IS FTP REALLY ENOUGH?

THE BUSINESS RISKS OF USING FTP

GLOBALSCAPE

FTP IS A CLIENT/SERVER PROTOCOL THAT IS TRANSFERS FILES FROM ONE HOST TO ANOTHER HOST OVER A TCP-BASED NETWORK, SUCH AS THE INTERNET.

THE EVOLUTION OF FTP

Exchanging information is the lifeblood of every organization, and sending and receiving that information securely is paramount. One way companies have moved data for decades is with the file transfer protocol (FTP), but the ever-growing demands of daily business and legal responsibilities are prompting companies look for new ways to send their data.

THE BEGINNING

First developed in the 1970s, FTP was one of the original programs used for accessing information on the Internet, before HTTP became popular to access Web pages. FTP is a client/server protocol that is transfers files from one host to another host over a TCP-based network, such as the Internet. It uses separate control and data connections between the client and the server.

During a typical session, the command channel transmits commands and replies to them, and the data channel transfers information. Clients can initiate different commands including uploading, downloading, deleting, renaming, moving and copying files to servers. Users generally need to enter their username and password to get into a FTP server.

Information can be accessed two ways: actively or passively. In an active connection, the client initiates the command channel, while the server establishes the data channel. The passive connection solves problems when firewalls and routers prevent an active connection from happening.

In a passive connection, the client establishes both channels and the server tells the client which port to use for the data channel. Most FTP clients connect passively by default, because server administers tend to find this safer than active connections.

As data evolved, all sizes and types of information have been transmitted and stored over networks and in the cloud. Hospitals are exchanging confidential patient medical records. Financial institutions are collecting and sharing consumers' personal financial information. Organizations, including online retailers, are storing customers' credit card and other information for future purposes.

Over time, laws in various industries, such as the Health Information Portability and Accountability Act (HIPPA), the Gramm-Leahy-Biley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS), were developed to standardize ways to transfer, store and protect the most sensitive data.

THE DRAWBACKS OF FTP

FTP is a common way to transmit information but there's a hitch: it ultimately lacks visibility, control and important data protections when files are being transferred. Ultimately, FTP is only a mechanism, which presents the following issues:

SECURITY

FTP doesn't encrypt the data as it's sent, and all transmissions are in clear text, putting data at risk when it's transferred. In addition, users' login credentials (or username and password), as well as commands, are visible. Data leakage can also happen when sensitive data is sent across an unsecured or on an anonymous enabled FTP site.

If you are using FTP to transfer business data, you are ultimately sacrificing convenience for security. Additionally, FTP servers that are often installed for one reason or another, are generally forgotten about, not updated, and receive little to no oversight on the data that resides on them. The FBI even put out an alert about attacks targeting anonymous FTP servers at small health providers.

The potential security challenges and risks associated with FTP is a serious problem that needs to be considered carefully.

AUTOMATION

FTP doesn't have the ability to automate directions, such as scheduling information to be received or sent across numerous servers or at specific times. System administrators have to develop custom scripts that talk to the FTP servers, saying what files will be sent and where they should go on the server in order to make specific automation actions a reality.

All of the manual coding and scripting required to create the appropriate automation functions create a tax on man hours. The more manual processes required, the more time it will take for members of the IT team to manage.

RELIABILITY

There isn't any provision in FTP to determine when an error occurs in transmission, letting the operator know when something needs to be fixed. As such, it could take hours, days or weeks to find where an error in transmission occurs. Or worse, errors in transmission could result in a loss of business or confidence if relied upon data does not meet its intended destination on time.

FTP also doesn't have the ability to filter data to enforce corporate information policies, have checkpoint and restart functionality that ensures messages are delivered, and can't effectively support sending large file transfers concurrently or transferring them simultaneously to multiple recipients.

TOP 3 MISCONCEPTIONS ABOUT FTP

Misconception 1: All that matters when transferring files is getting data from point A to point B

This is an incredibly common misconception. Employees are going to do anything to get the job done, even if that means skirting the rules of data security to make way for their productivity. Unfortunately, just getting a file or data from point A to point B is just the beginning of the story. There are many other considerations that need to be understood.

VISIBILITY INTO YOUR DATA

You can't secure what you don't know about and you can't act in accordance with compliance mandates if you have no idea who is exchanging data and with whom. Full visibility into data moving inside and outside of your network is a necessity in file transfer security and compliance, and it's just as important (if not more important) than the file simply reaching its intended destination.

SETTING AND ENFORCING GRANULAR CONTROLS AND PERMISSIONS

Some files are just too sensitive to sit in the intended recipient's inbox for weeks. Other employees need specific permissions for certain levels of sensitive data in an organization, but not others. Do you know who has access to the information? Password-protected files can be a step in the right direction, but they're not a cure-all. It's important to be able to implement and enforce file security controls that extend to specific file or data types, data sizes, and ultimately down to the employee level.

MOVING LARGE FILES

It's no surprise that Big Data needs to be moved. Whether it's regularly backing up daily financial data or moving raw video footage from a remote location for the next movie, data is increasing and as a result, our bandwidth needs are growing, but moving big files isn't as easy as you might think. For security and operations, it's important to have an in-house solution for moving large and/or sensitive files efficiently. You can easily do this by automating recurring transfers and timing large transfers to take place during off-peak network hours.

Misconception 2: Homegrown FTP is 'good enough'

You're probably telling yourself, "My homegrown FTP works just fine…" Think again.

Homegrown FTP solutions are littered with inefficiencies, risks and limitations, and they can cost you in lost productivity and software or hardware maintenance costs. Scripts and disparate homegrown FTP solutions eventually become impossible to manage and, having numerous point applications and tools from several vendors poking holes in your firewall isn't an ideal scenario for file transfer security. An organization's IT professionals often must improvise and spend an inordinate amount of time on scripting data workflows and reworking data workflow processes in order for file transfers to work.

Also with homegrown file transfer systems, organizations face problems with scalability. Organizations that grow and continue to use FTP lack flexibility and scalability in their data transfer infrastructure, unless they can drastically increase their IT resources.

Misconception 3: My business doesn't transfer any sensitive 'big data'

Big Data can be comprised of anything that's too big to fit in a stand-alone email. Now, you personally might not transfer sensitive big data, but your company does–especially if it is using large integrated enterprise applications. And those transfers (typically large batch, flat or video files) are usually ungoverned and often contain sensitive or proprietary company, employee, or customer information. And if you're using an FTP server for those large enterprise data transfers it was not designed to handle big data sets and ultimately will put serious constraints on your network resources.

When thinking about your network architecture, assume that sensitive big data sets are only going to get bigger and evaluate effective, flexible file transfer solutions that can manage large, sensitive files better than FTP servers or legacy middleware solutions and more securely.

A REMEDY IN MANAGED FILE TRANSFER

INTEGRATION

These systems lack core data integration capabilities, increasing risks to the organization. Often, this inability to easily exchange data increases an organization's costs and complexity by forcing them to build individual FTP servers or buy patchwork solutions, which include time intensive manual processes just to keep business and vendor transactions running. When your users rely on manual and intermittent batch processes to deliver the data they need, day-to-day productivity becomes dangerously vulnerable. You need a way to easily, effectively, and securely transfer files and data between all systems required to ensure business productivity.

> 57%

of organizations are using gateway technology that's more than 5 years old.

– Ovum Research

VISIBILITY

This impact includes missing internal and customer service level agreements and major loss of revenue. Yet, for something so critical, many organizations are littered with non-compliant and rogue data exchange solutions, making the environment ripe for failed data transactions. Often, the IT team has little to no visibility or control over how company data is being exchanged, or if it is being exchanged securely. It's important to consolidate data transfer solutions and gain control and visibility over your company's mission-critical data exchanges and file transfers.

> 77%

of organizations say that data exchange failures would have a critical business impact.

– Ovum Research

SCALABILITY

Companies that are unable to exchange data for a single hour could lose between **$250,000** and **$500,000**.

Unfortunately, the number of data stakeholders that IT must support increases year over year. As the number of stakeholders increases, so do their needs and demands. Efforts to maintain the uptime and complex functionality that stakeholders want could also strain the infrastructure, hurt performance and affect compliance.

Dealing with personalities, disparate—and at times conflicting—service level agreements (SLAs), as well as competing priorities and numerous points of failure is highly complex and often too much for one person to manage effectively, increasing the risk of failure. Your organization needs a way to eliminate the downtime due to complexity and resource constraints, while scaling as the needs of your business grow.

Enterprise-level managed file transfer (MFT) technologies offer a higher level of control and security than FTP. MFT technology's features include in-depth reporting (specifically, notification of successful file transfers), global visibility into your data at all times, end-to-end security with encryption of data in transit and at rest, performance metrics/monitoring to meet stringent SLAs and compliance mandates, and the automation of file transfer-related processes.

A study, commissioned by Globalscape and conducted by Forrester Consulting, examined the potential return on investment for those organizations who implement Globalscape's MFT technology, Enhanced File Transfer™ (EFT™).

Forrester interviewed current Globalscape customers who have used EFT for several years and replaced homegrown solutions within their IT infrastructure with Globalscape EFT to meet regulatory and compliance mandates. The composite organization, based on customer interviews, within three years, were able to:

- ☑ CREATE AND SUPPORT **10 TIMES** THE EXISTING NUMBER OF SECURE FILE TRANSFER PROCESSES
- ☑ SAW A NET PRESENT VALUE OF **$3,251,809**
- ☑ A REDUCTION IN SUPPORT HOURS BY **6,885 HOURS**

Other overall benefits the study identified included:

TIME EFFICIENCY

Globalscape customers revealed that their IT teams spent a large amount of time having to recreate and develop workflows that would enable the functionality the organization needed. When EFT was deployed, the organization could increase their file transfers from 40 to 400 with the same amount of internal resources.

COST SAVINGS

The majority of costs for EFT were one-time fees; EFT paid for itself in the time saved to better manage the flow of data in a secure and compliant way, not to mention the reduction in overall support time needed to address issues. The composite organization previously received more than 200 file transfer-related support calls a week, and after deploying Globalscape EFT, saved some 2,080 hours—the equivalent of one full-time employee working 40 hours per week for an entire year.

STAFFING CONSIDERATIONS

Previous file transfer system required specialized programmers to work through errors or create new processes. With Globalscape's technology, a larger number of current IT team members could manage issues or changes required, allowing organizations to bring on IT employees with more generalized skill sets rather than a specialized workforce to manage the file transfer system.

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit **www.globalscape.com** or follow the blog and Twitter updates.

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support

GLOBALSCAPE