Security architecture impact and analysis for **Citrix ShareFile @ NCDOR / NC COMMERCE**

NC Department of Revenue | Information Security Division

This security review is an analysis of the security architecture requirements and impact for the integration of the Citrix ShareFile system as it relates to the Department of Commerce integration. It covers details of the initial deployment criteria, architecture, services, requirements, and expected integration. A layout of security concerns and responses are also included to assist in recommendations and approvals. A sample group from IT and Information Security architecture reviewed the application

Citrix ShareFile features and use cases

The Citrix ShareFile application provides enterprise file sharing capabilities. It provides the following:

- Securely shares files between co-workers or from staff to external grantee.
- Sends encrypted files securely through an electronic workflow process for approval and modification.
- Data type for files loaded within the Sharefile system is CONFIDENTIAL / PII

Security analysis

The analysis was conducted considering security impact, security controls, and compliance regulations related to the type of data in the system and how it effects existing security measures.

The high level considerations are as follows:

1. Authentication and authorization control are handled by 3rd party (Citrix)
2. Ensure users only share only allowed data files
3. File Metadata is stored in cloud
4. Ensure data is only disclosed to authorize staff and devices

Summary

The Sharefile application meets the key security expectations for a CONFIDENTIAL file management as long as users maintain existing security controls and staff adheres to policy and best practice. There are inherent risks associated with any cloud provided service. However, a review of the internal security controls in the application has been completed. NCDOR applied security appropriately so that the data remains secure in this architecture.

Security design

There are 4 Major components in the design:

	SERVICES	SECURITY CONTROLS
Citrix (Saas cloud) Application tier	• Provides Web / Management interface • Provides Account management & authentication • Provides Citrix Accounts store • Is an API Web server • Stores: File Metadata, User Metadata, and authentication Hashes	• (IRM)Rights Management (Authorization) • Logging – SIEM /QRadar via an API • The database stores hashes (pw /file) , security question / answer, ACL info • AES256 encryption @Rest • Malware protection
Security Layer	• Provides on-site Load balancer / Proxy • Provides User management tool for provisioning	• Passwords never cross the firewall • Terminates incoming requests in DMZ (Proxy) • Verifies all request come from sharefile.com • Commerce (PII) and NCDOR (FTI) data are stored within separate data repositories.
Storage Zone	• Stores data files on SAN, CIFS shares, or SharePoint cloud • On premise, files are protected / backed up by DOR. Cloud repository is maintained and backed up by Citrix daily. • Requires a Public DNS name via Proxy	• Uses TLS Cert for IIS • There are 2 keys (Shared Zone key, storage encryption key) • Uses a storage encryption key with a passphrase using AES 256 bit encryption • Data @ rest encrypted via Citrix sckeys.txt or native SAN or SharePoint encryption). If Citrix encrypts, no AV or indexing • File tagging for ACLs and Policies • Encrypts metadata with customer owned encryption key before writing the data to the cloud.
Clients	Can be Windows, Mac, or Mobile devices (IOS)	• Encryption cache can be wiped remotely to block access for lost devices • When provisioning, only First, Last, Email are sent to UMT/cloud from specified AD groups

Security controls & responses

Compliance security controls	Response
Account management (AC-2) • CE-3 – The system automatically disable inactive user accounts after 120 days of inactivity	*Set.*
Access Enforcement (AC-3) • access control policies and access enforcement (e.g., ACL) • Role-based access control • Encrypting stored information using NIST certified cryptographic modules on mobile computers/devices carrying agency data	*Roles based privileges controls which users have access to files and what they can do. Data is encrypted in transit and at rest based on FIPS 140-2 standard. Uses hashes for passwords. Cloud service used to authenticate / authorize access to files / download*
Session termination (AC-12) and (SC-10) • Must automatically terminate a user session or network connection after 30 minutes of inactivity	*Must terminate after max 30 min*
Least Privilege (AC-6). Enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	*The access controls and information rights management feature controls every aspect of who can access a data file and for how long. Rights are given for printing, opening, and viewing the file.*
Remote Access (AC-17). If remote access is permitted, the organization should ensure that the communications are encrypted.	*Data is encrypted in transit and at rest based on FIPS 140-2 standard. Remote access is not granted. Users must connect to their own network (VPN) prior to using Sharefile.*
Access Control for Mobile Devices (AC-19). For Portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), ensure that the devices are properly secured and regularly scan the devices to verify their security status (e.g., anti-malware and patches).	*Our mobile devices are secured and patched via internal processes already in place. External users/ clients are responsible for the security of their own data within their control. These users will not have access to any other data other than their own.*
Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6). Monitor, regularly review, and analyze information system audit records for indications of inappropriate or unusual activity. Investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.	*Data and account access is logged via an API and locally within the Sharefile solution.*
Identification and Authentication (Organizational Users) (IA-2). Uniquely identify and authenticate users. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access and use a time-out function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity	*All users have a unique user account to access the data and must login with validated credentials. MFA is implemented via all remote VPN access. User accounts and OAuth tokens expire after a given time.*
Authenticator management (IA-5). • Eight characters, at least one numeric and at least one special character • A mixture of at least one uppercase and at least one lowercase letter • Storing and transmitting only encrypted representations of passwords	*PW requirements are set as indicated.*

• Enforce password minimum lifetime restriction of one day • Enforce non-privileged account passwords to be changed at least every 90 days • Enforce privileged account passwords to be changed at least every 60 days • Prohibit password reuse for 24 generations • Allow the use of a temporary password for system logon requiring an immediate change to a permanent password • Password-protect system initialization (boot) settings	
Media Marking (MP-3) - Label information system media	*All data can be tagged with Watermarks as needed by staff.*
Media Sanitization (MP-6) - Sanitize digital and non-digital media before reuse	*All data is stored in NCDOR's data center and follows standard sanitation procedures already in place. Data within the cloud is sanitized with cryptographic wipe.*
Transmission Confidentiality (SC-8) - Encrypting the communications or encrypting the information before it is transmitted	*Data is encrypted in transit and at rest based on FIPS 140-2 standard. TLS 1.2 with (128 Bit encryption). Hashes are used for file integrity checks (HBMAC). All data is sent between the client & storage zone*
Protection of Information at Rest (SC-28) - Encrypting the stored information	*Data is encrypted in transit and at rest based on FIPS 140-2 standard.*
Information System Monitoring (SI-4) Automated tools to monitor internally or at network boundaries for unusual or suspicious transfers or events. I.e. DLP technologies, Firewalls, IDS	*Yes, We can monitor the data for suspicious activity through our Palo Alto Firewalls for data stored on premise. Data transfers within the cloud are also monitored for malware.*
Other security risks	Response
Can we ensure only DOR/DOR HW is used?	*Proxy services, VPN, and IP filtering limits which equipment can connect to the internal Storage zone and cloud storage for Commerce. Commerce only allows systems that are able to connect to their VPN or that connect to their internal network.*
Can we limit invitations to staff only? Not public accounts?	*Yes, via user policies*
Data isolation for Software, data, and services from other cloud customers (physical or virtual)	*Cloud data is encrypted from other tenants. Only DOR has encryption keys for on premise data. (AES-256 encryption)*

Notable security measures

Information Rights Management – This feature extends the basic security for a file and follows the file wherever the file is sent, not only while the file is on our networks or servers. For instance, if a file is re-distributed to someone unintended, that user will not be able to open the file without a valid account in Sharefile. Security is enforced no matter where the data goes. The security is packaged with the file. We can control:

- If you can only View a file
- Print capability
- Edit capability
- Expiration of access after a number of days
- Screenshots
- Watermark
- Requirement for authentication

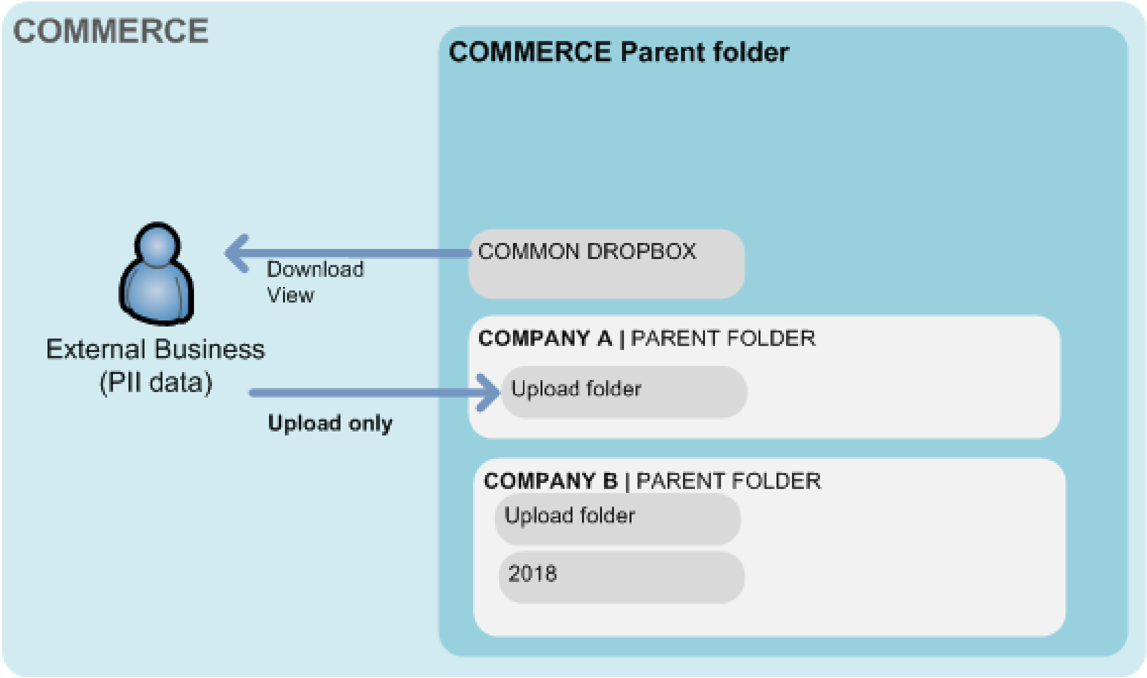
User Management rights (UMT)

- Enables us to provision employee user accounts and groups with Active Directory (AD).
- It allows us to set access rights for a user and file / folder rights

Additional security – These controls require additional Configuration, but are available as needed.

- Password policies
- MFA (Ours is Integrated into remove VPN)
- Jail break detection
- Constrain clip board
- Block camera or Microphone
- Constrain network / Wi-Fi access
- Email white/black listing
- File integrity verification (Hash)

COMMERCE FILE STRUCTURE DESIGN / LAYOUT:


COMMERCE
COMMERCE Parent folder
External Business
(PII data)
Download
View
Upload only
COMMON DROPBOX
COMPANY A | PARENT FOLDER
Upload folder
COMPANY B | PARENT FOLDER
Upload folder
2018