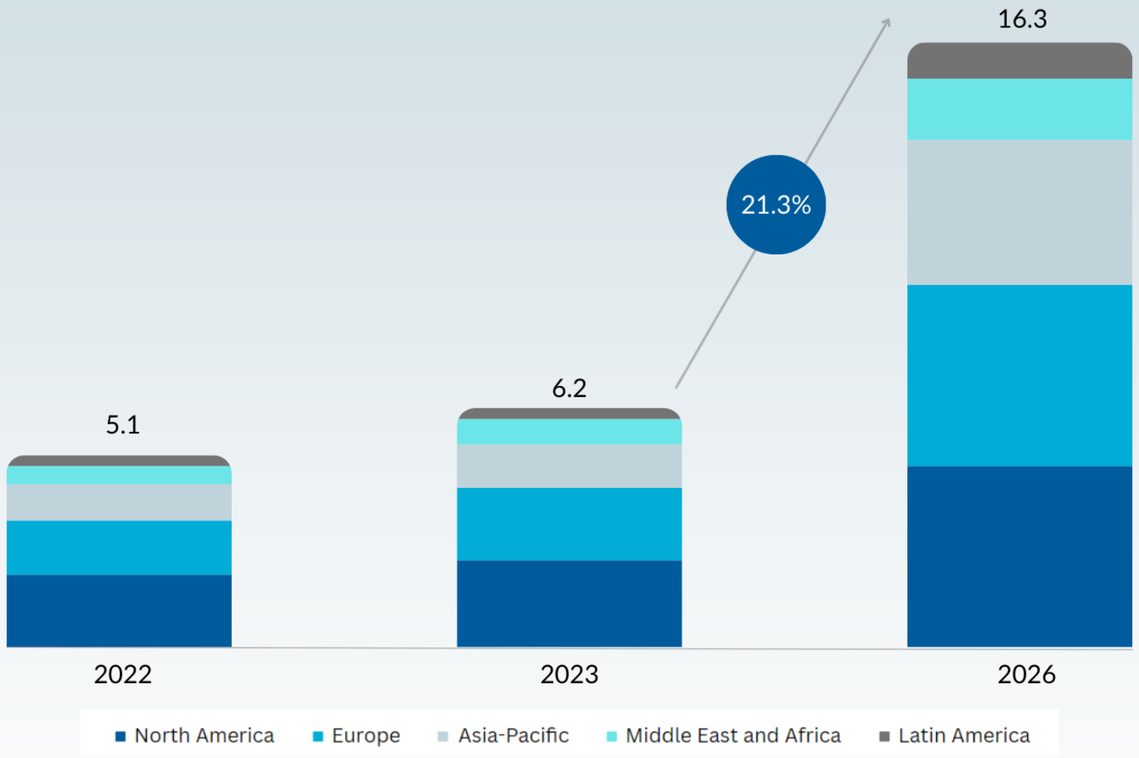
ECHOWORX™

IT PAYS TO BE SECURE

Unraveling the Growing Demand for Advanced Email Encryption

Table of contents

Email Encryption Market Global Forecast to 2028 (USD Billion)



Source: MARKETSANDMARKETS, Email Encryption Market - Global Forecast to 2028

Introduction

Demand for advanced email encryption is skyrocketing, with no signs of slowing down. Imagine a client who encrypted 18 million messages annually six years ago.

Today, they send well over a hundred million encrypted messages per year. This exponential growth reflects the widespread adoption of encryption solutions by global enterprises, spanning business units and acquisitions.

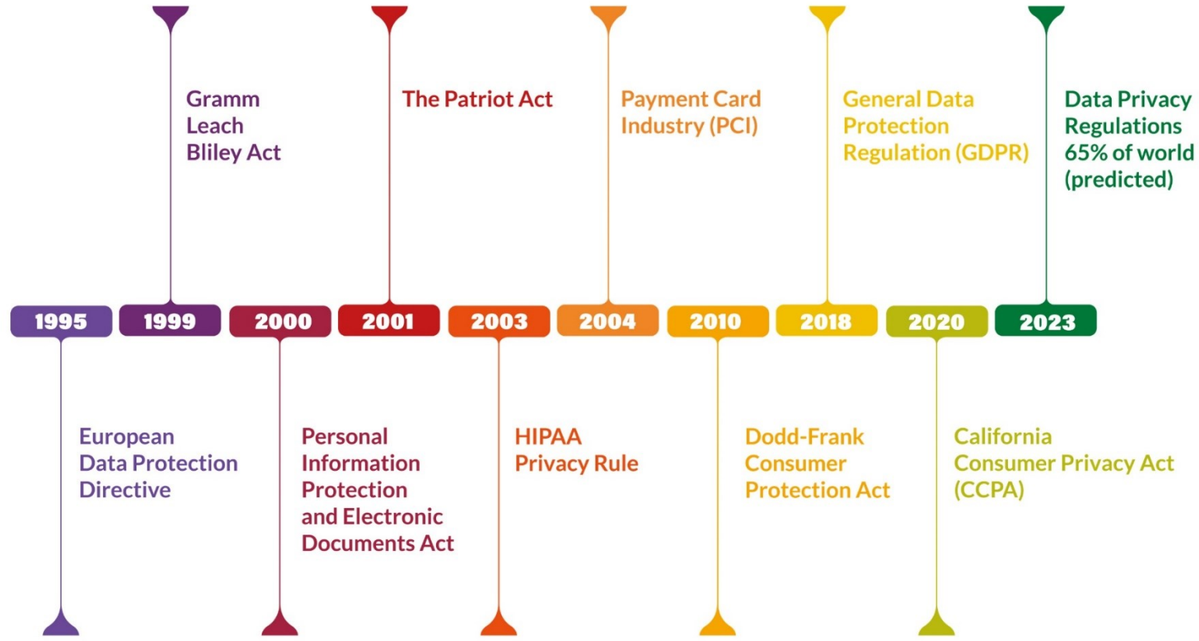
In this eBook, we explore the reasons behind this increase and discuss the significance of stakeholders in the decision-making process when implementing or replacing an encryption system.

Key Drivers Fueling Organizations' Demand for Advanced Email Encryption

Navigating Ever-Changing Privacy and Data Legislation

The landscape of privacy and data legislation is in a constant state of evolution, with changes taking place on a country-by-country basis nearly every year.

Moreover, even during recessions or economic fluctuations, regulatory compliance mandates for data protection remain unwavering. This boosts the demand for advanced encryption solutions, meaning businesses need to maintain or enhance their encryption standards, regardless of economic conditions. This is particularly pertinent for global companies that operate across multiple jurisdictions, such as Germany, the United States, and the UK, each with its own unique considerations when it comes to legislation. To illustrate this point, let's explore a couple of real-world examples.



Key Drivers Fueling Organizations' Demand for Advanced Email Encryption

Navigating Ever-Changing Privacy and Data Legislation (Con't)

Imagine a multinational UK bank that diligently adhered to European data regulations even before the Brexit vote. However, post-vote, they faced the crucial task of aligning themselves with EU data legislation. To meet this challenge head-on, they took the strategic decision of establishing a brand new data center in Ireland.

In a similar vein, a prominent law firm based in the UK faced the challenge of meeting the data needs of their German clients. As a solution, they established a data center in Germany. These examples highlight situations where client circumstances evolved, necessitating corresponding adaptations in email encryption services.

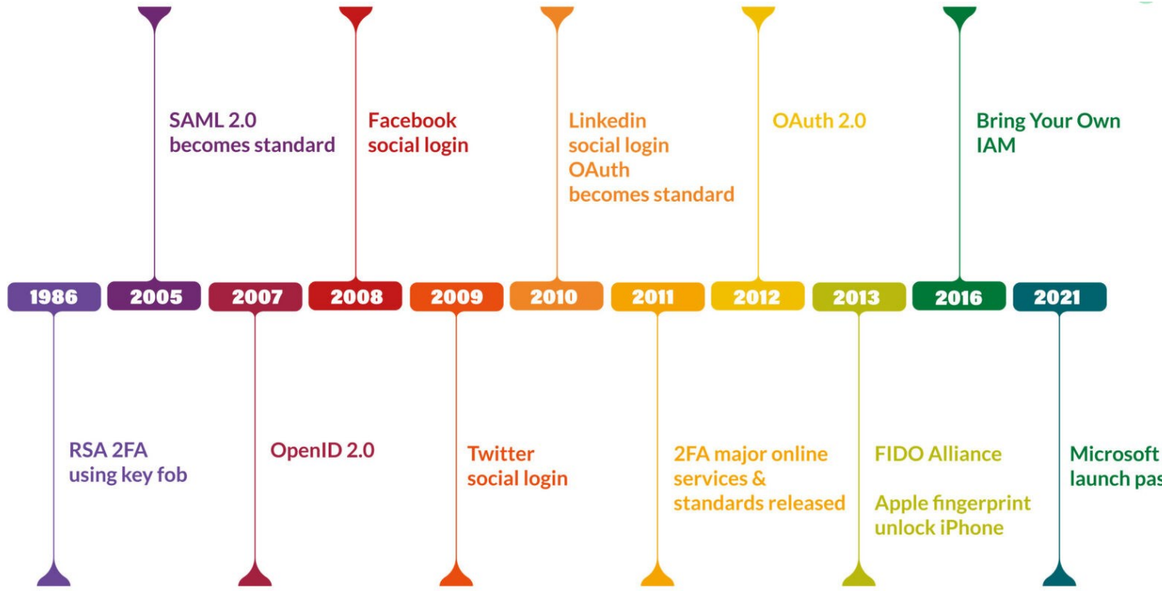
Now, let's delve into a captivating scenario featuring a prominent Saudi petroleum and petrochemical company. They were in need of a robust gateway system to safeguard their message exchange, guaranteeing the sender's non-repudiation. Echoworx Email Encryption stepped up to the plate and flawlessly met their requirements.

When organizations are unaware of their obligations or fail to comply due to limitations in their existing solutions, they face regulatory risks. This underscores the intricacy of the secure email landscape in which Echoworx operates. Our primary objective is to anticipate and meet clients' needs by proactively considering regulatory changes.

Authentication: Embracing Innovation

Evolution of Authentication: RSA 2FA to Biometrics

Over time, authentication methods have undergone significant advancements with the goal of reducing reliance on passwords. In the past, the RSA 2FA key fob was extensively used by treasury departments of investment banks and regular banks. Surprisingly, it continues to be in use today, especially for banking activities and large money transfers. **As the landscape of authentication standards and acceptance evolves, staying updated with the latest developments is crucial.**



Authentication: Embracing Innovation

Evolution of Authentication: RSA 2FA to Biometrics (Con't)

Organizations began implementing password-only authentication using Gmail passwords a few years ago. Although more advanced methods like SAML can pose challenges for end users, certain clients still prefer them. There are methods to minimize authentication obstacles and eliminate the need to manually enter passwords. Users are increasingly opting for authentication through social connectors. Two-factor authentication and biometric authentication, including face recognition and fingerprint recognition, greatly enhance security. Echoworx introduced these features last year, much to the satisfaction of their large clients who eagerly embraced them. This is again bolstering the need for advanced email encryption solutions.

Let's share a couple of examples. An American multinational automobile manufacturer permits recipients to utilize their Office 365 login for access. Although this is highly beneficial for most users, it can prove to be a less than satisfactory experience for non-Office 365 users. Additionally, the storage of numerous Office 365 keys in the United States raises concerns among European clients, primarily due to the Patriot Act.

A commercial bank Ireland is committed to enhancing the user experience by streamlining password management. They provide a range of up to six authentication methods, placing utmost importance on ensuring clients feel comfortable throughout the authentication process. In contrast, Nordic banks prioritize two-factor authentication, employing methods such as SMS text messages or fingerprints.

The crucial point to remember is that the current solution must possess the **flexibility to adapt to future access management methods**. This sentiment holds true for both security officers and user experience experts, emphasizing the importance of providing a wide range of options and the need for advanced email encryption solutions.

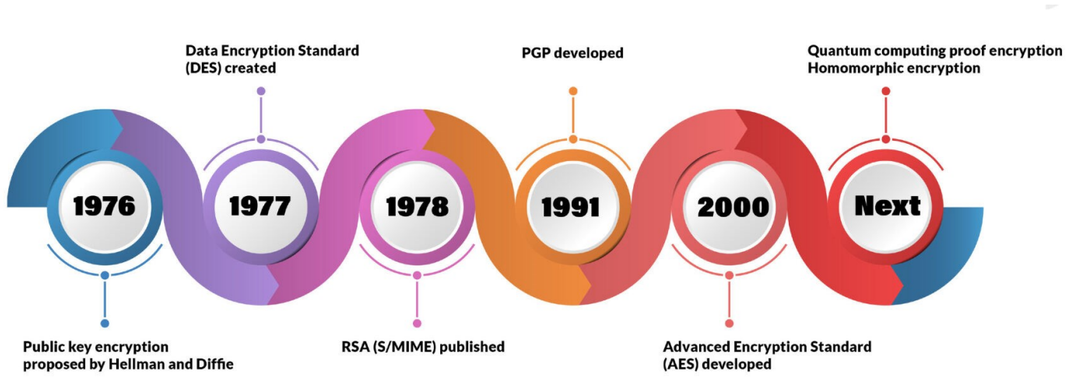
Encryption Standards: Ensuring Robust Data Protection

Encryption Standards Evolution

Another driver behind the increasing demand for advanced email encryption solutions in enterprises is the past limitations of many email encryption platforms. These platforms were rigidly designed around specific encryption standards, lacking the required flexibility and adaptability.

To ensure robust data protection, it is crucial for organizations to comply with a range of encryption standards. These standards encompass diverse encryption types, such as traditional public key encryption, RSA, and S/MIME. Additionally, there is a rising interest in quantum-proof and homomorphic encryption, which offer advanced security capabilities. Enterprises employ various encryption methods, including PGP, which was once widely utilized but now receives limited support. By adhering to these encryption standards, organizations can safeguard their sensitive information effectively.

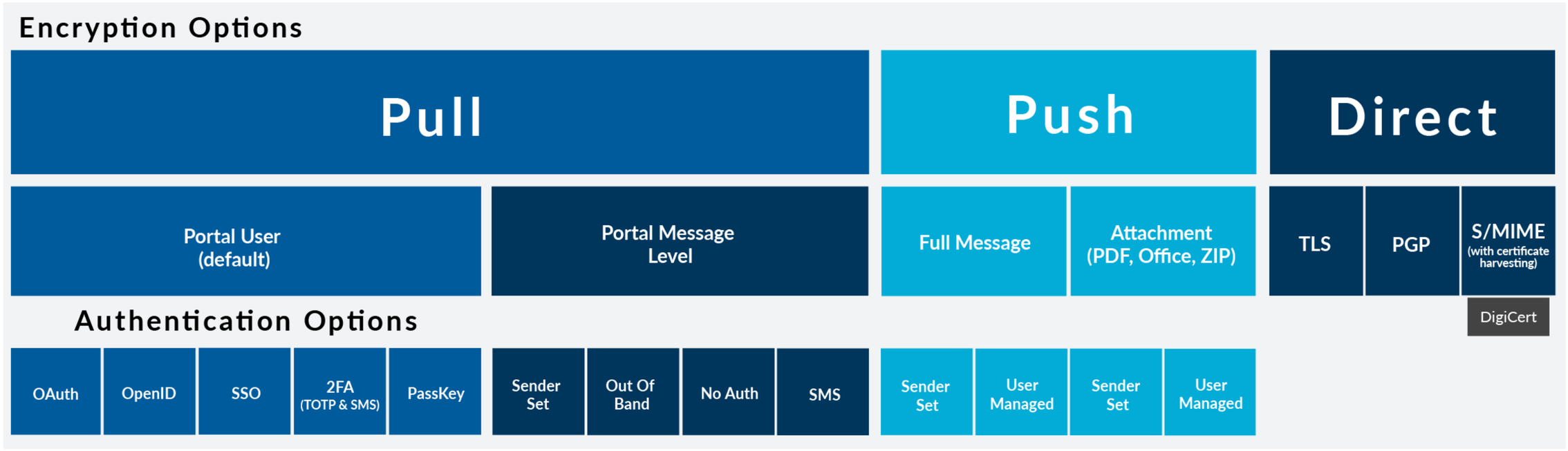
For instance, Echoworx's banking client consistently submits encrypted reports to the Bank of England, using PGP keys as required. Echoworx remains flexible in meeting the needs of customers and partners, without showing preference for any specific encryption method.



Delivery Options:
Prioritizing Security and Accessibility

Tailoring Delivery for Security

Organizations give utmost importance to delivery options as they have a direct impact on message security, accessibility, and the elimination of workflow disruptions and interoperability issues. These options include office attachments, email PDFs, PDFs as attachments, zipped files, encrypted portals, and the use of TLS (Transport Layer Security). These methods are constantly evolving, and the presence of these examples showcases their extensive range.



Delivery Options:
Prioritizing Security and Accessibility

Tailoring Delivery for Security (Con't)

A stock exchange facilitates secure communication with business partners by establishing an active TLS connection. In instances where TLS is not feasible, portal delivery achieves encryption, ensuring data protection and confidentiality.

A retail bank based in Scotland currently sends secure attachments, but the marketing department contemplates transitioning users from PDF to a user-friendly portal. This transition seamlessly accommodates convenience for all users.

Client needs are dynamic and can be influenced by legislation or evolving business requirements. Take, for instance, a British multinational bank that predominantly relies on encrypted PDFs but occasionally employs ZIP files.

A multinational pharmaceutical company is currently transitioning from delivering content through portals to using PDFs. Regulations mandate recipients to have persistent data accessible in their email inboxes, driving this change.

Furthermore, an international client utilizes six distinct delivery methods, tailored to each country's specific laws and regulations. This approach allows for a comprehensive and compliant solution to meet the diverse needs of the global customer base.

A one-size-fits-all approach may not always be suitable. What proves effective today might pose challenges in the future.

Exploring New Encryption Use Cases

Enhancing Business Security with Innovative Solutions

New encryption use cases for business continue to emerge. One example is a pharmaceutical distributor that develops new brands to cater to communication requirements for drug trials. Whenever a trial commences, participants receive encrypted documents or emails adorned with the logo style corresponding to their specific trial. This demand has remained steady since they became our client.

Language plays a vital role in communications as well. Organizations operating in Canada, a bilingual country, must determine if an email is in Quebec and send communications in French or if it's in an English-speaking province and send them in English. For clients, a total of 28 language options are offered, including links if necessary.

The satisfaction of clients is prioritized by ensuring that every aspect of the service, from instructions to user interface, is tailored to their needs. Moreover, our expertise extends to supporting mergers and acquisitions. A notable example is the successful consolidation of multiple financial institutions under the unified platform, while preserving their unique brands.

In the midst of it all, **it's crucial to strike a balance between simplification and flexibility**. Organizations are now blending remote and on-site work, leveraging platforms like Microsoft 365 and Google Workspace. This trend is driving the need for advanced encryption solutions that seamlessly integrate with cloud and existing workflows. **The goal is to achieve seamless work across diverse organizational capabilities**.

Crucial Role of Stakeholders

When it comes to email encryption, remember its integral role in the infrastructure.

When it comes to email encryption, it is crucial to remember its integral role in the infrastructure. Serving as a fundamental component of the messaging system, encryption enhances the user experience for customers and partners, both internally and externally. Its importance cannot be overstated, despite the challenges that may arise.

To ensure comprehensive consideration of all requirements, involving various stakeholders is advisable. The security team, compliance officers, risk teams, and even members of the marketing team who are involved in user interface aspects should be included. Inclusive discussions with a diverse group of six to twelve individuals during initial meetings and demonstrations guarantee that all perspectives and needs are adequately addressed. The involvement of these stakeholders is crucial for examining the architecture and ensuring its effectiveness. It is important to distinguish between building an architecture that allows for modular expansion and one that leads to dead ends. These discussions not only explain current accomplishments but also emphasize future capabilities, as the software is designed to be extendable.

Considering the key areas of focus mentioned earlier—authentication options, standards, delivery options, and privacy legislation—prioritizing product demonstrations as an unmissable starting point would be prudent. These demonstrations provide interested parties with valuable insights.

ECHOWORX™

IT PAYS TO BE SECURE

In the dynamic landscape of digital communication, email encryption emerges as a crucial player, underlining the importance of security, flexibility, and adaptability. It becomes a tool that bridges the gap between necessity and efficiency, shaping the way organizations worldwide communicate confidentially. As they continue to adapt to evolving legislation, technological advancements, and diverse business needs, the demand for advanced and tailored email encryption solutions grows. Ultimately, the rise of email encryption signifies not just the growing consciousness about data security but also the commitment to ensuring seamless, secure communication in an increasingly interconnected digital world.

Learn more:

Echoworx Email Encryption – Delivery Options

Discover Customer Success Stories