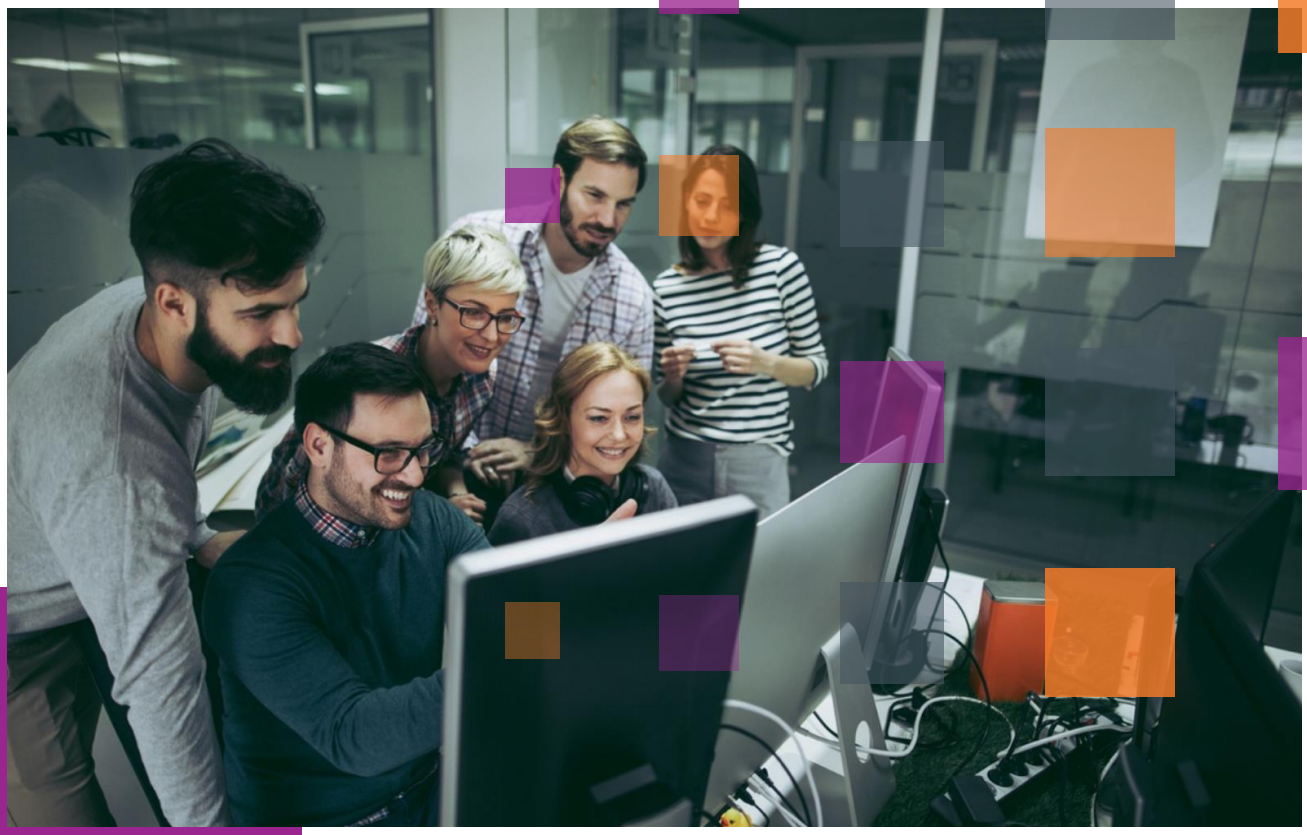
DataMotion™



Selection Guide:

Enterprise Email Encryption

FINDING THE RIGHT SOLUTION

Email Encryption - Eight Elements to Look For

The best way to ensure that your messages and attachments remain confidential is to transmit them through an encryption platform that integrates with existing apps, systems and workflows. Optimally, users should be able to send and receive encrypted messages directly from the desktop applications or cloud services they use most. Policy filters that automatically detect sensitive information in email and attached files should automate the encryption process to further ensure security (and regulatory compliance). There are eight key elements to look for in an enterprise class solution:

1. Ease of Use

Look for solutions that are simple and easy to use for users and recipients, without a lot of extra steps, even when sent outside your network. Ease of use is directly related to user compliance. The harder it is and more steps that need to be taken, the less likely they will comply and use it.

Ask yourself these questions:

- Can messages and files be delivered directly to a recipient's inbox, decrypted and ready to read, through a SafeTLS function?
- Does the solution follow a natural intuitive workflow?
- Can recipients easily respond, without the need to install anything?
- Does the solution work in conjunction with enterprise tools, such as Outlook, CRMs or contact centers?
- Does the solution leverage existing authentication resources for SSO?

When it comes to user and recipient ease of use, transparency and simplicity are key elements. Today's modern and evolved encryption solutions can do the complex work of encrypting, decrypting, managing keys, delivery and tracking in the background, making usage seamless.

2. Policy-based Filtering

Automated, policy-based filtering reduces the need for user action, working transparently behind the scenes to protect data in motion. Verify the solution uses policy-based filtering to check all email, file attachments and other messages for sensitive, regulated information. Make sure to deploy technology that can filter messages and the wide variety of file format attachments used in business today. To avoid false-positives and an ensuing drain on IT hours and resources, use technology that is designed to minimize false positives yet catch data that cannot leave the company in an unencrypted state.

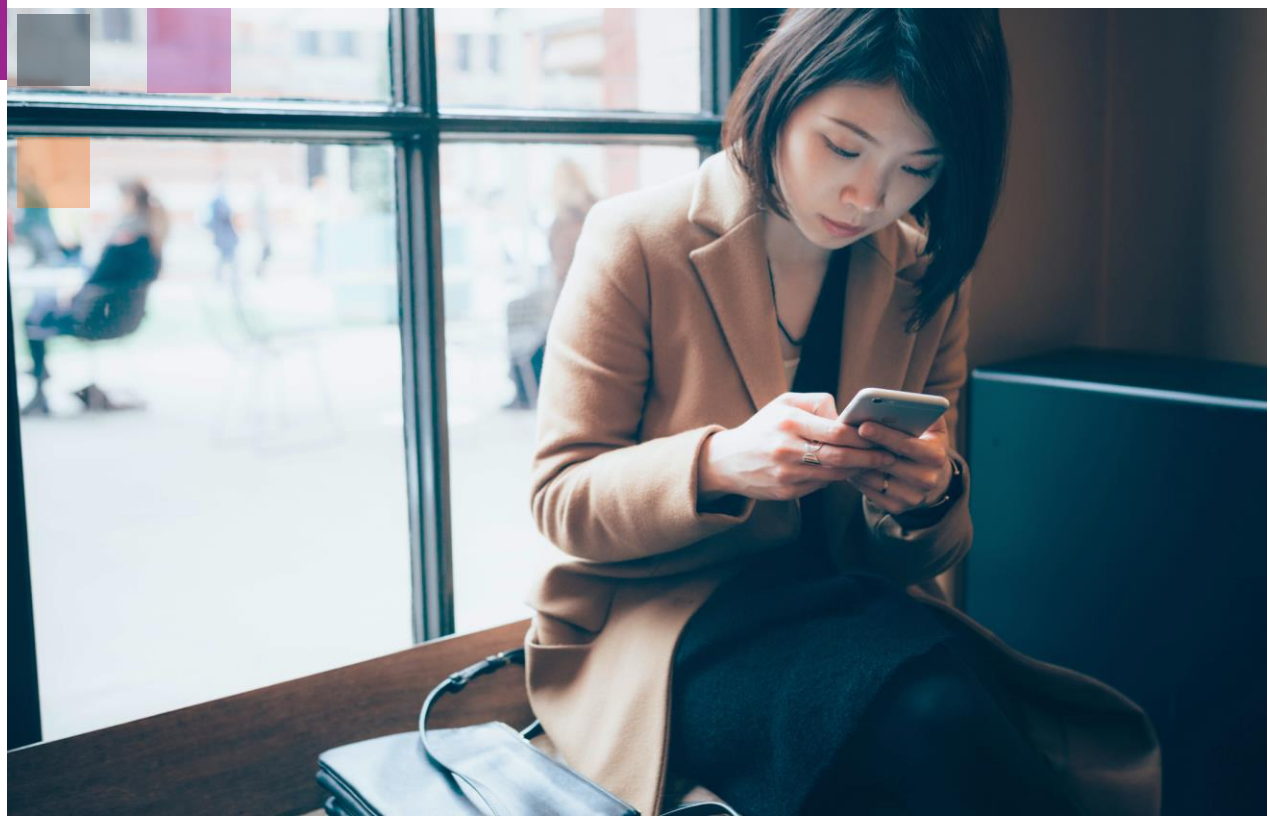
The ability to customize email filtering has virtually eliminated false positives, and it's easy to update and change the filtering rules.

—Stillwater Medical Center

Stillwater Medical Center

Automatic email encryption for PHI

This case study from Stillwater Medical Center, highlights the value of implementing an email policy gateway as part of an overall HIPAA data loss prevention policy. Stillwater used a manual and automatic email encryption process to help ensure HIPAA email compliance and data loss prevention for the medical center – with great success!



3. Secure Message Center

Customers, clients, members and patients are starting to demand the ability to ask questions and send sensitive data from websites, portals and mobile apps, and they want these communications protected as well. Be sure the provider can integrate a secure message center, into your customer facing user interfaces.

4. End-to-End Security

The solution should provide end-to-end security and multiple delivery methods. Many solutions, including Office 365 utilize TLS, but not all TLS implementations are the same and not all recipient organizations are enabled to receive email via TLS. To ensure compliance, be sure your implementation covers those situations where TLS can't be used. Multiple delivery options that happen automatically when one path is not secure is ideal.

5. Mobile Optimization

With today's more mobile workforce, employees conduct a great deal of business outside of the office. Look for a solution that is optimized for mobile devices and works with existing email clients on mobile devices so no separate app is needed.

6 Ways Customers Want to Use Websites, Member Portals and Mobile Apps for customer service:

1. *Using any device, anytime, anywhere*
2. *Asking for assistance or information when self-service options fall short.*
3. *Exchanging sensitive documents with a support rep*
4. *Clicking an upload link in an email sent by an agent during a conversation on the phone*
5. *Sending a message through the publicly available customer message link on the website*
6. *By sending an email to the publicly available support email address*

6. Email Encryption API Integration

Digitally transforming business processes and workflow applications that handle sensitive information sometimes requires the encryption to be "baked in" or integrated with the application. Availability of a wide range of email encryption APIs from the provider, will give more control over how the API works with an app and should include:

- Messaging APIs. These are the APIs that send and retrieve data. Look for APIs that can handle multiple types of data, including email, files and form data.
- Administrative APIs. Password reset, managing users and their account settings, and integrating with Single Sign-On (SSO) are all features to look for.
- Provisioning APIs. Your API needs to grow with your application. Look for programmatic provisioning, servicing and on-boarding new users.

Full support from the API provider is another requirement. In addition to standard consulting and ongoing technical guidance be sure the vendor can provide:

- Multiple language support, including C#, VB.Net, Java and PHP, along with SOAP and REST.
- Technical reference guides that accurately document each API function and data structure. Sloppy documentation could indicate subpar operations.
- Demos for each programming language supported, including working sample applications with documented source code that demonstrates the implementation.

Lastly, be sure they can provide a pre-production sandbox environment. A full-service, fully-contained, pre-production environment allows you to quickly and safely create, test and preview your application.

7. SaaS, Cloud, MSP or On-Premises

While SaaS encryption solutions are easy to deploy and use, many organizations need the enhanced security and control of a dedicated cloud instance, managed service, or even an on-premises solution. For some law enforcement applications, CJIS rules will dictate on-premises deployment in a CJIS data center. Make sure the provider offers the flexibility to provision service to meet your needs best.

8. Service and Support

Delivery of a full range of support options is a must. Large enterprises in particular often have complex systems, infrastructure and custom needs. Professional implementation services, managed services and full service 24/7 engagements can make the implementation process and on-going operations smooth sailing.

Published by **DataMotion**

DataMotion, Inc. provides PaaS (API) and SaaS (pre-built) solutions that redefine how organizations collaborate and share information with their customers and partners. Leaders in government, financial services, healthcare, insurance, and call center markets leverage our services to accelerate their business processes through modern, secure digital exchange. Our PaaS connectors and APIs enable secure, modern information exchange, allowing developers, software vendors and system integrators to enhance their solutions rapidly and seamlessly. In the healthcare sector, DataMotion is an accredited HISP (health information service provider), Certificate Authority (CA) and Registration Authority (RA) of Direct Secure Messaging. DataMotion is privately held and based in Morristown, N.J.

DataMotion, Inc.
67 Park Place East Suite 301
Morristown, New Jersey 07960
datamotion.com

Email Encryption
Selection Guide