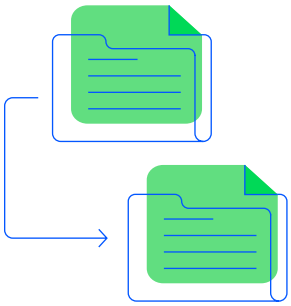
Progress® WS_FTP®

The Definitive Guide to Secure FTP

WHITEPAPER



The Importance of File Transfer

Are you concerned with the security of file transfer processes in your company? According to a survey of IT pros familiar with the file transfer solutions used within their organizations - you're certainly not alone.

Customers, remote employees and business partners have to exchange critical data over the Internet. Effective file transfer is often key to the way organizations run their business and their ability to compete.

However, many companies today are challenged with finding more secure, efficient and reliable ways to manage file transfers. Electronically exchanging company information — such as financial data, client data, health records, employee data and other intellectual property — carries with it the risk of sensitive data falling into the wrong hands.

Failure to adequately protect your data can lead to productivity loss, fines for non- compliance with data protection regulations or a tarnished public image. With this much at risk, it is imperative that you have effective management and control over your file transfer processes.

What are your greatest file transfer concerns?

Basic FTP is Not Secure

The original specification of the FTP protocol included minimal security features. It lacked strong authentication, such as encrypted passwords or authentication tokens. Login credential, connection data and files were transmitted outside the trusted network in clear text enabling interception by cybercriminals. Even today, however, IT professionals are surprised to discover legacy FTP implementations that are still in use transmitting valuable data.

In many cases, the focus on securing the perimeter of the trusted network causes file transfer systems to be overlooked as part of the IT security infrastructure. File transfer implementation are often left to IT administrators.

You should quickly audit your FTP servers, scripts and manual file transfer workflows to assure they are using secure protocols to handle customer, employee and corporate business data.

As admins leave IT organizations, home grown FTP solutions that are not well understood, documented or easily maintained may be left unattended to transfer sensitive data.

Data security auditors tell countless stories of incredible security lapses concerning the handling of sensitive or regulated data. Many business line managers simply don't understand the full scope of regulations and how they apply to the data their operations transmit externally on a daily basis.

Even within the last few years, high-profile data breaches have resulted from cyber attacks that exploited legacy FTP systems. In some cases unencrypted data was intercepted in transit. In others, unencrypted logins were stolen and used to compromise FTP servers which then provided command and control channels for the attackers.

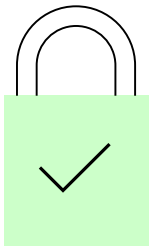
The fact is that your business is most likely covered by some form of data protection regulation or industry standards. Typically this involves Personally Identifiable Information (PII) pertaining to customers, partners or employees. Depending on the regulation, PII can include credit or banking data, names and addresses, data on age or religion, healthcare information and login credentials. Regulations may be enforced by governments on the state, provincial or federal level.

The majority of these regulations require that organizations take sufficient measures to secure sensitive data. These measures include access controls, physical security, governance through documented policies and processes and tracking of access and movement of data. The controls apply to data kept within your network as well as data transmitted externally and even (in some cases) data sent to and stored in external partner networks.

Over the years, a number of high profile data breaches have involved legacy FTP servers.

The combination of a businesses overlooking the risks associated with the loss of sensitive data and the likelihood of forgotten legacy FTP severs presents a huge security risk. If any of the above rings true in your organization, you should quickly audit your FTP servers, scripts and manual workflows to assure that they are using secure protocols to handle customer, employee and corporate business data.

Two common security protocols, Secure Sockets Layer (SSL) and Secure Shell (SSH), are specifically designed to overcome the security limitations of FTP. Both SSL and SSH enhance the security and reliability of file transfer by using encryption to prevent interception during transmission across open networks.



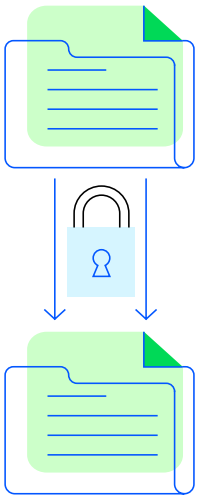
SSL/TLS

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) its predecessor are both frequently referred to simply as SSL. SSL is also known as FTPS or "Secure FTP over SSL". Used in conjunction with FTP it provides secure encryption over standard network connections. When secured by TLS, a client/server connection is private and enjoys one or more of the following security features:

- Symmetric cryptography to encrypt the transmitted data with unique encryption keys being generated for each connection
- Public-key encryption to authenticate the identity of the client and server
- Message integrity checks to prevent undetected loss or alteration of data in transmission.

SSL v3 was deprecated in 2015 and replaced by TLS as it contained a number of vulnerabilities that could be exploited by cybercriminals. TLS 1.2 is the most recent of version of the standard, which adds a Secure Hash Algorithm (SHA) to ensure data integrity. SHA-2 uses advanced cryptographic hash functions designed by the National Security Agency (NSA). With this level of security, you can see how SSL/TLS encryption not only ensures that the wrong eyes do not gain access to your data, but it also protects against attempts to modify data while in transit.

When using SSL to protect data on your file transfer server, you must also ensure that all connecting file transfer clients support the same SSL capability, as the security must be deployed at both ends of the data transport for it to work.



SSH

SSH, also known as SFTP or "Secure Shell File Transfer Protocol" is often considered the best option for secure file transfer. It improves on the security of standard FTP by using Secure Shell 2 (SSH2), a secure tunneling protocol, to emulate an FTP connection.

With SSH, the entire file transfer session, including all data traffic, connection control data and passwords, is entirely encrypted to eliminate eavesdropping, connection hijacking and other attacks.

SSH is a popular choice with IT teams because it offers additional benefits including:

- Using an encrypted channel for file transfers
- Only requiring a single port (TCP port 22) to be opened in the firewall
- Providing interoperability across operating systems and platforms using Secure Copy (SCP2)
- Support by most operating systems (including UNIX/Linux)
- Data compression to allow faster file transfers.

Many IT organizations prefer SSH as it enables cross-platform IT standardization. Standardization ensures consistent security policy enforcement and simpler administration.

Security Feature	FTPS/SSL	SFTP/SSH
Credential Encryption	✔	✔
Transport Encryption	✔	✔
FIPS 140-2 Cryptography	✔	✔
Certificate/Keys	Certificate	Keys
PGP (File at rest) Encryption	Optional	Optional
File Integrity Checks	✔	✔
Built-In Compression	–	✔
Secure Copy (SCP2)	–	✔

Further Security Considerations

To improve the security of your file transfer process, consider also taking the following steps:

Give careful consideration to your authentication practices

The authentication of both SSL and SSH connections can be based on passwords or certificates. If using passwords, they should be of sufficient strength so that they are hard to guess by attackers. Policy-based enforcement of strong cryptography algorithms (and passwords) and being able to control length of encryption keys will protect against unauthorized viewing of data. Such control should be enforced in compliance with your security policy.

Treat file transfer as a core business process

Do a full inventory of your file transfer requirements and have an executive sponsor. Then move to document, standardize, optimize and fully manage the file transfer activities of your organization. While technology can help in meeting these criteria, businesses must ensure that their file transfer architecture maps to a well thought out and well managed business process.

Require secure communications

Limit all file transfers of sensitive data to SSL/TLS or SSH protocols. Best practices include requiring the use of strong authentication (mutual authentication preferred), granular access control, secure audit logging of all activity and that file transfer clients connect over the strongest encryption strengths, such as 256-AES encryption over SSH and TLS 1.2 connections.

Standardize on a secure file transfer solution

An end-to-end solution must incorporate all end users who transfer files with company servers. Both the servers and all connecting clients must support the required security features – remember, your solution is only as strong as the weakest point. Provide a license of your chosen file transfer client to all employees, vendors, contractors and customers who exchange information with your file transfer server.

Progress®
WS_FTP®

Progress Secure FTP Products

WS_FTP Server

Advanced security features in WS_FTP Server include 256-bit AES encryption, SSH transfers, Secure Copy (SCP2), file integrity, SMTP server authentication, SSL certificate support, an SSH listener option, login authentication encryption, digital certificate management, and mutual authentication of server and clients. Powerful admin features include support for virtual servers, end user email notification, end user folder controls and IP whitelists for end user authentication.Start your free trial: www.ipswitch.com/ftp-server

WS_FTP Professional Client

With tens of millions of downloads to date, our WS_FTP client is the most popular premium Windows FTP server in the world. Security features include 256-bit AES, FIPS 140-2 validated cryptography and OpenPGP file encryption. It enables authentication and connection to SSH servers that require clients to respond to server-defined prompts, in addition to user name.

Try Progress WS_FTP Server for free:
www.ipswitch.com/forms/free-trials/ws_ftp-server

About Progress

Progress (NASDAQ: PRGS) provides the leading products to develop, deploy and manage high-impact business applications. Our comprehensive product stack is designed to make technology teams more productive and we have a deep commitment to the open source community. With Progress, organizations can accelerate the creation and delivery of strategic business applications, automate the process by which apps are configured, deployed and scaled, and make critical data and content more accessible and secure —leading to competitive differentiation and business success. Over 1,700 independent software vendors, 100,000+ enterprise customers, and a three-million-strong developer community rely on Progress to power their applications. Learn about Progress at www.progress.com or +1-800-477-6473.

Worldwide Headquarters

Progress, 14 Oak Park,
Bedford, MA 01730 USA
Tel: +1-800-477-6473

www.progress.com

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software

Progress®