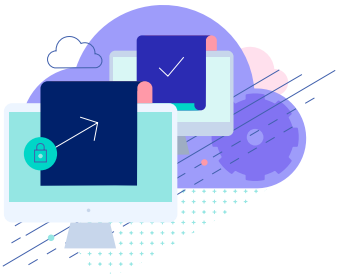
Progress® MOVEit®

The Cloud: Your Secret File Protection Weapon

How the cloud helps safeguard file transfers

WHITEPAPER

Files are the lifeblood of your organization and the holder of 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 highly crackable file transfer methods.



Files Are the Hacker's Biggest Targe

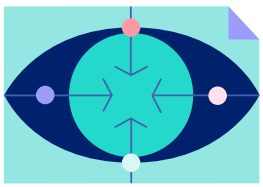
So why do hackers love files? Because that's where most of the good stuff is: confidential financials in Excel files, technical plans in Word docs, and sensitive data strewn throughout an array of file types to name a few goodies. All this information is too easily accessible even by unskilled hackers.

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?

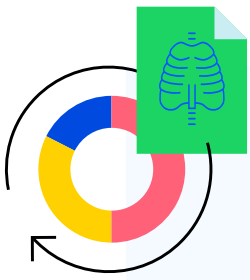
What data needs protecting? All data in an ideal world. But in reality, regulated data – payment card info, HIPAA data, items that fall under GDPR or CCPA which are high-value targets for malicious actors. For compliance-regulated data, you are working within those frameworks which provide good guidance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

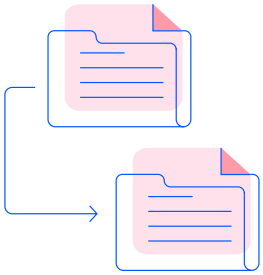
The Trouble with FTP

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 its 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.



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.



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 enthusiasts, 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 takes a vacation and no one knows what to do if the script breaks. Or worse, you might not even know that it's broken as there is no alerting to notify the team of an issue.

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. 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 it on a regular cycle?

Managed File Transfer (MFT) Solutions

Managed File Transfer (MFT) solutions are typically more secure and superior to traditional file sharing tools, FTP and homegrown solutions in multiple ways. MFT offers encryption at rest, automation and workflows, logging and auditing and even business continuity. With cloud MFT, you are better protected against outages and disruptive events that degrade operational efficiency. Ease of use is also important to look for in an MFT solution. Can users come in, log in to the system, do their workflow and get out within minutes? This is a key component to adoption and one of the biggest hurdles to overcome. Managed file transfer shouldn't be an overbearing process that requires a lot of time due to security controls. A good MFT solution simplifies data exchanges for non-technical stakeholders with user-friendly client interfaces and ad hoc sharing options.

It's All About Visibility

Verifying that users are authenticating can be done through a third-party identity provider, giving you the crucial visibility you need. 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.

Third-Party Integration

Integrating with third-party services is a fundamental MFT feature. Whether sharing, receiving, or modifying files from an external service, an MFT solution should have flexible integration and endpoint support options. Here, IT can automate the creation of user accounts, folders and permissions by leveraging API endpoints.

All this means a lot less work for users from a day-to-day perspective—at a certain point, they won't even need human interaction.

MFT Implementations: On-Premises, Virtual and Cloud Environments

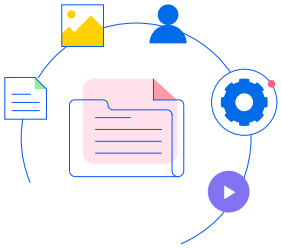
There are multiple ways to implement MFT. One of them is as an on-premises solution. Another one that's gaining popularity is to use it in the cloud Enterprise IT teams are gradually migrating MFT from on-premises to the cloud and new customers are increasingly going cloud-first to valuable time across the organization.

MFT in the cloud allows administrators to focus on higher-priority tasks rather than managing infrastructure, doing updates, adding network interface cards and spending time on other nonstrategic work.Also, IT doesn't need to worry about business continuity thanks to uptime availability. And IT can spin up the service quickly, without going through a provisioning process with VMs onsite.

The Beauty of File Transfer Consolidation

Consolidating all 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 a centralized service that offers a console, tracking, logging, auditing and reporting.

From the administrative and/or audit level, if a user needs to come in, view information, they can do that easily. They can 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

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

- **Progress® MOVEit® Automation** automates these file transactions. If 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.
- **Progress® 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 to deploy MOVEit Transfer within a secured network.
- **Progress® MOVEit® Cloud** puts the MOVEit Transfer server in the cloud. IT doesn't have to deal with storage, infrastructure, software and security updates, disaster recovery or high availability because it's all included in MOVEit Cloud.

This speaks to a common IT objective: to reroute administrator focusto 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 the environment for the specific 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.

If you are going through an audit, there might be additional things you need to prove, and MOVEit provides the tools to help you to better carry out that audit.

MOVEit Automation accesses a lot of internal resources, so it's 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.

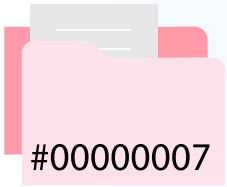
Logging

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 a powerful reporting feature that is a great tool to use if you want to get configuration or usage metrics out of the system. For example, when you're 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 feature can facilitate that.

This is just one example of a canned report. There are 100 or so pre-built reports in addition to custom reports. 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 an 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 single location is beneficial for admins who have a single pane of glass for logging. The same interface lets IT set service-level policies, such as password length and complexity, user account expiration, etc.

Request your free trial of MOVEit

About Progress

Progress (Nasdaq: PRGS) provides software that enables organizations to develop and deploy their mission-critical applications and experiences, as well as effectively manage their data platforms, cloud and IT infrastructure. As an experienced, trusted provider, we make the lives of technology professionals easier. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com

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

Rev 2024/12 RITM0266033

Progress