CITRIX

Citrix ShareFile

Share, store, sync, and secure data on any device, anywhere

ShareFile is a secure, enterprise data sync and sharing service with flexible storage options that allows IT to mobilize all business data. ShareFile enables mobile productivity with read-write access to data, workflows and collaboration and allows users to securely share files with anyone and sync files across all of their devices.

Throughout 2018, our products and portfolio will change in exciting ways to support the new unified Citrix Workspace experience. ShareFile will evolve to be Content Collaboration and be fully integrated with Citrix Workspace—as both a standalone and integrated product.

Our solutions deliver the **experience, security, and choice** that people and organizations need to innovate, engage customers and be productive – anytime and anywhere.

Experience

Feature	Function	Benefit
Standard Features		
Internal and external file sharing	Send files to anyone from within or outside the organization	Quickly and easily send and receive files with added security. External users do not contribute to the license count
Large file sharing	Send files up to 100GB	No more file size limitations. Secure FTP replacement, no longer share large amounts of data via USB drives
Multi-language support	User interface is offered in different languages including: English, French, German, Spanish, Japanese, Korean, Simplified Chinese, Russian, Dutch and Portuguese (Standalone offering only)	Allows for multi-language support for organizations worldwide
File check in / check out	Allows users to lock a file while making changes	Supports collaboration scenarios
Custom branding	Companies have the ability to custom brand the service	Highlight your brand front and center; make a great impression with clients
Offline access	Save files locally	Enables offline access and editing from mobile devices
Mobile & web app editing with Microsoft Office 365	Open and edit files stored in ShareFile without desktop versions of Microsoft Office (requires Office 365 License)	Enables quick and easy collaboration from any browser, computer or mobile devices, saving time and increasing productivity
Medical Image Viewer	View diagnostic-quality medical images	Enables users to share large medical images that can be viewed without downloading
Citrix Solution Integration		
Citrix product integrations	Integrates with the Citrix Workspace	Enables an all-in-one solution for any workplace environment.
Secure Mail Integration	Attachments open in ShareFile	Enables users to attach files from their ShareFile repository without requiring that the file be downloaded to the device. Citrix provides SSO experience from the mail client into ShareFile when attaching documents to e-mails, removing the need for users to log into ShareFile during the workflow

Experience

Feature	Function	Benefit
Apps		
Citrix Files for Windows & Citrix Files for Mac	Access content via a drive letter, sync files across all devices including: PCs, Macs, tablets, and mobile devices and tablets	Optimized for use with virtual apps and desktops, users can view all their files and folders file will download and sync only when users want to view, edit, save or share, helping IT cut storage costs and optimize performance
Citrix Files for Outlook and Gmail	Integration with email clients to converts attachments into links	Simplifies large file sharing both inside and outside the organization. Eliminates file size restrictions. Users can convert all attachments into links by default; specify minimum file size for conversion. Users can also request files from co-workers or third parties by providing a link to upload attachments
Citrix Files for Android & Citrix Files for iOS	Accessing data from any device including: iPhones, iPads, Android Phones / Tablets, Chromebooks and BlackBerry devices	Securely access data from mobile devices. Support for multiple devices to meet each company's specific needs.
Workflows		
Feedback and approval Workflows	Collaborate on documents, generate approvals directly from the document	Allows users to collaborate and generate approvals and legally binding signatures in real time
Custom, automated workflows	Ability for users to define business rules which can be used either within a workflow or as a trigger for initiation or task transition	Solution that goes beyond addressing mobility needs, but also supports requirements that drive workflows. Provides a collaborative workspace where anyone can securely exchange, track, edit and e-sign content with unlimited cloud storage
Legally-binding e-signatures	Obtain legally binding signatures on documents entirely online	No software to download or install, and it can be accessed from any computer or mobile device
Mobile		
Mobile app containers	Personal apps run in a separate vault	Isolates personal apps from mobile enterprise apps and data
Mobile apps	Accessing data from any device including: iPhones, iPads, Android Phones, Android Tablets, Windows Phones, Chromebooks and BlackBerry devices	Securely access data from mobile devices. Support for multiple devices to meet each company's specific needs
Mobile access and productivity	Distribute content via different mobile devices	Securely view and edit content in home directories, file shares, SharePoint, OneDrive without VPN as a single point of access
Support for mobile phones and tablets	Access to critical data through mobile devices that ShareFile supports: Apple iPhone®, Android, iPad and Android tablets, Chromebooks	Enables mobile workstyles by giving users access to critical data on a variety of mobile devices
Built-in mobile content editor	Edit documents through ShareFile	Create, review, and edit Microsoft Office documents within the ShareFile app
Complete mobile device management	Manage and configure corporate and personal devices	IT manages and configures corporate and personally owned devices, including app blacklist/whitelists, full or selective device wipe, and enterprise integrations via LDAP and PKI
EMM Support	Integration with 3rd party EMM tools for remote wipe, provisioning, policies, etc.	Enable users to sync, share, open and edit data on any device they use while IT maintains security and control

Choice

Feature	Function	Benefit
Storage zones		
Flexibility to store data where you choose	Choose between customer-managed (on-prem) and Citrix-managed storage zones	Storage zones feature gives IT the flexibility and option to choose between customer-managed (on-prem) and Citrix-managed storage zones. Cloud storage zones are located around the world
Encrypt data with private keys (Key Management Service)	Files are encrypted with customer-owned keys	Enables customers to protect their data using encryption keys that they control
Geographic locations	Storing data in close proximity	Enhances performance for the users. A single ShareFile account can span multiple storage zones locations worldwide, enabling optimized performance for global performance
Customer-managed storage zones cloud options	Full support for data storage in Amazon S3, Azure Blob storage and Google Cloud Platform (GCP)	These deployment options provide all the elasticity and cost benefits of the cloud, together with security and control of customer management to their corporate encryption keys – an advantage typically only available on-premises
Customer-managed storage zones on-premises options	Integrates with an organization's existing Infrastructure	Customer-managed storage zones can be easily integrated with an organization's existing infrastructure as it is designed to support any CIFS-based network share, and customer-owned object storage
Connectors		
Storage zone connectors for network shares and ECM software (SharePoint, Documentum)	Web/mobile access and sharing of data stored in existing corporate network shares or ECM repositories	Eliminates the need for massive data migration, extends the benefits of mobile file sync and sharing services to existing network shares and ECM software like SharePoint or Documentum, enhances workforce productivity
Office 365 connectors	Access to SharePoint Online and OneDrive for Business	Enables secure access and editing for documents stored in SharePoint Online and OneDrive for Business
Personal cloud connectors	Extend businesses' data strategy to include third-party access to Box, Dropbox, Google Drive and OneDrive using Connectors.	IT can choose to enable this feature for a defined period and require users to migrate all corporate data from personal file sharing services to ShareFile or for communicating with third parties that have standardized on a different file sync and sharing service
Open and extensible platform		
API	API platform allows users to utilize the API to request data and perform actions against a ShareFile account. The API is fully RESTful, utilizing JSON format for request / response protocols and it has implemented a subset ODATA	The ODATA specification allows developers to extend base requests with Query Parameters to retrieve additional information

Security

Feature	Function	Benefit
Reporting, auditing and control		
End user and IT reporting	Access to account-wide reporting and permission to receive detailed info about activity, usage, storage and permissions.	Provides IT comprehensive capabilities to track, log and report on user file access, sync and sharing activity. Users have the ability to track sensitive data and receive reports on total activity to monitor file activity and security
Access control policies	Custom configured access	Limited download-only access. Users can be granted a combination of upload/edit/delete and admin access to folders
Storage quotas	Enterprise admins can set hard storage zone quotas	Gives IT increased visibility and control over the amount of storage each individual user can consume
Analytics	Security and usage insights into ShareFile user behavior	Applies Machine Learning algorithms to identify patterns and anomalies, and report them to the administrators so they could take actions to prevent security issues.
Protect Sharing	Track usage of sensitive data by requiring a login to access files	Adds layers of protection to files and provides full control over who has access to files
Policy-based Administration	Admins can define and manage the policies present in the system	Policies can be applied across groups to customize experience based on roles
Retention policies at the account and folder level	Define and manage the policies particular to files/folders retention/ disposition	Users and Admins can maintain security and storage needs across files and folders, scheduling disposition timelines
Archiving	Automatic document archiving based on definable rules	Enables companies to automatically comply with regulations based on archiving and accessing documents across users
Webhook and REST API integrations	Allows security integrations through APIs for Cloud Security Access Brokers (CASB), Security Information and Event Management (SIEM) solutions	Leverage existing security solutions for visibility and control
Data security		
Secure file sync and share	Sharing files securely	Detailed reports on unauthorized use of personal file sharing accounts with ShareFile, a secure alternative to personal file sharing services
Encryption in Storage and in-transit (email/shared links)	Transferring files through ShareFile	Ensuring files are shared over a secure SSL/TLS connection and stored at rest with AES 256-bit encryption
Better control and visibility	Track use of sensitive data by requiring a login to access the files	Senders can request a download notification and assign an expiration policy on files, revoking access to the recipient
Mobile device encryption	Enforces encryption on mobile devices	IT can leverage the mobile device's encryption capabilities and enforce encryption for all ShareFile data on the device
Data Loss Prevention	Integrates with McAfee DLP Prevent, Websense Forcepoint DLP, GTB Technologies and others for customer-managed storage zone deployments	Restricts document sharing based on the file's DLP classification. Connecting ShareFile with customer's existing DLP system enables the ability to classify files based on their content to enforce sharing restrictions per company policy
Anti Virus and Anti Malware integrations	Integrates with popular solutions like Symantec, McAfee, Trend Micro and others via ICAP	Leverage existing security solutions to detect and remediate malicious files
View-only sharing	Securely share sensitive documents with others with restrictions	Users can share "view-only" documents to prevent other users from adding, editing, or deleting files is required
Information Rights Management (IRM)	Securely share documents with others and have defined security parameters	Adds a layer of security to a shared file ensuring the recipient(s) are the only ones who can access the shared file with watermark options

Security

Feature	Function	Benefit
Compliance		
Compliance	SOC2 compliant, HIPAA configuration	Citrix implements and maintains commercially reasonable and appropriate physical, technical and organizational complimentary controls to protect customer data. ShareFile also offers a ShareFile Cloud for Healthcare – a secure enclave within a private cloud where IT can upload, store and share patient health information (PHI)
Device security policies		
Remote wipe	Wipe all ShareFile stored data and passwords	Allows both users and IT to wipe ShareFile stored data and passwords on mobile device in case of loss or theft. Alternatively, IT can lock the device to restrict its use for a limited time
Poison pill	Prescribe data expiration policies	Enables IT to prescribe data expiration policies for mobile devices and activate audit controls to track user logging activity
Restrict modified devices	Restrict use of devices	IT can restrict the use of modified or jailbroken devices
Restrict third party apps	Restrict use of third party apps that can store copies of sensitive data	Provides build-in capabilities like a mobile content editor as a secure alternative
Passcode lock	Require users to enter a passcode	IT has the ability to require users to enter a passcode every time the user wants to access their ShareFile account on a mobile device, making it easier for users to access their data while ensuring unauthorized access is denied
Identity and Access Control		
User Directory Integrations	Integrates AD and Citrix Endpoint Management	Offers support for Active Directory integration via SAML or Citrix Endpoint Management
Identity Security Integrations	Integration via SAML for Identity Providers (IDP's) including Okta, Ping, Oracle, Azure AD, etc. We also support Basic and Windows Integrated Authentication	ShareFile provides a consistent SSO log-in experience across all device and apps, supporting company managed user stores via SAML
Two-Step / Mandatory Two-Step Verification	Multi-factor authentication and forced authentication features	Admins can increase the security around authentication
Single sign-on and federated identity	Enterprise directory integration though policy-based administration within the User Management Tool	Simplifies and accelerates role-based provisioning and deprovisioning. Enforces two-factor authentication and helps monitor service levels and license usage

CiTRIX®