clearswift

A HelpSystems Company

Best Practice Guide

Email Encryption and Secure File Transfer

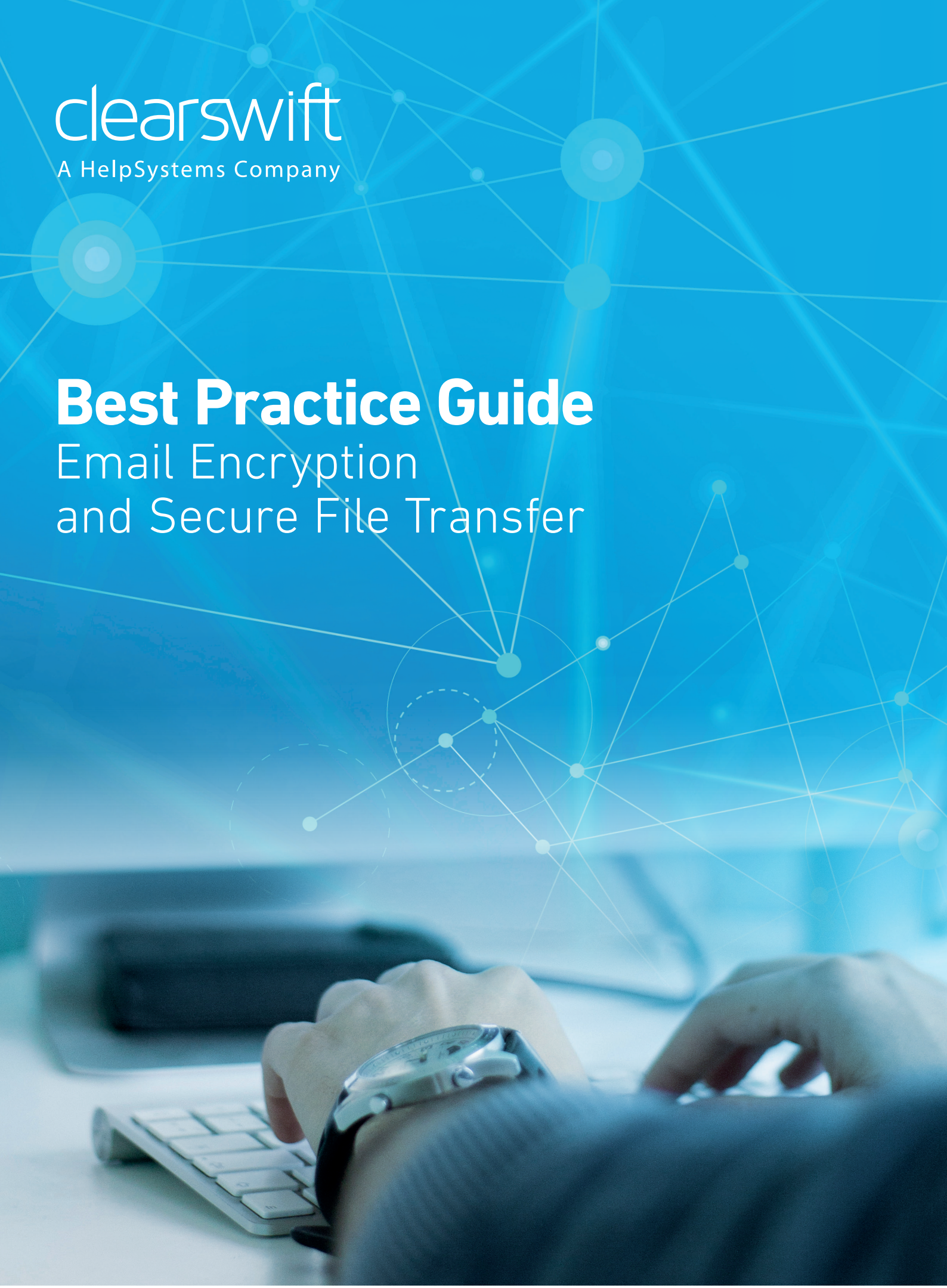


Table of Contents

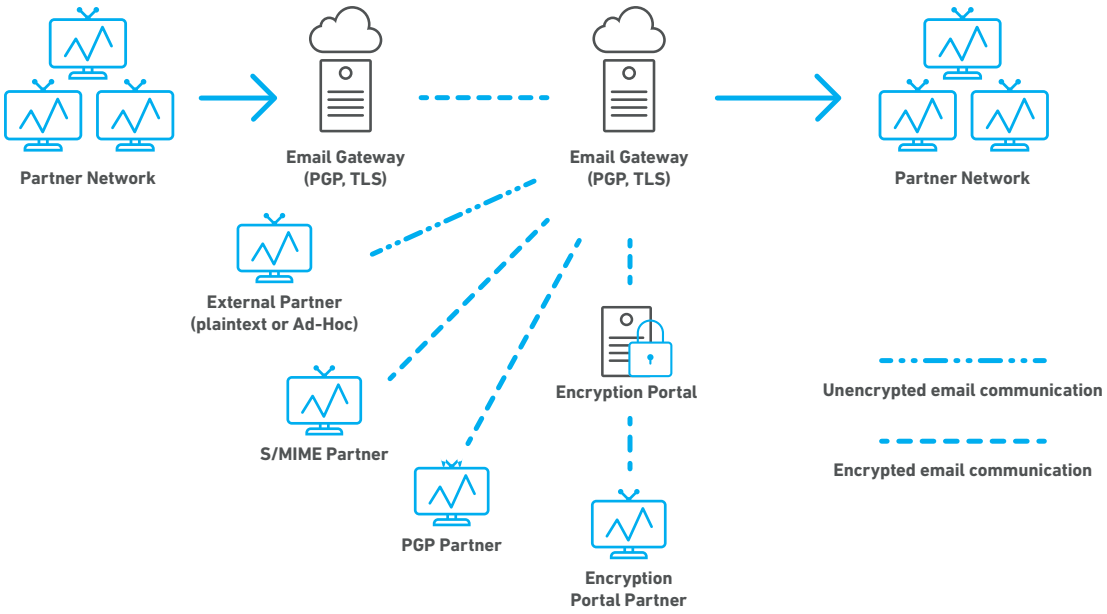
Introduction

Email continues to be the lifeblood of organizations today. With changes to legislation and the increased attention on data breaches now is the time to revisit your email solution and policies to improve the security of the information that flows through it – both inbound and outbound.

While it has been commonplace to have anti-virus scanning and anti-spam on the incoming email stream for many years, organizations are now improving security around outbound email, through the increased use of encryption and deployment of data loss prevention (DLP) solutions. The reason for this is two-fold; the first is understanding the benefits and differences of the myriad of options available. The second is around the cost and ease of use for the solutions. In the past, both encryption and DLP solutions have been notoriously difficult to configure and maintain, making them only options for larger organizations with specialist IT skills.

Today's solutions to make email secure have become increasingly sophisticated but hide the complexity and the management costs, see Figure 1. And yet, there is no silver bullet. Choices have to be made. The real answer is that different solutions are needed at different times and the decision as to which is needed needs to be made automatically - based on the recipient and the information being communicated.

Figure 1: Secure email options



Encryption

Let us start with encryption. Encryption is used to ensure that the contents of an email are not intercepted and read, particularly when it travels outside the organization. Therefore, the ideal place for encryption to occur is on the egress point, as the email enters or leaves the organization. Today's email gateways which protect against inbound threats can also provide automatic encryption of outbound email. There are several different encryption options available, see Table 1 and further explanation on the different types is given below.

	Encrypted Site-to-Site	Encrypted Site-to-Recipient	Encrypted Desktop-to-Desktop	Standards Based	Crypto Strength	Key Exchange or Password	Recipient Transparency
TLS	Yes	No	No	Yes	Medium	No	Yes
S/MIME, PGP	Yes	Yes	Yes	Yes	High	Yes	Site to Site - Yes Encrypted to Recipient may require key and client plugin
Password (Windows)	No	Yes	No	Yes	Medium	Yes	Yes
Password (AES)	No	Yes	No	Yes	High	Yes	Requires Zip package that supports AES256
Portal	No	Yes	No	Yes	High	No	May require plugin for "push" messages

Transport Layer Security (TLS)

For users who simply require encryption on messages between themselves and other organizations, a TLS capability can be used. TLS connections can be 'opportunistic', allowing encrypted messages sent in this mode to automatically seek out and favour a connection using TLS. Alternatively, connections between organizations can be mandated and have pre-specified encryption strengths and ensure that messages are only sent if the appropriate level of security is achieved during the handshake.

Message Encryption (S/MIME, PGP and Password Protected Zips)

Good encryption solutions support international standards for OpenPGP and S/MIME message formats, enabling communications between recipients who use standard email clients.

Sophisticated email gateways can also use S/MIME and OpenPGP to create policy based secure connections between Gateways or from Gateways to Recipients. With integrated encryption, email gateways can decrypt messages and then use the other tools such as anti-spam, anti-virus, and content filtering engines to ensure that communications adhere fully to corporate email policy.

Ad-Hoc Encryption

For recipients who use neither PGP nor S/MIME, the new generation of email gateways can still send messages in a secure format using password protected zips, aka ad-hoc encryption. Even here there are options on whether to use Windows compatible or AES encrypted zip formats.

Windows compatible zip formats can be opened without the need for any additional software. However, for organizations requiring stronger encryption algorithms, for example AES256, there is a need for the recipients to have one of the many Zip clients capable of processing this format.

This can also be achieved using protected PDF files to deliver a sensitive message or attachment. This format is popular for secure statement or document delivery.

Passwords created during the ad-hoc encryption process can be dynamically created for individual users or message-specific. In many cases it is then the responsibility of the sender to inform the recipient of the password, but some systems enable a delayed email to be sent automatically to the recipient.

Web Portal Based Encryption (Pull)

The technological savvy of your intended recipient can often dictate which method of encryption you use, and portal-based encryption is an easy-to-use method needing no knowledge of encryption. Encrypted email messages are sent using an encryption portal which can then be opened on all types of devices, from PCs to phones and tablets using a web browser. When this method is invoked the user receives an email to say that they have received an encrypted message through the portal.

Portal based encryption can be done 'off-premise', i.e. through a service provider, or it can be provided 'on-premise', where the system can be completely under the organizations control.

Data Loss Prevention (DLP)

For some information, even email encryption is not sufficient – this information needs to be kept within the organization at all times. For this, data loss prevention technologies need to be used to watch for restricted information crossing the egress points and automatically blocking it. A DLP solution enables an organization to inspect the content of an email and its attachments looking for specific information and then carrying out an action on the email should the information be found.

One simple use-case is to block any email leaving the organization which contains profanity, while other more sophisticated policies may look for credit card or bank information and prevent that from leaving the organization. As with email encryption solutions, the simplest place to implement DLP is at the egress point, on the email gateway. By putting the solution on the gateway, rather than every computer, all devices which are connected to the corporate network are protected.

Web Based Email

For many organizations, when it comes to information security, there is now a need to consider web-based email as well as corporate email. Most organizations now require that employees use their work email for work, and work alone – the result is that employees often have a personal email address for use with friends and for other social reasons. However, the rise of personal email has also resulted in a rise in corporate information risk, with employees sending critical information to their home email accounts (more often than not so they can work on the document at home). When looking at securing corporate information, this communication channel needs to be considered.

A gateway solution which intercepts all web-based traffic (as well as traditional corporate email) is an excellent way of ensuring that corporate information remains inside the corporation. The same DLP policies which are used for corporate email can also be used for web-based email (and for other web-based activities, such as social networking). Having consistent information security policies and technology to enforce them, makes it easier for the IT department and the CIO or CISO who is ultimately responsible for corporate information to define common policies and view any violations.

Secure File Transfer

When it comes to very large files, typically those over 1GB, email is not an option for effective transfer and alternatives need to be sorted. While this size issue has not been an issue for most organisations, the advent of video and rich media means that it is increasingly becoming an issue. Several mechanisms can be used to transfer the file with FTP (File Transfer Protocol) probably the most common as it is easy to use. FTP transfers the file from source to destination – but without any forms of security check. Whereas information sent through email can be scanned for viruses and other malware inbound and have data loss policies applied when outbound - this does not occur with standard FTP. Enter the secure file gateway which enables secure file transfer. This inserts the policies and technology used in email to protect the content into file transfer mechanisms such as FTP. The processing can be completely transparent, automated by the file gateway with the user being unaware of the content inspection being carried out.

Secure file gateways have been used for several years within the defence sector, where information needs to be transferred from one network with one security clearance to another with a different clearance level. However, they are now being increasingly used in the commercial sector, enabling secure transfer of files between partners and increasingly inside organisations which want to segregate information internally. Guaranteeing that only information which complies with policy is shared with other parts of the organization.

Summary

Email continues to be a critical business tool for organizations big and small. Almost all an organizations intellectual property and company confidential information will travel through email at some point in its lifecycle. This coupled with increased needs for collaboration, imposed legislation and cyber-attacks on corporate information means that organizations need to revisit their email security polices and solutions to protect their critical information. An increased emphasis on Information Governance, the understanding and protection of information, especially that which flows in and out of an organization, is driving all organizations regardless of size to look at technologies for securing email.

In the past secure email technology needed specialist skills to administer, but today even the smallest of organizations can readily encrypt their email and apply DLP policies without increasing management costs. The same security policies which are applied to corporate email can also be applied to web-based email by using combined web and email gateways, giving organizations the assurance, they need that their information is secured no matter which communication channel is used.

Furthermore, the increasing use of web-based collaboration tools and very large files means that organizations need to look at secure file transfer technologies to enable the same policies that are applied to email to also be applied to files as they are moved between organizations or even departments.

clearswift

A HelpSystems Company

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have 100% visibility of their critical information 100% of the time.

For more information, please visit **www.clearswift.com.**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
AUSTRALIA