is also giving rise to new business demands - particularly in the area of user experience.

If you are considering EDRM technology for your enterprise, this white paper will help you fully consider and evaluate the latest capabilities available in the current generation of EDRM products.

Capabilities	Vendor 1	Vendor 2
Granular Data Centric Security Controls		
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		

Capabilities	Vendor 1	Vendor 2
Granular Data Centric Security Controls (continued)		
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 Controls		
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 Controls		
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		

Capabilities	Vendor 1	Vendor 2
Dynamic Watermarking		
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		
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		
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		
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		

Capabilities	Vendor 1	Vendor 2
Automated Protection		
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 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		
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		

Capabilities	Vendor 1	Vendor 2
Email Security (continued)		
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 decryption of protected emails and attachments for Discovery, Classification, and DLP systems to inspect, followed by automatic re-protection		
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		

Capabilities	Vendor 1	Vendor 2
Authentication		
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		
End-User Experience		
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		
Open protected files online directly 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		

Capabilities	Vendor 1	Vendor 2
End-User Experience (Continued)		
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		
A web-based audit trail and dashboard for all activities performed on all files by all users		
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/ OUs and performing administrative tasks		
Ability to configure default permissions for email protection		
Ability to view installation report detailing agent installations throughout the organization		

Capabilities	Vendor 1	Vendor 2
Administration (Continued)		
Centralized license management for admins		
Ability to auto-assign license based on usage		
Customized user interface with your company's logo		
Report builder tool for easy custom reporting based on user needs		
Ability to transfer file ownership instantly		
Ability to replace users on protected files		
Ability to replicate user permissions on protected files		
Tracking		
Instant email alerts to file owners for unauthorized file activities		
Daily digest email sent to file owners summarizing all the day's activities on protected files		
Ability to export activity logs for monitoring purposes		
Ability to export audit logs for regulatory compliance reporting		
Ability to log forensic audit details (machine name, IP address, file path etc.)		
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 track and revoke access to files/emails for internal users		
Ability to track and revoke access to files/emails for external users		
Ability to revoke access for a specific user/user group		
Ability to import/publish logs into SIEM tools		

Capabilities	Vendor 1	Vendor 2
Integration with Microsoft 365		
Connector for Microsoft 365 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		
Access protected files of any format 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 SharePoint Server (On-Premises)		
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		
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		

Capabilities	Vendor 1	Vendor 2
Integration with SharePoint Server (On-Premises) (Continued)		
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 (e.g., Boldon James, Titus, Spirion, etc.)		
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 Symantec		
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 McAfee		
Connector for McAfee DLP, CASB		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) on endpoint devices		
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		

Capabilities	Vendor 1	Vendor 2
Integration with McAfee (Continued)		
Automatic protection of files based on discovery of sensitive keywords or regular expressions (e.g., credit card numbers) in cloud		
Automatic protection of files / emails based on classification labels after they are discovered by McAfee		
Allow for inspection of protected emails and its attachments on the network		
Integration with Forcepoint		
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		
Compatibility with MDM/EMM systems		
Connector for Boldon James data classification tool to automatically protect classified content		
Connector for Titus data classification tool to automatically protect classified content		
APIs available for custom integrations		
Availability of SDKs in Java and .NET		

Capabilities	Vendor 1	Vendor 2
Operating System Support		
All major Windows versions		
All major MacOS versions		
iOS devices		
Android devices		
File Formats and Applications Support		
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: 2010, 2013, 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		
Availability as a hosted service in cloud		
Availability to deploy on-premises		
Ability to deploy in hybrid mode		
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		

Capabilities	Vendor 1	Vendor 2
Deployment and Customer Support (Continued)		
Support for automatic and silent client upgrades		
Silent installation of agent via central deployment tools for Windows and MAC		
Availability of 24x7, 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		
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		
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 offers the market's first fully browser-based Data-Centric Security Platform, which gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and analyze the usage of data wherever it goes, both within and outside of the organization's boundaries. The ability to automate the Data-Centric Security process enables organizations to fully protect information with minimal friction and cost. Over 2000 companies in 29 countries are using Seclore to achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.
Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

SECLORE