JSCAPE by Redwood

How to secure file transfers in the breach era

5 critical signs it's time to assess your provider
and how to find one committed to protecting your data

Redwood

Contents

Are your file transfers leaving you vulnerable? 1

5 warning signs you need a new provider 2

Data exposure, penalties and headlines: The real consequences 3

What to look for when vetting a new file transfer provider 4

Security features and certifications: The non-negotiables 4

Readiness for any eventuality 4

Zero-day response plans 5

A track record of accountability 5

Checklist for committing to a new MFT provider 6

Switch to peace of mind: How JSCAPE by Redwood is different 7

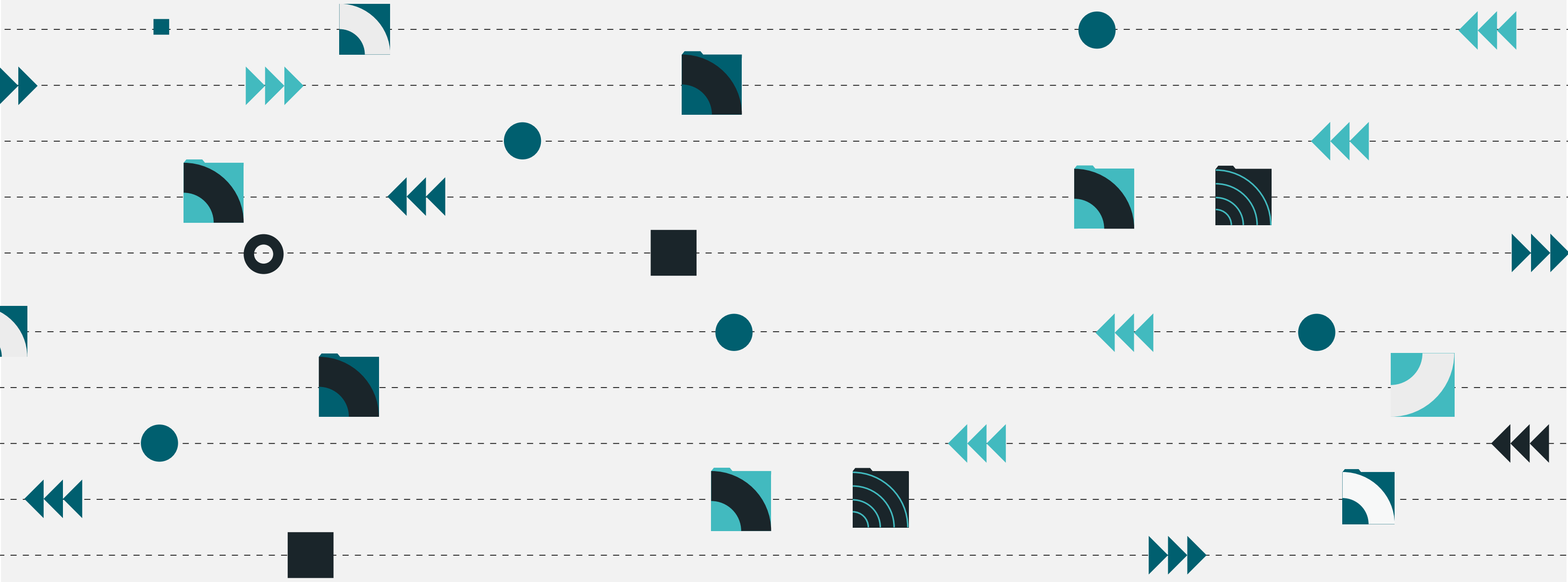
Are your file transfers leaving you vulnerable?

There's nothing worse than paying for a service and feeling like you're not reaping its full value. If that service is as critical as business file transfer, the stakes are indescribably high.

Managed file transfer (MFT) systems are essential for secure data exchange. If they don't offer the level of security or support you need, your sensitive data (and that of your trading partners, employees and customers) could be exposed. That isn't a risk any business leader today should be willing to take.

The consequences of inadequate data protection are severe. A breach in your file transfer processes doesn't just entail disrupting operations. For many organizations, it means financial loss, regulatory penalties and irreparable damage to reputations.

Staying out of the news means staying ahead of threats and anticipating vulnerabilities before they do harm. If you're unsure whether your current MFT solution delivers the security your business requires, it's time to reassess.



5 warning signs you need a new provider

Even if you have yet to experience a security breach, there could be indications that you need to start looking for another MFT solution.

01. Stagnant security practices

One of the clearest signs that a provider may be inadequate is their inattention to evolving cybersecurity practices. A strong security posture requires constantly anticipating new digital threats. If your MFT provider doesn't regularly release updates, enhance security features or conduct penetration testing, look elsewhere.

02. Inadequate support

Around-the-clock, follow-the-sun support is a must because data doesn't rest. Lack of 24/7 support is a glaring, yet unfortunately common, issue. Without immediate access to a support team equipped to handle security incidents, you could be left to manage a crisis on your own. Your IT staff might need to work long hours to diagnose the root cause of a failed file transfer, and the delay could lead to bottlenecks in other departments. Worst case, your clients or partners who rely on the data could notice and become frustrated. If your organization is large and global, this could be particularly challenging.

03. Inaccurate or incomplete communications

A transparent provider should proactively communicate about threats, vulnerabilities and how they're being addressed, as well as take accountability when things go wrong. Failing to provide you with clear and accurate updates during a breach can mean preventing your internal teams from effectively responding. You deserve complete details about the extent of data compromise. Any ambiguity can increase your damage control costs.

04. Delayed response

Time is of the essence when you identify a vulnerability or experience a breach. Rapid detection and swift remediation are critical in minimizing damage, while delayed action suggests inadequate systems or support. Your business and data could be at risk for longer if your first line of defense fails.

> If your current MFT provider lags in detecting and addressing issues, **it's a red flag.**

05. Lack of root-cause analysis

After a breach, it's not enough to fix the immediate issue. Understanding the root cause is essential to preventing future incidents. If your provider doesn't conduct a thorough post-incident analysis to review logs and audit trails, examine endpoint security and trace the entry point, your business could be susceptible to repeated attacks. Knowing exactly how and why a breach occurred gives you an opportunity to adjust your defenses.

Data exposure, penalties and headlines: The real consequences

Like many difficult things in life, it's easy to keep data security incidents at arm's length when they're not happening to us. The following stories make data breaches and their potentially devastating outcomes more real.

Fortra GoAnywhere hack compromises PII of nearly 1 million people

Source: The HIPAA Journal

Fortra's GoAnywhere MFT solution experienced a major attack due to a zero-day vulnerability. Despite the fact that 130 companies, including HIPAA-covered entities, were impacted and the personally identifiable information of at least 964,300 individuals was leaked, one impacted company claims Fortra waited five days to notify them and refused to notify individuals and regulators. The United States Department of Health and Human Services' Office of Civil Rights is still investigating.

Global ransomware group attacks MOVEit due to patch delay

Source: NCC Group

In one of the most significant data breach incidents in recent history, the Cl0p ransomware group exploited a vulnerability in the file transfer platform MOVEit. The company's slow patching response exacerbated the damage incurred to over 2,500 organizations and over 90 million people worldwide.

Zero-day exploits rapidly target CrushFTP

Source: Cybersecurity Dive

Crush FTP experienced a significant data breach when a zero-day vulnerability allowed remote attackers to bypass its sandbox and read sensitive files. While the company released patches and encouraged updating on the day it was reported, many of its customers were affected.

What to look for when vetting a new file transfer provider

Simply ticking boxes won't do when you're looking for a partner as committed to protecting your data as you are. Let's break down the signals of a superior MFT provider.

Security features and certifications: The non-negotiables

If security isn't the backbone of your MFT provider's offering, you've already lost the game. Since the goal of this type of software is to safeguard your data, they should have industry-recognized certifications. These aren't just badges — they're proof that the provider has undergone rigorous testing to meet the highest security standards and isn't cutting corners.

ISO 27001: An international standard that confirms adherence to a comprehensive set of information security management practices

SOC 2: A compliance framework that focuses on how well a company provides security, availability, processing integrity, confidentiality and privacy

These are just part of the picture. It's important also to ascertain whether they offer encryption protocols beyond the basics and are conducting regular penetration testing to uncover vulnerabilities before they become problems.

Ask how often they undergo third-party security audits and whether they can share the results. A truly transparent partner will offer this information without hesitation.

Readiness for any eventuality

Cyber threats are always changing. The people you pay to keep your data safe should be forward-thinking. That means they should have an up-to-date feature roadmap that shows their commitment to staying ahead of emerging threats. Use this list of questions to determine whether their efforts in this area are enough:

01. Are they proactively introducing new security features like multi-factor authentication (MFA) or advanced threat detection algorithms?

02. What specific security innovations have they rolled out in the past 12 months?

03. How often do they revise their roadmap to include the latest security standards?

04. Do they regularly release software updates to address new vulnerabilities?

Request a copy of their feature roadmap and confirm whether they include security enhancements in each release.

Zero-day response plans

Zero-day vulnerabilities are the ones you don't see coming. Thus, they're the greatest test of a provider's capabilities. Every MFT provider should have clear policies in place for addressing vulnerabilities as soon as they're discovered, including timely patching, communication and team mobilization. If they can't give you a concrete answer about how they handle zero-day incidents, it's a sign they won't be the most attentive when it matters most.

! **Have the provider walk you through a real-life example of how they've handled a zero-day vulnerability in the past.**

A track record of accountability

It's one thing for a provider to claim they're secure, and it's another for them to prove it. Dig into a potential provider's history of handling security incidents. If they've experienced a breach before, how did they manage it? How long did it take them to notify customers, and did they patch vulnerabilities quickly?

You shouldn't be met with vague or evasive responses about past breaches, as you deserve to partner with a company that owns up to issues and works diligently to correct them. Anything less puts your business at risk.

! **Seek out case studies or customer testimonials that detail how they handled a past breach, and observe whether your sales rep is willing and able to share lessons learned.**

The value of your InfoSec team

Your information security team is your greatest asset when it comes to evaluating MFT platforms and providers. They possess the technical expertise to know whether a given provider's security capabilities will align with your organization's needs. With their involvement in demos and vendor discussions, you'll ask the right questions and avoid overlooking key points in your business case.

Checklist for committing to a new MFT provider

Use this list to guide your search and interactions with vendors.

Create a shortlist:

□ Identify providers that can meet most of your organization’s security and scalability requirements on the timelines you need.

Engage internal stakeholders:

□ Consult with your infosec and IT teams to understand the mission-critical features you’re looking for.

Review provider security:

□ Look for certifications like ISO 27001 and SOC 2, regular penetration testing and strong encryption protocols.

Research customer feedback:

□ Check reputable websites like G2, Capterra and Gartner for reviews and experiences from current and past customers.

Assess roadmap and innovation:

□ Ensure the provider regularly updates their platform with new security features and enhancements.

Demo the product:

□ Schedule demos to see the product in action and bring along your infosec team members to ask security-specific questions.

Evaluate vulnerability handling:

□ Ask how they’ve handled recent incidents or vulnerability discoveries, and be skeptical if they claim to have had none.

Verify investment in security:

□ Investigate whether the provider can demonstrate ongoing investment in infrastructure, threat management and proactive security measures.

Balance features and security:

□ Weigh your top features against a provider’s security posture to make the most informed decision.

Switch to peace of mind:

How JSCAPE by Redwood is different

Bad actors will always try to find ways to steal what's most valuable to people, especially successful businesses. And data is akin to currency today. Therefore, data breaches are inevitable.

Since these threats will always exist and become more sophisticated over time, staying with an MFT provider that has failed to protect your organization — or worse, been involved in a high-profile breach — can have catastrophic consequences.

With all the innocence and trust of children looking to a parental figure, your customers and employees depend on your leadership team to make the best decision about who handles your data. You wouldn't choose a childcare provider whose history or practices you doubted, nor should you put precious data in the hands of just any file transfer company.

Furthermore, if you're in an industry with strict regulations, you have no choice but to opt for the most secure technologies and partners.

By choosing a provider with a proven commitment to security and a reputation for truly supporting its customers, you and your team can leave worry behind and focus on growth and innovation.

JSCAPE by Redwood takes data protection seriously.

If you're in an industry with **strict regulations,** you have no choice but to opt for the most **secure technologies** and **partners.**

> JSCAPE continuously evolves with each upgrade, providing enhanced security features that customers can leverage to further reduce their risk. Its feature roadmap offers a proactive approach to evolving digital threats, emphasizing ongoing enhancement and adherence to the latest security standards.
>
> The JSCAPE team acknowledges the dynamic nature of security, ensuring continuous innovation and vigilance and keeping defenses strong against evolving threats and vulnerabilities. We look at the data we are protecting, the threat landscape and the likelihood of an adverse situation to assess risk and then apply controls to mitigate risk and reduce the impact for our customers.

Andy Sharma

Redwood Software's VP of Information Technology and Security

Redwood's approach to information security is first-rate. It includes:

A thorough approach to product security

Manual PEN Test (MAST)	Architecture review	Secure SDLC	SecOps platform	Ongoing assessments
• Zero critical and high vulnerabilities after re-test	• 90% of product vulnerabilities found and remediated before reaching production	• 90% of critical remediated in less than seven days	• Critical and high incidents resolved in seven days	• 100% of existing certifications maintained • 95% of annual security trainings completed on time

A robust framework for application security testing

01. **Penetration (PEN) Testing** →

- Conducted by a third party annually
- Followed by re-test if issues found
- **Expectation:** Clean report

02. **Static Application Security Testing (SAST)** →

- Conducted at will by developers
- Required at least once every two weeks
- **Expectation:** Zero critical or high-severity issues

03. **Software Composition Analysis (SCA)** →

- Conducted at will by developers
- Required at least once every two weeks
- **Expectation:** Zero critical or high-severity issues

04. **Dynamic Application Security Testing (DAST)** →

- Conducted by InfoSec team before each release
- Required at least once every quarter
- **Expectation:** Zero critical or high-severity issues

Exhaustive annual PEN testing that covers four areas

External	Internal	Social Engineering	Product
• **Discover public** corporate footprint (aside from the disclosed IPs) • Perform **scanning** for potential vulnerable attack vectors for exploitation • Develop and execute an attack plan to **gain access** to systems via vulnerabilities and password cracking	• **Discover targets** using passive means (FTP, Telnet, Clear Text Passwords) • Perform **network surveying** and services identification for potential vulnerable attack vectors for exploitation • **Gain access** to systems via vulnerabilities and password cracking	• **Phishing** AND **vishing** (targeted as well as un-targeted campaigns) • Reconnaissance to **gather information** about the organization • **Tech testing** (spoof, attachment filtering, endpoint protection • Harvest credentials and try to **exploit user systems**	• **Attack surface** enumeration (identify app functionality and key system components) • **Manual and automated fault injection** (manually or using tools to inject malicious inputs) • **Vulnerability testing** (identify vulnerabilities in components) • Exploitation and validation (**attempt to exploit** vulnerabilities)

Comprehensive SAST, DAST and SCA coverage

SAST

VERACODE

Frequency

- Weekly

DAST

RAPID7

Insight AppSec

Frequency

- Before each release
- Quarterly (if not release)

SCA

VERACODE

Frequency

- Weekly

If you've identified warning signs that your data may be at risk, there's no time to waste. Don't wait to find a provider with a track record of commitment to industry-leading security.

Demo JSCAPE today

Explore the power of enterprise-grade MFT, offered as SaaS and upheld by Redwood's world-class support.