GIGAOM | SITUATION PUBLISHING

Image credit: Alex

Paul Stringfellow

Jan 6, 2022

Encryption Solutions Buyers Checklist

Security & Risk

Encryption Solutions Buyers Checklist

Table of Contents

1. Summary

This GigaOm Buyers Checklist is aimed at decision makers and technology buyers seeking to evaluate email encryption solutions for the enterprise.

Encryption Solutions Primer

Information is critical to today's enterprise and is the currency of modern business. Therefore, protecting it has to be at the heart of data strategy and at the top of the priority list of any enterprise.

However, organizations cannot protect data by just keeping it locked in a data center, as the need to share it is also a critical part of doing business today. Therefore, finding ways to secure that information effectively is a must. This challenge is perhaps never more pronounced than it is with email.

Email by its very nature is built to be shared — primarily externally. Even as the way we communicate evolves, with the adoption of more messaging and collaboration tools, email still remains the number one way of sharing information. However, because email can contain extremely sensitive information, we need ways to secure it to make sure it can only be read by its intended audience.

As with other elements of information security, encryption plays a key part in email security. The ability to encrypt a message and its contents so that it can only be opened by an intended recipient is a powerful, and in many cases necessary, element of modern security.

Organizations may already have one or more encryption solutions, which could have been brought in for a specific reason, or might be part of a larger bundle. Whether they have something in place or not, it may be a good time to review what is needed by the organization and the ramifications of delivering a solution.

To start this process, we must first understand our potential requirements.

- Do we just need to encrypt the transport?
- Do we need to encrypt the message itself?
- Should we encrypt attachments?

- What are our needs in terms of compliance?

It is also important to recognize that any approach we take should not fundamentally change how we use emails, or make its adoption onerous for the sender. We also must consider the impact on a recipient. If we are encrypting email content, what mechanisms do we employ to ensure that they can easily and securely decrypt email? What if you have multiple mail systems? Hybrid solutions? How do you ensure you gain consistent email encryption capabilities across each of them?

All of these are critical considerations and can help ensure you find the right fit for your enterprise.

The remainder of this paper will help to outline potential solutions, architectures, and assessment criteria that you can use to help identify whether an email encryption solution is appropriate to your organization and how to select one that best meets your needs.

2. Solution Approaches

A first question to ask about email encryption is, can I encrypt with my native email systems? Depending on the requirements, then potentially yes. Exchange on-premises and online and Gmail in Google Workspace all support native email encryption. But these are limited to the transport of the message and this transport encryption comes with its own challenges. And what if we need more than transport level encryption?

This is where email encryption platforms can be helpful. By adding these additional capabilities, organizations can meet these broader use cases.

How Does an Email Encryption Solution Work?

Normally, they sit outside of your email systems (whether on-premises or in the cloud). Messages that require encryption are then rerouted to the encryption service.

It is at this point, dependent on the type of service, that your encryption platform will make its decision and apply a suitable encryption technology. This may be transport encryption, or for more advanced approaches it may encrypt the message contents. Depending on the solution, the platform may send the email message on itself or will route the now encrypted message back through your mail system's SMTP queues and onto the intended recipient.

The recipient will then be provided options to decrypt this message—MFA token, separate email message, SMS, or work in conjunction with the sender to ensure decryption information only reaches the intended recipient. Some solutions will also provide an encryption access portal with the recipient receiving a link with which they can access the secure message. This provides the added security of sharing the message and its contents while it never leaves the system or the sender's control. **Figure 1** illustrates a typical architecture.

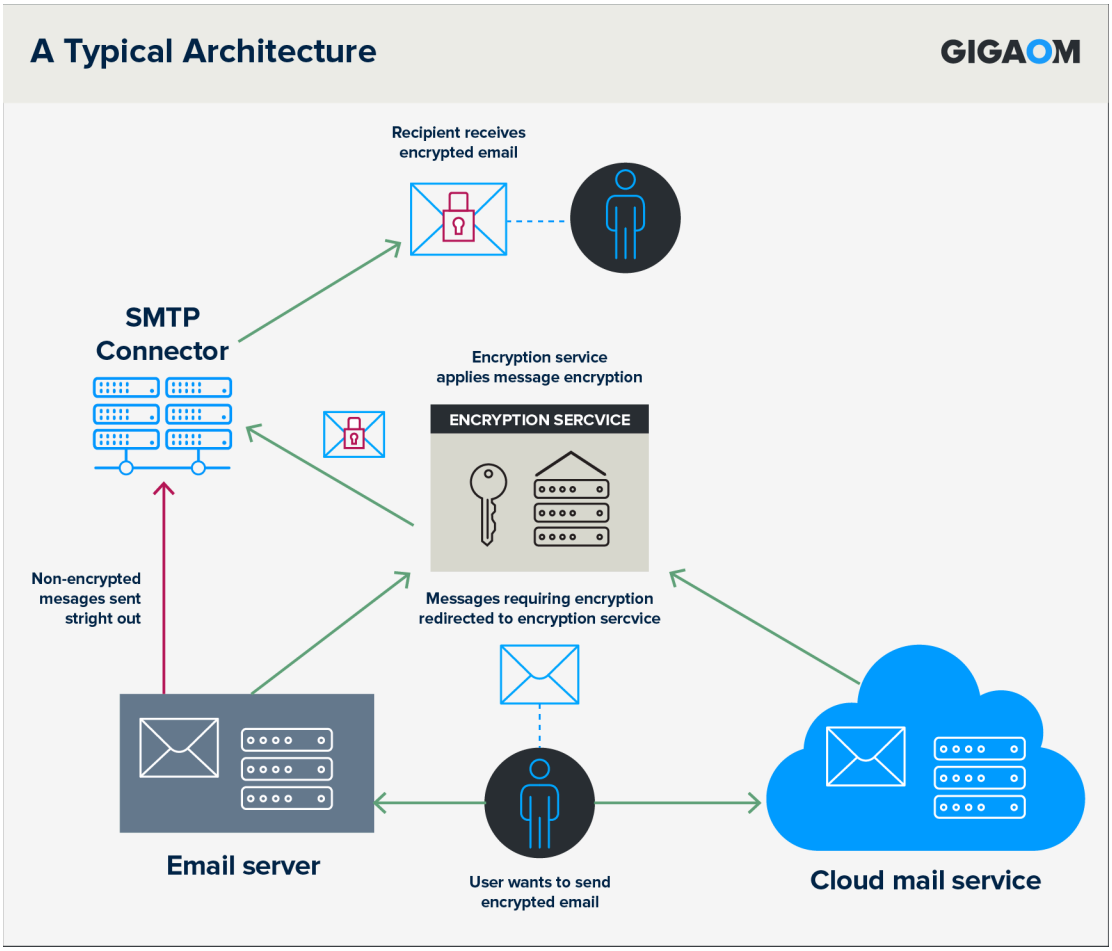

Figure 1. A Typical Architecture

Deployment Considerations for Email Encryption

When deploying a solution into a system that is as essential as email, we must be careful to consider its impact and minimize it. How should this be approached?

A flexible approach can be the most effective in these scenarios—one that allows us the ability to choose whether we want users to enforce message encryption, whether we want to automate it, or provide a mix of the two.

Client Driven

This is where the end user can make a decision to encrypt a message. This can be either done with the aid of a plug-in into the mail client, or by allowing some simple identifier (normally in the email subject) that will then trigger an intervention from the encryption system to carry out its process.

Automated

In this scenario, the encryption platform automates the decision, in conjunction with the email system. This is usually done by identifying key sensitive data inside of an email message or attachment or by looking at an alternative indicator such as the application of a data classification label.

What is imperative with either approach is that neither the standard mail workflow or user experience is severely impacted.

Potential Challenges

Email encryption does require careful planning and consideration regardless of how unobtrusive the technology may be. When using message encryption (more than transport encryption), an enterprise must understand the potential impact on both its users and, more importantly, its recipients. Challenges include:

- Creating an overhead for the user, in which case they might seek to circumvent the solution
- Adding complexity to the business process, which will incur a cost in terms of efficiency or productivity.

To address such challenges, it is important to deliver a solution that minimizes friction of email sending. Given that this cannot be reduced to zero, users must also be educated as to why encryption is important and how the policies define which emails, content, or attachments should be encrypted and how.

It is also important when using such systems to give consideration to the recipient experience. Do we need recipients to register some kind of service to decrypt messages? Will they need special software? Access to external services to authenticate before accessing a secure message or file? All of these considerations are critical to ensure that your deployment enhances security, but does not do so by negatively impacting the user experience.

3. Assessment Criteria

As discussed, there are many considerations for identifying both the need for email encryption and for assessing an appropriate solution. What are some guidance criteria to consider?

The following section outlines our buyers' criteria for evaluating and selecting your email encryption platform. This information can be used to help you develop appropriate criteria for your own gap analysis and vendor assessment.

As can be seen in **Table 1, 2, and 3**, we outline what we see as the main criteria to consider. By using this information and making your own judgment to the level of importance of each criterion to your organization, this will provide a useful tool for assessment and gap analysis.

Table 1. Criteria Considerations – Table Stakes

Criteria Considerations GIGAOM

Table Stakes		Top Priority	Secondary Priority	Not a Priority
Transport Encryption	Support for standard transport encryption such as TLS and S/MIME ensuring messages meet minimum standards for safe transport of email.			
Message encryption	The ability to not only encrypt the transport but the ability to encrypt the message content itself.			
Plug-In free integration	Plug-ins can increase complexity, introduce security risks and make deployment difficult. While they can be a valuable option they should not be a requirement.			
Simple user encryption	Encryption should be frictionless for the user, making it easy to select information for encryption as and when needed.			
Flexible recipient decryption options	It must be straightforward for the recipient to decrypt the inbound message. Options should be flexible and able to provide all recipients with the ability to decrypt a message regardless of technical skill level.			

Table 2. Criteria Considerations – Key Criteria

Criteria Considerations

GIGAOM

Key Criteria		Top Priority	Secondary Priority	Not a Priority
Flexible encryption standards support	The range of standards for encryption are broad. The platform should allow us to utilize those most relevant to meet our needs.			
Multiple recipient options	Flexible options for our recipient to access and decrypt messages must be available.			
Ability to keep encrypted information "in house"	The ability to allow access to information from a central repository, rather than sending it externally can be valuable to those with demands for it. This can, for those with strict requirements, help to de-risk data sharing.			
Integration with other internal security and encryption tools	Email encryption is only part of our solution stack. It must integrate well with our other enterprise tools.			
Automation	The ability to automate will help to ensure that emails and information that demands encryption is always captured.			
Broad authentication support	We need to offer broad authentication support for our recipients. Our platform should be capable of integrating with widely available authentication systems and standards.			
Broad mail platform support	Where multiple email systems exist, our system should be able to integrate with them all, consolidating encryption into a single platform.			
Branding support	Email is a key part of a businesses branding, our system should be able to retain that through our secured messages. In both the message itself or when retrieved through a messaging repository.			
Multiple language support	Our enterprises exist in a global business environment, our platforms should reflect this and support multiple languages effectively.			

Table 3. Criteria Considerations – Non-Functional Requirements

Criteria Considerations GIGAOM

Non-Functional Requirements		Top Priority	Secondary Priority	Not a Priority
Ease of implementation	We want our solution to sit alongside our email systems, reducing time to deploy and reducing the risk of impacting our business critical email flow.			
Ability to consolidate	Email encryption is where we have encryption solutions already. Our new platform should ease the consolidation of and migration away from these multiple solutions.			
Seamless user experience	It should be easy to adopt by sender and recipient alike. Any solution that adds unnecessary complexity for either will greatly reduce its value.			
Improve our security posture	While many technology solutions must focus on return on investment, it is crucial when discussing security that our solution must improve our security posture. Doing so will make our business more digitally resilient.			

While many technology solutions must focus on return on investment, it is crucial when discussing security that our solution must improve our security posture. By enhancing the security of our information, we make a business more digitally resilient and reduce the potential high costs associated with a data breach.

4. About Echoworx

Echoworx protects the privacy of people and businesses throughout the world by making email data protection easier. The cloud-based platform and SaaS delivery help transform communication chaos into order for world leading organizations who understand — it pays to be secure.

Echoworx focuses exclusively on providing organizations with secure email services. Protecting millions of users and thousands of deployments in over 30 countries, Echoworx is the email protection platform of choice for some of the world's leading brands in banking, insurance, government, and healthcare. To learn more, visit Echoworx.com.

5. About Paul Stringfellow

Paul Stringfellow has more than 25 years of experience in the IT industry helping organizations of all kinds and sizes to use technology to deliver strong business outcomes. Today that work focuses mainly on helping enterprises understand how to manage their data to ensure it is protected, secure, compliant, and available. He is still very much a “hands-on” practitioner and continues to be involved in a diverse range of data projects. Paul has been recognized across the industry and has spoken at many industry, vendor, and community events. He writes for a number of industry publications to share his enthusiasm for technology and to help others to realize its value.

Paul hosts his own enterprise technology webcast and writes regularly on his blog.

6. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

7. Copyright