BlueFinch

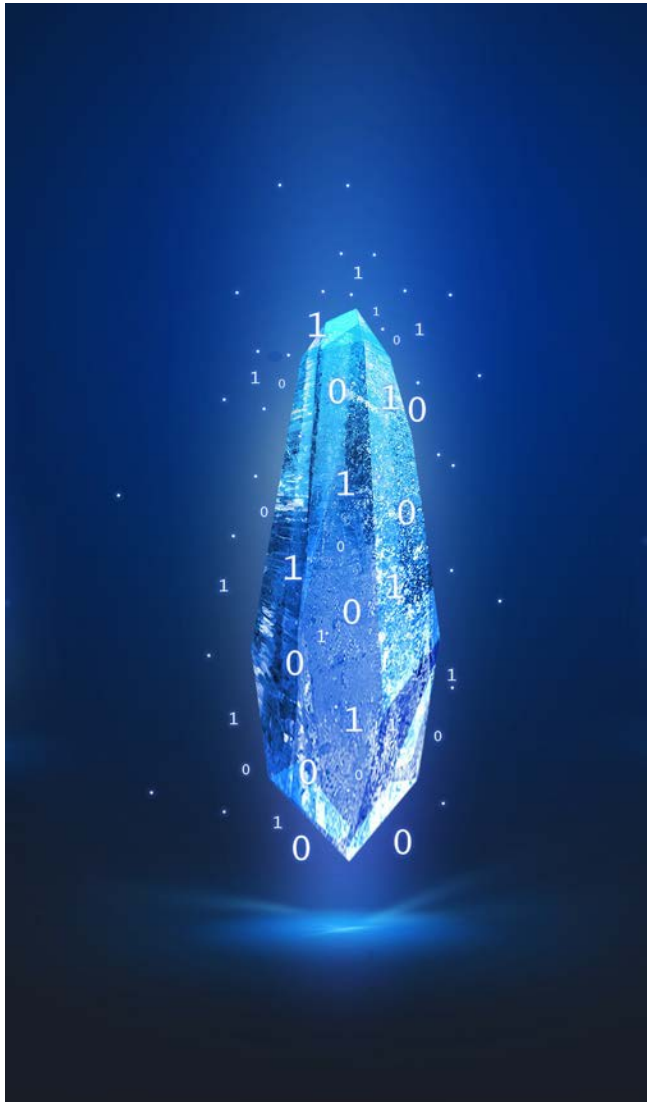
goanywhere
by HelpSystems

Why Automating Encryption and Decryption Makes Good Cybersecurity Sense

INTRODUCTION

Defense.

That's the tactic organizations and their IT teams need to take against cybersecurity threats. Taking defensive, proactive steps, long before a data breach or misuse of your sensitive data, helps shield against potential incidents that can wreak havoc with budgets, reputations, and resources. One such move is the implementation of encryption and decryption of data.



What is Encryption and How Does it Work?

What it is:

Encryption is a method of encoding data (messages or files) so that it is unusable or unreadable until it is decrypted. With encryption in place, only authorized parties with keys can read or access that data. **Encryption** uses complex algorithms, or set of rules, to scramble the data being sent. Once received, the data can be decrypted using the key provided by the message originator.

The effectiveness of any given encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected.

Because encryption renders information unreadable to an unauthorized party, the information remains private and confidential, whether being transmitted or stored on a system. Unauthorized parties will see nothing but an unorganized assembly of bytes. Furthermore, encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering. The ability of the technology to protect the information requires that the encryption and decryption keys be properly managed by authorized parties.

How it works:

Not every message or piece of data is for everyone's eyes. That's the basic premise of why organizations need encryption. But how does it work? Do you need different types of encryption for different situations? Can encryption be integrated with your existing business technology? Let's take a look.

HOW IT WORKS:

Unlocking Encryption Keys: Symmetric vs Asymmetric Systems

There are two types of cryptographic key systems essential to encryption technology, symmetric and asymmetric.

- **Symmetric key system:** This is also known as a secret key system. With this system, all parties have the same key. The keys can be used to encrypt and decrypt messages and must be kept secret or the security is compromised.

  For the parties to get the same key, there must be a way to securely distribute the keys. While this can be done, the security controls needed can make this system impractical for widespread and commercial use on an open network like the Internet.

- **Asymmetric key system:** This system, also known as a public/private key system, solves the problem of distributing the keys used in the symmetric key system. Two keys are used in this system. One key is kept secret, or "private," while the other key is made widely available to anyone that needs it and is referred to as the "public key."

  The private and public keys are mathematically related so that information encrypted with the public key can only be decrypted by the corresponding private key.

ENCRYPTION TERMS TO KNOW

AES:
Short for Advanced Encryption Standard. It is a popular encryption standard that is approved by the NIST.

Algorithm:
Also known as ciphers, algorithms are the rules or specific instructions for the encryption process. Triple DES, RSA, and AES are examples of algorithms, or ciphers.

Ciphertext:
The result of encryption performed on plaintext using an algorithm, known as a cipher.

Decryption:
The process of converting unreadable cipher text to readable information.

Email Encryption:
Email encryption can secure email online via a number of options using encryption. These include TLS, password, push/pull, S/MIME, and PGP encryption.

Encryption:
The science of protecting information by transforming it into a secure format.

Key:
A randomized strong of bits used to encrypt and/or decrypt data. Each key is unique, and longer keys are harder to break. Common key lengths are 128 and 256 bits for private keys and 2048 bits for public keys.

PGP:
Short for Pretty Good Privacy. PGP is an encryption program that provides cryptographic privacy and authentication for data communication.

WHY DOES ENCRYPTION MATTER?

Encryption matters because cybersecurity threats exist and are continually growing in number. In addition, inadvertent data leaks from internal staff are also responsible for nearly half of all data loss incidents. Also, many industries such as banking, healthcare and more, require encryption to ensure compliance requirements are met.

Locking data down and away from both deliberate, malicious threats, as well as from accidental mishandling, is your best protection from the huge financial toll a data breach can have on your organization, along with loss of reputation and trust from trading partners and more.

Data needs to be safely encrypted both while it is in transfer or transit to an intended recipient and while it is at rest, such as while stored on a server. Doing so is one of the most important practices in your cybersecurity arsenal, and for good reason: it's your last line of defense.

If you haven't done so yet, consider building an IT cybersecurity strategy that includes file encryption; it's time. Some IT teams use free OpenPGP tools to achieve file security. Others opt for a centralized managed file transfer solution, like GoAnywhere MFT, to protect their data with more features and benefits surrounding the process.

Your unique business needs can help determine which method is best for your file transfer and security needs.

HOW TO CHOOSE THE RIGHT ENCRYPTION METHOD FOR YOUR ORGANIZATION

Several factors must be considered when choosing which encryption standards to implement at your organization. Before choosing an encryption standard to use, ask the following questions:

- How sensitive is the data being exchanged?
- How will the data be transmitted (FTP, email, HTTP, etc.)?
- Are large files, which should be compressed, being exchanged?
- Should the actual files be encrypted (before transmission) or should the connection itself be encrypted?
- What encryption standards do your trading partners support?

A trading partner may ultimately dictate the encryption standards which they support. For instance, many banking institutions require that customers encrypt files using the **OpenPGP** encryption standard.

A WIDE VARIETY OF ENCRYPTION NEEDS ARE EASILY MET BY MFT SOLUTIONS

Scenario #1: Low sensitivity, password protection needed
You need to send your price list file to your customers over email. You want it to be easy to for these customers to open the file. While this price list information is not extremely sensitive, you would like to at least password-protect it.

Recommendation:
ZIP with AES encryption

Scenario #2: Highly sensitive banking information, FTP connection
You need to send your company's payroll direct-deposit information to the bank. This is considered highly sensitive information. Your bank wants you to send this information over a standard FTP connection.

Recommendation:
OpenPGP

Scenario #3: Authentication with password or public key, FTP connection
Your trading partner wants to exchange information with you over a secure FTP connection. This trading partner also wants to authenticate your company with a password or public key.

Recommendation:
SFTP (SSH File Transfer Protocol)

Scenario #4: Authentication with signed certificate, FTP connection
Your trading partner wants to exchange information with you over a secure FTP connection. This trading partner also wants to authenticate your company with a signed certificate.

Recommendation:
FTPS (FTP over SSL)

Scenario #5: Large, sensitive files, FTP or email distribution
You need to send purchase orders to your vendors, which you consider fairly sensitive data. The files can be rather large in size and should be compressed before being sent. The purchase orders could be sent over standard FTP connections or via email.

Recommendation:
ZIP with AES Encryption, Secure Mail, or Open PGP

Scenario #6: EDI files requiring confirmation
You need to send EDI information securely to a trading partner and you also need confirmation that they received the exact document(s) you sent them.

Recommendation:
AS2 (S/MIME over HTTP/S) or AS4

Scenario #7: Sensitive files sent via email
You need to send sensitive information in the body of an email.

Recommendation:
Secure Email

GOANYWHERE MFT ENCRYPTION FEATURES

Feature	Encryption Standard	Key Time	Encryption
ZIP Tasks	Password-based symmetric key encryption	Symmetric	Files
PGP Tasks	OpenPGP	Asymmetric	Files
AS2	TLS	Asymmetric	Files and Connections
AS3	TLS	Asymmetric	Files and Connections
AS4	TLS	Asymmetric	Files and Connections
Secure Mail	TLS	Asymmetric	Files and Connections
SCP	SSH	Asymmetric	Connections
SFTP	SSH	Asymmetric	Connections
FTPS	TLS	Asymmetric	Connections
HTTPS	TLS	Asymmetric	Connections

As you can see, GoAnywhere MFT can automate the encryption and decryption process, keeping files secure both at rest and in transit. With ultimate flexibility and security, you can choose the encryption standard required by your trading partners for each individual transfer, whether it is AS2, AS3, AS4, Open PGP, ZIP with AES, SFTP, FTPS, or HTTPS.

In addition, GoAnywhere MFT integrates securely with the cloud and third-party applications, manages keys and certificates, tracks all file transfer activity, complies with strict regulations, and more.

Check out how GoAnywhere can meet your encryption needs

Download Free Open PGP | **I'd Like a Demo**

About BlueFinch

BlueFinch offers confident data protection solutions for corporate and multinational organisations across diverse industries. We manage and secure critical information against loss, theft and non-compliance.

Call +31 (0)88 2583346

Email sales@bluefinch.com

Visit www.bluefinch.com

goanywhere
by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind.