whitepaper

Understanding the Need for Self-Hosted File Transfer Solutions

solarwinds

In the normal day-to-day business process, organizations transfer enormous amounts of information, both internally as well as externally to partners and customers. During these transfers, sensitive corporate data can be exposed to unauthorized 3rd-parties—especially when the file transfers occur over insecure channels, or when data gets stored on the public cloud.

As work environments become more collaborative, file sharing becomes necessary for productivity. Unfortunately, the security aspect is often overlooked, putting organizations at risk for confidential data leakage. To mitigate this risk, it's critical that IT departments maintain visibility and control over file transfer activity at all times.

The need for a simple way to access and share files over the Internet has led to an increase in the number of available enterprise file transfer solutions. However, there are different security and regulatory compliance factors that need to be considered when selecting a file sharing solution in order to ensure that critical requirements are not compromised.

Are Cloud-based Solutions the Answer?

Cloud-based file transfer and data storage solutions like Dropbox, Google Drive, and Microsoft SkyDrive help you speed up communication and are easy to use, but they also come with significant risks that need to be mitigated in order to be compliant with security regulations.

As your employees use these public cloud solutions to share confidential data, it becomes easier for hackers to gain access to the data. This can lead to a costly breach that can have a direct impact on your business reputation and customers' trust level.

In most cases, employees use these file sharing solutions without the consent of their IT organization. When your end-users transmit and store critical corporate information outside the purview of IT, your control over data is relinquished.

A recent research report revealed that about 48% of the surveyed organizations in the UK and North America were using cloud-based file hosting services. Some major revelations were:

- For 74% of the surveyed organizations, the major concern with sharing files outside of the corporate firewall was malware infection.
- For 54%, the major concern was information theft.

Rightly so, more organizations are concerned with information security when control is relinquished to a cloud-based service.

How Secure Are Cloud Solutions?

Cloud solutions provide a certain level of convenience, but this convenience comes at a cost in terms of security and compliance. When dealing with confidential and sensitive data, it's imperative to have strict security and accountability controls in place, especially around file transfers and the end-users who transfer or receive the files. This is a weakness in cloud-based solutions.

When using cloud-based file management services with regulated data such as healthcare, payments, private financial data and sensitive customer data further, the complexity and risk is further increased. With data breach notification costs currently estimated at $136 per record globally and $188 per record in the United States, entrusting regulated data to a cloud-based file management provider increases risk of not only financial, but customer loss. If the cloud-based provider has a lapse in security and if data is exposed, the organization that is using the service is still responsible for data breach notification and subject to regulatory sanctions. In some, instances, such as HIPAA, the ability to use a cloud based service is dependent on the provider's ability and willingness to sign a business associate agreement. Most providers will refuse due to increased legal and financial risk. Given these risks, assuming control over the security of regulated data through managing secure file sharing and management internally, often costs less than the complexity and cost of employing additional controls to protect the organization from third party cloud provider risks.

Consider Dropbox. Last year, a number of usernames and passwords of Dropbox accounts were compromised, resulting in a spamming campaign to numerous Dropbox users. Similarly, there was another breach in 2011 that exposed hundreds of accounts without proper authentication. Further adding to the users' woes, the Dropbox service as a whole went down early this year.

As evidenced by the Dropbox incident, when data is stored in the public cloud, there's not only the risk of exposure to private information, but also the risk of costly downtime and subsequent penalties for organizations that must adhere to specific service level agreements (SLAs) for compliance.

A better option is a secure managed file transfer (MFT) server that is hosted on your premises and enables you to maintain the integrity of data shared between two entities. Below is a set of criteria for an effective managed file transfer solution:

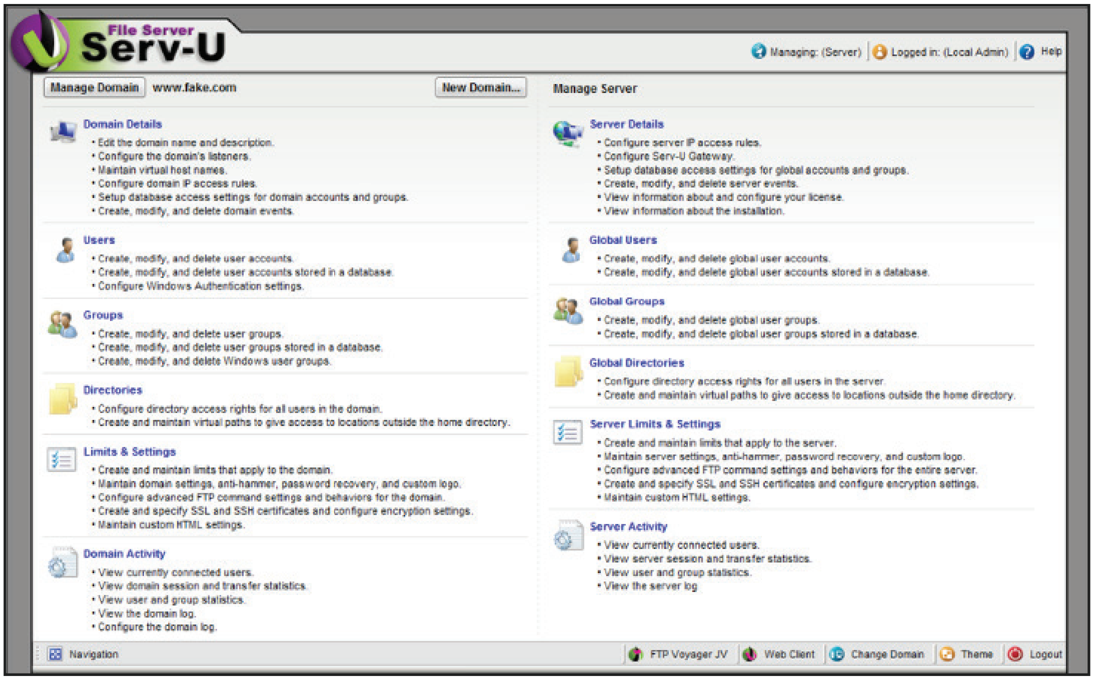
- Security: Both at rest and in motion
- Access Control: Limit access by role, individual, and time
- Certificate-based authentication
- File Storage: Limited access after upload, default file access policy, and security logs
- Monitoring: View "real-time" file transfer progress
- Reporting: Transfer activity and access
- Internal Resource Protection (Proxy Server): DMZ resident - conceal internal IP addresses
- B2B/E-Commerce Protocol Support: HTTP, HTTPS, FTP, FTPS, SFTP
- Endpoint Management: Create, edit, and remove trading partner profiles

Self-Hosted Managed File Transfer Solution

Serv-U MFT Server is a self-hosted managed file transfer server from SolarWinds that serves as a secure alternative to the cloud-based solutions for transferring files inside and outside the enterprise. From an ease-of-use standpoint, Serv-U provides flexible, anywhere file access and administration. End-users can view and upload documents from anywhere using a Web browser or mobile device—without the need for extra software. Similarly, IT admins can manage, monitor, and configure Serv-U from anywhere through a secure Web management console, and even from an iPad®. Plus, it integrates with Active Directory® and existing storage infrastructure.

From a security standpoint, Serv-U provides granular access control to protect sensitive data, including:

- Secure data transmissions with strong encryption and strong authentication
- Support for FTPS, SFTP, and HTTPS over IPv4 or IPv6 networks
- Real-time session monitoring and file transfer activity logging
- Event-driven automation to send alerts and trigger actions
- Virtual directories with advanced permissions
- File expiration and deletion after a configurable period of time
- Automatic IP lockouts to prevent brute-force attacks



Domain Details
- Edit the domain name and description.
- Configure the domain's listeners.
- Maintain virtual host names.
- Configure domain IP access rules.
- Setup database access settings for domain accounts and groups.
- Create, modify, and delete domain events.

Users
- Create, modify, and delete user accounts.
- Create, modify, and delete user accounts stored in a database.
- Configure Windows Authentication settings.

Groups
- Create, modify, and delete user groups.
- Create, modify, and delete user groups stored in a database.
- Create, modify, and delete Windows user groups.

Directories
- Configure directory access rights for all users in the domain.
- Create and maintain virtual paths to give access to locations outside the home directory.

Limits & Settings
- Create and maintain limits that apply to the domain.
- Maintain domain settings, anti-hammer, password recovery, and custom logo.
- Configure advanced FTP command settings and behaviors for the domain.
- Create and specify SSL and SSH certificates and configure encryption settings.
- Maintain custom HTML settings.

Domain Activity
- View currently connected users.
- View domain session and transfer statistics.
- View user and group statistics.
- View the domain log.
- Configure the domain log.

Server Details
- Configure server IP access rules.
- Configure Serv-U Gateway.
- Setup database access settings for global accounts and groups.
- Create, modify, and delete server events.
- View information about and configure your license.
- View information about the installation.

Global Users
- Create, modify, and delete global user accounts.
- Create, modify, and delete global user accounts stored in a database.

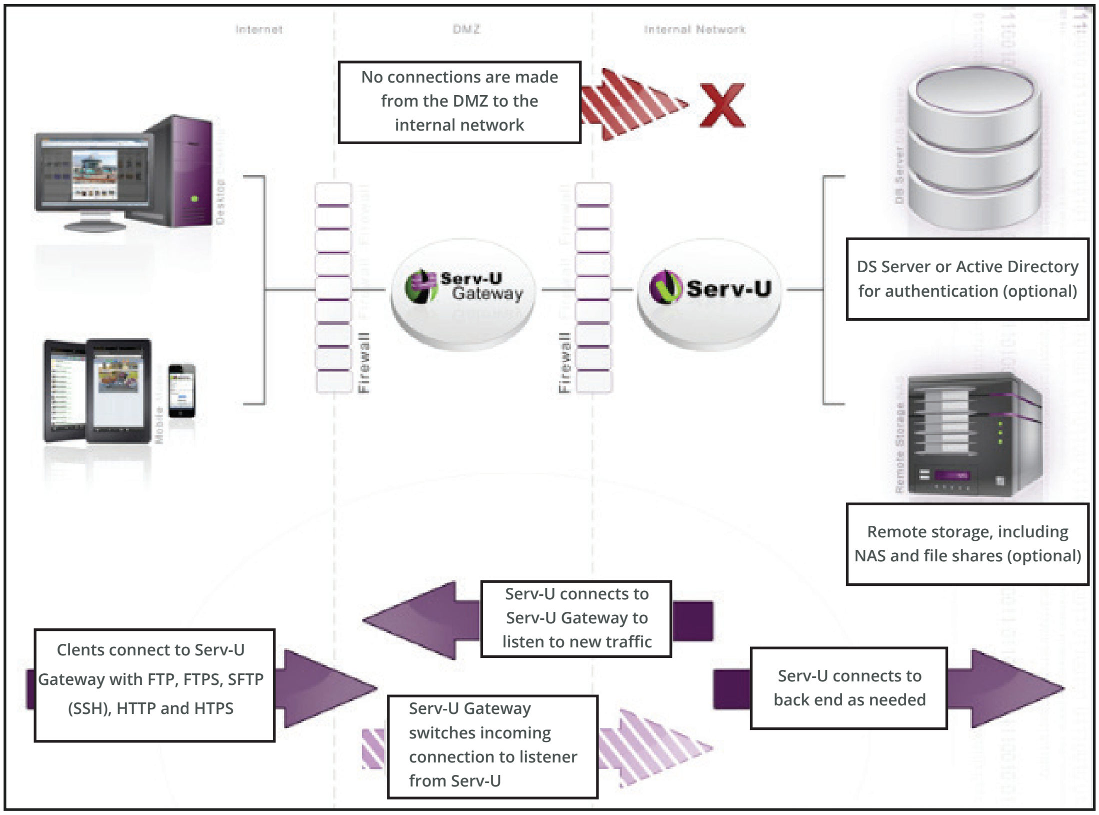
Global Groups
- Create, modify, and delete global user groups.
- Create, modify, and delete global user groups stored in a database.

Global Directories
- Configure directory access rights for all users in the server.
- Create and maintain virtual paths to give access to locations outside the home directory.

Server Limits & Settings
- Create and maintain limits that apply to the server.
- Maintain server settings, anti-hammer, password recovery, and custom logo.
- Configure advanced FTP command settings and behaviors for the entire server.
- Create and specify SSL and SSH certificates and configure encryption settings.
- Maintain custom HTML settings.

Server Activity
- View currently connected users.
- View server session and transfer statistics.
- View user and group statistics.
- View the server log

Serv-U also provides the ability to run in FIPS-140-2 mode. It offers a separate module called the Serv-U Gateway to provide reverse proxy capabilities, preventing data from ever being at rest in your DMZ or opening connections directly from the DMZ to your internal network. When you use Serv-U MFT Server together with Serv-U Gateway, it provides an architecture that is not only PCI-DSS compliant, but it also meets other high-end security requirements. The reference architecture below provides an example.



No connections are made from the DMZ to the internal network

DS Server or Active Directory for authentication (optional)

Remote storage, including NAS and file shares (optional)

Serv-U connects to Serv-U Gateway to listen to new traffic

Clents connect to Serv-U Gateway with FTP, FTPS, SFTP (SSH), HTTP and HTPS

Serv-U Gateway switches incoming connection to listener from Serv-U

Serv-U connects to back end as needed

Resources for Additional Learning

[Secure File Sharing with SolarWinds Serv-U MFT Server]

[Control Access to Data with Managed File Transfer]

[Key Considerations for Effective Data Loss Prevention]

[Serv-U Solves Media Challenges of Washington TV Station KSPS]

Serv-U Managed File Transfer

Serv-U® MFT Server deploys in your own datacenter to deliver reliable, affordable, secure file sharing and managed file transfer capabilities with the ease of use end-users want and the administrative control IT departments need.

Serv-U Highlights:

- Host a secure and easy-to-use file sharing solution in your own datacenter
- Provide flexible, secure, anywhere file access and administration
- Enable IT oversight and control into file transfer activity
- Comply with security and privacy regulations such as PCI-DSS, HIPAA, FISMA and SOX
- Leverage existing infrastructure to reduce costs and increase security

LEARN MORE »   DOWNLOAD FREE TRIAL

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at solarwinds.com.