Evaluation Checklist for
Enterprise Email Encryption Solutions

A Comprehensive Checklist for Choosing the Right Enterprise Email Encryption Solution

End-User Driven Email Classification	SECLORE™	Vendor
Ability to apply classification to emails within Outlook		
Ability to show classification add-in in MS Outlook		
Ability to present users with guidance (tooltip) on classification labels within Outlook		
Ability to suggest / recommend classification for emails to the user based on keywords and pattern recognition within Outlook email message and attachments		
Ability to seek justification from the users on downgrading the label or violating the suggestion		
Ability to prompt the user to mandatorily classify emails		
Ability to auto-upgrade email classification based on attachments		
Ability to change / update classification for emails		
Ability to de-classify emails		
Ability to automatically apply EDRM controls based on email classification label		
Ability to prevent user from sending emails to blacklisted domains		
Ability to apply classification to emails within Ability to allow users to send emails only to whitelisted domains		
Language Support : Arabic, English		

EDRM Security for Email	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		

EDRM Security for Email (continued)	SECLORE™	Vendor
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		
Granular EDRM Controls	**SECLORE™**	**Vendor**
Protect email body and attachments while sending emails		
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.		
Restrict email and attachments access and usage to specific users and/or user groups		
Protect email attachments of any file format		
Ability to provide read-only permission		
Restrict editing of files by unauthorized users		

Granular EDRM Controls (continued)	SECLORE™	Vendor
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		
Restrict saving unprotected copy with 'Save As' and other similar options		
Enforce same set of controls when files and emails accessed in native application vis-à-vis accessed online via browser		

Advanced EDRM Controls	SECLORE™	Vendor
Restrict access to a specific computer		
Restrict access to a specific mobile device		
Restrict access and usage based on date, time		
Restrict access and usage based on number of days		
Expire all copies remotely at any time		
Restrict access to a particular IP address		
Restrict access to a range of IP addresses		
Same level of security in collaboration with internal and external users		
Enable domain based protection / access for recipients		
Dynamic EDRM Controls	**SECLORE™**	**Vendor**
Change permissions 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		

Visual Markings and Classification Metadata	SECLORE™	Vendor
Ability to apply visual markings like header/footer to emails and attachments		
Ability to add classification metadata / x-header to classified files & emails		
Ability to preserve classification metadata even when DRM protected for ease of interoperability		
Dynamic Watermarking	**SECLORE™**	**Vendor**
Enforce watermarked viewing of protected files and emails		
Enforce watermarked viewing of protected files and emails in the native applications		
Enforce watermarked printing of protected files and emails		
Ability to configure dynamic watermark content (Classification, date, time, username, etc.)		
Enforce watermark printing of protected files and emails in browser		
Enforce watermarked viewing of protected files and emails in a browser		
Display a combination of static and dynamic content in the watermark		
Display watermark on files and emails accessed on mobile devices (iOS and Android)		
Customize the font and color of watermark content		

Automated Protection	SECLORE™	Vendor
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		
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		

Authentication (continued)	SECLORE™	Vendor
Support for 2FA with time based OTP (TOTP)		
Support any authentication providers with OpenID Connect protocol		
End-User Experience with Protected Emails and File Attachments	**SECLORE™**	**Vendor**
View protected emails online without installing any software or depending on any particular email client		
View protected emails and file attachments online on desktop platforms without installing any software		
Edit protected files online on desktop platforms without installing any software		
Reply to protected emails online without installing any software or depending on any particular email client		
Open protected files and email in native applications		
Access protected emails and attachments on any device (Windows OS, MacOS, iOS, Android)		
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		

End-User Experience with Protected Emails and File Attachments (continued)	SECLORE™	Vendor
Ability to request for permissions on protected files/ emails		
Seamless and consistent external user experience with protected emails and/or files		
Ability to add custom text (disclaimers, etc) in the footer in encrypted emails		
Ability to add custom links in the footer in encrypted emails		
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 - Classification Policies	**SECLORE™**	**Vendor**
Must offer an Admin GUI for classification policy administration		
Ability to define and configure classification label list		

Administration - Classification Policies (continued)	SECLORE™	Vendor
Ability to define color for different classification labels		
Ability to define a tooltip for each of the classification labels		
Ability to define sub-labels for a classification label		
Ability to define font size, color, text alignment for Header, Footer visual markings.		
Ability to configure EDRM protection policies for a classification label		
Ability to define blacklisting of emails domains		
Ability to define whitelisting of email domains		
Ability to define priority for classification labels		
Ability to create exceptions (for a certain set of users) against the label policies		
Ability to configure content discovery policies based on keywords and patterns		
Ability to publish classification labels to users, user groups		
Ability to configure default classification in Office apps and Outlook		
Ability to configure mandatory classification for documents and emails		
Ability to publish classification for documents or email or both		
Ability to enable / disable classification via in-app menu within MS Office apps - Word, Excel, Powerpoint, Outlook		

Administration - Classification Policies (continued)	SECLORE™	Vendor
Ability to enable / disable classification via right click menu option in explorer		
Single GUI to manage and administer Classification and EDRM policies		
Administration - EDRM Policies	**SECLORE™**	**Vendor**
Must offer an Admin GUI for EDRM policy administration		
Ability to configure default EDRM permissions for email and attachments		
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 email and attachments		
Ability to replace users on EDRM protected email and attachments		
Ability to replicate user permissions on EDRM protected email and attachments		
Tracking	**SECLORE™**	**Vendor**
Instant email alerts to file owners for unauthorized email access		
Instant email alerts to file owners for unauthorized activities performed by users on EDRM protected email attachments		
Daily digest email sent to file owners summarizing all the day's activities on protected files / emails		
Ability track and revoke access to EDRM protected emails and attachments for internal users		

Tracking (continued)	SECLORE™	Vendor
Ability to track and revoke access to EDRM protected emails and attachments 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 / email 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		
A web-based audit trail for all classification activities performed on emails and file attachments by users		
Report builder tool for easy custom reporting based on user needs		

Reporting (continued)	SECLORE™	Vendor
Ability to log activities for current classification, previous classification, suggested classification, Ignored classification, justification provided by user for policy violations		
Ability to log classification policy applied on the emails and attachments based on classification label selected		
Ability to log de-classification of files, email activities		
Ability to log forensic details - Name, Email id, IP Address, Device, Method of classification		
Ability to log date/time on which the activity was performed by the user		
Dashboard	**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		

Dashboard (continued)	SECLORE™	Vendor
Centralized dashboard for executive reporting via Insights into Risks - Present and Averted		
Centralized dashboard for executive reporting on Classified 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 Classified data		
Solution must be able to show a map-based view for classification activities performed		
Integration with Email Inspection Tools: Discovery, DLP, CASB, Classification, Email Gateway, etc	**SECLORE™**	**Vendor**
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		
Allow for protection of emails and attachments on server side without having any dependency on endpoint, device type, email client used...etc		
Allow for inspection of protected emails and its attachments on the network		
Compatibility with MDM/EMM systems for mobile access		

Operating System Support	SECLORE™	Vendor
All major Windows versions		
All major MacOS versions		
iOS devices		
Android devices		
Deployment and Customer Support	**SECLORE™**	**Vendor**
Availability as a hosted service in cloud		
Availability to deploy on-premises		
Ability to deploy in hybrid mode		
Single agent / client for Digital Asset Classification		
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-premisesdeployment		
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 24x7, SLA-bound support		
Data Classification professional consulting services		
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		

SECLORE™

About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Join industry leaders like American Express in choosing Seclore for superior digital asset protection without sacrificing seamless collaboration and sharing.

Visit **www.seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054