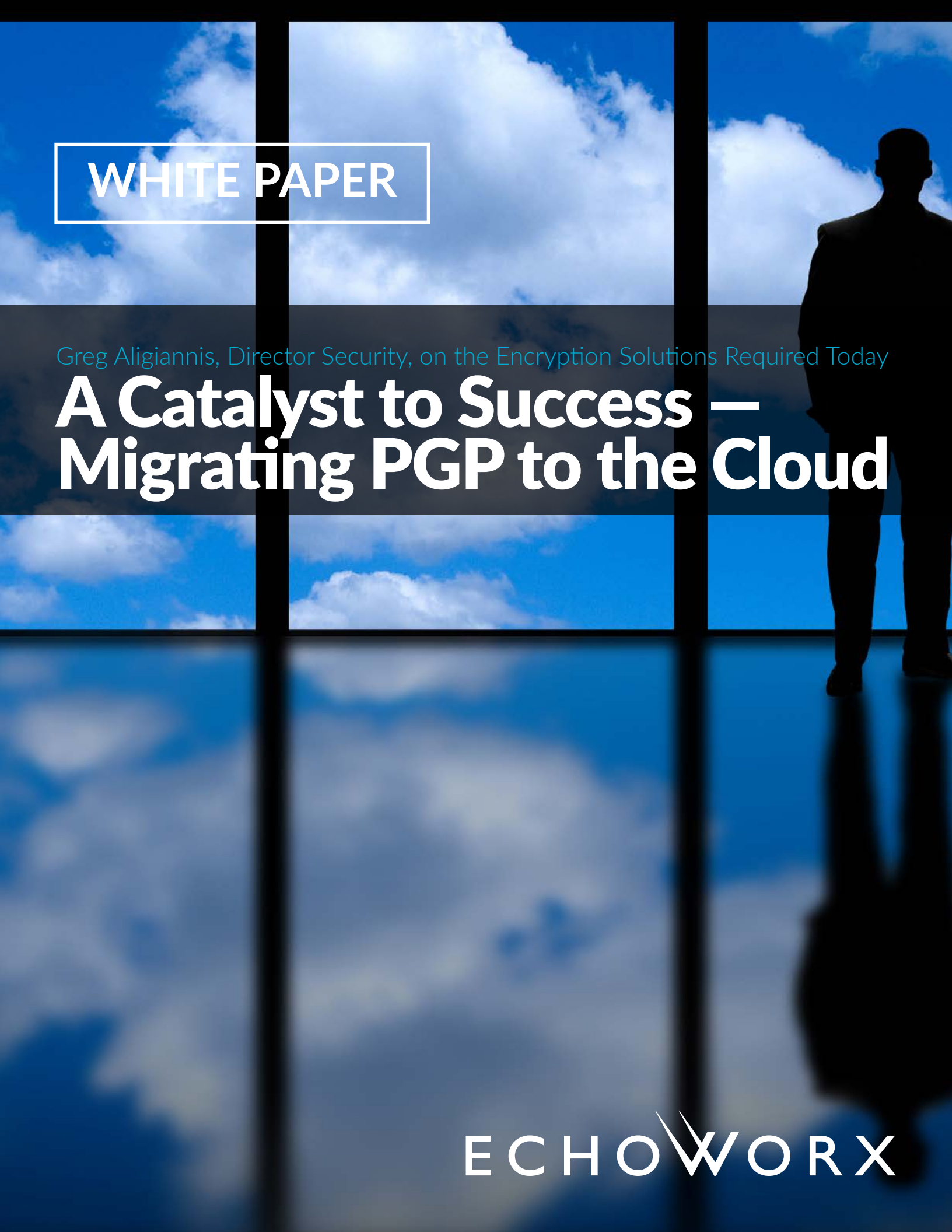


WHITE PAPER

Greg Aligiannis, Director Security, on the Encryption Solutions Required Today

A Catalyst to Success — Migrating PGP to the Cloud

ECHOWORX

A Catalyst to Success - Migrating PGP to the Cloud

CONTENTS

INTRODUCTION

A recurring theme among organizations is that customers and partners want to receive important documents and emails faster than ever before. They want them delivered in a way they can trust and in a way that is easy to access. Greg Aligiannis, Echoworx's Director of Security, discusses what's needed to secure today's digital communications.

The security and technology challenges that banks face today are at an all-time high. Customers are informed and demanding. Communication channels have become wide-ranging. Competition is as tough as ever.

Add onto this list the fact that, 2016 ended as a record year for finance merger and acquisitions (M&A), surging last year to about $18 billion, the highest level since 2009! Following an M&A, organizations find themselves facing a significant post-merger challenge: ensuring the smooth integration of disparate IT systems. Sound familiar?

Companies need to adapt their infrastructure and technology to create additional value for their customers, improve performance, and introduce new innovations if they expect to remain competitive.

Greg Aligiannis is Senior Director of Security at Echoworx and has more than 20 years of experience in IT security. For the past 10 years, he's been helping Echoworx's global partners and large organizations across Canada, US and Europe to implement cutting-edge communication security solutions. Prior to Echoworx, he spent nine years as director of operations for innovative digital healthcare and e-commerce organizations.

In an interview about legacy integration and migrating secure communications to the cloud, Greg discusses:

- How a top challenger bank's security forward focus and modernization directives became their competitive advantage.
- How organizations can easily take PGP to the cloud.

CRITICAL ROLE OF ENCRYPTION

MAGEE: Hi. I'm Lorena Magee, Vice President of Marketing with Echoworx. I'm talking today about Pretty-Good-Privacy (PGP) encryption and its migration to the cloud. It's my pleasure to be speaking with Greg Aligiannis. He's the Senior Director of Security here at Echoworx.

Greg, I thought I'd kick off our discussion with this quote I saw in the New Yorker Magazine about the critical role of encryption.

> "If you're sending email "in the clear," you no longer have to ask if it's being read—we know it is. The question is who's reading it? In this environment, we're not going to preserve our privacy from dragnet surveillance through legislation or wishful thinking. The only guaranteed way forward is through technological solutions, and these can't just be modestly better or easier to use than what we have today.
> They must be spectacular." – *The New Yorker*

ALIGIANNIS: This quote does a fantastic job summarizing the current state of email privacy and what organizations, as a customer, should be demanding from an encryption vendor.

We all know that the days of email messages being sent without needing to worry about the prying eyes of third parties are long gone. In my opinion they never truly existed. Reading email messages in transit has always been technically possible, but the majority of us didn't really give it much consideration. Perhaps we thought it was too difficult to intercept the emails, so the risk of it occurring didn't warrant the cost of implementing systems to protect against it. Suffice it to say, times have changed.

As the quote from the New Yorker reminds us, ***our email is being read***, and can be done so relatively easily from within our organizations, or by third party providers who regularly scan our email for data mining.

It is our responsibility to ensure that the sensitive information we send over email is protected on route to our recipient. It needs to be done in such a way that it is simple and transparent to both the sender and recipient, which subsequently drives user adoption.

Protecting these messages in a manner that doesn't get in the way of business requires a truly spectacular encryption email system.

A SPECTACULAR ENCRYPTION SOLUTION

MAGEE: So, how would you describe a 'spectacular' encryption solution?

ALIGIANNIS: A spectacular email encryption solution must possess these three high level qualities:

It must be easy to implement.

Today's organizations want projects completed quickly so they can take advantage of the solutions and associated cost savings. They are interested in the minimal amount of changes to their internal environments, thereby assuring the least disruptive implementation possible. When all the pieces are working together seamlessly, the solution must be easy to manage and configure to suit their particular requirements.

It must be able to scale dynamically as email volumes increase.

"My existing solution does not scale." I've heard this complaint many times. 'Does not scale' can be due to a technical limitation of their existing product which doesn't lend itself well to several instances running simultaneously. It may also mean, that it is cost prohibitive to add additional resources to accommodate growth, or doing so takes far too much time and effort. So, the solution must scale to accommodate both long and short term growth, ie. Those spikes in volume that may only come a couple of times a month. In essence, the system performance must not degrade as demand increases.

It must be feature rich, standards based and current.

By that I mean, that it must recognize that this is no encryption technologies that suits everyone. It must support all the encryption technologies in widespread use today. And it must do so in a manner that is automatic and transparent to the sender, while catering to the recipients requirements as well. The system must support multiple languages, and lastly and perhaps most importantly, it must be operated securely, by a reputable and trustworthy vendor which dedicates itself to security above all.

MODERNIZE OR FAIL!

MAGEE: Greg, I heard 2016 was a record year for mergers and aquisitions (M&A) in the finance sector. Can these post-merger disparate systems be migrated to a secure cloud based solution?

ALIGIANNIS: Let me give you an example of a recent case study where a large financial institution, who in the process of an M&A, acquired an existing PGP based email encryption system.

They did not want to disrupt existing relationships, which depended on PGP encryption for secure communication, and they didn't want to invest additional resources to build and maintain an enhanced solution which would accommodate the entire organization and its 5 million customers.

They wanted a solution that would accommodate their existing daily encrypted email volume demands and scale up as requirements increased. In addition to making PGP encryption available to the new organization as a whole, it was imperative that the new solution accommodate other popular encryption methods in use today and it had to be able to intelligently decide which encryption method to use to communicate with one recipient over another. And of course, this all had to be done transparently.

They were interested in the most secure solution, with the least amount of hands-on management and ongoing maintenance.

Another important requirement, it must be jurisdictionally aware. For example, it was important that messages originating in the UK were not stored in the US. In essence, the cloud-based solution had to be deployed in many locales allowing them to meet their compliance requirements.

EXECUTIVE SUMMARY

Industry: Financial Services

Background:

- Large financial institution tasked with integrating various PGP systems, acquired through a M&A, into a centralized, cloud based email infrastructure

Challenge:

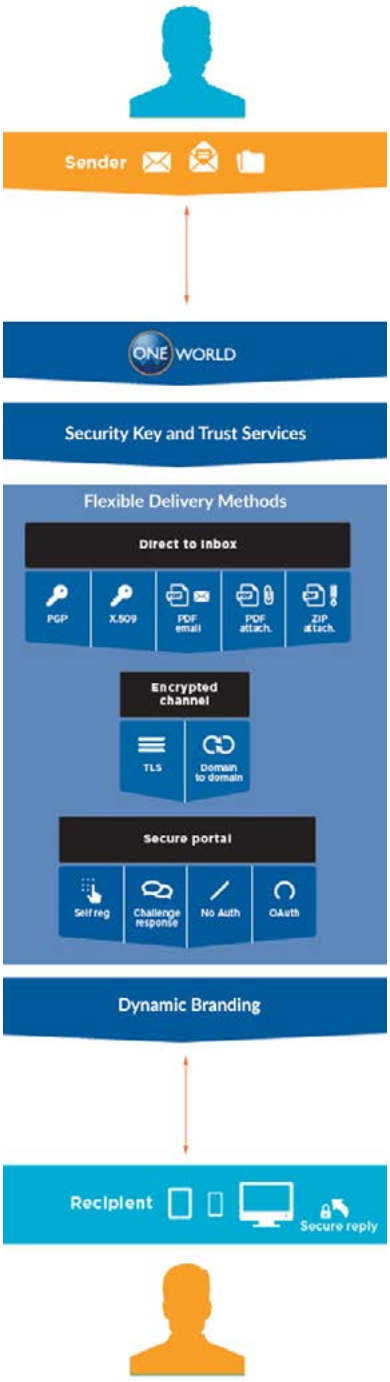
- Eliminate on premise legacy encryption
- Migrate 19th century technology into a 21st century cloud based infrastructure
- Simplify key management, move it entirely to the cloud
- Seamless migration process; transparent to users

Solution: OneWorld Enterprise Encryption

Result:

- Consolidated email encryption into a single infinitely scalable cloud based platform
- Centralized PGP key management system
- Existing PGP users maintain familiar tools
- Zero in-house resources required for encryption (hardware, software, or staff)
- Prioritized email queues
- Support for ALL popular encryption methods in use today: PDF, PGP, S/MIME, Web Portal, TLS, Secure Attachments
- Support for 21 languages out of the box
- Available in 13 geographical jurisdictions

A CUSTOMER STORY



The project, which began as a relatively straight forward request to migrate an on-premise PGP environment to the cloud, quickly grew into a full-featured encryption wish list.

The critical requirement of **migrating and eliminating their on-premise PGP environment** was easily accomplished.

As a result, PGP encryption became available to every user in the organization, simply and transparently without any additional training or installation of software on any desktop. The disruption to their staff and customers was essentially non-existent.

Their **PGP key management were migrated to the cloud** as well. Users who had PGP keys prior to the migration were given the opportunity to upload their key pairs securely to the cloud, or to have the system create and manage a new key pair on their behalf.

Additionally, all the users in the organization were provided with **access to half a dozen additional encryption methods** which we refer to as delivery channels. Including, Secure PDF, S/MIME, Web Portal, TLS and Encrypted Attachments. Using our intelligent encryption platform to automatically determine which channel best suits the recipient of the message.

Moreover, the solution **scales dynamically** to handle planned and unplanned bursts of email throughout the month using an automated method of prioritizing their mail volume so that delays are non- existent.

Recognizing that not everyone speaks English, we added support for 21 languages, making it simple for their global recipient base to understand and use the system. And of course, it is very simple to manage and extend. This was key.

REALITY CHECK

MAGEE: That sounds like a successful and very secure solution Greg. Are there any drawbacks to using PGP encryption?

ALIGIANNIS: The sheer number of PGP keys which are in use means it's imperative that an email encryption solution support it. But, this can be difficult and costly to implement and maintain.

PGP is resource intensive, CPU specifically, and does require dedicated hardware and software be installed and maintained. There are several server components which must be deployed redundantly within an organization and in the case of PGP Desktop for email encryption, every workstation in the organization wishing to use PGP encryption must have the appropriate software installed.

I'm focusing on these issues to simply point out that on premise PGP deployments are not by any stretch a simple endeavor. They require skilled personnel and an ongoing investment in resources.

Many organizations have invested in certificate based encryption systems such as PGP and although they are generally cumbersome to implement and expensive to maintain, they are in use and a great encryption solution should be able to communicate with these types of recipients.

COST

- Requires dedicated hardware and resources to manage and maintain
- Per user license

COMPLEXITY

- Several server components must be deployed
- Software must be installed on every workstation – PGP Desktop
- Key access outside the organization is hit and miss

SECURITY

- No concept of trusted certificate authorities
- PGP works by the "web of trust" concept

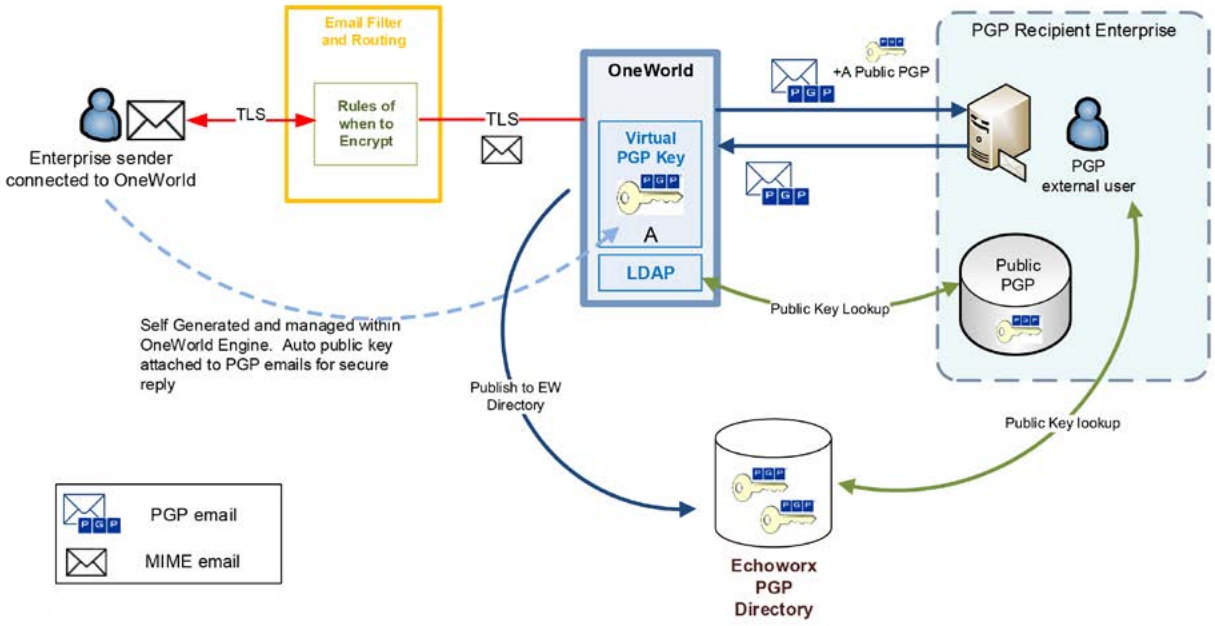
NOT THE ONLY SHOW IN TOWN

- There are other encryption standards in use globally; some recipients do not have PGP at all
- Jurisdictional considerations

FOCUSING ON PGP DELIVERY

MAGEE: How does Echoworx's encryption solution work with PGP encryption?

ALIGIANNIS: I can explain this by walking you through the flow of a message in our OneWorld encryption platform.



The email sender sends a message to their client. It will either be scanned for sensitive content by an existing Data Loss Prevention (DLP) system or the built-in rules engine included with OneWorld. The message sender and recipient are processed against predefined rules, where the best-suited encryption channel is chosen. The message is encrypted and sender-appropriate branding is applied and finally delivered, securely to the recipient, regardless of which device they use to read it.

If the organization you will be communicating with has exposed their universal PGP LDAP to the public, OneWorld will search it for the appropriate certificate, and encrypt for that recipient. Conversely, a virtual PGP key is created for you as the sender for the recipient to use to communicate back to you. OneWorld handles all the PGP intricacies. The sender has no idea it has even occurred.

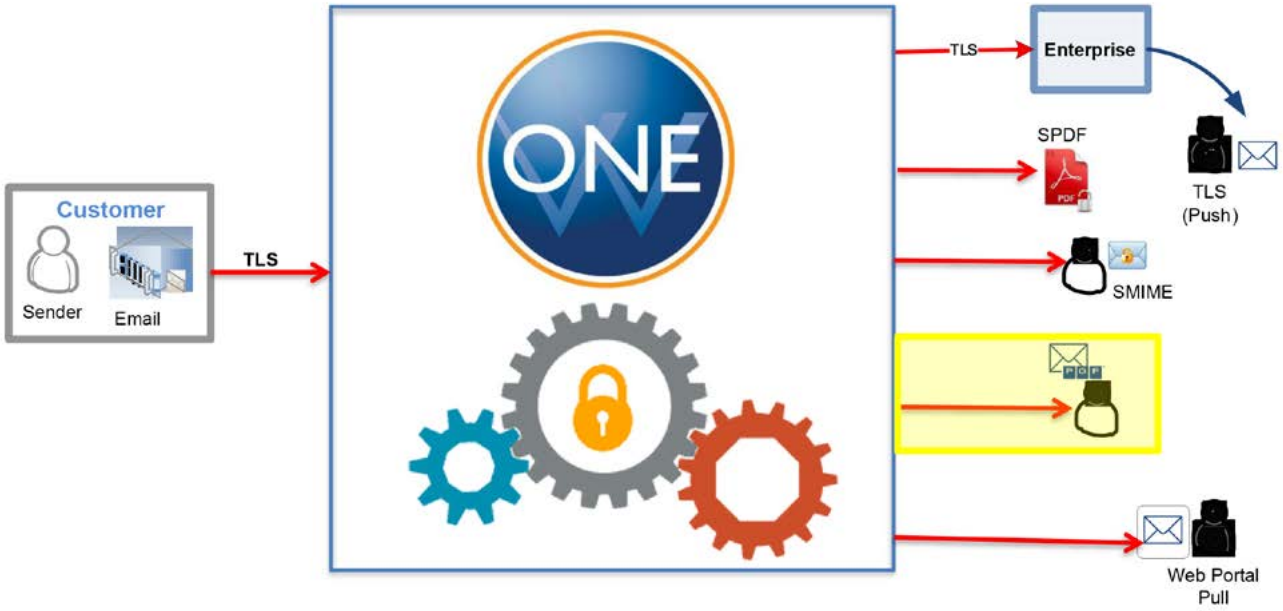
Everything that happens between receiving the message, encrypting it, and delivering it using the best encryption channel happens automatically in a fully scalable environment, designed to increase its capacity as demands increase.

I would like to reiterate that when using OneWorld, PGP is simply another delivery channel option.

SIMPLY ANOTHER DELIVERY OPTION

MAGEE: So in cases where PGP encryption isn't supported or can't be implemented due to whatever reasons, what happens? Is it complex for enterprises?

ALIGIANNIS: The complexity of the service should not be anything you ever need to worry about. Encryption is a complex process but that is something you should never need to worry about.

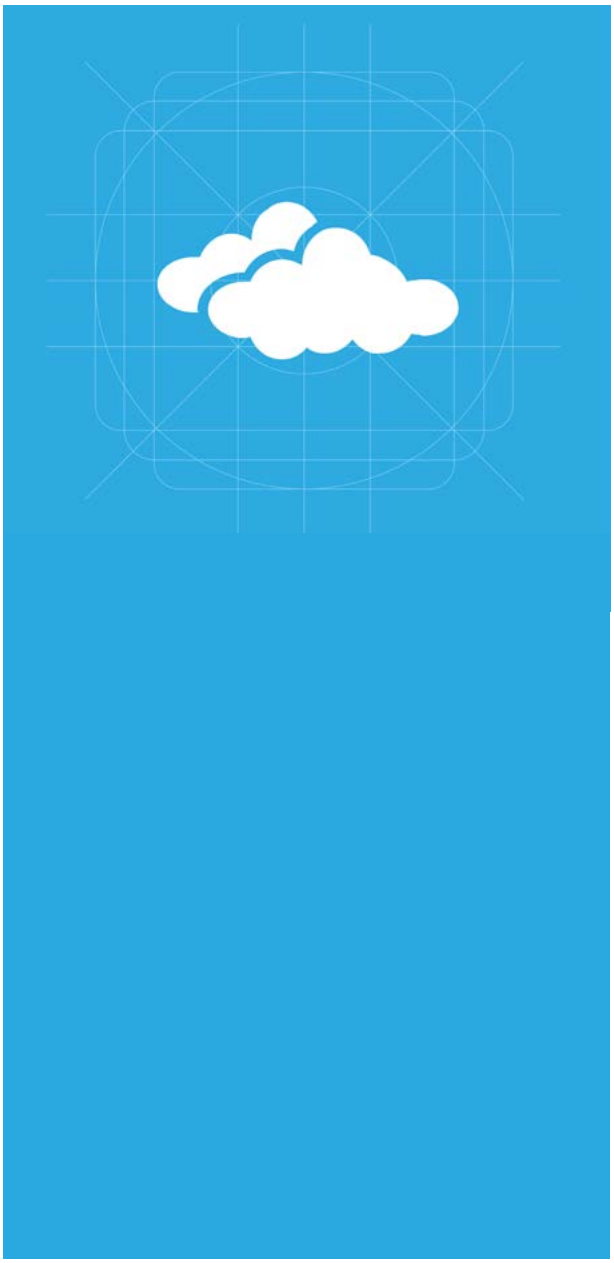


This diagram illustrates a typical email encryption solution. You, the email sender are on the far left. Your email infrastructure may be hosted by Microsoft Office 365 or AWS. You could be operating your own email servers in-house, you may even be running Lotus Notes. It doesn't matter. The important thing is that is you on the left, managing your organization's email infrastructure, worried about data leakage, and email security.

Your concern is being able to securely communicate to your customers, having auditable reporting, ensuring you're compliant with the regulations which are impacting your business. You're responsible for those things and, your email system integrates to it via a simple Transport Layer Security (TLS) connection. The messages you send have been prequalified for encryption based on the policies you have defined. Ultimately, being encrypted using the appropriate encryption channel such as: TLS, Secure PDF, S/MIME, PGP, or Web Portal. Like I mentioned before, when using OneWorld, PGP is simply another delivery channel option.

ENCRYPTION AS A SERVICE

MAGEE: Can organizations use just on premise PGP encryption?



ALIGIANNIS: They can, but they shouldn't. When considering PGP on premise as the only application, it is important to realize that the technology on its own can be quite limiting as an email encryption solution. It does not take into consideration that there are other encryption standards in use. Many recipients are not enabled to use PGP at all.

An increasingly important consideration when evaluating an email encryption platform these days is its ability to accommodate jurisdictional requirements. This is extremely tough to accomplis with an on premise implementation of PGP as it requires having instances running within several geographic regions to ensure compliance.

Organizations with multiple physical offices must look at on premise email encryption the same way they do their internal email servers. In most cases, multiple instances of encryption technology must be deployed alongside existing email servers in multiple locations.

However, the complexities of managing internal environments are alleviated by a secure cloud-based solution. In the case study example we decommissioned their in-house PGP servers and complex desktop software, and replaced it with a single solution, OneWorld.

They simply deliver the messages they want encrypted over a secure TLS channel to OneWorld, and the rest happens automatically. As far as their users are concerned PGP no longer exists. It does, we've just made it a whole lot easier and much more effective.

HOW ECHOWORX CAN HELP

MAGEE: That's a great overview Greg. As a final question, can you tell me more about Echoworx. What is your organization doing to help other organizations secure their email communications?

ALIGIANNIS: Echoworx is an industry leading encryption vendor with roots in PKI. We are a long standing trusted certificate authority. I mention this because it's important to point out that security is all we do.

Our solution, OneWorld Enterprise Encryption, leverages the highly scalable Echoworx Security Cloud Services platform, with several deployment models to suit most customer implementation requirements. It is offered as fully managed cloud, on premises or hybrid deployments, and supports virtualization technology making it easy to scale.

OneWorld is generally deployed in what I will refer to as an instance. Each instance can process about 10,000 messages per hour on today's commodity hardware. That metric is always increasing. For the sake of discussion, let's just say it's 10,000 messages per hour per instance. If your email volume spikes for whatever reason, and exceeds 80% utilization of a single OneWorld instance, another will be started automatically to handle the increased load. Inbound messages are balanced across OneWorld instances, encrypted, and securely delivered. As the load drops, so does your requirement on OneWorld instances, and they are systematically shutdown.

Now that's efficient. No need to buy additional hardware. No hardware sitting idle, not being used.

We also offer a fully managed cloud based SaaS service and fully managed SaaS service inside your private cloud. The latter two options leave the management of the system to encryption engineers. The service is redundant by design, and easily deployable as a fully managed SaaS service in 13 countries to accommodate your jurisdictional requirements.

21 languages are supported out of the box. New languages are being added all the time with consistent branding across all the channels. The branding capabilities ensure that the recipients understand that the message originated from the sending organization and contains secure information, with instructions in their language. OneWorld can handle multiple brands at a company, allowing for the centralized management of a single solution that can be deployed across different business units.

It bears repeating, complexity of encryption shouldn't matter to the user!

ABOUT US

Since 2000, Echoworx has been bringing simplicity and flexibility to encryption. Headquartered in North America with offices in the US and UK, our certified, redundant and replicated data centres are located in the US, UK, and Canada. Our passionate encryption experts transform chaos into order for world leading enterprises and OEM providers who understand the requirement for secure communication is of the upmost importance. We are proud to have clients in 30 countries worldwide, with more than 5,000 enterprise-level deployments.

Encryption is an investment in brand, maximizing competitive advantage.

Echoworx's flagship solution, OneWorld Enterprise Encryption, provides an adaptive, fully flexible approach to encryption that ensures the privacy of sensitive messages. Enterprises investing in Echoworx's OneWorld platform, are gaining an adaptive, fully flexible approach to encryption, creating seamless customer experiences and in turn earning their loyalty and trust.

For more information www.echoworx.com

info@echoworx.com
North America 1 800.346.4193 | UK 44 0.800.368.5334 | Mexico 52 800.123.9553
@Echoworx