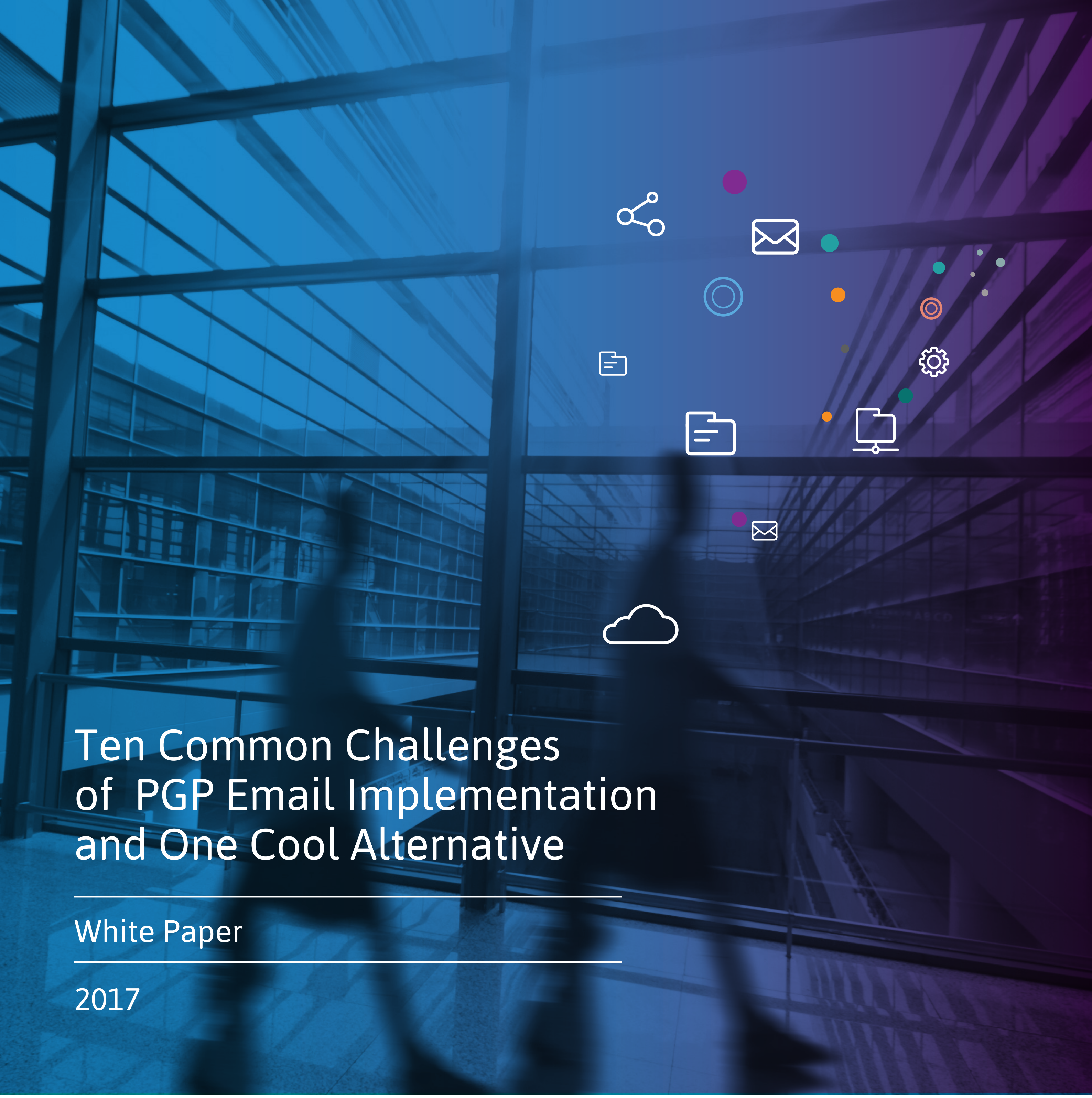

Ten Common Challenges of PGP Email Implementation and One Cool Alternative

White Paper

2017

SAFE-T

Keeping Data in the Right Hands

The benefits of PGP based email encryption have been well documented since the introduction of PGP in the early 90s. PGP enables organizations to encrypt email messages and to share sensitive information securely while achieving regulatory compliance. However, PGP implementations raise significant challenges to organizations, especially ones with complicated maintenance, limited functionality and high total costs of ownership.

This document reveals some of the challenges of PGP implementations while offering a unique and innovative alternative to PGP, known as Safe-T secure email solution. Safe-T's approach is fundamentally different from PGP encrypted emails, yet enables organizations to achieve compliance and to share their sensitive information in a secure and simple way.

PGP Email Encryption Challenges

Challenge #1

Complicated, cumbersome maintenance

PGP keys require high maintenance, as each key has an expiration date after which it won't be useful for encryption and decryption of emails. Even if the organization can update the private key with a new expiration date, every public instance of that key is not updated. This results in keys that are not useful for email encryption. Moreover, in a case of a disaster and loss of a key, all the data that was encrypted with that key is lost forever. To maintain enterprise grade keys management, the organization is required to deploy a keys backup system and to spend its IT staffs' valuable time well as its financial resources.

Challenge #2

PGP encrypted emails have limited size

The size of a PGP based encrypted email message is limited by the maximum size that is allowed by the enterprise email gateway or the centralized PGP server. In most cases, email messages with file attachments that are larger than 10MB may double in size to 20MB after PGP encryption, exceeding the maximum allowed message size. This means that organizations cannot share large files using PGP emails in a secure way.

Challenge #3

No support for ad-hoc PGP encrypted emails

Since the recipient of PGP encrypted email message must use a key for decrypting the message, the sender must retrieve first the public key of the recipient and to use this key for encryption. However, if the recipient is not using PGP and does not have a public key, the message cannot be sent in an encrypted method. This means that enterprises can share emails securely only with other organizations that use PGP.

Challenge #4

An email message can only be decrypted by the end user

Since the PGP key is owned by the end user, the email message must arrive first to the desktop of the user before it is decrypted. This creates a significant security blind spot for the enterprise as no centralized data scanner tool such as anti-virus can scan the email message and the attachment before it arrives to the user's desktop. To overcome this threat, organizations are required to deploy a decryption gateway server, which results in an additional costs and IT staff efforts.

Challenge #5

Lack of tracking information

The sender of a PGP based encrypted email does not receive any information from the recipient that the email was successfully delivered and decrypted.

Challenge #6

Email and attachments reside unencrypted in the DMZ

Enterprises that choose to deploy a centralized decryption gateway server often deploy the server at the DMZ. There, the decryption gateway server decrypts the emails and the attachments before it sends them to a data scanner tool. This creates an opportunity for attackers to gain access to sensitive data that is stored insecurely in the DMZ and is a significant blind spot in the organization’s data security.

Challenge #7

PGP emails cannot be integrated into a secure business workflow

Regardless of whether the PGP deployment is utilizing a centralized decryption gateway server, it cannot be integrated into a secure business workflow that makes use of additional tools such as DLP that can process/manipulate the emails and their attachments before sending them out of the organization.

Challenge #8

Cannot set an expiry date or limit the downloads of a message

Once the PGP encrypted email is sent, the message is forever available to the recipient. The sender cannot set an expiration date for the message and its attachments, limit the number of email views and limit the number of attachments downloads. This means that an organization’s sensitive data can be viewed insecurely by additional recipients and in an uncontrolled manner.

Challenge #9

PGP clients are complicated to maintain

In most PGP based email implementations, the enterprise chooses to install a client for each one of its email users. This result in the need to manage, support and maintain those clients, which implies additional costs and work effort to the IT staff. Alternatively, the enterprise can deploy a centralized gateway server, which again results in an additional costs and IT staff efforts.

Challenge #10

High total cost of ownership

The fully burdened costs of PGP based encrypted emails are high and include the cost of dedicated hardware, real estate, software licensing, service, support and user training.

Safe-T Secure Mail Alternative

Safe-T's Secure File and Email Access is an innovative yet simple solution that does not require keys exchange or complicated maintenance and leaves the organization with full control of their sensitive data.

Secure Email Access

How it Works

- Once sent, the encrypted email and the attachments are stored in the virtual safe of the sending organization
- The recipient receives an email that contains only a link to the stored email at the sender's organization, plus a one-time password, in case the recipient is a non-registered user. In case of a registered user, they use their username and password to login.
- Using the one-time password or username and password combination, the recipient can access the encrypted email and the attachments

Features & Benefits

- Downloads and setting an expiry date for the email
- Any file size and type can be sent using Safe-T secure email without overloading the email servers
- Since there is no exchange of keys, an ad-hoc email can be sent to anyone and an encrypted reply can be received from anyone
- The encrypted email can be scanned using DLP tools by the sending organization
- Safe-T secure email can be easily integrated into any business workflow to ensure sensitive information is kept secured
- Simple, intuitive access to emails from any device including mobile, tablet, web portal Miscosoft Outlook, Outlook Web Access (OWA), and Gmail.
- Flexible deployment options of centralized gateway and / or Outlook add-on
- Complete file-level audit trail information that tracks the movements of each email
- Enables organizations to achieve compliance with industry or governmental regulations such as SOX, GLBA, PCI, HIPAA, FDA, GDPR, and more.

Comparison Table

Capability	PGP based email encryption	Secure Email Access
File size limitation	Yes	No
Requires keys exchange	Yes	No
Ad hoc emails	No	Yes
Key management and maintenance	Complicated: • Keys have an expiry date • Lost key might result in all data lost • Requires keys backup	No keys management
Email can be decrypted by gateway and scan for malware	No, unless decryption gateway server is deployed	Yes
Move attachments to virtual safe	No	Yes
Limit number of email and attachments downloads	No	Yes
Set expiry date for the message	No	Yes
Can be part of a secure business workflow	No	Yes
Tracking information	No	Yes
Files reside in DMZ unencrypted	Yes	No
Enables achievement of regulations such as SOX, GLBA, PCI, HIPAA, FDA, GDPR and more	Yes	Yes
Client installation	Yes, in the majority of cases (optional centralized deployment is not common)	No (Optional centralized deployment Or Microsoft Outlook, Outlook Web Access, Chrome add-on)
TCO	High	Low

Summary

PGP based email encryption has been around for many years and while it enables organizations to share emails securely it also creates significant challenges.

Organizations should be aware that there are alternatives for the cumbersome PGP maintenance and usability, so they can offer their end users a more secure way to share sensitive information simply and without limitations.

If you'd like to hear more from us regarding a PGP alternative to securing your email

please contact us: http://www.safe-t.com/contact/

To learn more, please visit: https://www.safe-t.com/secure-file-and-email-access/