Progress® MOVEit®

The Cloud: Your Secret File Protection Weapon

How the cloud protects file transfers.

WHITEPAPER

Files are the lifeblood of your organization and the holder of most of its critical, sensitive and valuable information. Unfortunately, these files are not always stored securely and end users are not trained on how to protect them, leaving your organization unsafe through email, low-end file sharing solutions, and other eminently crackable file transfer methods.

Files are a Hacker's Biggest Target

So why do hackers love files? Because that's where most of the good stuff is: confidential financials in Excel files, technical plans in Word docs, and sensitive data strewn throughout an array of file types to name a few goodies. All this information is too easily accessible even by unskilled hackers.

Files are one of malicious actors' biggest targets. Files generate massive amounts of data, and contain confidential information such as credit card numbers, PII, HIPAA data, etc. It's obviously critical to protect this data.

While some of these files fall under regulatory compliance, they don't always, and yet still contain intellectual property or data that is pertinent to the processing of your business.

When users send files through email using Electronic File Sync and Share (EFSS) services or traditional FTP servers, they're not truly secure: they generally don't have encryption at rest. This makes them vulnerable to a side channel attack or other exploitations.

Clearly, confidential files need special care – not only ensuring the integrity of that data and making sure nobody's modifying it, but also storing the files securely so if there is a side channel attack, hackers are not accessing the data directly. Finally, IT should have visibility into where these files go.

Lack of Visibility

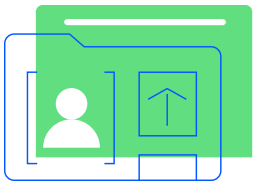
Hackers can be experts at gaining visibility into your files and file structures – that's how they steal them. IT doesn't necessarily have enough visibility – especially knowing if these files are accessed – or what is in them. Did a hacker come through a back door and access files? If so, that opens up a huge attack surface.

Transferring files is when they are most vulnerable. IT generally has no visibility into where these files are coming from and going to.

Due to the fact PGP or other encryption requires a key exchange to occur, these files are rarely encrypted. So you want something totally transparent to the user that secures those files while they're at rest.

File Sharing Dangers

Often, end users adopt file sharing since it offers the path of least resistance without a complicated process to share the data. But as an organization, IT has no visibility into this method, creating a Shadow IT environment.



What Data Needs Protecting?

What data needs protecting? All data in an ideal world. But in reality, regulated data – payment card info, HIPAA data, items that fall under GDPR or CCPA which are high-value targets for malicious actors. For compliance-regulated data, you are working within those frameworks which provide good guidance from a requirement standpoint of how that data should be handled.

Outside of that, there are corporate sensitive documents. Really, anything a user is generating within the organization you don't want publicly available should flow through a secure channel.

The Trouble with FTP

Many use FTP or FTP services for file transfer and may even have some automated processes. Here too, IT has limited visibility into these processes. Where are these files coming from? Where are they going? Often, IT has to hunt through a flat file to determine file source and destination and sift through a lot of protocol data to find it.

Even an FTP scenario can lead to Shadow IT, as you have users generating scripts on their own.

Homegrown Solutions

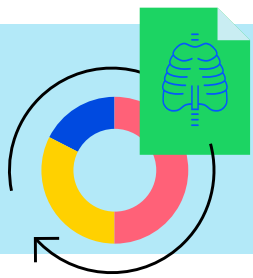
Facing secure file transfer challenges, many shops adopt homegrown solutions, using scripting in one of several languages to create custom file transfer processes and sometimes modest workflows.

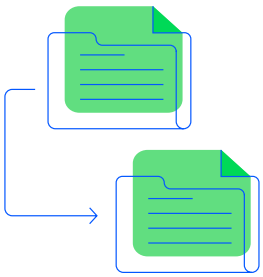
Written by IT pros or scripting aficionados, these are often pretty good. The problem comes from personnel issues where the party responsible for maintaining that solution leaves the organization, is out sick, or on vacation and no one knows what to do if the script breaks. In fact, you might not even know that it's broken as there is no alerting.

Even if someone understands the code, they may not have credentials to manage that service, nor is there enterprise support.

Often these scripts/processes leverage open-source modules, which is fine. But how is this managed going forward? Was there a security flaw in the version implemented, and how do you know what version of that open-source module is out so you can update on a regular cycle?

Often, IT has to hunt through a flat file to determine file source and destination and sift through a lot of protocol data to find it.





Managed File Transfer (MFT) Solutions

Managed File Transfer (MFT) solutions are more secure and superior to file sharing tools, FTP and homegrown solutions in myriad ways. MFT offers encryption at rest, often automation and workflows, logging and auditing, and even business continuity. With cloud MFT, you are protected in the event of an outage and can still operate. Cloud MFT can even come with an uptime guarantee.

Other things to look for in an MFT solution include how easy it is for users to interact with. Can users come in, log into the system, do their workflow, and get out within minutes? That is a key component to adoption, and one of the biggest hurdles to overcome. You don't want MFT to be an overbearing process where it takes an extreme amount of time to facilitate this process due to your security controls.

A good MFT solution simplifies this process by centralizing the administration, whether that is the users' interacting with a file repository or automating processes.

It's All About Visibility

It's really all about visibility – such as ensuring users are authenticating, which can be done through a third-party identity provider. This way you know the user is authorized to access the data or complete the workflow. At the same time, IT may want to lock down people to work groups within an organization, or only allow them to send files to an external party, for example.

Third-Party Integration

Integrating with third-party services is a fundamental MFT feature. There may be external services called for that are generating files. Here, IT can automate the creation of user accounts, folders, and permissions, often by leveraging API endpoints for those processes.

All this takes more off the plate of users from a day-to-day perspective – not even needing human interaction at a certain point.

MFT Implementations: On-Premises, Virtual Environments, and the Cloud

There are multiple ways to implement MFT. One is as an on-premises solution, but the cloud is the hot new way. IT is migrating MFT from on-premises to the cloud and new customers are increasingly going cloud-first.

MFT in the cloud allows administrators to focus on higher priority tasks than managing infrastructure, doing updates, adding network interface cards – all that nonstrategic work.

Nor does IT need to worry about business continuity thanks to uptime guarantees. And IT can spin up the service quickly, not going through a provisioning process with VMs on site.

The Beauty of File Transfer Consolidation

Consolidating all of your file transfer services – EFSS, FTP and email – into one solution is hugely beneficial. From the user perspective, they have one location to perform all their transfer processes. IT gains visibility with one centralized service that offers a console, tracking, logging, auditing, and reporting.

From the administrative and/or audit level, if we need to come in, view information, we can do that easily. Simply access logging information in an easy-to-use web interface and filter down to specific criteria. And with the ability to integrate with external authentication sources, IT can automate user creation as well. The first time an end user logs in, IT can automatically set them up with a local account and they are good to go.

The MOVEit Cloud Story

MOVEit has a family of solutions, including MOVEit Transfer, a server that is essentially the on-premises version of MOVEit Cloud. This acts as the file repository where users authenticate, upload and download files.

- **MOVEit Automation**, as you might surmise, automates these file transactions. Say a file is generated in a network share, and you need to route that to a vendor or make it available on the MOVEit server so an external party can come in and pick it up – automation can do that. MOVEit Automation has its own built-in scheduler and can be event driven.

- **MOVEit Gateway** is another on-premises offering. If you adopt MOVEit Cloud, you do not have to worry about the gateway, though for on-premises customers it provides a reverse proxy in the DMZ and ensures that no data is ever stored there.

- **MOVEit Cloud** puts the MOVEit Transfer server up in the cloud. Now IT doesn't have to deal with storage, infrastructure, service level, disaster recovery, or high availability. All of that is cooked into MOVEit Cloud.

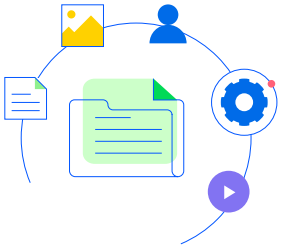
  This speaks to a common IT objective: to reroute administrator's processes to higher priority tasks than managing infrastructure.

  MOVEit Cloud server is hosted by and managed by the Progress cloud operations team. We spin up instances quickly. Then IT, as a local administrator, sets up that environment for their use case.

  Let's say you are dealing with regulated data, whether that's PCI, HIPAA or other rules. MOVEit Cloud goes through third party independent audits for both PCI and HIPAA. MOVEit also supports SOC 2, and other security standards.

Obviously, if you are going through an audit, there might be additional things you need to prove out, – and MOVEit provides all the tools to help you go through that audit.

MOVEit Automation, because it accesses a lot of internal resources, is generally deployed either on-premises or in a virtual deployment such as a private cloud.



User Scenarios

Let's look at MOVEit from a user and administrative level. Say you are a trading partner and need to deliver a file to this system. As a partner, your user account has already been provisioned and a credential established.

You can come in and navigate through the web interface right now. You can even come in over FTPS or SFTP if you like. Once connected, you specify what files to upload, and go ahead and upload. There are no file size limitations regardless of the protocol you are accessing the system through.

The files are automatically encrypted at rest using an AES-256. MOVEit ensures the integrity of these files, and that these files cannot be taken out from the backend and read in any way because they are encrypted. They are also obfuscated, so there are no file names, no file extensions on the back end, nothing like that.

The body of the message, by default, is stored securely on the MOVEit Cloud service, so it does not go out in an email. Files, same thing. They are uploaded to the MOVEit service, and do not leave the system until the user authenticates. Once MOVEit ensures they are authorized to access the data, they can download it.

IT can set additional controls, such as how long this data should be available for, or how many times it can be downloaded. These are all customizable options.

On the back end, MOVEit automatically generates the user account as a temporary user account, so it has a limited life cycle on the system in this particular use case.

Logging

We have detailed the importance of visibility, a key aspect of which is being able to look back. This is done through logging which shows what users do. This is great for day-to-day administration. If a user has an issue, IT can see all the activities that took place.

IT could validate if an external party uploaded files. If so, IT can click the timestamp and get additional information including how long the transfer took, the size of the file – that sort of information.

Additionally, every file uploaded to MOVEit gets its own unique ID number which tracks that file's lifecycle on the system. The system can filter to that ID number, so even if 10 files of the same name were uploaded, IT can track this specific one and everybody who accessed it throughout its lifecycle.

Logging is not limited to user interaction. Any administrative action, whether it is creating user accounts, folders, setting permissions, etc., are visible as well.

UNIQUE FILE, UNIQUE NUMBER...

Every file uploaded to MOVEit gets its own unique ID number which tracks that file's lifecycle on the system. The system can filter to that ID number, so even if 10 files of the same name were uploaded, IT can track this specific one and everybody who accessed it throughout its lifecycle.

Reporting

In addition to day-to-day logging, MOVEit has reporting which is useful if you want to get configuration or usage metrics out of the system. A good example is when you are going through an audit and the auditor asks for a user list, wanting to know all the user accounts, when they were created, when they last logged in, and when they reset their password.

This is just one example of a canned report. There's 100 or so pre-built reports and you can also create custom reports. We publish the schema, and you can create a report that has whatever information is relevant to your process. Not only that, you can schedule these reports, have them as deliverables, place them in folders, and alert a user that that report is available.

MOVEit is simple to set up from the administrative perspective, and even easier to use. Users simply log in, start their workflow, and deliver files as needed – all from a single location. That same single location is beneficial for admins who have a single pane of glass for logging. That same interface lets IT set service level policies such as password length and complexity, user account expiration, etc.

About Progress

Progress (NASDAQ: PRGS) provides the leading products to develop, deploy and manage high-impact business applications. Our comprehensive product stack is designed to make technology teams more productive and we have a deep commitment to the open source community. With Progress, organizations can accelerate the creation and delivery of strategic business applications, automate the process by which apps are configured, deployed and scaled, and make critical data and content more accessible and secure —leading to competitive differentiation and business success. Over 1,700 independent software vendors, 100,000+ enterprise customers, and a three-million-strong developer community rely on Progress to power their applications. Learn about Progress at www.progress.com or +1-800-477-6473.

Worldwide Headquarters

Progress, 14 Oak Park,
Bedford, MA 01730 USA
Tel: +1-800-477-6473

www.progress.com

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software

Progress®