GIGAOM | SITUATION PUBLISHING

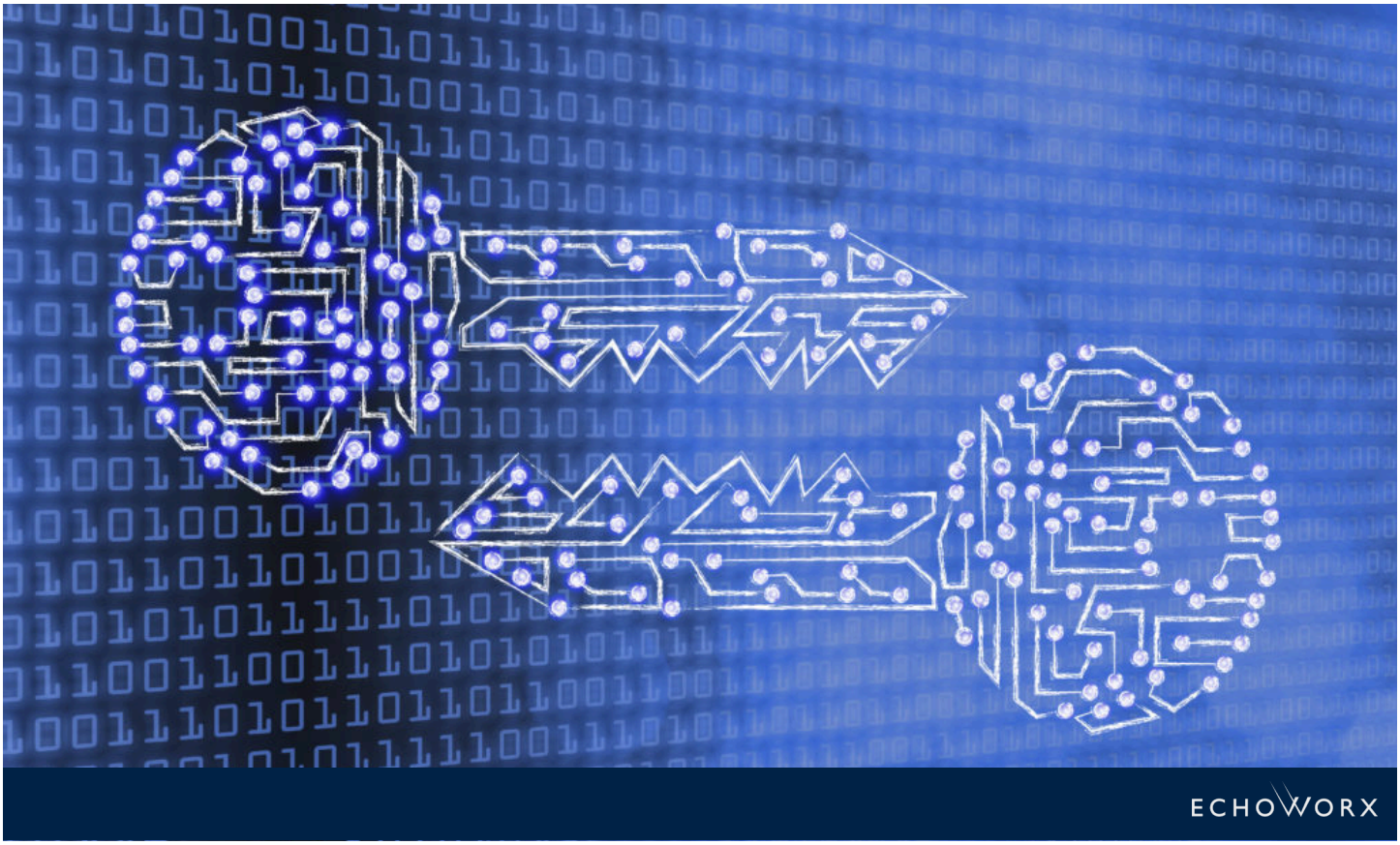

Image credit: faithie

Paul Stringfellow

Jan 6, 2022

Business Fit Report: Echoworx and Email Encryption

Security & Risk

Business Fit Report: Echoworx and Email Encryption

Table of Contents

1. Summary

While organizations continue to evolve their business communications with moves to collaboration platforms and sharing technologies, email remains the primary business communication tool. Whether B2B or B2C, its familiarity and ease of use means it continues to be the de-facto information sharing platform.

With this in mind, ensuring secure email communication is critical to modern business. The levels of security we need will, of course, differ. For some message transport, encryption at the protocol level is enough, while for others this will not be sufficient. Whether due to specific business use cases or regulatory demand, information sometimes must be shared only between the sender and the intended recipient, and that becomes a more complex issue to solve.

When it comes to this level of encryption, whether dealing with B2B or B2C information sharing, it is critical to get it right. Our approach to this cannot be complex, it cannot be intrusive in the way email is used, and, critically, it cannot be too difficult for the recipient to easily access the information in the message.

Failing to get this right will be detrimental to business and its efficiency, as well as to customer satisfaction and ultimately to the information security approach itself. Getting this challenge right by making the process simple and clear, and the recipient experience frictionless and efficient, will carry significant benefit. It will greatly enhance the security of information sharing and reduce the risk of a highly impactful data breach.

For the remainder of this document, when we discuss email encryption, we mean the encryption of the content as defined above, be that the message or its associated attachments.

2. Challenge: Enterprise Encryption Today

The way we use email as a communication tool presents a significant challenge to the enterprise when it comes to additional security. Email is, as discussed, the de-facto standard for communication for the vast majority of users. Whether it's a business communication, personal, or consumer message, people understand and are comfortable with the "standard" email experience. And that in itself poses a challenge.

How do we ensure that the experience of the sender and recipient is as simple and straightforward as a standard email exchange? How can we be sure that wherever our recipient receives the message, we provide them with the appropriate tools to access it and encrypt the message and its content?

Beyond that, there are other architectural considerations to consider. The solution must be seamless in its integration with the mail system. Those systems are too essential to business communication to introduce risk. An encryption solution must support all of the mail platforms, both on-premises and in the cloud.

And in cases where an organization has invested in or inherited an existing mail encryption system, is it possible to consolidate them into a single enterprise class solution that is fit to meet the diverse needs posed by a business's encryption demands?

Solving these challenges are key to addressing the enterprise email encryption challenge.

3. Solution: The Role Of Rationalizing Encryption

Before considering encryption solutions, the first question to ask is does the organization actually need the additional capabilities provided by an enterprise email encryption system? If your enterprise needs to go no further than enhancing the security of message transport, then most enterprise mail systems, both on-premises and in the public cloud, will provide this natively.

For organizations that have a valid business case or regulatory demand to dictate enhanced levels of security, the question then becomes: What is available natively in our enterprise platforms?

Microsoft, for example, has sensitivity labeling rules that can provide the user with the option to apply encryption to a message and its attachments. However, the user experience needs to be considered, as does the broader use of sensitivity labels. Sensitivity labels should only be considered as part of a wider compliance and governance approach.

We could also explore the use of secure sharing platforms as a way to encrypt and share sensitive data. However, this impacts the workflow of both sender and recipient and makes adoption more challenging and costly.

What if you already have encryption solutions deployed? Is it easier to maintain them? Consider that the costs, complexity, and management overhead of multiple encryption solutions can be prohibitive.

If your enterprise needs to effectively share sensitive information by using encryption, then we must consider whether our current approaches can give us the flexibility and simplicity needed to effectively deliver such a solution.

What Is Required From Encryption Tools?

If we have identified a demand for email encryption within the enterprise, what should we be looking for when it comes to selecting an appropriate platform? For each enterprise this is likely to be weighted differently based on specific needs, however the broad requirements will be similar.

For example, at a basic level we should expect the following.

- Ability to offer transport level encryption between systems

- Ability to encrypt at a message level
- Plug-in free installation, reducing risk and simplifying deployment
- Simple user experience to aid adoption
- Flexible decryption options to provide broad recipient options and access

Beyond this, what are other desirable capabilities to consider?

- Good support for multiple encryption standards
- Broad recipient access options for secured messages
- Ability to keep encrypted information “in house” while providing secure external access
- Integration with other internal security and encryption tools to protect current investments
- Automation of encryption to ensure all relevant messages are captured and encrypted as needed
- Broad authentication options to provide a wide range of identity and access controls to those who access our secured information
- Broad mail platform support
- Extensive control over branding
- Support for multiple languages

The importance of the above criteria will vary depending on requirements.

As with all technology implementations, there are also non-functional requirements that are worthy of consideration.

- Ease of implementation
- Ability to consolidate
- Seamless user experience
- Improvement to enterprise security posture

It is these non-functional requirements that will help to measure the solutions' overall business value to the enterprise.

Solution Brief: Meeting Criteria

How does Echoworx's approach to email encryption help to meet the demands outlined in this report?

The Echoworx platform opens a broad array of options and flexibility for those that require a more tailored encryption approach. It offers impressive support for encryption standards, a simple and unobtrusive end-user interface, and a broad set of recipient options. This flexibility can help an enterprise satisfy all sorts of use cases, regardless of whether their demands are business-to-business or business-to-consumer.

Let's look at how the company does this in more detail.

The platform is a SaaS offering, sitting outside of any deployed email systems, whether on-premises or in the cloud. As **Figure 1** shows, the mail flow is simply redirected to the Echoworx engine, where encryption rules are applied.

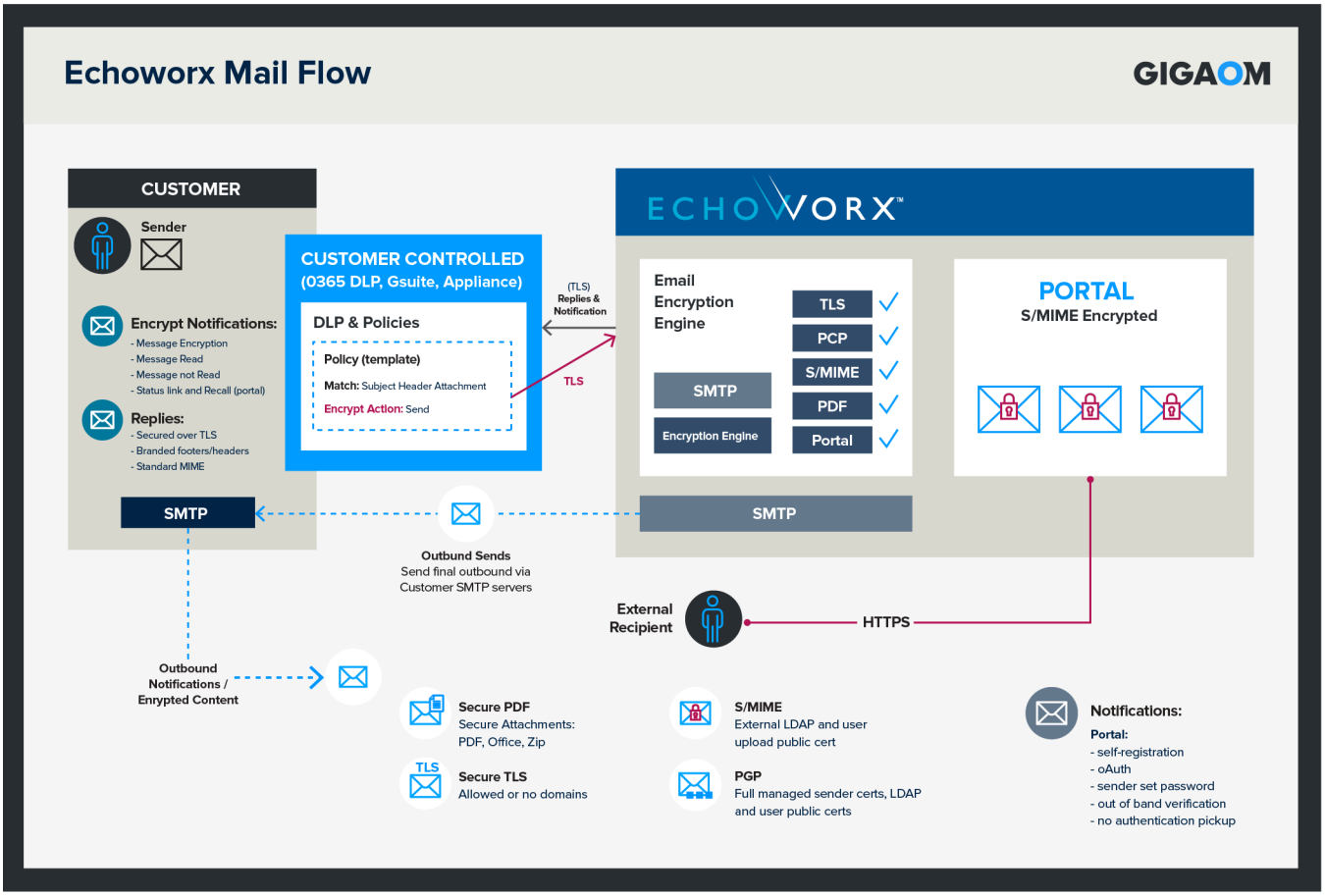

Figure 1. Echoworx Mail Flow

Not all messages need to be redirected, which reduces workload on the service and unnecessary complexity for users who do not need secure email communications. Those that do require encryption are redirected in two ways: Via a user choice, which can be done using a plug-in if desired, or by simply adding appropriate text in the subject line. It can also be redirected based on mail system rules, which include looking for message metadata or message content to ensure that all messages that require encryption are captured.

Once information is encrypted, it is rerouted to the mail system to be sent out via normal email services. This both simplifies email delivery and preserves important DNS-based email security. However, if needed, the solution also offers the ability to forward email directly from the Echoworx service.

Once delivered, it is here that Echoworx stands out, providing both recipient and sender a wide range of security models to protect the integrity of the information. **Figure 2** shows the various models.

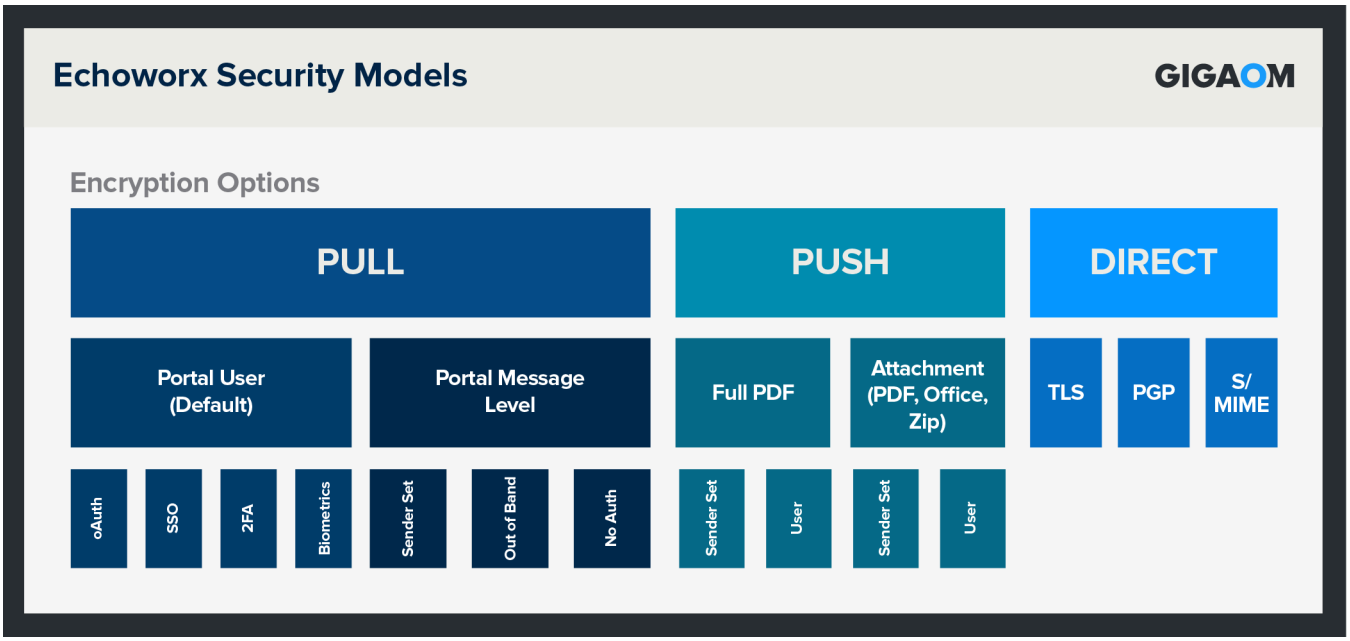

Figure 2. Echoworx Security Models

Options are broad, providing multiple encryption levels, authentication support for the recipient, and the ability to encrypt a wide range of information types. Some, like Office documents and PDFs, are supported natively; those not natively supported are handled by “wrapping” them in a PDF or ZIP file for encryption purposes.

For those who would rather secure information by retaining control rather than sending information externally, this is delivered via the recipient portal.This allows the recipient to receive a message that guides them to the portal to access it. A wide range of security and authentication options are available to support this access. This is a common practice for many organizations, especially those with B2C requirements.

It is this flexibility of operation that makes Echoworx a powerful option for those who must go beyond simple transport encryption—for example, enterprises that work extensively with consumers and seek to offer a highly secure service, but have very little in the way of standards to rely on at the recipient end. Those who need to secure sensitive information but are concerned about data sovereignty will also find the portal compelling.

There are many use cases that native email encryption either cannot support or cannot efficiently deliver, being too cumbersome or complex, and in those cases Echoworx provides a compelling technical solution.

4. Example: How an Organization Rationalized Encryption

As discussed, if you have a demand for email encryption, doing it properly is critical. A large investment bank we spoke with learned this lesson and saw the impact of a poor implementation. By re-evaluating and choosing Echoworx, it simplified the process and made a significant difference to the business.

The bank faces stringent regulatory requirements to fulfill when it comes to sharing data, and this was especially critical when sharing data via email. A previous email encryption platform investment had failed, proving cumbersome and difficult to use and introducing delays to workflows as well as difficulty for recipients accessing the information they were sent.

This had a big impact on productivity, and eventually on the security of their data transfers—users both internally and externally were finding ways to circumvent the solution, leading to emails either not being encrypted or users finding alternative encryption tools. This introduced significant problems and potential data loss and breach risks.

Nonetheless, enterprise email encryption remained a critical requirement, and the bank again reviewed the market to address its governance requirements, selecting Echoworx to meet its demands. IT leadership was impressed by Echoworx's simplicity, efficiency, and seamless integration into current email systems and the ease with which it could be included in user workflows, greatly improving the experience from the previous system.

The bank also appreciated the solution's as-a-service nature, which fit into its strategy of "cloud first" and greatly reduced implementation complexity, allowing for the solution to be delivered quickly.

Technically, the Echoworx platform delivered key features to meet demand. The client portal allowed the organization to deliver a high quality customer experience. Secure emails are no longer "sent" to an external recipient; rather, a link is sent to the recipient that directs them to the secure portal where they can then access the encrypted information. While the bank already uses multiple authentication methods, it is keen to investigate Echoworx's delivery of "social" logon support, using logon federation to popular platforms to ease the customer experience.

Another major technical advantage was the support Echoworx provided for shared mailboxes. These are widely used across the bank, but many of the solutions under consideration lacked support for this feature.

The rollout was complicated by the bank's own internal governance and change control procedures, however, the technical deployment and adoption has been impressively rapid.

As a "border" only solution, Echoworx sits outside of the organization and emails that demand encryption are simply forwarded to the platform from the mail system. Due to the use of the portal for accessing this secured information, the information travels no further than the platform. The simplicity with which the email encryption option is offered to the sender has been a powerful driver in its rapid and successful adoption. The bank chose to install the Echoworx agent to its endpoints. While not a requirement, this helped the organization take advantage of both a simple option to choose to encrypt, as well as to employ an agent to identify messages that are being sent externally and provide a prompt ("Would you like to encrypt?") to the end user.

The simplicity of this approach in comparison to its predecessor has impressed the team and improved adoption both in terms of speed and usage. While the previous solution was rarely used because of its complexity and cumbersome operation, Echoworx has been embraced both internally and externally, with thousands of customers embracing the solution and registering to use it for secure messaging.

On top of its technical value, the bank also found the responsive nature of the Echoworx support and account management extremely impressive, providing rapid response to queries as well as rapid development of new features to improve the platform and effectively meet their needs.

We have discussed how email encryption, where the use case dictates, is a value weapon in our data security toolkit. However, done badly it can be counterproductive and negatively impact security posture. But when delivered well with a vendor such as Echoworx, the solution can not only improve security of information transfer, it can improve user experience, customer satisfaction, and engagement.

5. Conclusion: Review, Assess, Deliver

The security of our data is, without question, at the top of any enterprise's priority list. It is not just an IT problem; this is an issue that impacts all facets of business. Securing email communication is an important part of this effort.

However, email encryption is a topic that needs careful consideration. Email is core to the way business operates and is still the primary method for sharing information, especially when it comes to sharing outside of the enterprise.

The need to offer a hardened approach is not something that all organizations must or should have. For those that do adopt the solution, it is important to understand why and what impact such a deployment will have. A poorly designed or implemented solution will have a negative impact, leading to low adoption and potentially increasing the security risk as users look to circumvent a poorly thought-out solution.

By the same token, getting it right can deliver significant value by enhancing the enterprise's security and by helping to drive adoption and provide a better experience for those with whom you do business.

Email encryption platforms, when the business case dictates, are a necessity. Trying to rely on native capabilities can be complex and time consuming, while often failing to deliver the required benefit.

Echoworx stands out as an example of how to deliver this solution well, with simple deployment and an ease of adoption that allows an organization to quickly enhance its email security.

Before you consider such a solution, ensure you fully understand your requirements, use case, and impact on your business messaging flow and recipient experience. Only then can you be sure that an email encryption solution will be suitable for your needs and you can begin the task of identifying the right one for you.

6. 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.

7. 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.

8. 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.

9. Copyright