ShareFile Enterprise technical overview

Secure data sync and sharing services

ShareFile empowers users to securely share files with anyone and to sync files across all of their devices

CITRIX®

The role of IT organizations is changing rapidly as the forces of consumerization pose new challenges. IT is transitioning from the sole provider of user services to an aggregator and administrator of both in-house and third-party services, devices and applications. In the wake of this transition, IT must be prepared for everything that employees are bringing to work, including personal devices and applications.

Mobile workstyles—the notion that employees should be able to work from the most optimal location—prompted IT to look for solutions that could support flexible working while ensuring employees remained productive. Employees also started using personal devices at work, which led some IT organizations to adopt a formal bring-your-own-device (BYOD) strategy. These trends, along with continued growth in dispersed and global workforces, clientele and operations, drove the need for instant access to data for easy collaboration. However, the lack of an IT-managed data sync and sharing service led employees to turn to consumer-style file-sharing products for self-service access to their files, as well as the ability to share those files with others within and outside their organization. Such unsecure solutions, unfortunately, put sensitive corporate data, regulated data and intellectual property at risk.

Simply blocking these unsecure services without providing a secure and IT-managed alternative will result in user frustration and lower productivity. It will also be regressive for IT, which is emerging as a strategic organization that fosters change to increase business productivity. To help IT regain control over employee file sharing, Citrix offers ShareFile – an enterprise-class, IT-managed, follow-me data service.

ShareFile Enterprise

ShareFile is a secure data sync and sharing service that allows IT to mobilize all enterprise data and empower user productivity anywhere. ShareFile seamlessly integrates with workflow tools such as Microsoft Outlook and provides a rich user experience on any device to enhance productivity.

Unlike consumer-style file sync and sharing tools, ShareFile provides management and control functionality that allows IT to deliver a secure service and store enterprise data in optimal locations to meet corporate data policies and unique compliance requirements. ShareFile is a powerful service that is simple for IT to implement and manage and to fully integrate with existing security infrastructure and policies.

With ShareFile, IT can:

- **Empower users with instant, mobile and read-write access to data** synchronized across all of their devices
- **Improve collaboration and business productivity** through secure file sharing with people inside and outside the organization, regardless of data location
- **Meet corporate data protection and compliance standards** via a service providing strong security and the flexibility to store data on or off premise, or both
- **Mobilize existing investments** such as network shares and SharePoint through StorageZone Connectors
- **Deliver a managed service** that helps IT control the way corporate data is accessed, stored and shared

Product architecture

The ShareFile product architecture consists of two key components: the ShareFile Control Plane and Citrix-managed or customer-managed StorageZones. The client device can request access to the follow-me data service through a mobile app, native desktop client, virtual desktop, web or mobile browser, or directly through the ShareFile API.

Control Plane

The Control Plane performs functions such as user authentication, access control, reporting and brokering. The Control Plane is hosted in Citrix datacenters and managed by Citrix as a service.

Following are the components of the Control Plane:

- SSL web application servers for ShareFile web interface/web portal access.
- SSL web API servers for client devices, including all native ShareFile apps and tools.
- A clustered database that stores user account information, access rights information for file and folder metadata and user login information. The database in the Control Plane does not contain any user files or user/corporate data. The database is also securely replicated to a secondary, failover datacenter location for backup and recovery.
- NetScaler appliances load balance all client requests across the web servers. The NetScaler appliances and web servers run in the demilitarized zone (DMZ) and the database cluster runs in the production network behind the firewall.

All traffic from a client device, the web interface or a native tool connects to the Control Plane using 256-bit SSL encryption. The NetScaler appliances then load balance traffic/requests across the various web servers. Once the connection with the web servers is made, they communicate with the clustered database for retrieval of requested information.

ShareFile StorageZones

The ShareFile StorageZones feature in ShareFile Enterprise allows IT administrators to choose where corporate data is stored. Administrators can choose Citrix-managed secure cloud storage options and/or customer-managed StorageZones to leverage their storage infrastructure whether on premise or in cloud-based object storage.

Citrix-managed StorageZones

Customers can place their data in a choice of worldwide locations managed by Citrix. They can choose between Microsoft Azure and Amazon Web Services enterprise-class datacenters employing industry-proven caching and storage architectures that use the most advanced encryption standards available today.

The StorageZone architecture has various components, all of which are managed by Citrix, including ShareFile Storage Center, the main component managing all file operations. Other components include the utility servers responsible for antivirus, full text index and backup functions. Refer to Figure 1.

Figure 1. Citrix-managed StorageZones

Customer-managed StorageZones

With customer-managed StorageZones, IT can place data in the organization's own datacenter to help meet unique data sovereignty and compliance requirements or leverage Microsoft Azure or Amazon S3 cloud storage. Customer-managed StorageZones can be easily integrated with an organization's existing infrastructure as the solution is designed to support any Common Internet File System (CIFS)-based network share, Microsoft Azure's binary large object storage and Amazon Simple Storage Service (Amazon S3) storage. Refer to Figure 2.

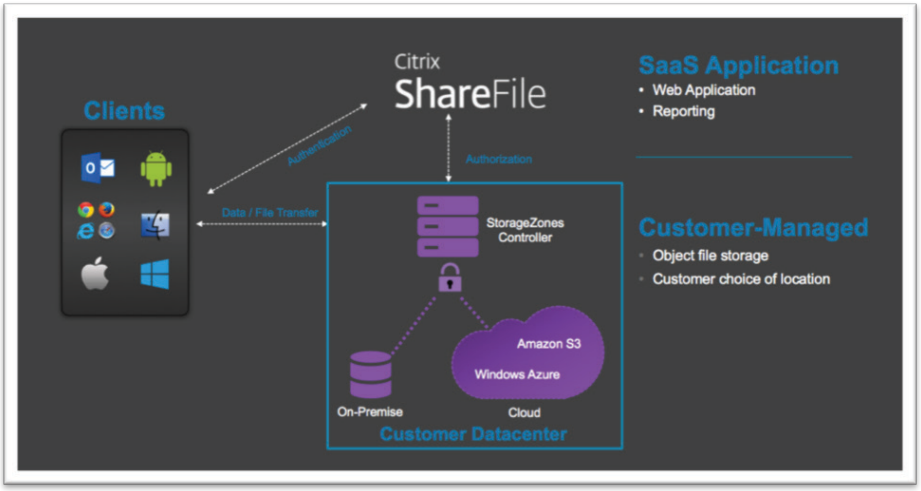

Figure 2. Customer-managed on-premise StorageZones

The Azure and Amazon S3 storage architecture is similar to the customer-managed on-premise StorageZones architecture in Figure 2, with one minor difference.

Azure and Amazon S3 storage is customer managed but hosted in their respective clouds. File uploads are initially deposited in a temporary storage area shared by all StorageZone controllers. Then, a background service copies those files to the appropriate storage location and deletes the local cached copy of the file(s). Please refer to the Install StorageZones Controller and create a StorageZone webpage for detailed information on configuring and using ShareFile hosted on either the Microsoft Azure or Amazon S3 cloud service.

Additionally if you are a Citrix Service Provider (CSP) you can create and manage a single StorageZone shared by multiple tenants. This is done through a feature called "Multi-tenant StorageZones". You can place your tenants into a single storage repository but still provide them a unique ShareFile Account and leverage all the features of ShareFile. This is available to partners who are registered as Citrix Service Providers and have a Partner ShareFile Account.

StorageZone Connectors

With the StorageZone Connectors feature (refer to Figure 3), mobile users can connect from iOS or Android phones or tablets to ShareFile data, existing CIFS network shares and

SharePoint document libraries. Further, the mobile editing capabilities in the ShareFile application, listed below, help mobile users achieve high productivity while on the go:

- Browse SharePoint document libraries and download documents to the mobile device for offline reading
- Check out SharePoint documents, edit them and check them back in
- Upload or download documents from network drives, including the same network "home" drive employees use in their XenApp or XenDesktop environment, right from the mobile device
- Share on-premises files from network shares or SharePoint with recipients outside your organization via Connector Sharing without needing to grant access to your on-premises storage

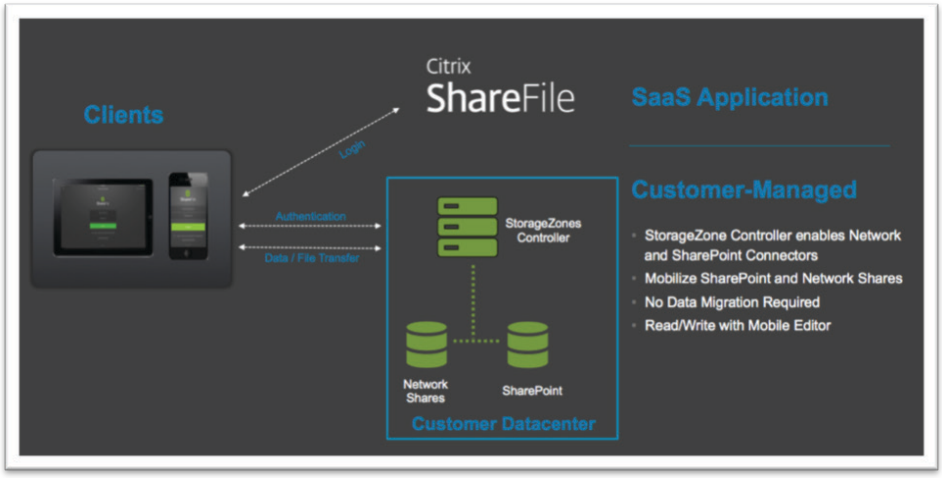

Figure 3. StorageZone Connector architecture

StorageZones Controller

The main component in a customer-managed StorageZone is the StorageZones Controller server. The StorageZones Controller software is a web service installed on a Windows Server 2008 R2 or Windows Server 2012R2 server and is used to enable StorageZone Connectors (see Fig. 3), as well as handle all the HTTPS operations from users and the control subsystem (see Fig. 2). In essence, it is a web front end to the StorageZone storage repository. Citrix recommends using a dedicated server or virtual machine for the StorageZones controller server due to the high demands placed on these servers during peak usage.

Following are the key requirements for setting up customer-managed StorageZones:

- Install Windows Server 2008 R2 SP1 or Windows Server 2012R2
- Use a publicly resolvable Internet host name (not an IP address)
- Enable the web server (IIS) role
- Enable the ASP.NET and basic authentication IIS role services
- Install ASP.NET 4.5
- Enable SSL for communications with ShareFile

- If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service
- Use an SSL certificate from a commercially trusted certificate authority ShareFile does not support self-signed or unsigned certificates
- Use a CIFS share for private data storage. If you plan to store ShareFile files in a Windows Azure storage container, the CIFS share is used for temporary files (encryption keys, queued files) and as a temporary storage cache

Secure DMZ Deployment

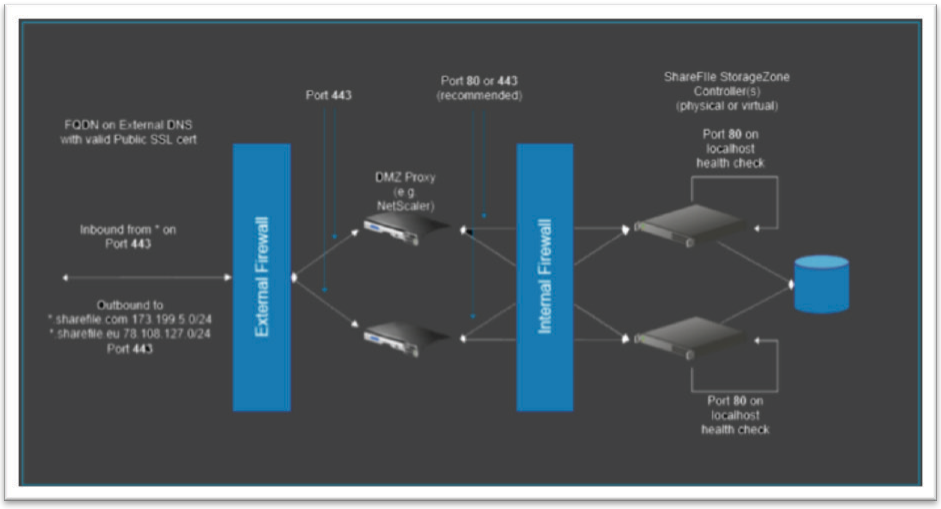

Figure 4. NetScaler reference architecture

For secure DMZ deployments, Citrix recommends NetScaler to load balance and authenticate all requests for data entering a customer's datacenter.

Regardless of the customer's choice of StorageZones, the Control Plane will reside in a Citrix-managed secure datacenter making this a hybrid model. Client connectivity and communication run the same way as for the Citrix-managed StorageZones: customer data will not go through the Control Plane. With on-premise StorageZones, IT will also generate encryption keys. StorageZones can be set at the user level or root folder level, allowing IT to store data based on user profile or type of data.

Security features

ShareFile architecture is secure by design and provides additional robust features that IT can use to control, manage and audit the use of data.

Secure architecture

All Citrix-managed datacenters containing ShareFile servers are certified to SSAE 16, demonstrating high standards for security. The servers are firewall protected and regularly updated to ensure that all of the latest security patches and updates are in place. Files are transferred to and from ShareFile servers using 256-bit SSL encryption and files may be stored with AES 256-bit encryption at rest.

Comprehensive disaster recovery mechanisms protect against loss of data. Files are frequently backed up to a disaster recovery datacenter and mirrored in real time to a secondary server location to ensure service can be quickly resumed in case of a disruption at the primary server location. In the event of accidental deletion of files by a user, these files can be recovered within 28 days through the lazy file deletion option.

With customer-managed StorageZones, admins should use their existing policies to protect the data ShareFile places in their CIFS repository; however, ShareFile.com will archive all account metadata for a period of three years (configurable) to allow admins to easily find and identify user files that may need to be recovered from their backups.

Additional security features

Restricted StorageZones: Customer-managed Restricted StorageZones delivers an end-to-end encrypted solution. The on-premises StorageZones Controller encrypts the metadata with a customer-owned encryption key before writing that data to the Citrix SaaS application tier (sharefile.com/sharefile.eu). Access to decrypted files and metadata only happens via the StorageZones Controller server, which acts as an authenticating encryption/decryption proxy.

Data Loss Prevention (DLP) Integration: ShareFile integrates with existing Data Loss Prevention systems to apply corporate DLP policies on files that reside in an on-premises StorageZone addressing stringent data security and compliance requirements while leveraging existing systems to prevent additional costs. ShareFile can be set up to connect to your DLP system (Symantec Data Loss Prevention, McAfee DLP Prevent, Websense, RSA Data Loss Prevention and others) to restrict document sharing based on the file's DLP classification for files uploaded to the StorageZone.

Remote wipe: If a device is lost or stolen, both the user and IT have the ability to wipe all of its ShareFile-stored data and passwords. In the event of a security breach, IT can remove the device from the list of devices that can access ShareFile accounts, lock the device to restrict its use for a limited time or completely wipe all the ShareFile data and passwords that reside on it.

Reporting and auditing: Users can receive comprehensive reports on file-sharing activity within their workspaces. IT can track and log all user activity. Both users and IT can also create custom reports on account usage and access.

Modified device restriction: IT can restrict the use of modified or jail-broken mobile devices to avoid the security vulnerabilities they can introduce.

Mobile device access control and encryption: Users can be required enter a passcode each time they access their ShareFile account on a mobile device. By providing the option to enter a short PIN instead of a lengthy password, IT can make it easier for users to access their data while ensuring that unauthorized access is denied.

Poison pill: IT can set data expiration policies for mobile devices and activate audit controls to track user logging activity.

Mobile device encryption: Through the passcode lock feature, IT can leverage the mobile device's encryption capabilities and enforce encryption for all ShareFile data on the device.

ShareFile cloud for healthcare: Customers can safeguard patient files in a datacenter enclave dedicated to protected health information (PHI). ShareFile supports HIPAA compliance and Citrix will provide and sign a HIPAA Business Associate Agreement upon request.

Added security with XenMobile: While ShareFile offers a number of security features on its own, XenMobile customers can deploy ShareFile with MDX enabled to add even more security capabilities, such as single sign-on, WorxMail integration, constraint of external applications and an application-specific micro VPN.

Restrict downloading of shared files: View-only sharing can be used to ensure that a shared file is not downloaded, printed or re-shared with other unintended recipients. In addition clipboard actions are also disabled when working with a view-only share.

Secure authentication with enterprise Active Directory integration

ShareFile offers multiple options for Active Directory integration to simplify and accelerate provisioning and de-provisioning of the follow-me data service. IT can enforce two-factor authentication with XenMobile and effectively monitor service levels and license usage. Support is also provided for Active Directory integration with existing SAML solutions to enable single sign-on through the same SAML identity provider used for other web applications.

Conclusion

To embrace workforce mobility and users' demands for instant access to data, ShareFile Enterprise helps IT organizations retain control while improving collaboration and productivity. Citrix has long provided IT the power to deliver a rich and powerful follow-me desktop and app experience. Now, ShareFile completes the mobility story with a rich, enterprise-ready, follow-me data solution.

Try ShareFile

- or -

Contact us
+1 855 216 4330

- **Enterprise follow-me data service:** ShareFile Enterprise offers a best-in-class follow-me data service with features that enterprise IT and users expect.
- **Optimized for mobile workstyles:** ShareFile Enterprise helps IT embrace user mobility requirements by enabling employees to work and collaborate from anywhere, on any device.
  - **StorageZone Connectors:** Mobile workers enjoy effortless access to data stored in corporate network shares and SharePoint libraries from tablets and smartphones.
  - **Mobile editing:** Rich editing for Microsoft Office documents and PDF annotation capabilities are available through the built-in mobile content editor, which is available to users even when offline with standard SharePoint functions like check-out and check-in. Any changes made to the documents can be saved.
- **Flexible storage options:** The innovative StorageZones feature gives IT the flexibility to choose between using Citrix-managed, secure StorageZones in multiple worldwide locations or on-premise StorageZones hosted in their private cloud or the Microsoft Azure cloud service, or to combine the two options.
- **Managed and secure data sharing:** ShareFile Enterprise is a secure, managed service with robust security features that allow IT to determine how sensitive data is stored, accessed and shared.

Citrix understands the importance of data access from the perspectives of the mobile user and the IT organization. Citrix continues to drive innovation by investing in new features that make the user experience more delightful and support IT goals by simplifying management, enhancing control and helping IT retain its strategic role in the organization.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.