Technical Validation

Echoworx Email Encryption

User-focused Email Encryption for the Enterprise

By Justin Boyer, Validation Analyst

This Enterprise Strategy Group Technical Validation was commissioned by Echoworx and is distributed under license from TechTarget, Inc.

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group (ESG) details the evaluation of Echoworx email encryption. We validated Echoworx's focus on user experience, flexibility to handle multiple use cases, and extensive branding and language support. Echoworx email encryption keeps sensitive information safe without sacrificing user experience.

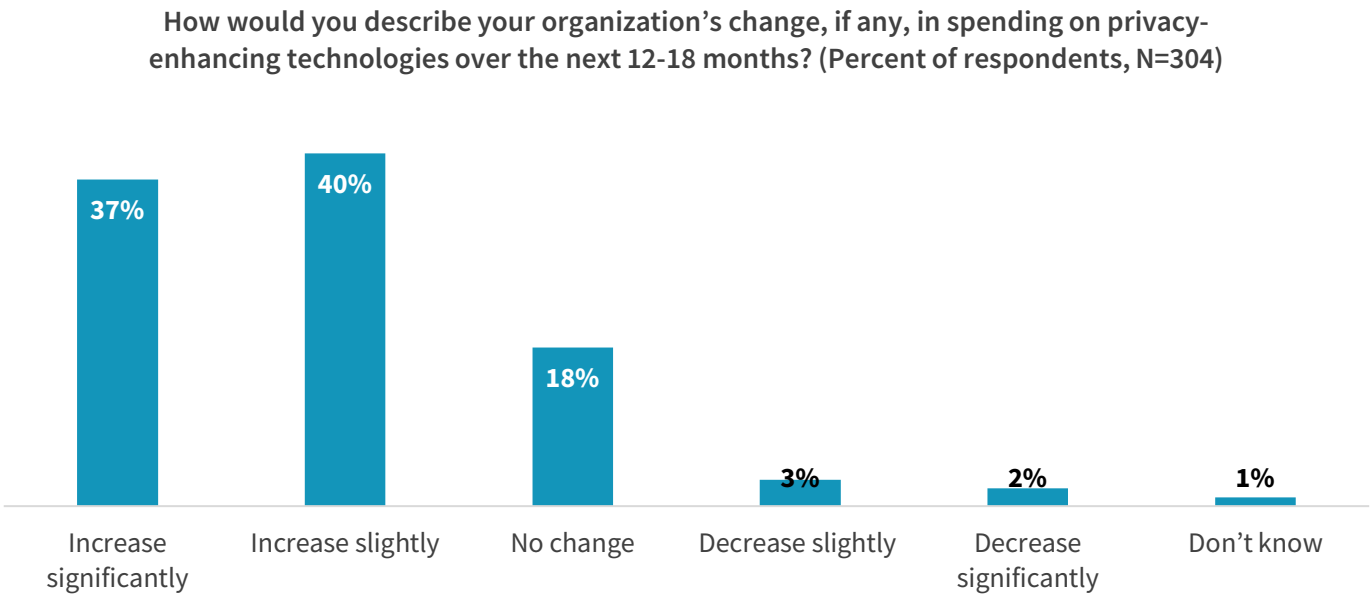
Background

Digital transformation is a leading trend across industries. The benefits of digital transformation include increased efficiency, collaboration, and a better user experience. Enterprise Strategy Group (ESG) research found that 45% of companies surveyed saw providing a better and more differentiated customer experience as an important objective for digital transformation initiatives.[1]

As more technology is added, security and privacy become a bigger challenge, as does making the transition easy for users. Email is a technology often addressed in digital transformation initiatives. It's a convenient way to communicate with partners and customers but isn't a secure channel on its own. Personally identifiable information (PII), personal health information (PHI), and other sensitive information must be protected. Emails sent with this information can be intercepted and used maliciously.

Organizations are aware of the need for privacy. According to ESG research, 77% of survey respondents plan to increase spending on privacy-enhancing technologies over the next 12-18 months (see Figure 1).[2]

Figure 1. Organizations Are Increasing Spending on Privacy-enhancing Technologies



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations need to protect private information sent through email without impairing customer experience.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.
[2] Source: Enterprise Strategy Group Research Report, *The State of Data Privacy and Compliance*, March 2022.

Echoworx Email Encryption

Echoworx is an enterprise-grade email encryption solution that protects company and customer private data. Echoworx offers an optional Microsoft Outlook and Gmail plugin to give users control over which messages need to be encrypted. Echoworx integrates with third-party email gateways so users keep using the email systems they use today.

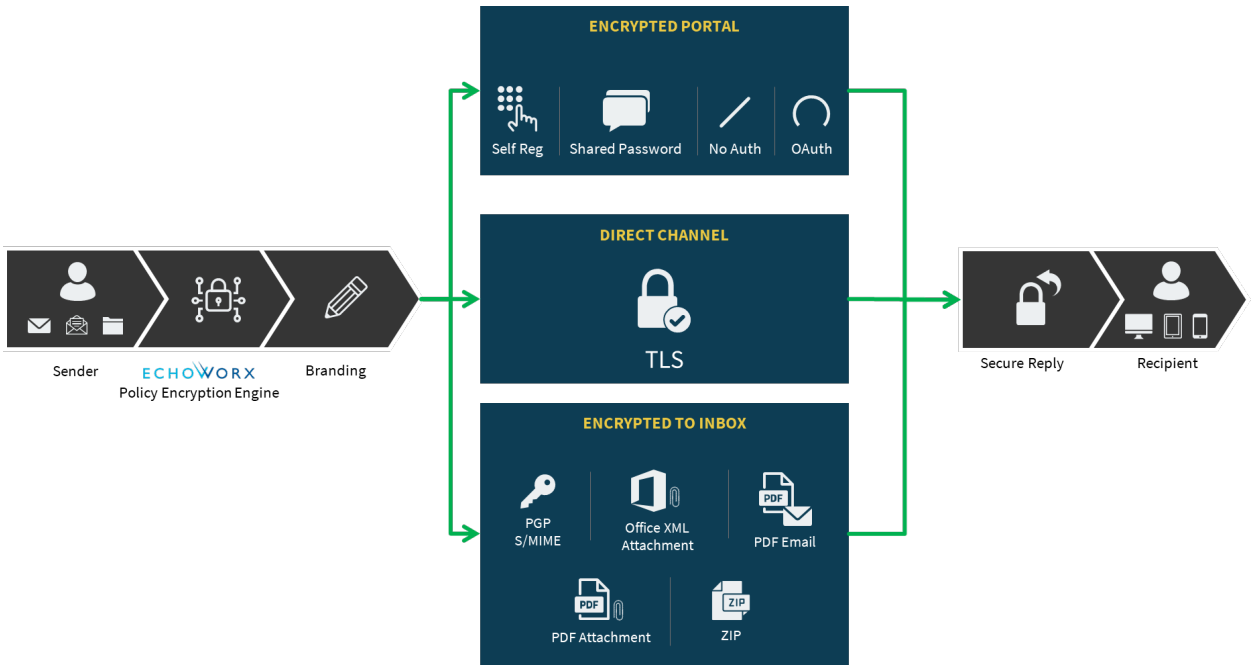
A focus on user experience helps companies to keep customer data private without compromising the ease of use that makes email so popular. For example, emails can be tagged to be encrypted by adding keywords to the subject line. The Outlook plugin can also be used to encrypt with the click of a button, including options such as encrypting attachments or protecting the email with a passphrase. Echoworx provides this usability while maintaining high compliance standards for regulations such as PCI-DSS, SOC2, and GDPR.

Extensive branding and language support give companies the ability to use Echoworx at locations around the world. Echoworx supports 28 languages. Global deployments in the US, Canada, UK, Ireland, and Germany (with more on the way) help organizations comply with residency regulations.

Echoworx features a SaaS model that fits many use cases with high configurability and ease of administration. Many use cases can be covered with configuration and without custom code. In addition, Echoworx can be deployed as multi-tenant (logical separation from other tenants) and dedicated tenant (physical separation from other tenants).

Figure 2 illustrates the overall workflow of sending an email. An email marked for encryption first travels through the Policy Encryption Engine to encrypt the message based on the organization's policies. Next, Echoworx applies any branding rules. There are several options for email delivery based on the needs of the organization. Users can retrieve the message from an encrypted portal, which can be branded and integrated with an organization's website. Emails can be encrypted and sent as PDF attachments, or users or enterprises can choose to encrypt only the attachments. Finally, Echoworx offers PGP and S/MIME direct delivery options. All emails are sent over TLS between the organization and Echoworx for encryption in transit and at rest. Finally, recipients have the option to reply to any message securely via the encrypted portal.

Figure 2. Echoworx Email Encryption



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group (ESG) Technical Validation

Enterprise Strategy Group (ESG) validated Echoworx's capabilities with the goal of assessing how Echoworx protects private and sensitive information sent via email. We focused on Echoworx's user experience, flexibility, and extensive branding and language support.

Focus on User Experience

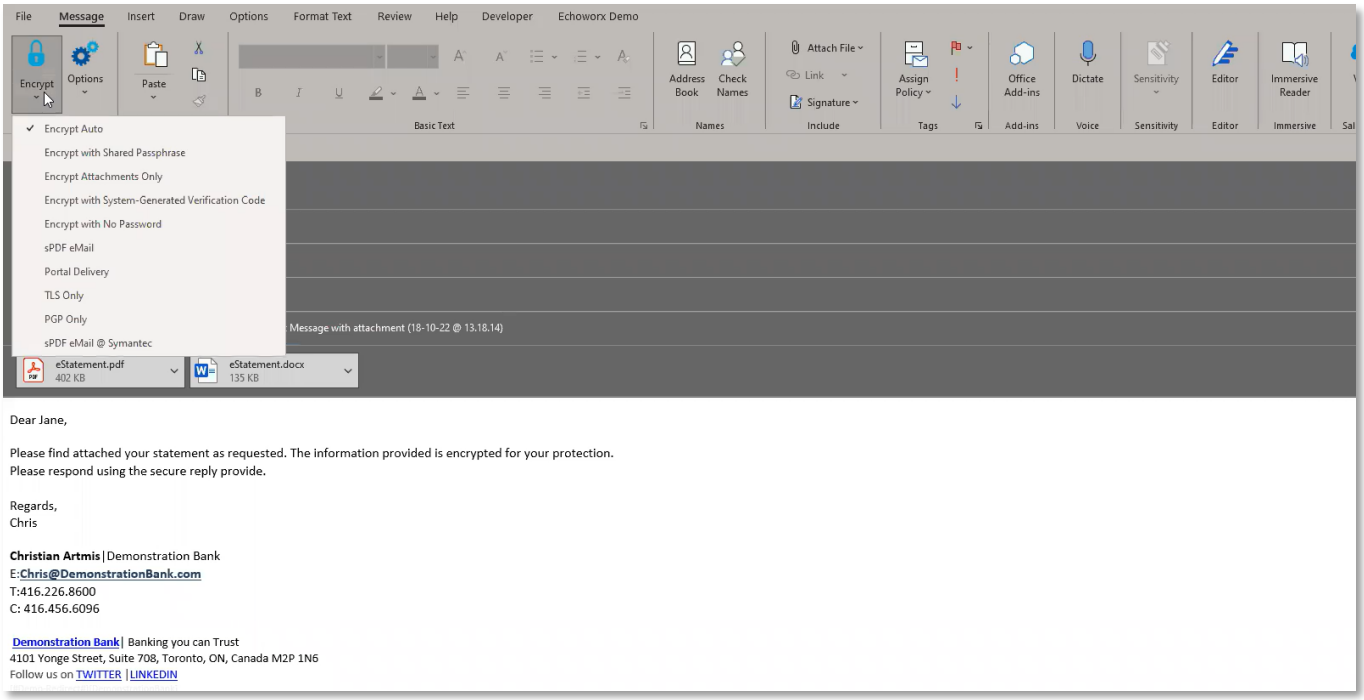
We validated Echoworx's focus on user experience. This focus ensures that organizations can protect sensitive data without making that data difficult to access to those who have a right to see it. Difficult-to-use security controls often are not adopted by end users, defeating the purpose of using them.

Email Integration

Enterprise Strategy Group (ESG) observed the ease of use when sending an email. Echoworx integrates with the end user's existing email platform. An Outlook and Gmail plugin allows users to send encrypted emails with a familiar user interface. Echoworx integrates with third-party email gateways, such as Office 365 and G-Suite, allowing organizations to continue using the tools they use today.

For our demonstration, the end user was able to send an encrypted email using an add-on installed on Microsoft Outlook. The add-on allows several options for encryption chosen by the sender based on business requirements (see Figure 3). The user can also tag the email within the subject line to trigger encryption when it leaves the company's network. This flexibility accommodates different working styles while providing the same protection.

Figure 3. Microsoft Outlook Add-on Used to Encrypt an Email



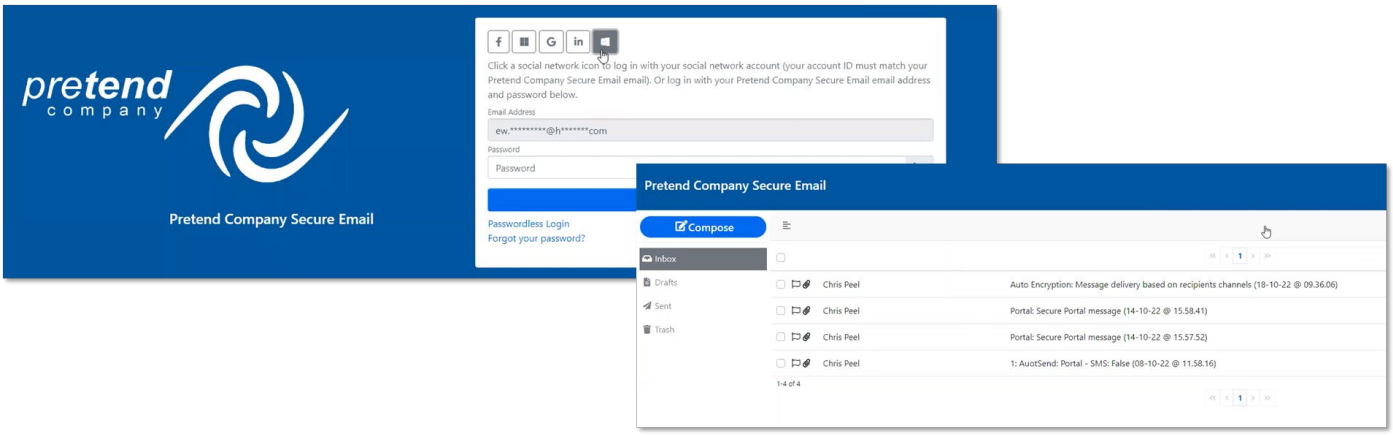
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Authentication Options

We also validated some of the many authentication options available to Echoworx customers. There are currently seven authentication options available: OAuth, self-registration, shared secret passphrase, single sign-on (SSO), system-generated verification codes, biometrics, SMS, and multifactor authentication (MFA).

Figure 4 shows the process of logging into the encrypted portal using OAuth authentication. There are several social connector options available, such as Facebook, Google, Office 365, LinkedIn, and Hotmail. We observed the use of Hotmail to gain access to the encrypted portal. The user clicked the Hotmail button on the login screen, entered their Hotmail credentials, and was granted access to the portal.

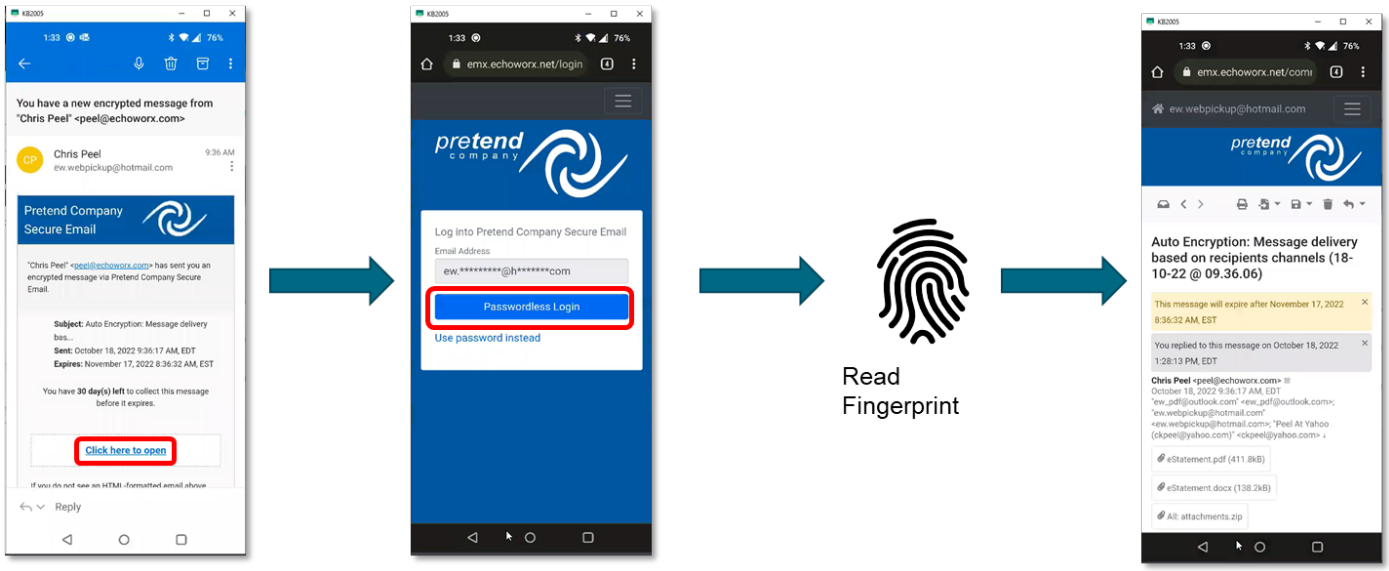
Figure 4. Social Connector (OAuth) Authentication to Retrieve an Encrypted Message



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group (ESG) also observed the use of biometrics to retrieve secure emails via a mobile device (see Figure 5). First, the user received an email stating that a new encrypted message was available. After clicking the link, the portal login screen is presented to the user. Clicking the "Passwordless Login" button prompts the user to scan their fingerprint to authenticate. After the fingerprint is read and verified, the user can view the message and reply securely, if desired.

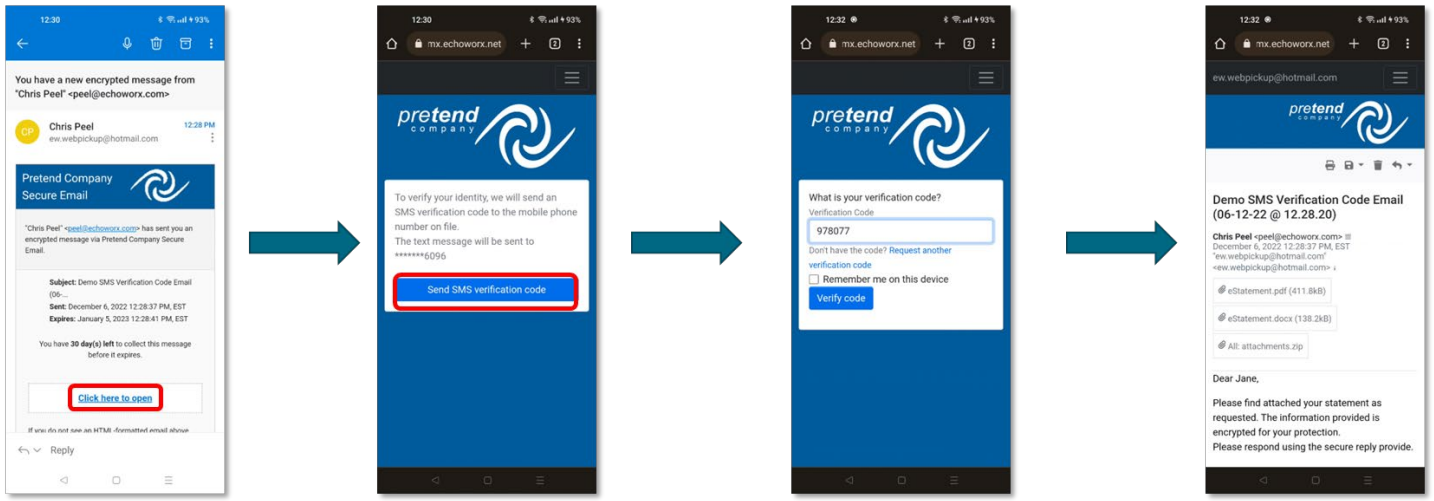
Figure 5. Using Biometrics to Retrieve a Message on a Mobile Device



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 6 shows how a user accesses a secure email message using SMS authentication. The recipient receives a notification that a secure email has been sent to them with a link to view the message. After confirming their phone number, the user receives a code via SMS to their phone. The recipient enters the code and retrieves the message.

Figure 6. Using Biometrics to Retrieve a Message on a Mobile Device



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Organizations across industries are working to digitally transform their businesses, and improving the customer experience continues to be a critical objective for their digital transformation initiatives. 45% of companies cited a differentiated customer experience as an important digital transformation goal.[3] Security solutions often sacrifice user experience for the sake of security, leading to frustration and lack of adoption.

Enterprise Strategy Group (ESG) validated Echoworx's focus on user experience. Exchoworx integrates with the email tools employees are already using. There are several authentication methods such as social connectors, biometrics, and SMS, ensuring that both employees and customers have choices in how to authenticate to retrieve messages.

Echoworx is showing that user experience doesn't have to be sacrificed for security. When security is made easy for end users and customers, they'll use it. Private and sensitive data can be protected while not getting in the way of doing business.

Flexibility to Handle Multiple Use Cases

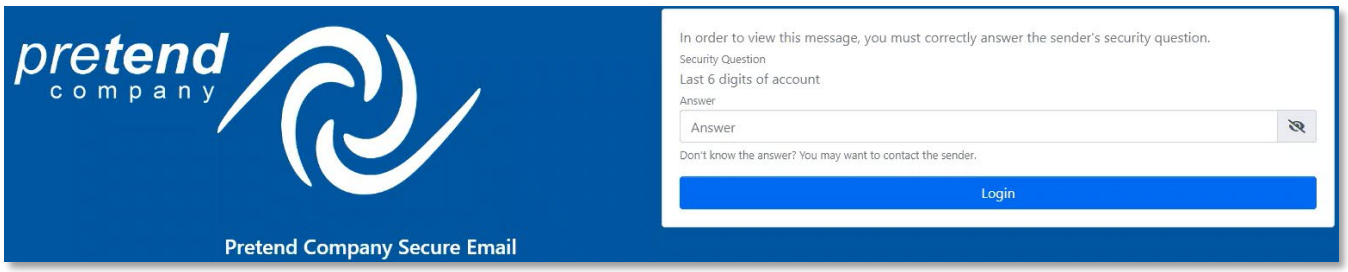
Enterprise Strategy Group (ESG) validated Echoworx's high level of configurability and its ability to handle multiple use cases. Organizations vary in their use of email. Therefore, any email encryption service needs to be as flexible as possible to accommodate various workflows and business processes.

Flexibility in Delivery and Access

Enterprise Strategy Group (ESG) validated Echoworx's ability to offer multiple delivery methods based on business requirements. Businesses can configure Echoworx to support multiple use cases at the same time. Organizations can decide how best to secure and send email according to their business requirements.

The encryption portal can be used to send secure information or to request information from a customer (for example, a bank or accountant that requires documents from the customer that may contain PII). The customer enters a code (in this example, the last 6 digits of an account number) to access and clicks reply to return the required documentation (see Figure 7).

Figure 7. Challenge/Response Screen to Retrieve a Secure Message



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

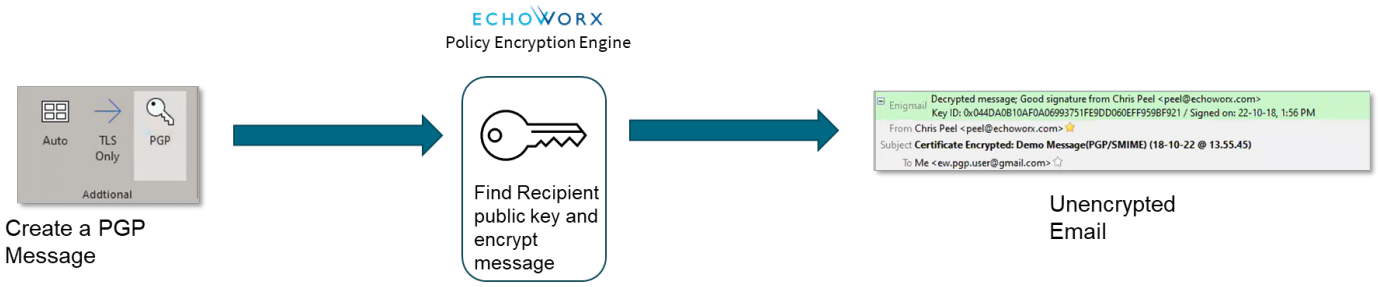
ESG next validated the direct-to-inbox delivery methods. These include encrypted messages sent as attachments, encrypted attachments, PGP, and S/MIME. Specifically, ESG observed an email sent using PGP (see Figure 8). The sender

[3] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.

didn't need to use special software or know the public keys of potential recipients. In this example, the sender clicked the "PGP" button in the Outlook ribbon to indicate the email should be sent via PGP.

The Echoworx policy encryption engine will then find a public key for the recipient if one exists. If it finds a public key, it knows the recipient is a PGP user and encrypts the email with the public key automatically. The encryption engine also creates a private key for the sender automatically. The recipient then uses their private key to decrypt the message once they receive it. Echoworx simplifies the use of PGP, which can be difficult to implement, so users can focus on securing emails instead of complicated and time-consuming setup.

Figure 8. Encrypting and Decrypting an Email using PGP



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

With 77% of organizations planning to increase their spending on privacy-enhancing technologies,[4] security and privacy are clearly huge factors in the success of modern companies, especially those in highly regulated industries that regularly deal with customer PII. Breaches can be catastrophic for companies and customers alike.

We validated that Echoworx can meet the various use cases enterprises need to provide secure email within their existing business workflows. The encrypted portal can be used to deliver email to customers securely, using a challenge/response method or a code sent via an outside channel. Customers can reply through the portal to provide sensitive documents and not worry that they will fall into the wrong hands. Echoworx also features user-friendly PGP and S/MIME support.

Using Echoworx opens many possibilities for companies to adapt their business workflows to include secure communications. It integrates with existing tools while simplifying potentially difficult-to-use technologies such as one-time passwords and PGP encryption. Echoworx is highly configurable, so businesses won't need multiple solutions for secure communication.

[4] Source: Enterprise Strategy Group Research Report, *The State of Data Privacy and Compliance*, March 2022.

Extensive Branding and Language Support

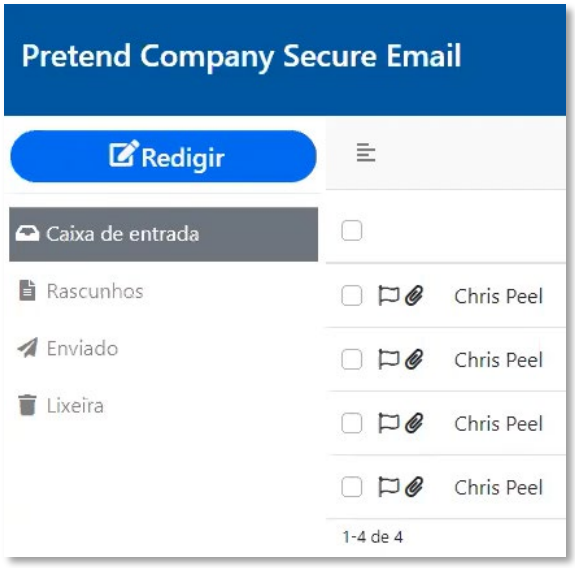
Enterprise Strategy Group (ESG) validated Echoworx's branding and language support. These help companies present a consistent brand to customers using the encrypted portal. Echoworx offers unlimited branding including message headers, footers, notifications, encrypted PDFs, colors, and URLs.

Branding Focused on User Experience

Company branding helps to communicate a clear identity to customers. Consistent branding options help users and customers to know immediately that they are still being served by the organization they trust, even if there may be a different piece of software underneath.

Enterprise Strategy Group (ESG) observed the ability to change the language used in the Echoworx user interface (UI) to a user's preferred language instantly with just a couple of clicks (see Figure 9). In this example, after entering the portal, the user changed their preferred language to Portuguese. Once a language preference is made, the UI instantly updates, as does the language of the messages received within the portal.

Figure 9. The Encrypted Portal in Portuguese



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

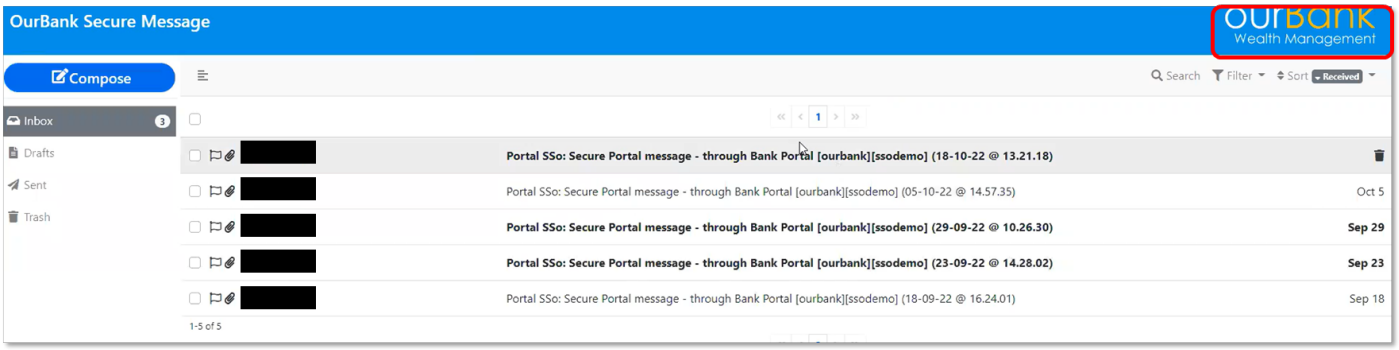
Next, ESG saw a bank workflow where a user was able to retrieve a secure message via the company's website. After logging into the bank website, a link to secure email is displayed along with an indicator that new messages are available (see Figure 10).

Figure 10. Bank Website with Integrated Link to Echoworx Encrypted Portal

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

After clicking the "Secure Email" link on the bank website, the user is sent to the Echoworx encrypted portal to retrieve the message. As seen in Figure 11, the portal is branded to match the bank's website. The end user doesn't need to register to access the portal. Creating an account with the bank is all that is required to access the secure messages. The user sees a look and feel consistent with that of their bank and can trust that their data is safe.

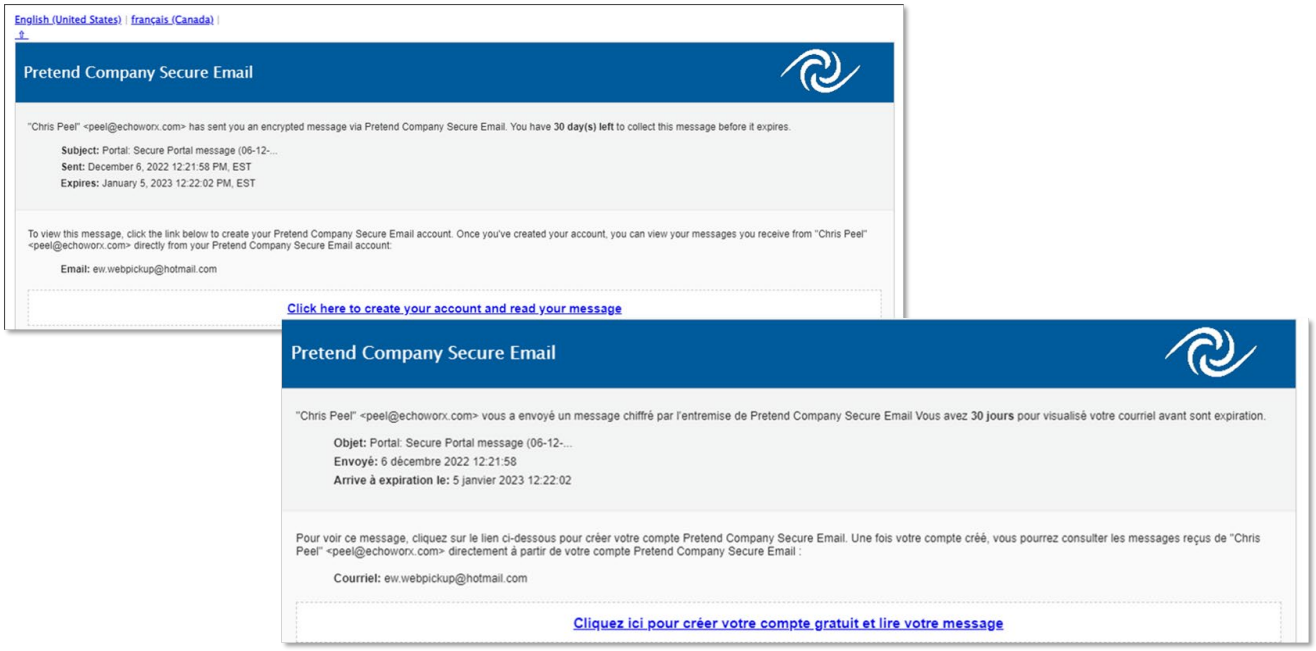
Figure 11. Branded Encrypted Portal Used by Customers



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Through the combination of branding and language configurations, Echoworx can accommodate many use cases. For example, a case study presented to ESG described a Canadian company that can send messages in English and French. Through configuration, the order of languages presented in the email changes based on the Canadian province of the recipient (see Figure 12). This level of configuration helps organizations stay secure without introducing large amounts of expensive customization for more uncommon requirements.

Figure 12. English and French Messages Sent Based on Recipient Location



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Accessibility is also a growing concern for modern enterprises. All customers need to access secure messages no matter their circumstances. Echoworx is rated AA level according to the Web Content Accessibility Guidelines (WCAG), the World Wide Web Consortium (W3C) technical guidelines to improve the accessibility of web content. The experience for those with disabilities isn't affected by customization choices.

Why This Matters

Large enterprises are often global in scale, requiring extensive language support for communications systems. In addition, customer-facing portals need to have extensive branding options to present a consistent look and feel.

Enterprise Strategy Group (ESG) validated Echoworx's branding and language options. The encrypted portal can be branded with corporate logos and colors to present a consistent look and feel when moving from the company website to the portal. Echoworx supports 27 languages, and users can choose their preferred language within the portal. The branding engine can also be used to update the contents of messages based on tags added to the message by the author.

The branding and language support available through Echoworx allow companies to secure their email without compromising their brand. The encrypted portal can be integrated within existing workflows without users knowing it's a different system. The language support allows multi-national enterprises to roll out Echoworx across all locations, providing a single solution for secure email across the world.

The Bigger Truth

Organizations across industries see the benefits of digital transformation, with particular interest in providing a better user experience. Enterprise Strategy Group (ESG) research found that 45% of companies surveyed saw providing a better and more differentiated customer experience as a important goal for their digital transformation initiatives.[5]

Email remains ubiquitous in business-to-business (B2B) and business-to-consumer (B2C) applications. It's a convenient way to communicate with partners and customers but exposes PII, PHI, and other sensitive information, if it's not protected. According to ESG research, 77% of survey respondents plan to increase spending for privacy enhancing technologies over the next 12-18 months.[6]

ESG validated Echoworx to see how it protects private information sent via email through a focus on user experience, flexibility, and strong branding and language support. Echoworx allows organizations to provide secure communications without introducing challenging workflows to employees and customers. The user decides when a message requires encryption and can activate encryption with a tag or the Outlook plugin. Multiple integrations make encryption easy within existing email gateways, such as Office 365 and G-Suite. Language and branding support provide a consistent look and feel for customers. Echoworx stores data in multiple data centers, helping organizations to remain compliant with residency regulations.

Echoworx's flexibility provides organizations with a single tool that can manage many use cases, from encrypted portals and attachments to advanced functionality such as one-time codes and PGP encryption. This flexibility allows for various use cases to be handled using configuration instead of custom code, from the methods used to secure messages to the content of the messages themselves.

If your organization communicates potentially sensitive data to your customers and needs a highly configurable tool to protect your customers' privacy, then ESG suggests that you take a serious look at Echoworx email encryption.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

[5] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.
[6] Source: Enterprise Strategy Group Research Report, *The State of Data Privacy and Compliance*, March 2022.