FORTRA

Taking File Transfer Security to Another Level

"Sharing data is now simpler than ever, but it's also less secure because of the widespread use of collaboration tools and cloud-based file-sharing services. BYOD, remote workers, and work-from-anywhere personnel exacerbate the security issue."

ANASTASIOS ARAMPATZIS,
Information Security Content at Bora

As companies move to adopt zero trust architecture, the security of files and the confidential information they contain is top of mind. As security expert Anastasios Arampatzis states, "Sharing data is now simpler than ever, but it's also less secure because of the widespread use of collaboration tools and cloud-based file-sharing services. BYOD, remote workers, and work-from-anywhere personnel exacerbate the security issue." PGP (Pretty Good Privacy) is still in use and effective in many capacities, but as file transfers travel over increasingly complex (and possibly unsecured) networks, more might be needed.

Enterprises must be compliant with international and domestic data privacy and security standards such as HIPAA, PCI DSS, FISMA, and GDPR. Purchase orders, payment transactions, audit files, and sensitive documents containing intellectual property are exchanged daily. They are essential to making a business run. However, in an effort to comply with unrelenting business demands, many organizations fail to take proper note of how to secure this data. What was meant to provide a business boost becomes a liability. Headline-making data breaches, million-dollar settlements, and ransom payments ensue.

Consequently, the task of securely sending large amounts of business-critical data in a timely fashion poses a significant challenge to most enterprises today. As Anastasios sums up, "Secure file transfers must be given top priority by organizations since company files frequently contain confidential, proprietary, and sensitive information." Digital Rights Management (DRM) supports zero trust tolerance by giving you full control over your data, allowing you to retain the rights to your files – and the information they contain – no matter whose hands they fall into.

WHAT IS MFT AND HOW DOES IT WORK?

Managed File Transfer (MFT) addresses the issue of exchanging files over widening networks. It automates and transfers data across your systems, networks, applications, cloud environments, and trading partners from a central user interface, putting an overwhelming amount of file security needs within your control and safeguarding your data in transit and at rest.

Most secure File Transfer Protocols (FTPs) rely on encryption, such as SFTP, FTPS, HTTPS, and AS2. MFT encrypts data at rest and in motion, provides strong authentication methods, and secures against unauthorized data modifications, protecting sensitive, proprietary, and often compliance-regulated data. Chris Bailey, Senior Product Manager at HelpSystems, noted "MFT generally has three use cases: machine-to-machine, machine-to-person, or person-to-person. Machine-to-machine is incredibly potent. It gives you an orchestration system that can grab files from one location, bring them into another system, perform an action on those files, and then push them to another location."

While relying heavily on SFTP, MFT goes far beyond an SFTP automation tool. It not only offers file transfer automation, but reporting, compliance, and security functionalities that far outstrip any of its individual encryption protocols. Because of its ability to combine multiple parts of the file transfer process – security, automation, auditing, troubleshooting, parsing out data and ETL files – in one interface, MFT is widely in use and considered the industry standard for secure file sharing.

However, the industry is changing. "We're getting to the point where simply sending confidential information with basic encryption is no longer an acceptable method," states Ian Thornton-Trump, CISO at Cyjax. "It's an area where we need to make sure that we have that visibility, automation, and orchestration." Providing visibility in secure file transfer is a key component of a file management method that compliments and completes MFT: **Digital Rights Management (DRM).**

"We're getting to the point where simply sending confidential information with basic encryption is no longer an acceptable method."

IAN THORNTON-TRUMP
CISO at Cyjax

WHAT IS DRM AND HOW DOES IT WORK?

"If you're in a boardroom and you're passing around printed financial information, the executives are aware of the sensitivity of the information, so they protect it," Bailey explained. "However, with the emergence of remote work, much of that information needed to be shared digitally." So, while Digital Rights Management (DRM) was originally designed to protect the copyrights of digital media, its utility has now established it as a data security solution.

"DRM gives the sender the ability to control what the recipient can and can't do with the data," states Scott Messick, Cybersecurity Sales Engineer at HelpSystems. "The sender has the ability at any point in time to modify the permissions on the file." DRM places data ownership in the hands of the sender. It enables you to control your sensitive data as it travels by setting file expiration dates, limits access to specified IP addresses only, and prevents users from editing, saving, or sharing your content.

Rather than making the data impossible to catch, it makes it impossible to use. Bill Stubbles, a Solutions Engineer at HelpSystems, explains that "A DRM solution integrates data protection and access control, and allows levels of protection that a conventional file encryption solution such as PGP simply cannot match. With PGP, once a file you send out has been decrypted, it is completely outside of your control. A DRM solution allows you to apply and revoke rights management to your files at any time."

As the workplace becomes increasingly collaborative, it's more important than ever to maintain security as you reach for interoperability.

"DRM gives the sender the ability to control what the recipient can and can't do with the data. The sender has the ability at any point in time to modify the permissions on the file."

SCOTT MESSICK
Cyber Security Sales Engineer

INDUSTRY-SPECIFIC CHALLENGES OF **MFT**

Relying on MFT alone can uncover some inherent challenges. While mostly secure, instances of accidental file sharing do happen, and in those cases, additional technology may be needed to fill the gap.

"I was working with a company that was bidding on an important project," shared Ayman Wassif, Principal Software Architect at HelpSystems. "One of the teams was having trouble answering a vague technical question on a Request for Proposal (RFP) and asked a third party for clarification. The problem was that the third party was bidding on the same project. The third party notified the client that information regarding their RFP had been leaked and the first company was disqualified from the bid." While a seemingly insignificant error, the mistake cost the company millions of dollars in a lost contract. Noted Wassif, "If they used a DRM solution to protect that information, even if the competitor got access to the file, they would not have been able to open it."

Specific industries face unique difficulties in implementing an MFT **solution** without the additional protections of DRM.

INDUSTRY-SPECIFIC CHALLENGES OF MFT

Entertainment. While every precaution was taken to prevent leaks of HBO's popular *Game of Thrones,* leaks inevitably do occur. Delivering the show to streaming services and cable providers worldwide left it vulnerable to pirating and other breaches, especially as HBO did not retain full control of the distribution process. As one network insider explained, "When you have to deliver it to 180-something markets, it's just not going to be 100 percent secure." MFT is limited in that without DRM, it can only ensure the safety of the files up through delivery and senders must trust that whoever has the decryption key is the intended recipient. However, once the file is opened, there are no limits on what can be done with it and piracy may occur. And decryption keys can always be stolen. With DRM, protection rests with the data itself, not the transfer method. DRM prevents piracy by attaching rights set by the owner of the intellectual property.

Hospitality. You don't need to be sending files over the ether to have files in transit. One recent social engineering attack resulted in a compromised physical system and 20GB of stolen data from a popular hotel chain. Implementing protections on the files themselves, coupled with strict access controls, may have prevented unauthorized use of the files, by attacker or employee.

Healthcare. What was referred to as one of the biggest healthcare breaches of 2021 resulted, ironically, from its connection to an FTP service. Zero-day vulnerabilities were exploited in the vendor's 20-year-old FTP platform, allowing attackers to deploy malicious web shell DEWMODE, pivot through the network, steal valuable data, and affect over 3.51 million healthcare patients worldwide. Sensitive, HIPAA-regulated data was exfiltrated from the over 100 affected healthcare companies and posted on a leak site.

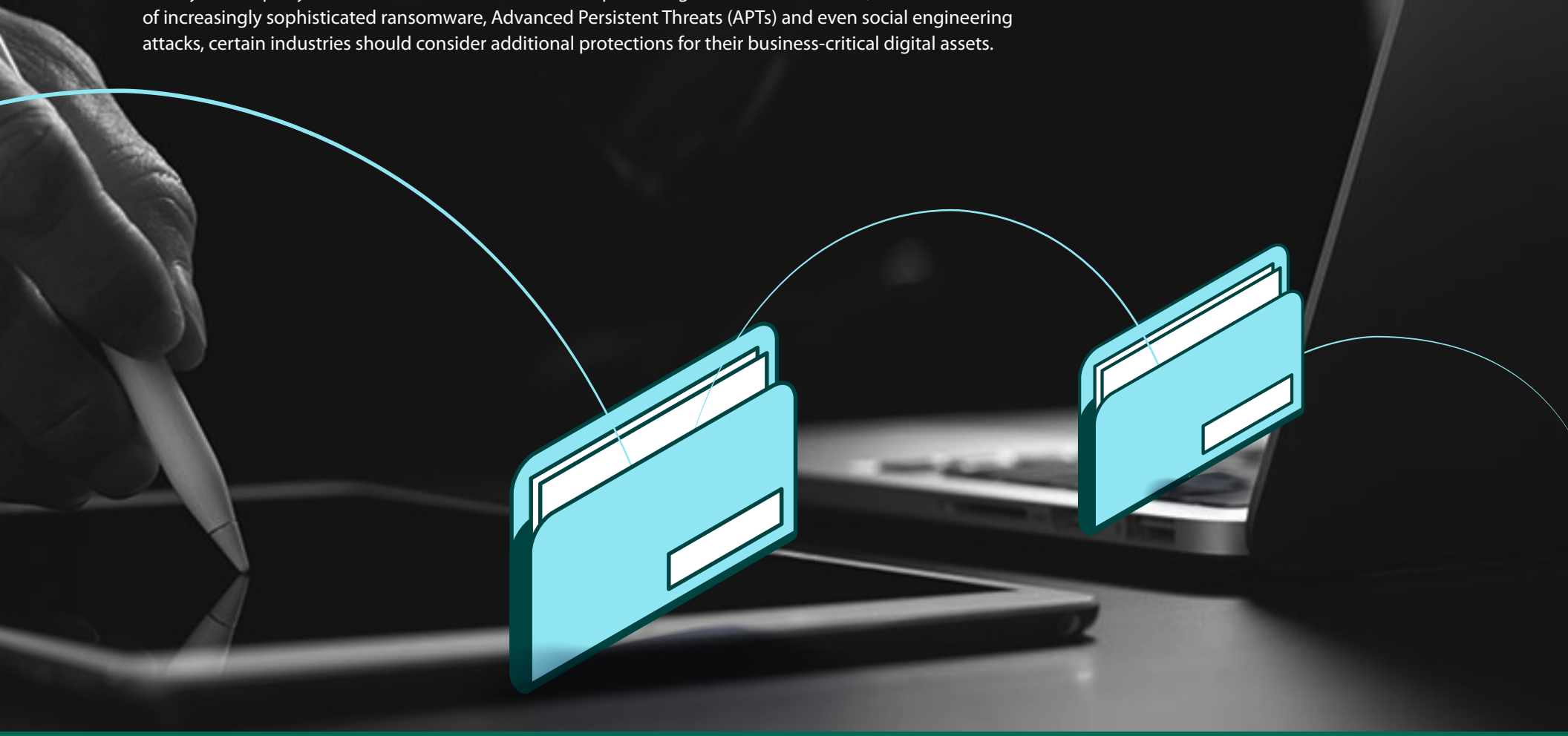
Finance. The notable 2017 Equifax breach made headlines when an exploited vulnerability, an expired certificate and an unsegmented network, allowed malicious hackers to exfiltrate data undetected for months. Over 143 million Americans were affected, their usernames and passwords stolen, and their privileges on financial accounts escalated and abused. Equifax lost nearly $4 billion USD in the crisis. The breach occurred as a combination of unsafe practices, not all of which MFT could have prevented. For that reason, a solution that defends by file may be the key to helping ensure full data protection.

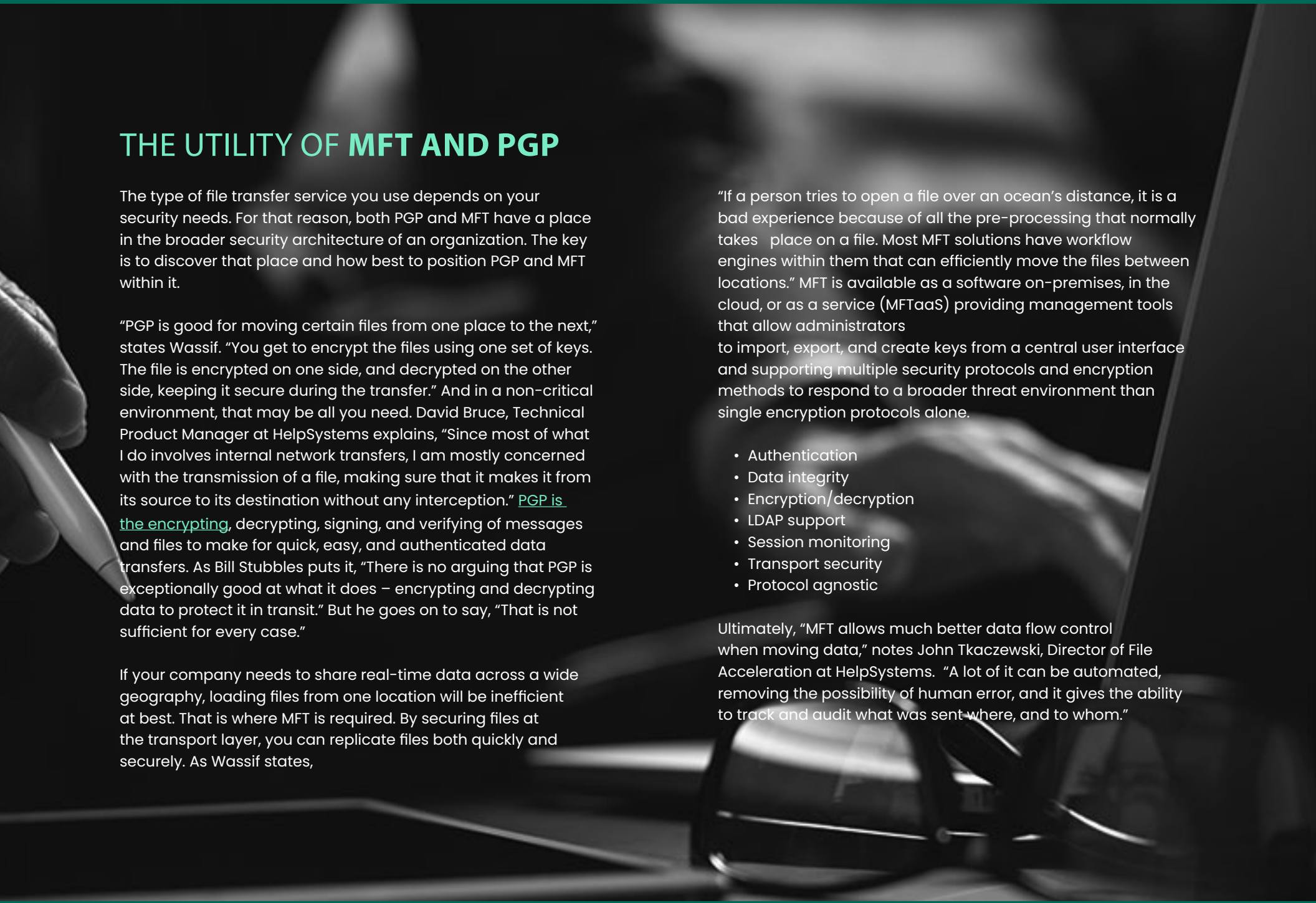
To further illustrate the point, Ayman Wassif shares another workplace encounter in which unsecure data practices could have led to dire financial consequences. "I was working with a large financial institution that held a lot of proprietary information about their investment approach, and technical algorithms for assessing and responding to market movements," Wassif shares. "When we scanned the public shared folders on their system, we discovered that all their intellectual property was on those shared drives with nothing protecting them at all. This was the code that gave the company its competitive advantage in the market. In the hands of a competitor, this could have meant absolute ruin for this organization."

To compound the problem, employees were sharing pirated movies and storing them on the company-shared folders, opening the firm up to risks, not only from copyright infringement but possible embedded malware. In this instance, the protective reach of MFT only goes so far. While it does allow you to encrypt files at rest, if an unauthorized attacker infiltrates the network or comes into possession of the decryption key, the data is no longer protected. With DRM, an additional layer of security can be applied which grants access rights only to those designated by the file owner, rendering the data inaccessible to anyone else, regardless of where it is stored.

INDUSTRY-SPECIFIC CHALLENGES OF **MFT**

Sometimes there are certain assets that need to be secured beyond what MFT alone can protect. In 2019, a file-sharing service admitted inadvertently sending emails to the wrong recipients. As Scott Messick stated, "Once a file you send out has been decrypted, it is completely outside of your control." The file-sharing service had to cancel the links in order to prevent unauthorized access of the data. Securing files at rest, in transit, and by a third-party is a viable and valuable method for protecting sensitive information, but with the advent of increasingly sophisticated ransomware, Advanced Persistent Threats (APTs) and even social engineering attacks, certain industries should consider additional protections for their business-critical digital assets.





THE UTILITY OF **MFT AND PGP**

The type of file transfer service you use depends on your security needs. For that reason, both PGP and MFT have a place in the broader security architecture of an organization. The key is to discover that place and how best to position PGP and MFT within it.

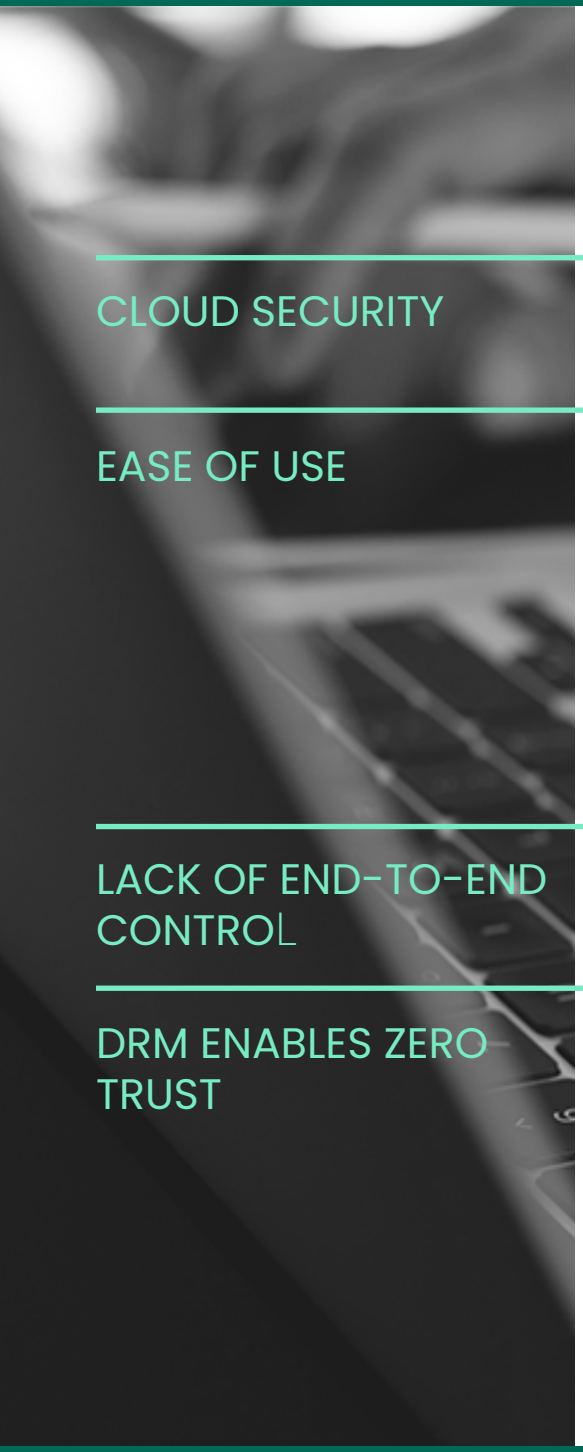
"PGP is good for moving certain files from one place to the next," states Wassif. "You get to encrypt the files using one set of keys. The file is encrypted on one side, and decrypted on the other side, keeping it secure during the transfer." And in a non-critical environment, that may be all you need. David Bruce, Technical Product Manager at HelpSystems explains, "Since most of what I do involves internal network transfers, I am mostly concerned with the transmission of a file, making sure that it makes it from its source to its destination without any interception." PGP is the encrypting, decrypting, signing, and verifying of messages and files to make for quick, easy, and authenticated data transfers. As Bill Stubbles puts it, "There is no arguing that PGP is exceptionally good at what it does – encrypting and decrypting data to protect it in transit." But he goes on to say, "That is not sufficient for every case."

If your company needs to share real-time data across a wide geography, loading files from one location will be inefficient at best. That is where MFT is required. By securing files at the transport layer, you can replicate files both quickly and securely. As Wassif states,

"If a person tries to open a file over an ocean's distance, it is a bad experience because of all the pre-processing that normally takes place on a file. Most MFT solutions have workflow engines within them that can efficiently move the files between locations." MFT is available as a software on-premises, in the cloud, or as a service (MFTaaS) providing management tools that allow administrators
to import, export, and create keys from a central user interface and supporting multiple security protocols and encryption methods to respond to a broader threat environment than single encryption protocols alone.

- Authentication
- Data integrity
- Encryption/decryption
- LDAP support
- Session monitoring
- Transport security
- Protocol agnostic

Ultimately, "MFT allows much better data flow control when moving data," notes John Tkaczewski, Director of File Acceleration at HelpSystems. "A lot of it can be automated, removing the possibility of human error, and it gives the ability to track and audit what was sent where, and to whom."



THE DRAWBACKS OF **MFT AND PGP**

While a good option for securing files in transit and at rest, MFT and PGP have their limitations.

CLOUD SECURITY

As Tyler Reguly, Senior Manager at HelpSystems, puts it, the limitations of current file transfer methods really become apparent in "the cloud services that so many people use for file storage. With many of the publicly available offerings, the sharing mechanism isn't as secure as it could be."

EASE OF USE

While he agrees that the single biggest challenge with current file transfer methods is cloud security, Craig Smith, Security Engineer, HelpSystems, suggests that "The second biggest limitation is that when transferring sensitive files, you have to use a secondary method to encrypt them...this is a clunky process." While all files are encrypted in transit when you use a secure protocol, PGP acts as a secondary layer of security to ensure that only the person with the Private PGP key can decrypt the message once received. Alone, this requires manual PGP encryption over every file you send. To do that for every file, every time, requires standardized, automated policies, and a company-wide commitment to enforcing security best practices. Nigel Sampson, Cybersecurity leader at IDG, opined that "The limitations surrounding the current procedures regarding sending sensitive files are mainly around education. Ensuring that sensitive files are encrypted when sent externally requires constant education and training."

LACK OF END-TO-END CONTROL

When a file is sent using PGP, the sender no longer has access to, or control of, what happens to it. Says Stubbles, "This is where DRM outshines the conventional encryption methods like PGP. With DRM, you can maintain control of the data no matter where it travels after it leaves your system."

DRM ENABLES ZERO TRUST

Lastly, one of the primary setbacks of the two methodologies is an inability to completely support zero-trust. As companies move to a zero-trust model, architecture might be secured, but outdated or insufficient file transfer methods may be the weakest link. With DRM, permissions allow a third party to access a file or document for a certain amount of time, or with certain privileges only. The sender retains full control. Permissions can be both enabled and revoked, allowing you to maintain full ownership even after the data has been delivered. As Wassif noted, "Even a print screen can be blocked."

When it comes to business transactions, a company can secure all proprietary documents until the deal is closed. Then, Bailey states, "The company can remove the entitlements to their work. DRM enables an organization to extend its zero-trust profile." He concludes, "This is a powerful protection mechanism."

DRM TODAY

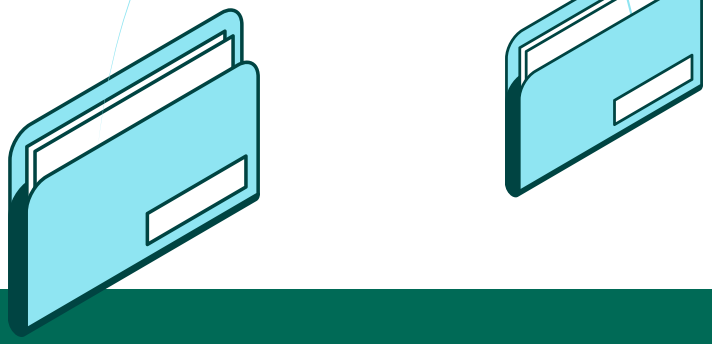
A major inhibitor of DRM previously was that, although useful, it was difficult to use. Because some software manufacturers restricted DRM use to their own proprietary system, DRM developed a reputation for being cumbersome. As David Bruce, Technical Product Manager at Tripwire noted, "if you make the process difficult for users, they're likely to try and subvert that and find a way around it."

Today, the landscape has changed. The need for DRM technology has become so ubiquitous that if you use DRM today, you'll find a significantly more enjoyable user experience that is not only simpler but more widely used. As the industry moves towards an openly adopted, "native" DRM standard, the interface will continue to improve.

As it does, organizations will increasingly be able to capitalize on its benefits:

- **Full file ownership.** Retain full control of permissions to your file before you send it and the ability to adjust them after it's sent.
- **Anywhere file protection.** If a file is stored insecurely or stolen in transit, the security stays with the data, not the transfer system.
- **Secure file transfer in the cloud.** Transfer documents, data, and proprietary information quickly and securely in the cloud, scaling securely at your rate.
- **Maintain data security compliance.** Be compliant with data security regulations in any environment. "As enterprises rushed to adopt cloud, vast portions of the data lakes inadvertently were also moved to cloud," explains Stuart Coulson, a manager of business engagement. "Then came GDPR and the rise of the laws, regulations, and compliances that focused the attention on who could access data, how, and when." Using DRM will allow you to stay on the right side of data privacy laws with rights-protected files and control over how they are shared.
- **Protect against accidental file sharing.** If your sensitive documents end up in the wrong hands, a bad actor has just wasted their time. "Files that are protected with DRM have that extra layer of security," states Tkaczewski, "where you can decide who can see inside of the file. If you mistakenly send it to the wrong person, that person is not going to be able to access the data."
- **Do remote work safely**. If an employee is working remotely, on an unsecured network or machine, no additional software is necessary when opening files. The employee can work in their browser with a fully encrypted file.

DRM enables you to create a seamless workflow that allows you to customize data to any compliance standards as it enters. From an end-user standpoint, it doesn't create friction; it integrates. "The process remains very efficient. There are no noticeable key exchange processes to slow everything down," notes Tkaczewski. Current DRM tools are designed to provide access control and integrated data protection unmatched by any other encryption protocol in use today.



THERE IS A PLACE **FOR MFT AND DRM,** TOGETHER

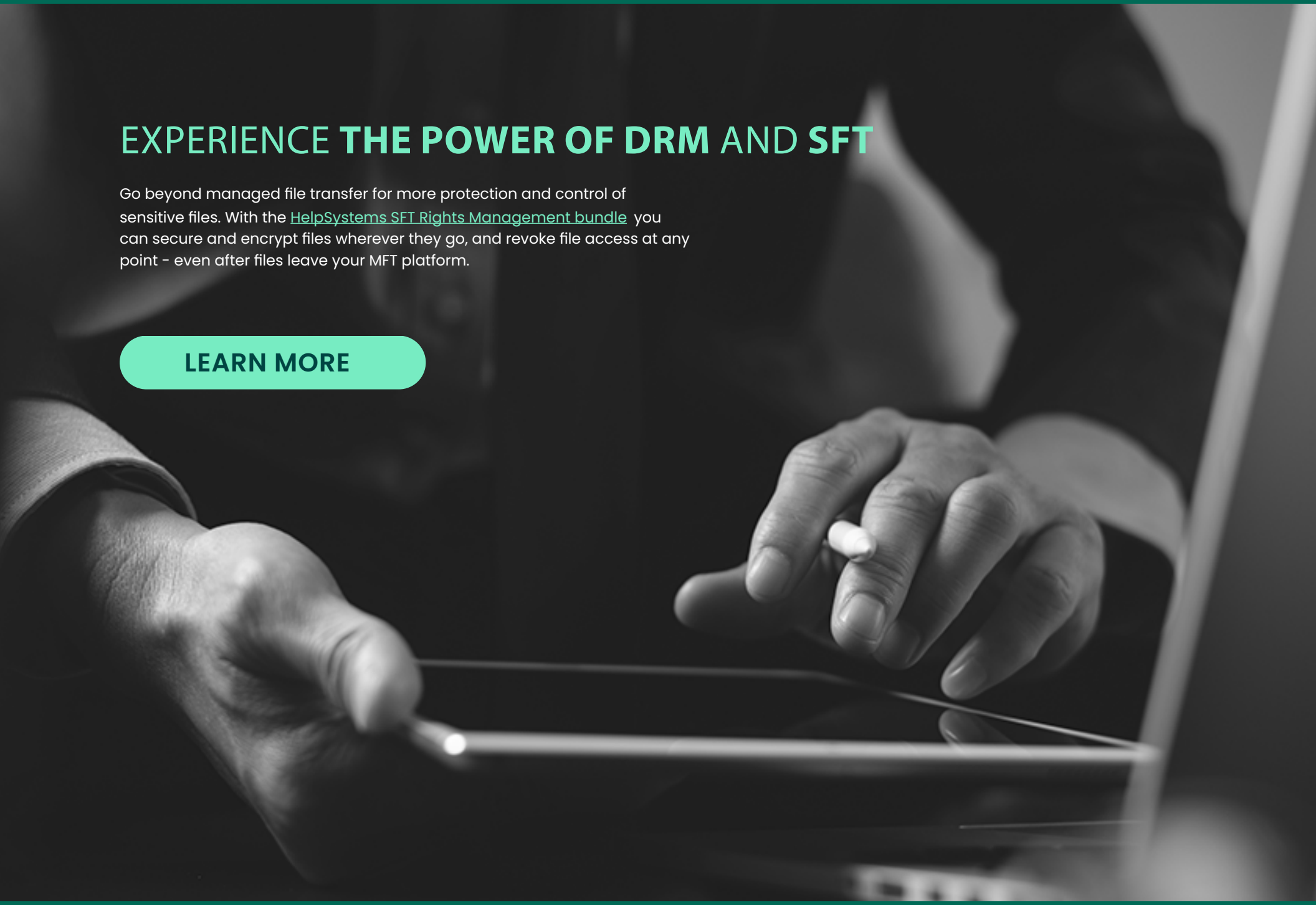
DRM is a solution that more companies should be, and will be, adopting. Combined with MFT, DRM can leverage its full capabilities to support a zero-trust strategy, enabling strict access controls on a per-file basis while simultaneously being able to handle the demands of multiple large transfers. DRM wraps an access control list around the file that specifies role-based permissions while still allowing users to open the file easily in Word or Excel. Then, MFT compliments the solution by enabling the same strict access controls to be applied to any file within the MFT platform – no additional software or protections necessary.

Selecting the right technologies is paramount to achieving full data security and privacy. Why not choose both? Together, MFT and DRM create a winning combination that can do:

1. **Secure folder collaboration**. MFT secures your folders with user access lists, and DRM dictates who can do what once the files inside are downloaded.
2. **Automate document distribution.** MFT can automatically monitor for files that need additional protection, and DRM can apply protective policies before they leave your organization.
3. **Secure emails.** Use MFT to enable large file sharing directly from a browser, and DRM can add encryption and access policies to each.

On a broader scope, an MFT/DRM approach makes business sense. While MFT does a lot to ensure safe passage of proprietary data, only DRM can follow the file beyond the endpoint, attaching policies, permissions, expiration dates, and regulation-compliant security measures to the files themselves. Bailey says, "Up at the C-level, the DRM and MFT solutions address relevant business concerns, such as protecting intellectual property, while also meeting regulatory requirements." Failure to use the correct technical and logical protocols can result in compromised data, reputational damage, and potentially millions of dollars lost in assets, damages, or ransomware payments.

In our current threat environment, the increasing sophistication and ingenuity of attackers demands that enterprise data be encrypted at rest and in transit, be compliant with data privacy and security standards, and be transferred when and as needed, securely. Combining MFT and DRM enables you to not only automate, orchestrate, and streamline large amounts of files within tight deadlines but to secure them all at a level of granularity previously unimagined.



EXPERIENCE **THE POWER OF DRM** AND **SFT**

Go beyond managed file transfer for more protection and control of sensitive files. With the HelpSystems SFT Rights Management bundle you can secure and encrypt files wherever they go, and revoke file access at any point - even after files leave your MFT platform.

LEARN MORE

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(hs-gd-0523-r2-gm)