

6 ways FTP is putting your business at risk

1

Weak security

- Log in credentials (IDs & passwords) are not protected
- Encryption is an afterthought
- FTP clients are common and free

4

Recovery from failures

- FTP cannot automatically recover from a failed connection:
- No checkpoint restart – all files must be resent
 - Lack of alerts for transmission failures
 - Manual outreach required to explore cause of failure

2

Poor management control

- Sending files via FTP, you cannot:
- Create enforceable policies
 - Schedule critical transfers
 - Reserve dedicated transmission channels for sensitive data transfers
 - Interrupt and prioritize transfers

5

Under/over utilization of resources

- FTP can require hours of custom coding to address:
- File transfers sent without prioritization
 - Complex labor-intensive onboarding of partners
 - Manual processes
 - Growing file transfer volumes

3

Lack of visibility

- FTP does not provide status on:
- Delayed or failed transmissions
 - Route notifications for issue remediation
 - Provide activity log files

6

Poor performance

- “Free” has hidden costs. Using FTP, you still need to monitor transmission performance to confirm:
- Successful data transfers occurred
 - Failure notifications
 - SLAs are achieved
 - Check for security alerts
 - Activity log details