COVIANT Software

# YOUR PLAN OF ACTION TO ENSURE FILE TRANSFER SECURITY

Using Diplomat MFT as a solution for file transfer security, HIPAA/HITECH, GDPR and PCI/DSS requirements.

## COVIANT SOFTWARE

Coviant Software is recognized globally and specializes in secure managed file transfer (MFT) solutions. Our **Diplomat MFT** product is trusted by organizations in many markets including healthcare and financial services.

www.coviantsoftware.com

# Contents

# Introduction

The task of keeping sensitive data safe is a major challenge in today's interconnected world. Data must move quickly and efficiently to be of maximum value, and so understanding every step of its journey is essential to security. And because the world still runs on files, securing sensitive data during file transfers is more important than ever. This fact was illustrated when cybercriminals targeted vulnerabilities in the popular managed file transfer (MFT) product MOVEit. The attacks compromised data belonging to the organizations affected directly, and those connected via their digital supply chains. In total, KonBriefing Research says the campaign affected more than **2,600 organizations** and the personal data of **90 million people.**

The challenge for many organizations is that their MFT systems sit at the crossroads of data security and data usability. MFT is their means of fetching business-critical files from where they are stored and delivering them safely to where they need to go. Those systems need to be easy to use and secure, but too often organizations are willing to sacrifice safety for convenience. That is always a bad choice. Instead, IT and security leaders must cooperate to ensure that when investing in and deploying MFT products they are also proactive in developing and executing a comprehensive plan of action for file transfer security to protect valuable data assets.

**Every organization is different, and so every organization's file transfer security plan must be different to meet specific needs. This guide will help you create a plan that is right for your organization by identifying:**

1. Current file transfer capabilities, needs and influences;
2. Common risks to file transfer integrity;
3. Processes essential to secure, reliable file transfers;
4. Features required for executing secure file transfers; and,
5. Steps for maintaining a secure file transfer program.

Ponemon Institute/IBM Security 2023 Cost of a Data Breach Report:

- **$4.45 million** – average cost of a data breach
- **$4.76 million** – average cost of a data breach due to business partner digital supply chain compromise

2023 Verizon Data Breach Investigations Report:

- **74%** – of breaches involve the "human element".
- **43%** – of breaches result from errors of "misdelivery".

# Assessing Your Current Security Measures

Before making any changes, it is essential to evaluate your current file transfer security measures. Use the checklist below to assess your organization's processes and security protocols:

- **Firewalls:** Ensure that your firewalls are properly configured to permit only authorized data traffic. Ensure file transfer administrative dashboards are deployed behind the firewall.
- **Encryption:** Verify that all sensitive files are encrypted during transit and at rest and that file encryption is automated.
- **Access:** Review user access levels and permissions to limit data exposure. Ensure strong passwords are in place and multi-factor authentication is enabled.
- **Auditing:** Monitor and capture all file transfer processes to ensure and affirm compliance, and to support troubleshooting and security audits.
- **Complementary security:** Use a secure, managed file transfer platform that supports process automation to minimize risk and costs of human error, integrates easily with cloud and on-premises systems, and confirm that robust security tools, anti-virus, and anti-malware solutions are in place to detect and prevent malware threats.

"Data is... easier to host and faster to download on the clear web, making it more likely stolen data will be downloaded. Whilst some of these tactics aren't novel, the combination of them and the scale of the [MOVEit] breach was of particular concern for organizations globally."
- **Chris Morgan, senior cyber threat intelligence analyst, ReliaQuest**

"A common thread in these recent attacks, whether the software is deployed on-premises or as a SaaS application, seems to be an internet-facing administration dashboard." **– Gregory Hoffer, CEO, Coviant Software**

"[An] effective audit logging program can be the difference between a low impact security incident which is detected before covered data is stolen or a severe data breach where attackers download large volume of covered data over a prolonged period of time." **– UC Berkeley Information Security Office**

# Identifying Vulnerabilities

Understanding potential vulnerabilities in your file transfer processes is crucial for effective security. Use the checklist below to identify and address weak points:

- **Outdated software:** Update all file transfer software and applications to the latest versions to mitigate known vulnerabilities.
- **Lack of multi-factor authentication:** Implement multi-factor authentication for enhanced user verification.
- **Unencrypted email attachments:** Prohibit the transfer of sensitive information via unencrypted email attachments.
- **Inadequate employee training:** Regularly train employees on secure file transfer best practices to reduce human errors.

"By exploiting unpatched vulnerabilities in the [file transfer appliance], attackers were able to gain access to the files of Accellion's clients from which they exfiltrated a sizable amount of data."

**– "Accellion Reaches $8.1m Data Breach Settlement," Jan. 17, 2022, Infosecurity Magazine**

"Our research shows that simply adding a recovery phone number to your Google Account can block up to 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks that occurred during our investigation."

**– Google, New York University, and University of California, San Diego**

# Building a Robust File Transfer Policy

A well-defined file transfer policy is the foundation of a secure file transfer environment. Use the following steps to create a comprehensive policy:

- **Define acceptable use guidelines:** Clearly outline the appropriate use of file transfer services and restrictions.
- **Identify compliance requirements:** align policies with applicable information security and data privacy regulations.
- **Specify encryption standards:** Establish encryption protocols that align with industry best practices.
- **Determine data retention policies:** Set guidelines for the secure storage and disposal of transferred data.
- **Address mobile device usage:** Outline security measures for file transfers involving mobile devices.
- **Establish incident response procedures:** Develop a clear plan to address and mitigate potential security incidents.

Partial list of information security and data privacy regulations from the U.S.

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley (SOX)
- Fair Credit Reporting Act (FCRA)
- Electronic Communications Privacy Act (ECPA)
- Fifty individual state privacy regimes

Partial list of information security and data privacy regulations from around the world

- General Personal Data Protection Act (LGPD), Brazil
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada
- Consumer Privacy Protection Act (CPPA), Canada
- General Data Protection Regulation (GDPR), European Union
- Digital Operations Resilience Act (DORA), European Union
- Act on the Protection of Personal Information (APPI), Japan
- Financial Instruments and Exchange Law (J-SOX), Japan
- Privacy Act of 2020, New Zealand
- Personal Information Protection Law (PIPL), People's Republic of China
- Cybersecurity Law (CSL), People's Republic of China
- Outbound Data Transfer Security Assessment; People's Republic of China
- Protection of Personal Information Act (POPIA), South Africa
- New Federal Act on Data Protection (nFADP), Switzerland
- Data Protection Act (DPA), UK

# Selecting Secure File Transfer Solutions

Choosing the right file transfer solution is crucial for maintaining the integrity of your data. Evaluate potential vendors or in-house solutions using this checklist:

- **Automation:** Minimize the risk of human error and save staff time by ensuring critical file transfer processes are automated, including file encryption and decryption, error notification, transfer scheduling
- **Encryption protocols and algorithms:** Ensure that the solution supports strong encryption standards (e.g., transport encryption using SFTP, and file encryption using FIPS 140-2 compliant encryption like PGP).
- **Compliance certifications:** Verify that the solution supports compliance with relevant regulations and industry standards (e.g., GDPR, HIPAA/HITECH, PCI DSS, ISO 27001).
- **Integration with existing systems:** Confirm that the solution can seamlessly integrate with your current infrastructure, including on-premises systems and cloud services (AWS, Google Cloud, Azure, etc.).
- **Scalability and performance:** Choose a solution that can handle your organization's current and future file transfer needs, including large files and robust concurrent scheduling with limitless capacity.
- **Auditability:** Ensure every step of your file transfer process is logged and captured automatically to prove compliance and to accelerate troubleshooting in the event of an error.
- **Multifactor authentication (MFA):** Restrict administration and user privileges based on role and need, and employ multifactor authentication to ensure security and compliance.
- **Technical Support:** Choose a managed file transfer vendor that has a track record of product improvement and of delivering excellent customer support.
- **Secure-by-design:** From architecture to configuration and deployment, ensure your MFT solution supports security best practices, minimizes risk human error, and is not vulnerable to attacks targeting MFT software.

# Educating Employees and Raising Awareness

Once you've chosen the secure, managed file transfer solution that is right for your organization, you can increase the value of your investment—and improve your data security posture—by employing additional strategies to educate and raise awareness among your employees:

- **Training:** Organize periodic training sessions to educate employees about file transfer security best practices.
- **Communication:** Regularly communicate security tips and reminders to reinforce good habits and digital hygiene.
- **Culture:** Create a culture where employees feel comfortable reporting potential security threats and suspicious activities.

COVIANT Software

Securing file transfers is an ongoing process that demands attention, education, and proactive measures. By following the plan of action outlined in this whitepaper, you can enhance your organization's file transfer security and safeguard your sensitive information from potential mishaps and cyber threats. Remember, a secure file transfer environment is not just a goal; it's an ongoing commitment to protect your valuable data and maintain the trust of your customers and partners.

If you'd like more information about how Coviant Software can help, please contact us for more information. Our Diplomat MFT family of secure managed file transfer products is trusted by respected organizations in healthcare, financial services, retail, manufacturing, logistics, government, legal, and other industries. Our pricing is ethical and transparent, and our customer support is rated highest in our industry.

**Phone:** +1 (210) 985-0985
**Phone:** +44 20 3970 9742 (UK)
**Email:** info@coviantsoftware.com

**Coviant Software LLC**
5804 Babcock Rd, #151
San Antonio, TX 78240