檔案傳輸—安全、合規、高效

Ethan Lin, Ipswitch Solution Engineer
FTP
Back to the Basic

Trusted Network

Internet

FIREWALL

FIREWALL
Moving Files is Business-critical
Key Principles

Data Loss Prevention

High Speed Traffic Through the Firewall

Secure Control
General Data Protection Regulation (GDPR)

❯ It becomes enforceable from **25 May 2018**.

❯ It applies if an organization that collects/processes data from **EU residents**.

❯ (one of) The sanctions can be imposed: a fine up to **€20 million** or up to **4% of the annual worldwide turnover**.
7 Principles

❯ **Principle 1 - Fair, Lawful and Transparent Processing**
❯ **Principle 2 - Data Security**
❯ **Principle 3 – Accuracy**
❯ **Principle 4 - Accountability**
❯ **Principle 5 – Purpose Limitation**
❯ **Principle 6 – Data Minimization**
❯ **Principle 7 – Retention Periods**
合規的資訊與檔案傳輸之作業方法

Ethan Lin– APAC Solution Sales Engineer
The Core in FSI – FTP/SFTP Server
## PCI DSS Requirements

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>Prohibit direct public access between the Internet and any system component in the cardholder data environment.</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td></td>
<td>Do not store sensitive authentication data after authorization</td>
</tr>
<tr>
<td></td>
<td>Limit cardholder data storage and retention time</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>Protect all systems against malware and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>Restrict physical access to cardholder data</td>
</tr>
<tr>
<td></td>
<td>Identify and authenticate access to system components</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>Implement audit trails to link all access to system components to each individual user.</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
# Data Protection Requirements

<table>
<thead>
<tr>
<th>Real-Time Alerting</th>
<th>Data Encrypted in Transit</th>
<th>Data Encrypted at Rest</th>
<th>DMZ Gateway</th>
<th>Proxy Server</th>
<th>File-Gained Access Controls</th>
<th>Content Scanning</th>
<th>File Integrity Checks</th>
<th>Nist Requirements</th>
<th>Task-Based File Transfers</th>
<th>At-Hoc File Transfers</th>
<th>Centralized Controls</th>
<th>Management Reporting</th>
<th>Tamper-Resistant Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fair, Lawful &amp; Transparent Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limitation of Purpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Minimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Retention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GDPR Requirements
Secure FTP is Non-Compliant

<table>
<thead>
<tr>
<th>Secure FTP</th>
<th>GDPR Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>□</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Security</th>
<th>Accountability</th>
<th>Data Minimization</th>
<th>Data Retention</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fair, Lawful &amp; Transparent Processing</th>
<th>Limitation of Purpose</th>
<th>File Integrity Checks</th>
<th>Non-Reputation</th>
<th>Task-Based File Transfers</th>
<th>Ad-Hoc File Transfers</th>
<th>Centralized Controls</th>
<th>Management Reporting</th>
<th>Tamper-Resistant Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 金檢基本要求

<table>
<thead>
<tr>
<th></th>
<th>Real-Time Alerting</th>
<th>Data Encrypted in Transit</th>
<th>Data Encrypted at Rest</th>
<th>DMZ Gateway</th>
<th>Proxy Server</th>
<th>Fine-Grained Access Controls</th>
<th>Content Scanning</th>
<th>File Integrity Checks</th>
<th>Non-Reputation</th>
<th>Task-Based File Transfers</th>
<th>Ad-Hoc File Transfers</th>
<th>Centralized Controls</th>
<th>Management Reporting</th>
<th>Tamper-Resistant Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fair, Lawful &amp; Transparent Processing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limitation of Purpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Minimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Retention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**GDPR Requirements**  

- Secure FTP ✓
Managed File Transfer Enables Compliance

<table>
<thead>
<tr>
<th>Security</th>
<th>Real-Time</th>
<th>Alerting</th>
<th>In Transit</th>
<th>Data at Rest</th>
<th>DMZ Gateway</th>
<th>Proxy Server</th>
<th>File-Gained Access Controls</th>
<th>Content Scanning</th>
<th>File Integrity Checks</th>
<th>Monitoring</th>
<th>Reputation</th>
<th>Task-Based File Transfers</th>
<th>Ad-hoc File Transfers</th>
<th>Centralized Controls</th>
<th>Management Reporting</th>
<th>Transfer-Bidient Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Accountability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fair, Lawful &amp; Transparent Processing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Limitation of Purpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Minimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Retention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- GDPR Requirements
- Secure FTP
- Managed File Transfer
How a MOVEit System can help

- FIPS 140-2 certified security modules
- AES Encrypted data at rest
- Encrypted data during transit
- SAML/LDAP/AD/Radius/ODBC
- ICAP AV Integration
- ICAP DLP Integration
- Corporate branding
- Tamper proof audit log
- Built in reporting
- Failover / HA support
- Virtualisation Support
How a MOVEit System can help

- Multi Protocol Support
- Task Automation
- End to End Encryption
- PGP payload encryption
- FIPS 140-2 Validated
- Tamper evident logging
- Complex workflows with conditional logic
- Synchronisation of files on different systems
- Remote and delegated management
- Automatic restart and Failover
Standard Architecture

INTERNET

- Any FTPS Server
- Any SFTP Server
- Any HTTPS Server
- Any ASx Server
- Email Server
- SMIME Server

Web Browser

- Any FTPS Client
- Any SFTP Client
- Any AS2 or AS3 Client
- Other Ipswitch Clients
- Mobile Users

DMZ

- FTPS, SFTP, HTTPS, AS1/AS2/AS3

SECURE NETWORK

- Mainframe / Unix Server
- Network Share
- Any FTPS Server
- Any SFTP Server
- Email Server

- Web Browser
- Microsoft Outlook
- Any FTPS Client
- Any SFTP Client
- Other Ipswitch Clients
- Mobile Users

HTTPS

FIREWALL

FTP, SFTP, HTTPS, AS1/AS2/AS3

OPEN FTP, ZIP OR OTHER PROCESSL
Gateway-No Data in DMZ

INTERNET

DMZ

SECURE NETWORK

Any FTPS Server
Any SFTP Server
Any HTTPS Server
Any ASx Server
Email Server
SMIME Server

Web Browser
Any FTPS Client
Any SFTP Client
Any AS2 or AS3 Client
Other Ipswitch Clients
Mobile Users

FTPS, SFTP, HTTPS, AS1/AS2/AS3
LOAD BALANCER (OPTIONAL)
SECURE TUNNEL

FIREWALL

FTPS, SFTP, HTTPS, AS1/AS2/AS3

Mainframe / Unix Server
Network Share
Any FTPS Server
Any SFTP Server
Email Server

Web Browser
Microsoft Outlook
Any FTPS Client
Any SFTP Server
Other Ipswitch Clients
Mobile Users

FTPS, SFTP, HTTPS

SMIME Server

Any HTTPS Server
Any ASx Server

FTPS, SFTP, HTTPS

Any FTPS Server
Any SFTP Server
Other Ipswitch Clients
Mobile Users
End-to-End Encryption (PGP)

1. User places file on share.
2. Some approval process invokes a MOVEit Automation task via the API to transfer file to Transfer server.
3. MOVEit Automation task at site automatically downloads file to local network share.

Network Share

R&D DMZ

R&D Secure Network

Email Server
Any FTPS Server
Any SFTP Server
Network Share

1. User places file on share.
2. Some approval process invokes a MOVEit Automation task via the API to transfer file to Transfer server.

Network Share

FIREWALL

HTTPS

FIREWALL

HTTPS

FIREWALL
Data Protection

INTERNET

Any FTPS Server
Any SFTP Server
Any HTTPS Server
Any ASx Server
Email Server
SMIME Server
Web Browser

DMZ

FTPS, SFTP, HTTPS, AS1/AS2/AS3
LOAD BALANCER (OPTIONAL)
SECURE TUNNEL

SECURE NETWORK

FFPS, SFTP, HTTPS, AS1/AS2/AS3

FIREWALL

NAS or NAS Cluster
Antivirus ICAP Servers
SQL Server Standalone or Cluster
DLP

User DB (AD/Radius/SSO)

Any FTPS Client
Any SFTP Client
Any AS2 or AS3 Client
Other Ipswitch Clients
Mobile Users

Any HTTPS Server
Any ASx Server
Other Ipswitch Clients
Other Ipswitch Clients
Any SFTP Client
Any FTPS Client
Any FTPS Server
Any HTTPS Server
Workflow and Automation - System to System

- Advanced Tasks with Conditional Logic
- Alternate Host Failover
- Easily Clone existing settings

- Advanced API Management
- Networked UNC Paths
- PGP, ZIP, External Processing
- Tamper evident audit
- Alerting
Introduction to MOVEit Automation
將資料遺失風險降到最低

安全工作流程控制檔案傳輸作業
End User
The Balance: Usability & Security

IT needs to deploy systems which **meets** users’ needs & provides **governance** required by IT

**Employee needs**
- Convenient
- Straightforward
- Easy to use
- Fast

**IT requirements**
- Control
- Visibility
- Security
- Compliance
Person to Person Transfers Made Easy!
Person to Person Transfers Made Easy!

Please find attached the secure installation document.

Andy Morris
Solutions Architect
T. +44 1295 701 328 | C. +44 7920 203 679 | amorris@ipswitch.com

www.ipswitchFIT.com
Person to Person Transfers Made Easy!

MOVEit Transfer

Automatic Encryption at Rest

Send email notification with link to message and attachment

Upload attachment and/or message

Sender (Email/web client)

Mail Server

ipswitch
Person to Person Transfers Made Easy!

Send email notification with link to message and attachment

Receive Message
Two Options
- Everything Secured
- File attachment only Secured

Send
Mail Server
Recipient
- Everything Secured
- File attachment only Secured

的一切内容加密
- 文件附件仅加密
Person to Person Transfers Made Easy!

MOVEnd Transfer

Sender (Email/web client)

Upload attachment and/or message

Mail Server

Receive Message

Two Options

- Everything Secured
- File attachment only Secured

Send email notification with link to message and attachment

Read message and download attachment

Recipient

Receive Message

Two Options
Data Protection

INTERNET

Any FTPS Server
Any SFTP Server
Any HTTPS Server
Any ASx Server
Email Server
SMIME Server

Web Browser

Any FTPS Client
Any SFTP Client
Any AS2 or AS3 Client
Other Ipswitch Clients
Mobile Users

DMZ

FTPS, SFTP, HTTPS, AS1/AS2/AS3
LOAD BALANCER (OPTIONAL)
SECURE TUNNEL

SECURE NETWORK

FTPS, SFTP, HTTPS, AS1/AS2/AS3

'iPswitch'
MOVEit AUTOMATION

'iPswitch'
MOVEit TRANSFER

NAS or NAS Cluster
Antivirus ICAP Servers
SQL Server Standalone or Cluster
User DB (AD/Radius/SSO)

DLP

FIREWALL

FIREWALL

OPEN FOR ZIP OR OTHER PROCESS

Any FTPS Client
Any SFTP Client
Any AS2 or AS3 Client
Other Ipswitch Clients
速度
Case Study

- Europe
- China
- Taiwan
- Hong Kong
檔案很大
距離很遠
網路很慢
Acceleration Technology

Proprietary Transport Protocol

- Minimizes the impact of latency
- Detects and remediates UDP packet loss
- Fully utilize available bandwidth
- Up to 200X faster than standard transfers

• Latency
• Packet Loss
Thank You
如有問題，歡迎聯絡我們
https://tw.ipswitch.com/contact-sales