

# OpenText Filr Security

Organizations handling any sort of sensitive information must converge security and effective collaboration. OpenText Filr provides file access and sharing from any device. Users get what they want and you remain in control of your files and security.

Many organizations handle sensitive, personal information when working with customers and employees. This kind of information can include any sort of personally identifiable information (PII) like social security numbers, identification numbers, banking information, etc.

PII, among other business-critical data, is vital for business success but can prove extremely costly for organizations if it gets into the wrong hands.

Security breaches can wreak havoc on an organization, so safeguarding that information is a good business strategy.

However, simply locking this information in a secure database prevents the business from sharing, collaborating, and using the data to help customers. The business needs to be able to securely share these files to operate, but many open file hosting services can leave your data vulnerable to misappropriation.

To effectively collaborate on and share critical documents, an organization will likely enlist some sort of file-sharing platform. These can include the following:

## Consumer-grade cloud services

These services are easy to use and are a popular choice for merely sharing files. However, these solutions are typically not conducive to regulatory compliance and can be bad news for organizations dealing with large amounts of sensitive data like financial, health, and government industries. They lack the authentication controls and security you've already established and depend on within your infrastructure. Even more, they require you to move your data, which prevents you from knowing where your files end up and leaves you vulnerable to security breaches or regulatory violations.

## Enterprise-targeted cloud services

While these solutions usually promote their enterprise-class security and control, they are still ineffective. Cloud data repositories are only useful when someone has taken the time to populate them with files. Without this, you've basically just bought a shiny new empty container which doesn't do you any good. These also leave you at the mercy of the provider in terms of compliance and adequate protection.

## Hybrid/on-premises solutions

Even though hybrid services allow you to keep some of your files in your organization's on-premises data centers, the provider is focused on moving mobile files to the cloud. Consequently, these services fall short in many of the same ways enterprise-targeted cloud services do. Plus, they double your management effort because they require you to manage two separate infrastructures.

## On-premises file-system integrated solutions

You need a best-of-both-worlds solution when it comes to HIPAA compliance and effective, mobile file sharing. Additionally, your solution should be able to use the files and file systems you already have in place. Your solution should allow you to mobilize your existing on-premises file system to leverage the security infrastructure, file access controls, and data management processes you've already invested in.

## OpenText Filr utilizes industry best practices for security

Data security is paramount for organizations handling sensitive data. OpenText™ Filr takes the guesswork out of data security so IT can be assured the data is safe and users can collaborate and work effectively on documents securely. OpenText Filr includes countless features focused on security including local desktop cache encryption, encryption of all communications, ransomware protection, Captcha for brute-force attacks, online editing, wiping of remote devices, and more.



## Unparalleled security meets unbound productivity

Data is most vulnerable when it is in motion. Because of this, organizations need a way to share files securely and efficiently. OpenText Filr is the connecting piece between your file servers and the endpoint devices in your organization. It connects to users' home directories and shared network folders, allowing for the data backup and security systems that your IT department has put in place to stay in place.

### On-premises solution

Rather than ripping and replacing your current servers and directory services, OpenText Filr uses the ones you already have in place. OpenText Filr integrates with the existing data backend of an enterprise, such as OES, AD, NAS, and SharePoint. It honors the file system rights model, mapping to four distinct roles: Contributor, Editor, Viewer, or None. Therefore, the existing strong file system's rights model is leveraged by OpenText Filr without any additional requirements. The data stays where it lives without any duplication for secure data protection. This allows users to be more productive with easy access to the data they need with a low total cost of ownership for the organization.

The security mechanisms you already have in place can remain intact, such as file access and enterprise directory support. You won't need to expand or change the backup and recovery systems you've already invested in. Because the files haven't moved, they're still protected. This model differs from other file-sharing platforms on the market because it requires no forklift to the cloud. All data is inside the organization and doesn't need to be moved to the cloud, eliminating potential data migration risks.

### File type blocking

Filr allows organizations to whitelist and blacklist certain file types to give maximum control to the enterprise about what gets uploaded to the OpenText Filr system.

Whitelisting certain file types will allow users to only upload the document types the organization specifies. Users aren't allowed to upload a file that OpenText Filr can't detect. IT can add or remove file types as needed.

Blacklisting certain file types blocks the upload of listed file types. Users can upload file types not listed in the blacklist, preventing dangerous files from entering the system.

### Multi-factor authentication (MFA)

OpenText Filr enlists NetIQ Advanced Authentication by OpenText, an MFA solution that enables you to protect your sensitive data by using a more advanced authentication method, in addition to the typical username and password. This additional layer of security helps ensure the identity of a user and reduces the risk of unauthorized access to OpenText Filr and sensitive data.

Advanced Authentication provides a single authentication framework that enables secure access to any device a user owns with minimal administration. You can use different types of authenticators such as a security question, PIN, and an OTP to authenticate on diverse platforms. Authentication comprises these factors:

- Something you know (password, PIN, security questions)
- Something you have (smartcard, token, mobile phone)
- Something you are (biometrics, fingerprint, iris)

You can achieve a secure MFA by using any two factors from this list.

## Resources

Learn more at  
[www.opentext.com/products/filr](http://www.opentext.com/products/filr) ›  
[www.opentext.com](http://www.opentext.com) ›

## Data leak prevention

OpenText Filr provides a feature that enables organizations to have fine-grain control over important organizational documents and helps you adhere to various global data protection policies, while still providing remote access to external partners and users working remotely.

Further, the Workspace Moderators option allows the OpenText Filr administrator to delegate the file sensitivity management privileges to users who have access to a workplace. These users are called moderators and they, along with administrators, can apply policy to files and manage them in the workspace. A system-generated policy called “Confidential” is available and the “Share Externally” file operation is mapped to this policy. When this policy is applied to a file, sharing a file with any external user will be restricted.

## Secure Enterprise File Sharing

OpenText Filr gives your users easy, anywhere, any-device access to your organization’s files, while keeping the process completely under your organization’s control. It delivers the mobile file access and collaborative file sharing users want, but through an enterprise-ready design that leverages your existing infrastructure and established controls. It eliminates the need to manage third-party services or create and manage hybrid file stores by allowing you to use your existing file servers, existing files, and existing file system rights.

Provide your organization with secure sync and file sharing—anywhere with OpenText Filr.