Kiteworks

12 Kiteworks Secure File Transfer Use Cases

Introduction

The ability to securely transfer files between individuals, teams, and organizations is more critical than ever before in the digital age. As companies across all industries have embraced digital workflows and remote collaboration, they require robust and reliable methods of sharing sensitive documents and data without putting security at risk. Implementing secure file transfer procedures has therefore become a top priority for IT leaders and security professionals seeking to enable business operations while protecting against cyber threats.

Secure file transfer refers to sending files and documents electronically through encrypted channels to prevent unauthorized access. There are several common methods used, including Managed File Transfer (MFT), Secure File Transfer Protocol (SFTP), and cloud-based file sharing platforms with built-in security features. The appropriate solution depends on the organization's infrastructure, compliance needs, and ease-of-use requirements. But regardless of the specific technology implemented, the overarching goal remains the same: to provide users with seamless file sharing capabilities while keeping sensitive data locked down.

Healthcare organizations, for example, rely heavily on the ability to securely share patient records and medical images between care providers. They must comply with strict HIPAA regulations around protected health information. Implementing an MFT solution with automated file encryption, user access controls, and audit logging helps them efficiently coordinate care across facilities while adhering to compliance mandates. Financial institutions similarly need to secure customer account data, transaction details, and other sensitive information when transmitting files. Cloud-based secure file transfer systems with identity management, authentication safeguards, strict access controls, strong encryption, and comprehensive, real-time audit logging enable real-time collaboration between employees without putting data at risk.

Five Secure File Transfer Standards

Before selecting a solution, organizations must understand the various standards—their strengths and weaknesses:

1 File Transfer Protocol (FTP)

is the backbone of most file transfers, allowing files to be downloaded and uploaded between devices. However, it lacks encryption and other security features, making it unsuitable for sensitive data.

2 FTP Over SSL/TLS (FTPS)

adds encryption to FTP for better security. But as threats become more advanced, experts urge caution using FTPS for highly sensitive data.

3 SFTP

encrypts credentials and files for secure transfer once devices authenticate each other. SFTP is compatible with firewalls, unlike FTPS.

4 OpenPGP

uses public-key cryptography for confidentiality and sender authentication in email and file transfers. Users can encrypt communications to prevent unauthorized access.

5 MFT

centralizes secure, efficient, compliant file transfers into one platform. MFT provides encryption, access controls, monitoring, and backup/recovery.

Secure File Transfer and Regulatory Compliance

Regulatory compliance is a critical factor that should inform the choice of file transfer standard. Industries like healthcare, government, financial services, and retail have strict regulations around protecting sensitive customer data during electronic transfers. For example, healthcare organizations must comply with HIPAA and HITECH rules to encrypt protected health information before sharing it externally. Government agencies must follow FISMA guidelines to reduce security risks around federal information and data. In the financial services sector, GLBA requires institutions to safeguard personally identifiable customer information and offer an opt-out for data sharing. Retailers collecting payment card data must adhere to PCI DSS encryption and security controls.

MFT is often the ideal solution to demonstrate compliance across regulated industries, as it provides end-to-end encryption, access controls, detailed audit logs, and other security safeguards. Choosing a file transfer standard that aligns with industry-specific regulatory mandates is crucial for avoiding stiff penalties and reputation damage that can result from noncompliance and exposure of confidential documents like personally identifiable information (PII), trade secrets, or controlled unclassified information (CUI). Investing in MFT or SFTP solutions with detailed audit logs provides the level of visibility required in the event of a potential data breach or audit.

Data Types That Pose the Greatest Risk

781 IT, security, risk, and compliance leaders representing 15 different countries were asked to rank data types based on risk:

56%
Legal Documents (Rank 1, 2, or 3)

50%
Merger & Acquisition Information

54%
Personally Identifiable Information (PII)

50%
Financial Documents

52%
Protected Health Information (PHI)

48%
Intellectual Property

Source: Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report

12 Use Cases for Secure File Transfer

Following are 12 different use cases for secure file transfer. In each of these scenarios, security is a critical requisite.

1.

Secure File Transfer for Client Data

Businesses often need to share sensitive client data. Kiteworks provides a secure file transfer solution that ensures data confidentiality and compliance with relevant regulations.

2.

Secure Inter-departmental File Transfers

Different departments often operate in silos, leading to delays and potential security lapses during file transfers. Unauthorized access or data loss in inter-departmental transfers can jeopardize an entire organization. Kiteworks creates a seamless communication bridge between departments, ensuring encrypted content sharing. It provides strict access controls, ensuring that only authorized personnel can access shared files, and robust tracking to dramatically improve audit preparation and execution.

3.

Financial Data Exchange

Financial data, being confidential, is susceptible to cyber threats and unauthorized access. Such breaches can lead to severe financial and reputational damage to the company. Kiteworks facilitates a highly encrypted environment for financial data exchanges. It maintains the confidentiality and integrity of the data, ensuring safe transmissions every time.

4.

Cloud Storage Transfers

As businesses adopt multiple cloud platforms, data transfers between them can introduce security vulnerabilities and inefficiencies. Such challenges often disrupt smooth business operations. Kiteworks acts as a unified platform for cloud storage transfers. It provides error detection, recovery mechanisms, and encryption, streamlining cloud-to-cloud data transfers.

5.

Remote Sales Team Support

Remote sales teams, spread across regions, often face hurdles in accessing vital sales materials. This distribution challenge can impede sales performance. Kiteworks ensures that remote sales teams can securely access and share content regardless of their location. The platform offers encryption, tracking, and compliance features tailored to the needs of sales teams.

6. Legal Documents Sharing

Legal documents carry sensitive information, and an insecure transfer can lead to legal disputes and data breaches. Sharing these documents requires a system that always upholds confidentiality. Kiteworks ensures that legal documents are shared with strong encryption and strict access controls to keep them away from unauthorized prying eyes. The system also allows for tracking and compliance, ensuring all legal standards are met.

7. Protected Health Information (PHI) Transfers

Medical data needs to adhere to strict compliance requirements like HIPAA. Insecure transfers of PHI can jeopardize patient privacy and attract regulatory actions. Kiteworks has designed its platform to simplify and streamline your compliance with healthcare regulations. By offering data security, encryption, and compliance tools, it ensures safe and compliant healthcare data transfers.

8. Automated Software Updates

Delivering product software updates to your customers securely is crucial, as vulnerabilities can lead to system compromises. Updates need to reach end-users without any malicious alterations. Kiteworks offers a secure distribution channel for software updates, ensuring the integrity of each update. With encryption and tracking, businesses can be confident that their software updates reach users securely.

9. Large Media File Sharing

Media files, often bulky, pose challenges during transfers due to their size. Security lapses during such transfers can lead to unauthorized access or data breaches. Kiteworks addresses the challenge of large media file sharing by providing efficient and fast transfer solutions. With encryption and tracking, users can be confident in the secure sharing of their media files. Kiteworks also enables the transfer of very large files, up to 16 TB.

10. Scientific Data Exchange

Scientific data often involves large datasets that require secure storage and transfer mechanisms. A breach in such data can invalidate research results and harm the scientific community. Kiteworks facilitates the secure exchange of scientific data, ensuring data integrity throughout. The platform offers robust encryption, making it a trusted choice for researchers.

Cybersecurity in an Era of National Adversaries

Listen to this Kitecast podcast with Katie Arrington, former CISO for the U.S. DoD and member of the U.S. House of Representatives, to learn about rogue nation-state attacks and what the defense industrial base (DIB) is doing to combat them. The conversation touches on Cybersecurity Maturity Model Certification (CMMC) 2.0 and NIST 800-171.

Listen to the Podcast

11. Biotech Data Exchange

Biotech data contains DNA sequences and other biological information that brings multiple risks. Loss of this intellectual property to a competitor can doom an organization's market position, while privacy regulations for such sensitive personal information can lead to massive fines. Meanwhile, massive file sizes can tempt employees to use insecure transfer methods just to get their jobs done. Kiteworks provides the protection, tracking, and control needed to protect IP and prevent privacy violations.

12. Access and Transfer of Sensitive Government Documents

Federal and national agencies handle highly sensitive documents that require robust security when stored or transferred. Using noncompliant or unauthorized tools can expose these documents to potential breaches or cyber threats. For six consecutive years, Kiteworks has offered a secure file sharing platform that is FedRAMP Authorized for Moderate Level Impact, which is now a requisite for certain federal agencies. Using a hardened virtual appliance that includes security layers, end-to-end encryption, AI anomaly detection, embedded antivirus, WAF, and network firewall capabilities, and integration with advanced security technologies such as ATP, DLP, and CDR, Kiteworks ensures secure file transfer internally and with third parties. Kiteworks also provides features like a dedicated private cloud, encrypted storage, remote wipe capabilities, and continuous monitoring.

Secure File Transfer a Fundamental Capability

No matter the specific drivers, organizations across sectors require protection when sharing sensitive data electronically. By implementing secure, controlled file transfer processes, they gain peace of mind that confidential business information will remain protected without limiting collaboration and workflows. In today's interconnected digital business environment, secure file transfer is a fundamental capability that allows organizations to operate both safely and efficiently.

Kiteworks

www.kiteworks.com

September 2023