File Transfer Encryption

Why You Need It and How to Implement It

Progress® | ipswitch®

In today's dangerous cyber environment, it's more important than ever to protect your data. Bad guys are always on the lookout for an easy score.

One way to do that is to ensure your network perimeter is secured to prevent any unauthorized access. However, what if your network is breached anyway? Perhaps someone physically comes into your data center and steals a server to gather valuable data you may have stored on it. If your data is not encrypted, kiss it goodbye. But, if you had the foresight to encrypt the data on that server beforehand, while your data might still be gone, at least you'll know it won't be read.

In 2019, encryption is everywhere. It's a standard feature on your iPhone, your messaging program of choice, and your file transfer tools. Encryption has gotten so powerful that the federal government wants a backdoor into consumer apps and devices, and criminals have weaponized it to great financial success. And encryption is an essential piece of any security program, and especially any file transfer system. In this eBook, we'll set out to explain what encryption is, and why you should be using it in the daily transfer and storage of files, as well as some popular encryption programs and protocols. But first, let's start with the basics.

What is Encryption?

There are basically two ways to protect a document containing confidential information from being hacked. One is to protect all the endpoints leading to it, so the data is not accessible to hackers. The other is to encrypt the data so that even if hackers get to the document, they cannot read it.

Both of these protective approaches can and should be used. But given the tough security environment that most IT pros work in, data encryption is, by a wide margin, the single most powerful tool for safeguarding data.

In the simplest terms possible, encryption is the transformation of plaintext data into a protected form called a ciphertext, which hides the original data's meaning. Ciphertext is typically completely unintelligible without an encryption key, which helps decrypt the data. Encryption is required as data protection best practice by multiple data protection laws, including HIPAA and GDPR.

Modern encryption keys, which are collections of extremely complex mathematical algorithms that encrypt and decrypt data into a form that can be read only by someone access to the encryption key. The more advanced the algorithm, the more secure the encryption. Encryption keys can also work as a pair, with one key used to encrypt data and another, or several, to decrypt it, this is known as asymmetric encryption. Encryption which uses just one key (or two identical keys) is known as symmetric encryption.

There are a variety of algorithmic types used for encryption, and the mathematics of encryption is an active area for research and development. As computers become more capable, formerly secure encryption algorithms can become more easily broken by unauthorized users.

Did You Know?

Encryption has been used since ancient times by generals, spies, rebels, and even politicians. The cipher is considered one of the earliest forms of encryption and was used in Ancient Rome to keep information secret. Not even the messenger would know what a message meant without the proper decoder rings.

Machine encryption became an important military tool during the Second World War, when it was used by Germans to secure communications and was cracked by English mathematician Alan Turing.

Nowadays, encryption is necessary to ensure that no one is listening in on our conversations and to keep would-be criminal actors from stealing or corrupting that data. However, the fundamentals of encryption today are much the same as they were in the ciphers of the past. Of course, the encryption algorithms today are far superior with the help of advanced mathematics and computers, thus making brute force attacks much harder to pull off.

Three Common Encryption Programs

Generally, wherever you find encryption at use, whether in business apps, security programs, or consumer apps, the encryption being used is actually being provided by an encryption program, which is a piece of software that creates encryption keys and ciphers. Below are outlines for three of the most common encryption programs.

PGP

Pretty Good Privacy, also known as PGP, was originally created by Phil Zimmerman in 1991 as a way for people to communicate without risking eavesdropping. Today, it is used to encrypt and decrypt text messages and email. In a nutshell, the idea is that when you want to send an encrypted message or file somewhere, you encrypt it with a random key that will then be encrypted with the receiver's public key. This public key can only be decrypted with a private key that only the designated receiver has. That way, even if people know your public key, the receiver is the only one who can decrypt the file or message. The thing with PGP is that it isn't an open patent and is currently owned by Symantec.

Following the development of PGP, there was a law passed in the US that restricted the export of cryptographic technology outside the US. PGP was soon found being used overseas, which led to a lengthy investigation in which no charges were ever pressed against Zimmerman. Following this ordeal, Zimmerman released the source code of PGP which would allow any party to create their own version of encryption software based off the original PGP source code. Since source code is protected under the first amendment, there was nothing the US government could do, and that's where OpenPGP came into play a few years later.

OpenPGP

Due to the patent issues mentioned above, PGP was not always practical for international use. That's why the OpenPGP Working Group was formed within the Internet Engineering Task Force (IETF). This eliminated the need to license PGP and got around some obsolete laws in the US at the time.

OpenPGP is a key-based encryption method used to encrypt files so that only their intended recipient can receive and decrypt them. OpenPGP is used widely to secure e-mail communications, but its technology can also be applied to FTP. OpenPGP works by using two cryptographic keys to secure files. A Public Key is used to encrypt the file so that only its corresponding Private Key can decrypt it.

Unlike SSL and SSH, OpenPGP is not a type of connection, but a method of encrypting a file prior to uploading it. As such, OpenPGP Mode can be used in conjunction with standard FTP, SSL or SSH connections.

Nowadays, many email clients provide support for OpenPGP, which is still being supported and under active development.

As you can see, it's similar to how PGP works. Now, since OpenPGP is an encryption standard supported by the IETF that is supported and developed by the PGP community, there are of course other standards that branch off of OpenPGP. The most common being the open source encryption standard called GnuPG, otherwise known as Gnu Privacy Guard, or GPG for short.

GnuPG

GnuPG is another free encryption standard that companies may use that is based on OpenPGP. GnuPG serves as a replacement for Symantec's PGP. The main difference is the supported algorithms. However, GnuPG plays nice with PGP by design. Because GnuPG is open, some businesses would prefer the technical support and the user interface that comes with Symantec's PGP. It is important to note, that there are some compatibility nuances between GnuPG and PGP, such as the compatibility between certain algorithms, but in most applications there are workarounds. One such algorithm is the IDEA Module, which isn't included in GnuPG out of the box due to patent issues.

What is File Transfer Encryption?

File transfer encryption is an essential security measure that prevents outsiders from being able to read or understand the data that is being transferred. This protects the information from potential hackers. When data is encrypted, the information gets manipulated into an unidentifiable format while in transit, and once it reaches its destination, the data becomes readable again. This way, the data is only accessible by those it is intended for. This process of encoding and scrambling information so that only the sender and receiver can see it is known as end-to-end encryption.

Encrypting Data in Transit and at Rest

DATA AT REST VS. DATA IN TRANSIT

This is a relatively simple definition, as far as cybersecurity terms go—Data at rest is data that is sitting, i.e., resting, in one place. Any data that is not actively moving from one place to another, such as device to device or network to network, is considered data at rest. On the other hand, Data in transit, or data in motion, is data that is moving from one location to another, whether from device to device or across a private network or the internet.

ENCRYPTING DATA IN TRANSIT PROTECTS YOUR DATA AT ITS MOST VULNERABLE

In securing file transfers, it's absolutely essential that you encrypt data as you transfer files from one server to the next—i.e., data in transit.

Any time data is traveling over a network—whether local, across the internet, or from local storage to cloud storage—there's some risk that it could be intercepted by a third party to be read and stolen. So, it stands to reason, that if you are simply encrypting data at rest, say via the automatic encryption on an Amazon S3 bucket, but are transferring it to that bucket unencrypted, that data is exposed at the most vulnerable stage of its lifecycle.

The best practice to combat that risk is to use end-to-end encryption that covers both data at rest and in transit when moving sensitive data. Transport encryption for data in transit uses protocols such as FTPS, SFTP, and HTTPS to protect files as they travel, with encryption strengths up to 256-bit.

Think of transport encryption as an armored truck that's transporting money from say a retail store to a bank. 99.999% of the time that armored Brinks truck will securely transport your delivery without any incident. But adding a second layer of protection – say you put the money in a safe before putting it in the truck – reduces the chance of compromise exponentially, both during and after transport.

ENCRYPT DATA AT REST

Not only is it important to encrypt data as you transfer files from one server to the next, but it is equally important to protect and encrypt this data as it rests on your home server. Why? Two reasons. One, data exchange files are particularly vulnerable because they are files in a very easily-consumed format. Encrypting this resting file adds a new level of protection against potential hackers. Two, file transfer servers on the Internet are more exposed to an attack than standard servers are. To counter this, all files should be encrypted so that if they ever ended up in someone else's possession, they couldn't open it or see the contents. PGP, along with the other programs listed above, is commonly used to encrypt files at rest. During today's threat of cyber theft, it is vital for organizations to take a strategic and defensive approach by protecting their data – regardless as to whether it is in motion or at rest.

End-to-End Encryption Options for File Transfer

So, we've established the importance of end-to-end encryption, but how can you implement it? There are a variety of file transfer encryption options, but there are three that are most common, and that's what we'll focus on in this guide. The three most common options for encrypting file transfer data are FTPS (File Transfer Protocol Secure), SFTP (SSH File Transfer Protocol) and HTTPS (HTTP Secure). All three are heavily used for internal to external, or business to business, transfers.

FTPS

The fastest of the three file transfer encryption options, and the most widely implemented is File Transfer Protocol Secure (FTPS), or FTP over SSL. FTPS has implicit and explicit notes, but both utilize SSL encryption. With FTPS Implicit SSL, the client and server institute an SSL session before any data can be transferred. Comparatively, in FTPS Explicit SSL, the client and server decide together what level of encryption standard is required for the data to transfer. This is helpful because both un-encrypted FTP and encrypted FTPS sessions can occur on a single port. However, this can't always happen, and a range of data ports must be available for use.

SFTP

If FTPS is too complicated for your needs, or if, for whatever reason, you only want to use one port for each file transfer, there is another option: SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. SFTP only requires one port, making it one of the more straightforward options for encryption. Secure FTP arose to meet the needs for enhanced security with tunneling. It uses Secure Shell 2 (SSH2), a secure tunneling protocol, to emulate an FTP connection and provides a firewall-friendly and encrypted channel for file transfers using the well-known TCP port 22. All data exchanged between an SFTP client and server will be protected by an encryption cipher, as well as through the use of public and private keys. These offer further protection through another form of authentication, called public key authentication.

HTTPS

FTPS and SFTP are great to use within servers, but what if your file transfer needs rely more on interactive, human-based transfers? That's where Hyper Text Transfer Protocol Secure, or HTTPS comes in. We can see HTTPs at work every day: on the vast majority of the web sites we use HTTPS protects data sent between web browsers and the websites we visit. Web browsers like Chrome and Firefox even visually display this security through a locked padlock in the security bar. HTTPS uses SSL or TSL protocols. Like SFTP, HTTPS also uses Public Key Infrastructure. In this system, the public and private keys depend on each other. Websites or data encrypted with the public key can only be decrypted with the private key, and vice-versa.

Which is Best?

Ultimately, all three of these options (FTPS, SFTP, and HTTPS) will automatically and transparently encrypt a company's data and protect it from being snipped as its traversing over the Internet. Which is the right for your company boils down to your specific file transfer encryption needs.

Let Managed File Transfer Handle Your File Transfer Encryption Needs

MOVEit Transfer enables the consolidation of all file transfer activities to one system to ensure better management control over core business processes. It provides the security, centralized access controls, file encryption, and activity tracking needed to ensure operational reliability and compliance with SLA, internal governance, and regulatory requirements.

For transport encryption, MOVEit uses SSL or SSH to encrypt communications. The minimum strength of the encryption used during web transport (e.g., 128-bit) is configurable within the MOVEit interface by individual organizations. When data is stored, MOVEit uses FIPS 140-2 validated 256-bit AES, the US federal standard for encryption. MOVEit Crypto, the encryption engine on which MOVEit relies, is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines. MOVEit also overwrites just-deleted files with random bytes to prevent even encrypted files from lingering on a physical disk after users thought them to have been destroyed.

Other security features include user authorization / authentication, delivery confirmation, non-repudiation, and hardened platform configurations. MOVEit Transfer logs activities in a tamper-evident database to comply with ISO 27001, HIPAA, PCI, GDPR, SOX, BASEL I/II/III, FIPS, FISMA, GLBA, FFEIC, ITAR and data privacy laws. It also integrates with your existing DLP and anti-virus systems, identity systems through SAML 2.0, AD, LDAP services, and SIEMs. Additionally, MOVEit offers API interfaces (including REST) for integration with other third-party applications.

To learn more or try MOVEit Transfer yourself, visit our website or download a free trial today.

For Your Free Trial of MOVEit Visit:
https://www.ipswitch.com/forms/free-trials/moveit

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and 2 million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.