

ONEWORLD ENCRYPTION PLATFORM

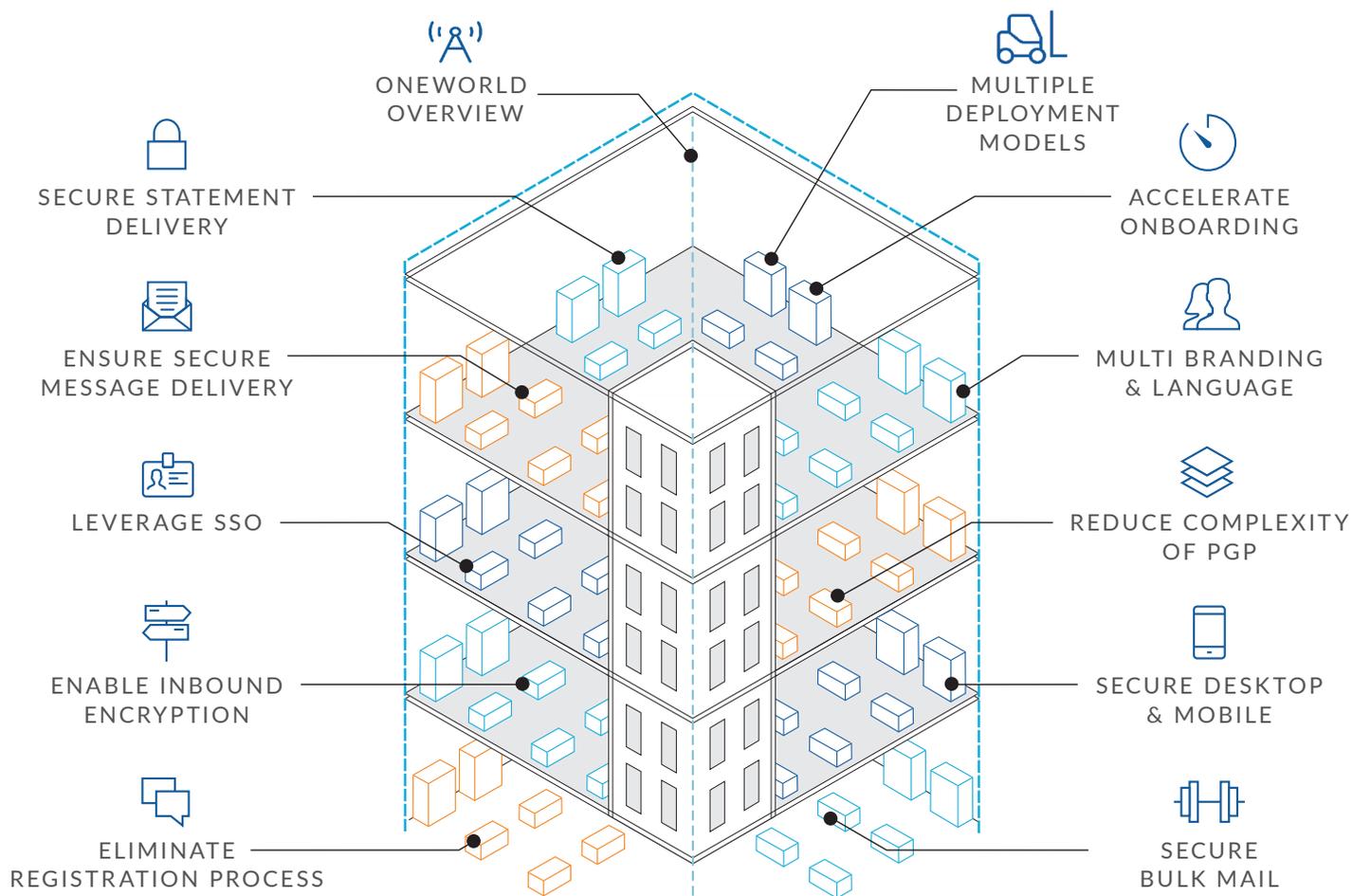
# ENCRYPTION

# USE CASES



# CONTENTS

- The Requirement ..... 3
- Use Case Scenarios
  - Secure Statement Delivery ..... 4
  - Accelerate Customer Onboarding ..... 5
  - B2B & B2C Communications ..... 5
  - Multi Branding & Language ..... 6
  - Leverage Single Sign On ..... 6
  - PGP & S/MIME Migration ..... 7
  - Enable Inbound Encryption ..... 7
  - User Experience ..... 8
  - Eliminate Registration Process ..... 8
  - Secure Personalized Bulk Mail ..... 9
- Modern Encryption Platform ..... 10
- Our Advantage ..... 11
- How OneWorld Works ..... 11



# The Requirement

Each business and industry faces its unique challenges when it comes to protecting the communication of confidential data, whether it's meeting compliance regulations, dealing with changing rules or reducing costs.

Clients are looking for comprehensive security solutions that can also automate or simplify processes.

Encryption solutions need to be flexible to meet each organization's specific requirements, as well as streamline processes and protect information. Echoworx's OneWorld encryption platform provides such a solution.

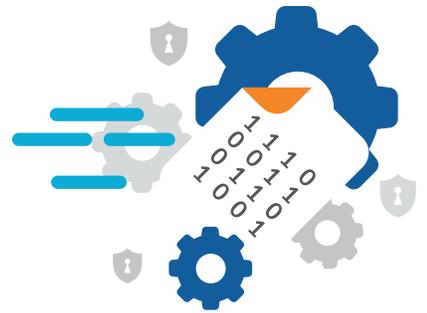


# Use Case **Scenarios**

## **HOW CAN ONEWORLD RAMP UP YOUR ENCRYPTION THROUGHPUT AND SPEED TO MEET YOUR BUSINESS DEMANDS?**

### OPTIMIZE SECURE STATEMENT DELIVERY

A leading US Bank recently asked the same of us. For their global, high net worth customers, sensitive information containing financial statements, financial performance documents, and trade confirmations were pushed directly to their email inboxes. But when these bulk application initiated emails, requiring encryption, hit the server their user initiated sensitive communications came to a grinding halt. Our OneWorld encryption platform employs a very clever and simple method of prioritizing mail volume so that delays are non-existent. By far the problem we hear most is “My existing encryption solution does not scale to my volume demands.” Most encryption solutions operate on a single mail queue with basic First In First Out processing. Our OneWorld encryption platform is deployed as an instance. Messages flow securely into the queue, are encrypted by a OneWorld instance and delivered securely to your recipient at a known rate. If your email volume spikes for whatever reason another instance will be started automatically to handle the increased load. As the load drops, so does your requirement on OneWorld instances, and they are systematically shutdown. This demonstrates how the OneWorld platform can adapt to deal with both user initiated email and application initiative email. Now that’s consistent, scalable performance.

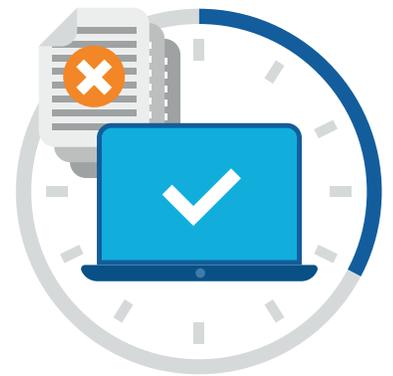


# Use Case **Scenarios**

## HOW CAN ONEWORLD SIGNIFICANTLY REDUCE YOUR ONBOARDING TIME - YET MAINTAIN COMPLIANCE?

### ACCELERATE NEW CUSTOMER ONBOARDING

With client onboarding taking several weeks to a month, its no wonder the move to digital customer onboarding has become a priority. The challenge is to strike the right balance between making the process easy to use and ensuring the security of the documents. With our OneWorld encryption platform all your application forms such as, demand accounts, loans, mortgages, and investment transactions can be emailed using our secure PDF delivery option. Your customers receive a password-protected PDF document directly in their email inbox. Their passwords are created and easily managed through a self-service registration page. Your applications forms are filled out and securely emailed back. In the past, this back-and-forth was done over standard mail or fax. This process is now digital, secured using OneWorld, and completed in a few days versus weeks – drastically reducing your document handling costs and the risks of regulatory non-compliance.



## HOW CAN ONEWORLD ENSURE A WIDE RANGE OF SENSITIVE MESSAGE DELIVERY OPTIONS?

### SECURE B2B AND B2C SENSITIVE COMMUNICATIONS

The world's 4th largest property and casualty insurer asked us that very same question. They were committed to sending sensitive emails containing personally identifiable information (PII) using a single delivery method, TLS. But, what if a TLS connection isn't available? Then what happens? Messages would be sent in the clear or not at all. Our OneWorld encryption platform offers six different encryption delivery methods to accommodate any business scenario you may have. Including Secure PDF, Web Portal, TLS and Encrypted Attachments, as well as support for S/MIME and PGP. All outgoing and incoming emails are processed against encryption rules you create in OneWorld. For example, in addition to simply checking if TLS is available or not, you can more accurately define encryption delivery actions based on domain or attachments. OneWorld ensures that any sensitive email sent, for a wide range of reasons, never goes to a recipient unencrypted.



# Use Case **Scenarios**

## **HOW CAN ONEWORLD PERSONALIZE THE USER EXPERIENCE OF YOUR ENCRYPTED COMMUNICATIONS?**

### ENABLE MULTI BRANDING AND LANGUAGE

Our OneWorld encryption platform uses attributes in the message to dynamically brand all outgoing encrypted messages, including language support. Given today's hyper-connected world, your recipients can be anywhere. We support 21 languages and personalize messages appropriately on a message by message basis. Our branding and language preferences can be applied to accommodate multiple brands at your company, whether that be different business units or different entities you own. Our branding capabilities ensure that your recipients will trust that the secure message originated from your organization and that it is personalized using instructions in their language.



## **HOW CAN ONEWORLD USE YOUR COMPANY'S IDENTITY PROVIDER FOR SINGLE SIGN-ON?**

### LEVERAGE SINGLE SIGN-ON (SSO)

When using the OneWorld encryption platform you can remove the registration process for your customers completely. By leveraging industry standard protocols like SAML and OAuth, we offer full support for Single Sign On. Your messages are encrypted according to policies and sent. Customers simply use their existing user-id and password to login to your corporate site to access the secure emails. OneWorld's support for Single Sign On provides a seamless customer experience while enforcing security policies and driving adoption.



# Use Case **Scenarios**

## **HOW CAN ONEWORLD TRANSFER YOUR PGP EMAIL INFRASTRUCTURE TO THE CLOUD?**

REDUCE THE COMPLEXITY OF PGP & S/MIME

Moving an existing legacy messaging system to a new platform is often compared to changing aircraft engines in flight. With our OneWorld encryption platform, migrating and eliminating an on-premise PGP environment, including bulk key creation and certificate management is accomplished simply and transparently without any additional training or installation of software on any desktop. PGP is simply another delivery channel. Easily upload both private and public keys into the OneWorld LDAP. Lookup certificates in other public LDAP servers. And, create on the fly sender PGP keys for recipients to use for communicating back to your organization – when needed. OneWorld encryption handles all the intricacies of PGP along with access to half a dozen additional encryption methods including, Secure PDF, S/MIME, Web Portal, TLS and Encrypted Attachments. Everything that happens between receiving the message, encrypting it, and delivering it happens automatically in a fully scalable environment.



## **HOW CAN ONEWORLD STOP SENSITIVE CONTENT FILTERING FROM BLOCKING YOUR INCOMING EMAILS?**

ENABLE INBOUND ENCRYPTION FOR PCI COMPLIANCE

If you accept inbound email into your corporate mail server, without applying any encryption, that email is stored in clear-text. PCI requirements mandate that sensitive information, like credit card numbers, must not be saved in clear-text on your network. To maintain compliance, email filtering servers will block or delete these incoming messages. The OneWorld encryption platform leverages its web portal delivery option to ensure incoming emails containing confidential information are encrypted as they arrive. Incoming sensitive messages identified through policy filtering are automatically routed to the OneWorld web portal and encrypted. Employees are notified of incoming messages via email and are provided a link to the web portal, where they can authenticate and view the secure incoming messages.

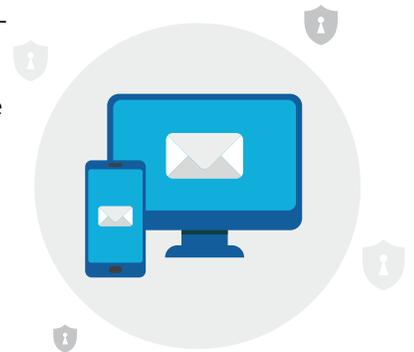


# Use Case **Scenarios**

## **HOW CAN ONEWORLD GIVE USERS REAL CONTROL OVER THEIR ENCRYPTION?**

### OUTLOOK & OFFICE 365 USER EXPERIENCE

With our OneWorld encryption platform each experience can be unique to the user. Why does that matter? There may be instances when your senders must control the encryption – over and above the standard enterprise policies that have been established with your existing DLP. Perhaps they need to send a very large attachment which the recipients corporate email system does not permit. Our platform integrates with a host of solutions including Office365, whether you're working on desktop or the web. Securing a specific message is as simple as pressing an encrypt button within Outlook. The encryption options available to senders match what your company has allowed. In addition to choosing an encryption method, senders can select the expiry period, request recipient notifications, read receipts, and request confirmation notices of encryption. And we offer the same experience in Office 365 Outlook on the web. The same sender encryption options available on the desktop are available with the OneWorld Encrypt Add-in for Office 365 Outlook on the web, including notifications and expiration periods.



## **HOW CAN ONEWORLD SEND SECURE EMAIL WITHOUT REQUIRING A REGISTRATION PROCESS FOR CLIENTS?**

### ELIMINATE THE REGISTRATION PROCESS

You're under tremendous pressure from senior executives and clients complaining about having to create user names and passwords just to read secure emails. Your problem is not unique. Encryption can make communicating securely difficult. The OneWorld encryption platform uses its shared passphrase capabilities to simplify this experience. The process simply requires the exchange of a shared secret phrase between the sender and recipient. Upon emailing, the sender is prompted to enter the shared secret phrase - this can be a word, a name, or even a series of numbers. To open the encrypted email, the recipient simply enters the shared passphrase, eliminating the registration process completely. Our shared passphrase capabilities ensure that no one else can read the message because the password is a secret, shared only with the recipient – enabling a higher level of trust with your customers.



# Use Case **Scenarios**

## **HOW CAN ONEWORLD AUTOMATE THE PROCESS OF SENDING MASS DOCUMENTS SECURELY?**

### SECURE PERSONALIZED BULK MAIL

In today's real-time culture, users want to receive important documents faster than ever. Whether that be account statements, insurance policies, legal documents. But emailing secure documents to a large number of customers comes at a significant cost to you in both time and money. For instance, for compliance reasons maybe your still sending these by standard mail or fax. Or you have moved to email but are using a distribution center to fulfill. The OneWorld Encryption platform helps automate the process of emailing mass documents securely by generating personalized emails and then leveraging a multitude of encryption delivery methods and reporting features, taking the heavy load off you. The process begins as soon as we receive confidential documents from your business application or from staff initiating a bulk job manually. That information, stored on Echoworx secure servers, is processed into fully formed personalized emails, encrypted, and delivered without any manual assistance on your end. Our secure bulk mail capabilities include all the options and benefits of the OneWorld encryption platform such as multiple encryption methods and the flexibility to brand the messages with your own look and feel. And for tracking purposes you receive a full report of which emails could and could not be delivered.



# Modern Encryption Platform



## DESIGNED TO ADAPT TO YOUR ENVIRONMENT

With our OneWorld Enterprise Encryption platform each experience can be unique to the user. OneWorld ensures protection without changing the way your employees, customers, and business partners send and receive emails. The solution enables your IT administrators to easily define and enable email policies to safeguard against information loss. And OneWorld's reporting facilitates regulatory compliance using an intuitive, easy-to-navigate, web-based management console.

## EASY TO DEPLOY. SIMPLE TO MANAGE.

The powerful web-based administration console helps you define rules to ensure encryption is applied by scanning email headers, subject, body, and attachments. If a phrase triggers a policy or rule, the message is automatically encrypted and delivered using the appropriate method whether that be TLS, PGP, S/MIME, Encrypted ZIP, Web Portal or Encrypted PDF.



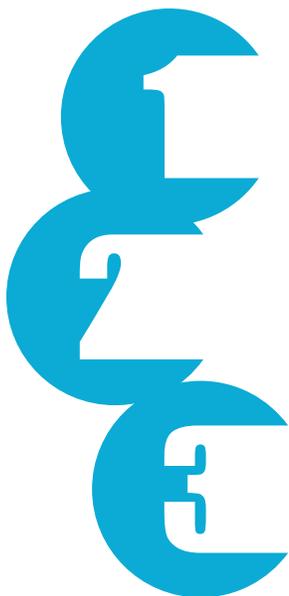
The configurable policy engine accommodates the addition of a wide variety of commonly used rules, dictionaries and expressions. Complex rule chains can be created to suit your organization's unique business needs. In addition to encrypting messages, you can monitor all messages and reject those that do not comply with company policies and procedures. OneWorld analytics track every message that has been processed and provides a snapshot of the system using summary diagrams. Detailed, indexed reports identify important information such as the most flagged policies, top offenders, bounces, open statistics, and messages forwarded or recalled.

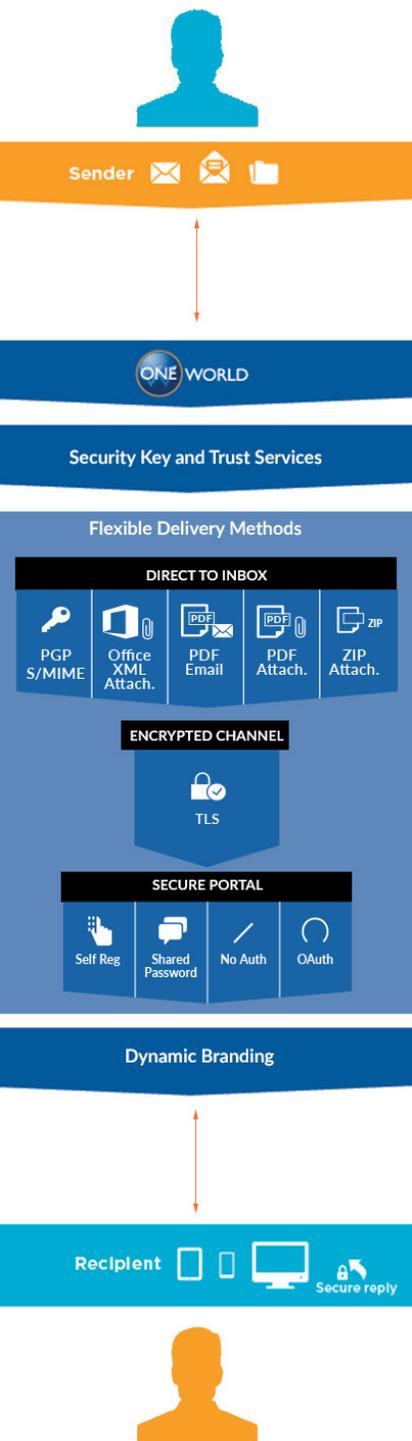
## TOP 3 BENEFITS

Puts control back into the hands of your IT with a turn-on and manage service; using a simple point-n-click interface with no need for hardware or software upgrades.

Applies your company's encryption policies automatically and transparently, protecting your organization against liabilities associated with the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), PCI Compliance, Securities and Exchange Commission (SEC) rules and more.

Hides complexities of encryption from users while providing consistent, scalable performance to ensure your encryption throughput and speed meets your mail volume demands.





# Our Advantage

## DIFFERENTIATING CAPABILITIES

OneWorld Enterprise Encryption is the encryption platform of choice for some of the world's leading brands in banking, insurance, government and healthcare. What makes our solution distinctive is its ability to balance security and compliance with user experience while providing an infinitely scalable and flexible platform that can be leveraged across your organization.

- Cloud, Private Cloud, and On Premise solution
- Supports industry standards based encryption (PKI, x.509, AES 256, PGP, S/MIME technology)
- Policy-based message routing and encryption management, from a simple to use web-based interface
- Push and pull message delivery using five flexible encryption methods: TLS , Encrypted PDF, Encrypted Attachment, Certificate Encryption, Web Portal Encryption
- Content-aware message filters that scan SMTP headers, subject, body, and attachments
- Plain text notifications are branded and trusted so recipients know it is not Spam
- Compliance driven reporting engine with detailed real-time reporting (bounce backs, tracking, device type open, email opened, viewed, forwarded, recalled)
- Bulk key creation and key certificate management (backup, expiry, and rollover)
- Multiple signing modes, providing a seamless experience when using digital signatures for compliance purposes
- Single Sign On (SSO) support for seamless secure email access from your corporate site
- Optimized for smart phones and tablets (iOS, Android, Blackberry)
- Integrates with a host of solutions including Office365, Simple one-click encryption, that auto selects best method encryption, on a per message basis
- Supports multi-business unit branding and 21 languages including Chinese and Japanese

# ECHOWORX

As a pure-play encryption solutions provider, Echoworx works with finance, government, healthcare, legal, and compliance professionals to tailor secure communication solutions that don't impede on customer experience. Our encryption experts take pride in transforming chaos into order for leading multi-national enterprises using our SaaS encryption platform. No matter how large your organization, Echoworx can help you protect your important data by providing you with a path to secure communications. Our scalable encryption platform can address multiple uses across your organization.

## **Encryption is an investment in brand, maximizing competitive advantage.**

Clients in 30 countries use the OneWorld encryption platform and more than 5,000 business, public sector, and institutional deployments are serviced through our data centers in the U.S., Canada, Germany, Ireland, Mexico, and the U.K.

**For more information [www.echoworx.com](http://www.echoworx.com)**

✉ [info@echoworx.com](mailto:info@echoworx.com)  
☎ North America 1 800.735.8916 | UK 44 0.800.024.6657 | Mexico 52 800.681.8080  
🐦 @Echoworx