ctera Your Files. Your Cloud.

CTERA White Paper

CTERA Platform Security Architecture

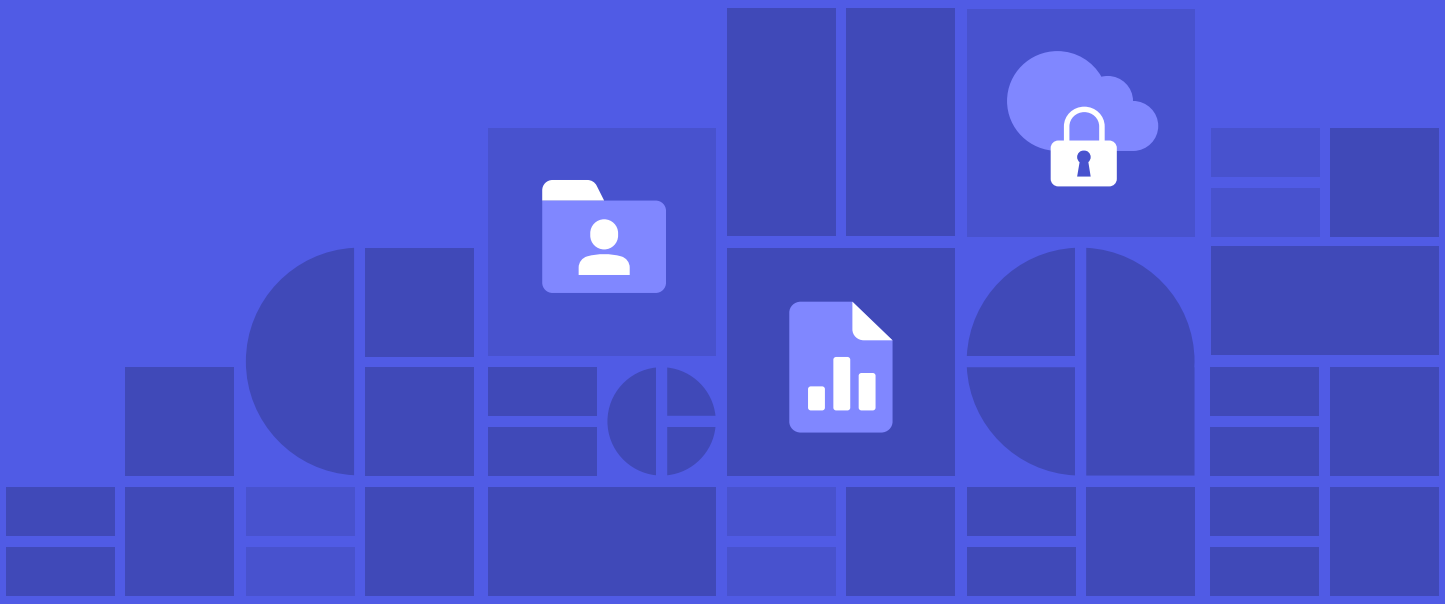
Integrating security into an enterprise-wide cloud-based file services platform

Table of Contents

Introduction

The CTERA Enterprise File Services Platform offers enterprises everything they need to deploy and manage file services such as remote office storage, multi-site file collaboration, and endpoint file sharing and backup. CTERA enables enterprise IT to manage how files are stored, accessed, shared and governed across endpoints, remote sites and the cloud.

Security for enterprises is always is a top consideration, and the CTERA platform was designed to fully protect data from attacks or unauthorized access. This whitepaper reviews the main security aspects of the platform and the steps taken to protect data handled by it. Security considerations are applied to every function of the CTERA platform. For a complete list of "all things security," please review the product documentation and relevant release notes.



What Needs to be Secured?

The CTERA platform supports a variety of file services that can be delivered throughout a distributed enterprise. Among the main file services are:

Remote Office Storage:

Delivering local file storage to remote offices/branch offices (ROBO), with seamless connection to the cloud for backup and synchronization purposes.

Backup/Restore:

Back up files residing on users' workstations or servers to the cloud, and restore them when needed.

Private File Sharing and Collaboration:

Automatically synchronize users' files between multiple devices (desktops, laptops, mobile); allow users to selectively share files and collaborate with others.

Each of the above file services involves handling, storing and transferring sensitive corporate data, which always needs to be secured and protected . To understand the security aspects of the CTERA platform, let's look at its high-level architecture (see Figure 1).

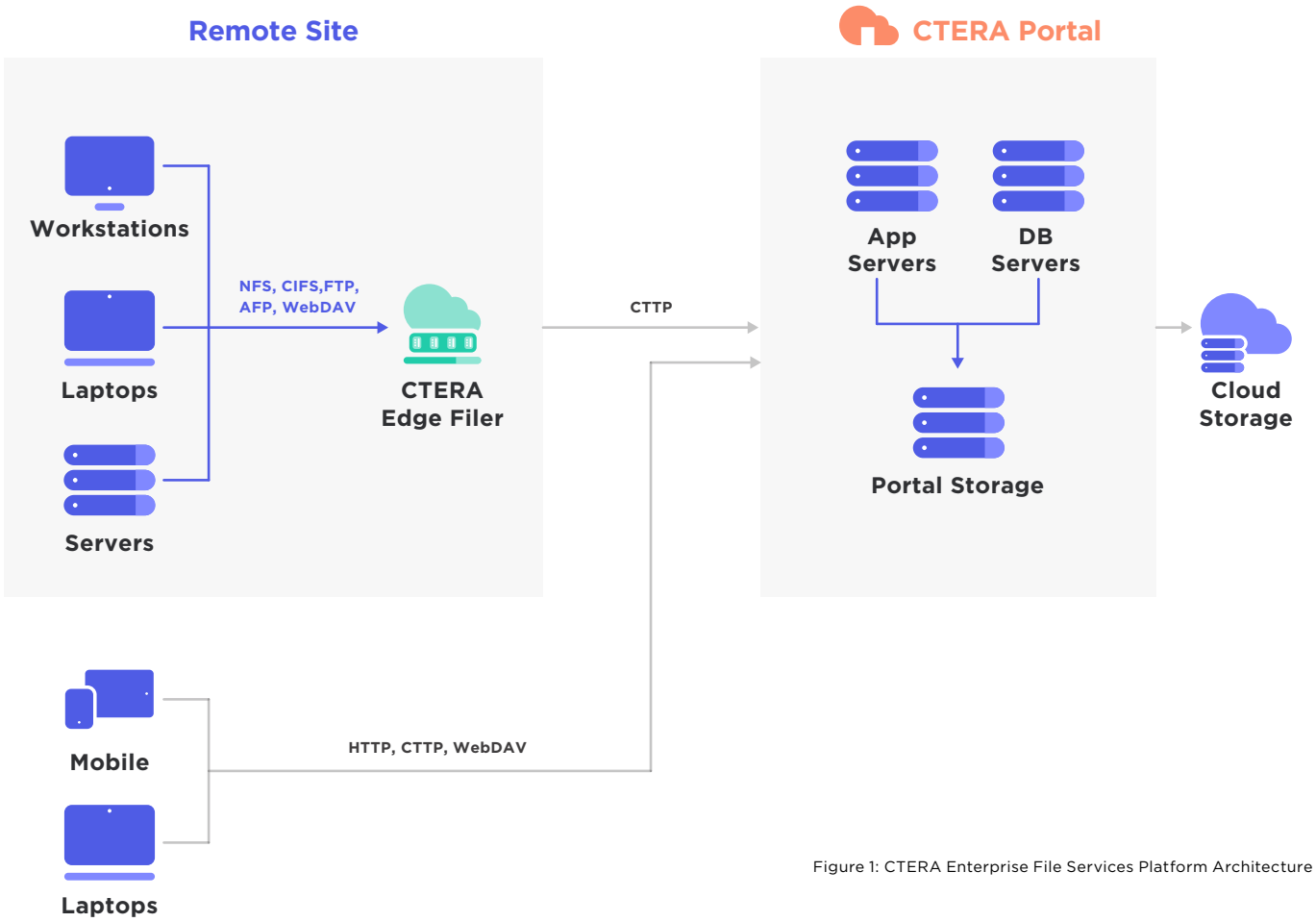


Figure 1: CTERA Enterprise File Services Platform Architecture

The key components of the architecture are:

CTERA Portal

the Portal is a key component of the solution architecture. It handles file traffic to and from the public or private cloud and handles the system management functions. The Portal must be protected from security breaches that may either compromise data or degrade performance. Note that the CTERA Portal can be accessed from a CTERA appliance, software agent or mobile app, and from any regular web browser.

CTERA Edge

Edge filers, or cloud storage gateways, deployed at remote sites to streamline access to/from the cloud. The CTERA appliances do store copies of file data, and therefore must be protected from unauthorized access.

CTERA Drive

Software agents installed on users' laptops/desktops, or on local servers. These agents facilitate communication and file transfer to/from the CTERA Portal, or edge filers. CTERA Drive establishes secure communication to the CTERA Portal/appliance, and encrypts files before they leave a user workstation or a local server.

CTERA Mobile

An app installed on users' smartphones or tablets that facilitates communication to/from the CTERA Portal. As with the software agents, the mobile app must handle encryption of files, and validate access right. Furthermore, in the event of a lost mobile device, the app should perform "remote wipe" of any locally stored data.

CTERA supports flexible deployment modes, including hybrid private/public cloud. The main cloud storage can reside on premises (private cloud); within a virtual private cloud; or on any public cloud. Regardless of its location, all data stored within the cloud is fully encrypted. The Portal and its sub- components are deployed independently of the cloud storage.

For example, the Portal can be hosted on a (virtual) private cloud, while using a public cloud to store encrypted file data.

Security considerations touch every aspect of the CTERA platform and include the following:

File data security
Because files require protection throughout the platform, we start with a discussion about common mechanisms used for protecting files.

Components security
Each component of the CTERA platform has its own unique security requirements. We describe how security is applied to CTERA Portal, Edge, Drive, and Mobile.

File sharing security
Each file sharing scenario with co-workers, outside partners or customers, introduces its own security requirements. We describe how enterprise file sync and share is securely handled in each of these scenarios.

Content security
Files are susceptible to content-related attacks, including viruses, malware, etc. We describe the measures taken to protect files against such attacks.

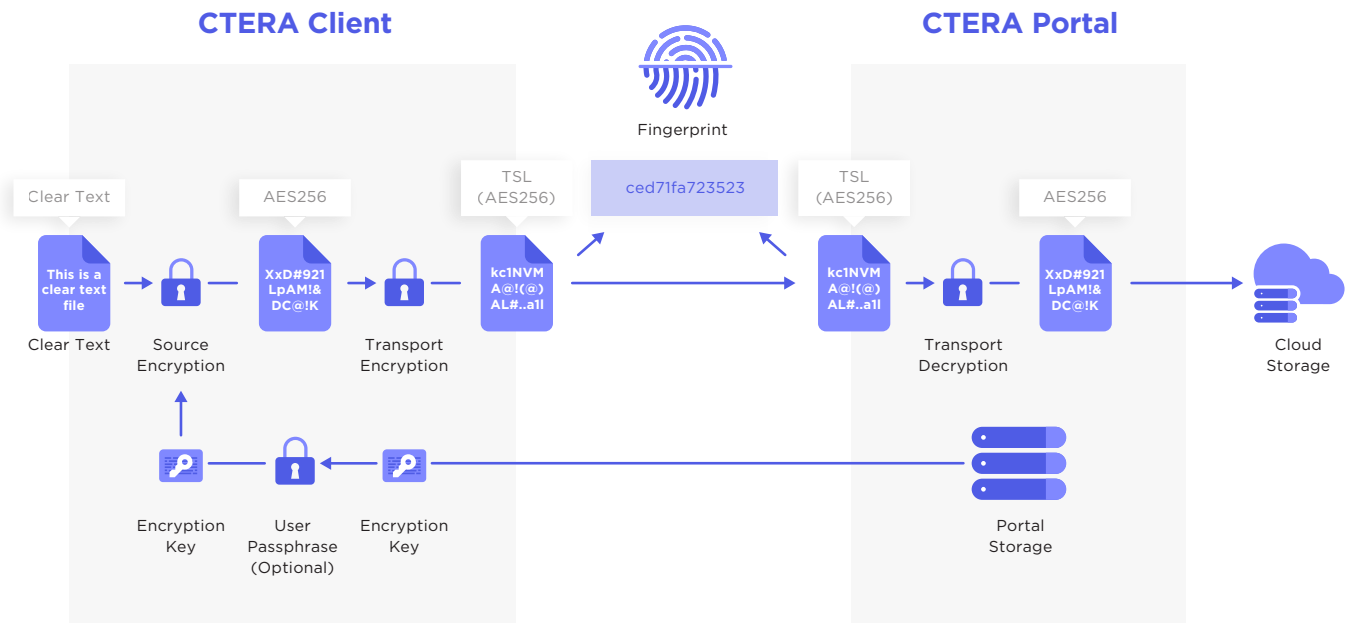
System management
CTERA's platform configuration and its attributes are set through management interfaces. Administrative tasks should be reserved to authorized users, and subject to auditing.

Network security
CTERA platform components are interconnected via the corporate network and use its Internet access. Network security policies should be applied to CTERA platform components as well.

Development methodology
Security is more than a set of features implemented in the system. It requires the use of specific methodologies through the development processes in order to ensure the outcome is indeed a secure system.

File Data Security

Files are the main information that must be secured and protected. They must be protected 'at rest' - when stored anywhere within the system (e.g. on an edge filer or in the cloud) - and also 'in transit' - when transferred between solution components (e.g. between CTERA Drive and CTERA Portal. The general scheme for file data security is described in the adjoined diagram (see Figure 2).



FIPS 140-2 Validation

CTERA's encryption adheres to the highest level of the U.S. military data security standard FIPS 140-2. All data at-rest and in-flight encryption performed by CTERA appliances, software agents, mobile app and Portal is done using FIPS-140-2-validated encryption libraries. The specific details about the various encryption processes are outlined in the sections below.

Encryption At-Rest

AES-256 encryption

Stored files are encrypted using the advanced encryption standard (AES) with its maximum strength of 256 bits.

Source-based encryption

The encryption process is performed by the edge client (e.g. CTERA Edge or Drive) before the files are sent across a network link. A source-based encryption approach ensures that sensitive data never leaves the customer environment before being fully protected.

Passphrase protection

Users who wish to add another layer of protection to files they back up on the cloud can do so via a 'passphrase' known only to them. The two-stage encryption process is as follows:

1. The CTERA client auto-generates a 'data encryption key' (DEK).
2. The designated files are encrypted using the DEK.
3. The user is prompted for a passphrase, known only to them
4. The passphrase is then used for generating a secure 'key encryption key' (KEK).
5. The DEK is encrypted using the KEK to generate an encryption folder key (EFK)
6. The files (which were encrypted using DEK) are stored along with the EFK on the cloud.

To gain access to the files, a "reverse" process is applied:

1. The user is authenticated by the CTERA Portal which grants them access to their folder.
2. The encrypted files and the encryption folder key (EFK) are retrieved by the CTERA client
3. The user is prompted for the passphrase, which is known only to them.
4. The passphrase is used to re-generate the key encryption key (KEK)
5. The KEK is used to decrypt the EFK and re- generate the original data encryption key (DEK)
6. Finally, the DEK is used to decrypt the data and provide the user with access to their files.

In transit

Files are sent across network links between different elements of the CTERA solution architecture (see Figure 1). For example, between the CTERA Edge Filer and the CTERA Portal, or between the CTERA Portal and CTERA Mobile. Every time information is sent across a network link, it must be protected against unauthorized access. This is achieved through various network protocol protection techniques:

CTERA Transfer Protocol (CTTP):

A proprietary and secure protocol used between components of the solution, for example between CTERA Drive and CTERA Portal, or between CTERA Edge and the Portal. The protocol uses Transport Level Security (TLS), with support for versions 1.1 and 1.2.

HTTPS:

On occasions when CTTP can't be used, for example between a web browser and CTERA Portal, a secured version of HTTP is used, using TLS encryption.

Fingerprinting:

To prevent tempering with files in transit, a "fingerprint" is generated for each file using the Secure Hash Algorithm (SHA-1). The fingerprint is checked upon file reception, before any further processing takes place.

Digital Certificates:

To ensure only authorized solution components can communicate with each other, CTERA Portal uses X.509 2048bit certificates, signed by a Certificate Authority (CA). The certificates are used to verify connections between the CTERA Portal and its clients, or with web browsers.

In the Cloud

The ultimate destination of files within the CTERA solution is naturally the cloud. This is where the customer's global file system is located, where file backup copies are stored, and where Cloud Drive folders are used for sharing files between users. CTERA supports three types of cloud storage: private cloud (on the customer premises/corporate datacenter); virtual private cloud (VPC) - hosted by a service provider, yet fully "isolated" from any other cloud customer; and public cloud. CTERA always uses AES-256 bit encryption for storing data – regardless of the type of cloud chosen.

The CTERA Portal uses a separate storage repository for management purposes (see Figure 1). CTERA Portal storage can be hosted separately from the main cloud storage. For example, while the main storage may reside on a public cloud, the Portal storage may reside on premise. The separation of repositories allows CTERA to store a small amount of sensitive data (e.g. encryption keys) in a fully secured site, while managing large amounts of encrypted file data in a less secure site (e.g. public cloud).

File Metadata

Apart from its actual content, each file has metadata associated with it. Metadata could include for example: file name, type, size, creation date, last modification date, access permissions, etc. Organizations usually treat metadata as sensitive information that should not be leaked outside. Within the CTERA solution architecture, metadata is kept in a metadata database, which can be hosted behind the organization firewall, separate from the encrypted bulk data.

Portal Security

The CTERA Portal handles both data processing and management functions. The Portal stores and retrieves files from the cloud on behalf of authenticated devices, software agents or users. In addition, the Portal handles administrative functions, such as user management (including limitations on maximum concurrent user sessions), storage quotas, file sharing policies, device administration, software updates, and many more.

Certificates

Each CTERA Portal is issued a digital certificate that uniquely identifies it. The Portal's digital certificate protects against "man-in-the-middle" attacks: whenever a CTERA client or a web browser tries to connect to the Portal, it uses the digital certificate to validate the true identity of the Portal before actually connecting to it.

CTERA supports standard X.509 TLS certificates, including extensions such as Wildcard certificates, and Subject Alternative Name (SAN) certificates that support the use of a single certificate for multiple (sub)domains. Certificates may be issued by a public and well known 'Certification Authority' (CA), or by a private enterprise CA.

CTERA Portal certificates have expiration dates and should be periodically renewed. Email reminders are sent by CTERA Portal to the Portal system administrator prior to the expiration of the security certificate.

Client Enrollment

CTERA clients must 'enroll' with the Portal before they can exchange data. The enrollment process applies to edge filers, endpoint clients, and mobile apps. The following method is used for enrolling and authenticating clients:

1. The client connects to the Portal and exchanges secure session keys using the TLS protocol
2. The client validates the Portal certificate and ensures it is issued by a trusted certificate authority and matches the Portal DNS address.
3. The client prompts the owner for credentials and sends them over the secure link oruses the SAML (Security Assertion Markup Language) protocol to authenticate with a separate identity provider.
4. The Portal authenticates the provided credentials or SAML token.
5. The Portal generates a unique token using a cryptographically secured random function and provides the token to the client.
6. The client stores the token locally. The owner's user credentials are never persistently stored by the client.

The token is used for authenticating the client to the Portal on all subsequent connections. The token stays in effect until the user signs out. Once the user signs-in again, re- enrollment is performed, a new random token is created, and the old token is invalidated.

User authentication

Users must first authenticate themselves to the Portal before attempting to perform file access or management functions. Administrators can choose to manage users' credentials locally within the Portal, integrate with existing directory services, or use identity management services.

When managing users' credentials locally, the Portal keeps the passwords in the main database, one-way hashed using the PBKDF2-HMAC-SHA-512 key derivation function. Administrators can enforce password policies, such as minimal length, character use, and renewal cycle. However, if the organization already has existing directory services (e.g. Active Directory or LDAP), the Portal can be easily configured to use these directory services for user authentication, avoiding duplicate management of user credentials. The CTERA Portal also supports a variety of Single Sign On (SSO) solutions, including ones based on Active Directory/Kerberos, Oracle Access Manager, or the industry standard Security Assertion Markup Language (SAML).

Client Certificate

For environments with increased security requirements, CTERA supports 'two-factor authentication' using client certificates. Users present an X.509 certificate (e.g. using a common access card (CAC)); the Portal validates their certificate and performs revocation checking via the online certificate status protocol (OCSP); if the certificate is valid, access is granted to the user.

The broad support of authentication methods ensures that services are granted only to authorized users of the CTERA solution.

Role-Based Access

Users are granted different levels of access to the CTERA Portal services. Each user is assigned a 'role' within the Portal that defines which operations can or cannot be performed by that user. There are two main categories of users: end users and administrators.

End users have access to their own data and may configure only their own clients. Administrators have broader access rights, but those are based on their specific administrative role.

Additionally, the Portal's application server requires users to re-authenticate when organization-defined circumstances or situations require re-authentication. Without re-authentication, users potentially would have access to resources or perform tasks for which they do not have authorization.

When applications provide the capability to change security roles or escalate the functional capability of the application, it is critical that the user re-authenticate.

The application server security model may require re-authentication of individuals in other situations, including (but not limited to) the following circumstances:

- When authenticators change
- When roles change
- When security categories of information systems change
- When the execution of privileged functions occurs
- After a fixed period of time or periodically.

Multi-Tenancy

Occasionally, there is a need to handle separate groups of users. This occurs most often when hosting data from multiple customers on a common public cloud, but it increasingly applies to large enterprises managing different organizational units and granting some level of administration autonomy to each of the units.

The CTERA Portal offers built-in multi-tenancy support. Different groups of users can be assigned to entirely separate logical instances of the Portal. Those Portal instances have fully segregated cloud storage data and use separate encryption keys and independent configuration settings. The multi-tenancy architecture ensures that different business units are completely isolated from each other while retaining administrative autonomy.

OS-Level security

The CTERA Portal launches a set of processes that run on its underlying hardened Linux operating system (OS). It is therefore important to block unauthorized OS-level access to the Portal processes and its data. Access to OS system-level accounts on the CTERA Portal is allowed only via the Secure Shell (SSH) protocol.

CTERA Portal's official image and firmware releases are enforced by a digital signature to protect customers during upgrades. As well, CTERA detects any unauthorized software from being installed on the Portal.

The Linux "root" account is used only once by the CTERA Portal - during the Portal installation. All processes run under a special user account which does not have root privileges. To perform system administration operations, CTERA Portal servers contact each other using the SSH protocol, with server-certificate authentication, and an SSH key pair that is automatically generated when the Portal is first installed.

Edge Filer Security

CTERA Edge appliances are used for providing fast, local access to cloud storage at remote sites. They may therefore store local copies of user files (e.g. for backup or file sharing purposes) that must be protected from unauthorized or malicious access. The following measures are taken by CTERA to protect the filers.

User Access and Authentication

Every user access to the filer is first authenticated. Similar to the Portal, authentication is performed either locally (username and password), or through existing directory services (Active Directory). CTERA Edge appliance support two types of user roles: administrator and regular user. The administrator has full access to the filer and can modify its configuration. For example: he can manage storage volumes, create user accounts, define the interaction with the cloud, etc. Regular users can only access their own files or configure policies for the CTERA Drive software agents they have installed on their workstation or laptop. This separation of roles prevents unauthorized access to data stored on the appliance.

Local and Remote Management Access

CTERA Edge filers feature a web-based management interface accessible via HTTPS. Once authenticated, users gain access based on their predefined roles: administrators have full access to the management interface, while regular users have access only to their own functions. The filer's management interface can be reached either locally over the LAN, or remotely via the CTERA Portal interface. When choosing remote access, users are first authenticated by the Portal, and then redirected to the CTERA Edge management interface that matches their specified role.

Data Encryption

User files are stored on the filer's hard disk drives. In order to protect unauthorized access to these files, the filer's storage volumes can be encrypted. When choosing to encrypt contents of a volume, the administrator is prompted to input a passphrase. First, a Password-Based Key Derivation Function (PBKDF2) is used to derive a key for the volume, and the passphrase is then used to encrypt the encryption key using AES-256. This ensures that even if the HDDs are compromised or stolen, user data remains protected.

File Server Security

The CTERA Edge filer functions as a local Windows file server, accessible via standard file protocols (i.e. SMB/CIFS). As such, the filer supports file server security functions such as:

Access Control List (ACLs):

CTERA Edge supports 'Windows ACL Emulation Mode', allowing creation of Windows-compatible access control lists for file shares.

User authentication:

CTERA Edge supports standard Windows authentication schemes, such as Kerberos/AES and NTLMv2

SMB signing:

Signatures of messages between the filer and a Windows client support the SMB protocol. This ensures that any file data exchange between a Windows client and the filer isn't tempered with.

Access-based enumeration:

Filtering the information a specific file share displays according to the user's access rights. If user A doesn't have permission to access Share "X", share "X" won't be displayed to the user.

Screening of file types:

Blocking users from storing certain types of files on the appliance using the SMB/CIFS protocol. For example, if the file screening policy is set to exclude ".exe" files, users will receive an error upon trying to write .exe files to the filer.

Agent Security

CTERA Drive performs two primary tasks: file synchronization (Drive Share) and/or backup (Drive Protect). The Drive agent connects either to a local filer or directly to a Portal. When connected to a filer, the agent backs up files from the workstation where it's installed to a local filer. When connected to the Portal, CTERA Drive may backup files directly to the cloud, and/or synchronize files between the user workstation and designated 'cloud folders'. Whether used for backup, file synchronization or both, CTERA Drive is designed to fully protect both access to the system and the data it handles.

Agent to Portal SSO

Certain user operations require interaction between CTERA Drive and CTERA Portal. For example, inviting team members to view a shared file is done through the Portal, not the local agent. Whenever users are "redirected" to the Portal, a Single Sign-On (SSO) mechanism is used. It spares the users the hassle of re-authenticating themselves, while maintaining full system security. If Active Directory is in place, then Windows based Kerberos tickets are used for the Agent-Portal SSO. Otherwise, the CTERA Portal issues time- limited "tickets' to the agent, and those used by the agent- Portal SSO.

Source-Based Encryption

Any data sent from CTERA Drive to CTERA Portal and then to the cloud is first protected using AES-256 encryption. This source-based encryption (see File data security) ensures that data cannot be compromised or tempered with along its path to the cloud.

Mobile App Security

The CTERA Mobile app can be installed on users' smartphones or tablets. CTERA Mobile can be used for accessing any files and folders shared through the cloud. Naturally, access to information stored in the cloud must be first authorized, and any data stored locally on the mobile device must be fully protected.

User Authentication

When launching CTERA Mobile, users are required to enter their credentials or use SAML authentication in order to authenticate themselves to CTERA Portal. Upon success, the Portal "enrolls" CTERA Mobile (see Client enrollment). In addition, the app can be configured to require a 4- digit PIN code each time it is activated. The PIN code itself is never stored on the device, and CTERA Mobile automatically locks up and removes all the stored confidential data after several failed PIN code entry attempts.

Data Encryption

CTERA Mobile stores any data downloaded from the Portal in an encrypted (AES-256) format. The encrypted data is "sandboxed" from other applications. Encryption keys are generated by the app during the first service enrollment with the Portal, using a secure random number generator.

Key Management

There are two layers of protection for encryption keys that are kept on the mobile device:

On a first level, encryption keys are stored in a device "keychain." The keychain is a secure, OS-provided area for storing keys on a mobile device, and it is supported on Apple iOS, Android and Windows-based mobile devices. The keychain is protected by hardware and cannot be accessed when the phone is locked. The implementation of the keychain varies based on the mobile device model, but in Apple devices, and some Android devices, the keychain is protected by a hardware security module (HSM).

As a second layer of protection, when a PIN code is enabled for CTERA Mobile, the encryption keys are encrypted once again using a key-encryption-key (KEK) derived from the 4- digit PIN. The key derivation process is similar to the one used for passphrase (see File data security). If the PIN code is changed, the encryption keys are re-encrypted with a new PIN code derived KEK.

Mobile Device Management (MDM)

CTERA Mobile supports a variety of mobile device management (MDM) solutions, such as GOOD, Mobile Iron, Airwatch, and XenMobile. These MDM solutions can be used to "sandbox" CTERA Mobile and isolate it from personal data, thus offering higher security for bring your own device (BYOD) scenarios.

Remote Data Wipe

Mobile devices may get lost or stolen, or their owners may leave the organization. CTERA Mobile supports a “remote wipe” feature for lost, stolen or de-authorized devices. The remote wipe process can be initiated by the user; in case his/her device was lost or stolen. Alternatively, the remote wipe can be initiated by a Portal administrator.

File Sharing Security

CTERA supports secure enterprise file sync & share (EFSS). This capability allows users to either synchronize their own files/folders across multiple devices they own or to share selected files with designated users.

Protecting Sync Files

The master copies of synchronized files/folders are stored in the cloud in an encrypted format. They can be viewed or updated through a user owned device: e.g. laptop, desktop, smartphone or tablet. Alternatively, synced files/folders can be accessed through a filer, or by connecting directly to the Portal using a web browser. Each of these access methods requires users to go through an authentication process. Once users are authenticated, the files are decrypted and made available for viewing or editing. The various authentication and data encryption/decryption methods are described in previous sections for each specific access method: CTERA Drive, Mobile, Edge, or Portal.

Protecting Shared Files

Users can mark certain files/folders to be shared other users within the organization, or with outside partners and customers.

CTERA supports collaboration with guests by means of external user invitations (see Figure 3). External user invitations are special time-limited URLs containing a secret code that grants the recipient the ability to view a specific file or folder and to optionally collaborate on those items. The CTERA Portal allows the organization to define which users can collaborate with external guests at the per-user or per-group level.

CTERA Portal supports two-factor authentication for external user invitations, based on random numeric passcodes or "challenges" which are sent to the invitation recipient (by SMS or email), in response to an attempt to access an external user invitation. This feature offers protection against unintended recipients accessing the external user invitation URL.

Two-factor authentication is protected against brute force attacks: Each user is given five tries to enter the code, after which the code is disabled. In addition, rate limits are employed to restrict the number of authentication requests to protect against denial of service attacks.

On private computers, after successfully authenticating using two-factor authentication, the user is given the option of setting their computer as "Trusted". When this option is selected, a 256-bit unique random key is stored on the user's computer as a persistent cookie, allowing the user to bypass two-factor authentication challenges and avoid answering challenges from the same device for the next 30 days.

All accesses to invitations, as well as successful or failed two- factor authentication attempts, are logged.

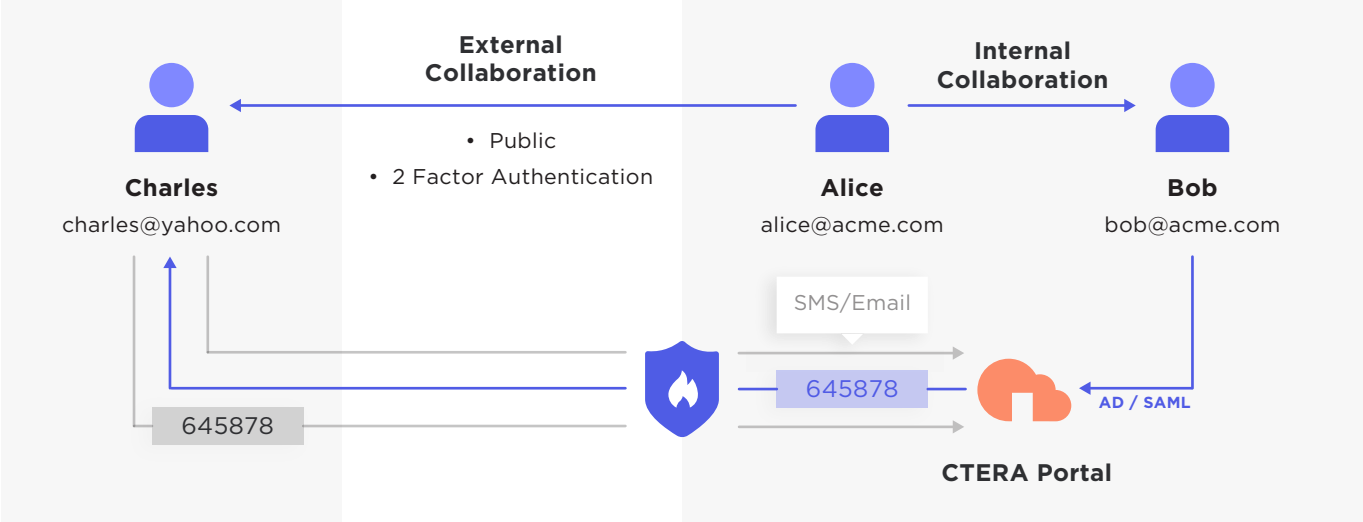


Figure 3 File sharing security

Preview-Only Shares

Users can mark a certain file share as 'preview-only' when inviting other users to access it. Recipients of preview-only invitations are unable to download, copy, or print files from that share. They can only view files via the Portal 'document preview server.' Files viewed that way have a watermark which includes the recipient e-mail address (if present) or its IP address. In addition, content shared as 'preview-only' cannot be synchronized for offline access by CTERA Drive clients, Edge filers, or mobile devices.

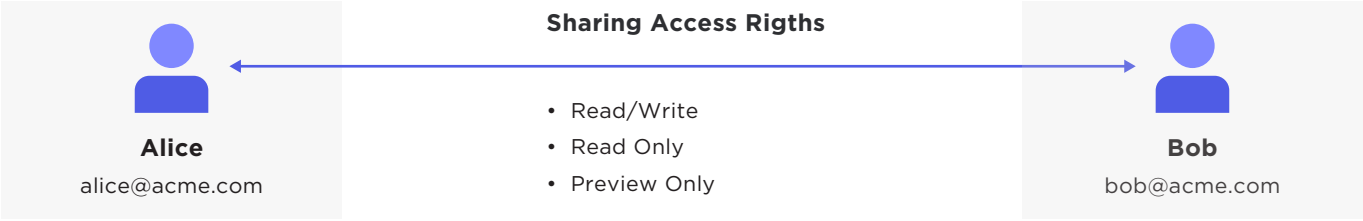
'Shared by Me'

Users and administrators can centrally govern both internal and external links and collaboration shares. If granted with permission, they can manage the list of recipients, their access rights or even choose to revoke file or folder access altogether.

File-Sharing Permissions

Users are granted different permission levels to files shared with them. Permissions are set to either: 'Read/Write,' 'Read-Only' or "Preview-Only'. The assigned permissions determine the type of file operations each user can perform on files shared with them.

The following table summarizes the permitted file operations associated with each user permission:



File Operation	Read/Write	Read	Preview
Preview	✓	✓	✓
Download	✓	✓	✗
Copy	✓	✗	✗
Move	✓	✗	✗
Delete	✓	✗	✗
Rename	✓	✗	✗
Edit	✓	✗	✗
Upload	✓	✗	✗
Print	✓	✓	✗
Create Folder	✓	✗	✗
The following are available to Portal users only			
Sync to Local	User defined	User defined	✗
Copy	User defined	User defined	✗
Re-share	User defined	User defined	✗
WebDAV access	✓	✓	✗

Note that the last three operations are available only to 'internal users' (i.e. known to the Portal). The ability to store a local copy, or re-share with another user is granted by the file owner, unless otherwise set by the Portal administrator.

Moreover, CTERA Portal supports the Windows NT standard for applying file and folder security permissions and access control list. The ability to enforce Window NT security permissions on CTERA Portal enables seamless disaster recovery from CTERA Edge appliances, as well as access via modern interfaces such as: web, mobile apps and more.

Content Security

Predefined content security policies can be applied to files processed and managed by the CTERA platform. Some of these policies are enforced natively by CTERA, while others leverage integration with 3rd party security tools.

Allow/Deny Policies

CTERA lets Portal administrators define rules specifying the type of data that can be synchronized or uploaded to the cloud. Both 'deny' and 'allow' rules are supported, based on the file size, name or extension. Each rule can be applied to everyone or to a specific user or group. It is also possible to apply allow/deny rules to external users, who were invited to collaborate on specific files or folders.

Antivirus

CTERA integrates with antivirus vendors through the ICAP protocol for file scanning, in order to ensure

data protection. Some of the supported antivirus vendors are McAfee, Symantec, Sophos and ESET. Files are scanned for malware automatically and transparently, before they are downloaded from the Portal for the first time (On-Access) or as part of a background scan.

Content Sharing Policies

Administrators can define granular policies that govern the way files are shared with external users. These policies define the allowed collaboration methods – for example allow/deny the use of public links, enforce preview-only shares, etc. Content sharing policies can prevent leakage of sensitive data out of the corporate firewall.

System Management Security

System-wide configuration and management of the CTERA solution is performed through the Portal. The Portal can also provide remote access to agents and filers, functioning as a central management platform.

Role-Based Access Control

The CTERA Portal can be configured to support multiple "virtual Portals," each representing a separate group of users. Accordingly, there are two levels of administrators:

- **Global administrators,** who have access to the global administration interface, and to the Portal administration interface for all virtual Portals.
- **Portal level administrators,** who have access to the administration interface of a single virtual Portal.

By default, CTERA Portal includes three built-in administrator roles:

- **Read/Write Administrator.**
  The administrator has read- write permissions throughout the CTERA Portal. Read Only Administrator. The administrator has read-only permissions throughout the CTERA Portal.
- **Support.**
  The administrator has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the CTERA Portal.

The Portal advanced role-based access control ensures that sensitive operations are accessible only to a limited set of authorized users.

- **File-based policies**
- **File permissions:** block access of certain file types and sizes
- **Collaboration policies** for specific domains

Logging and Auditing

In an era of data breaches and internal misuse of information, it's critical for IT administrators to have a clear view into their network. Logging is an important security function that allows administrators and external auditors to trace and analyze system actions over time.

In general, logged events belong to one of the following categories:

- Management changes: any changes made to the system configuration, policies, plans, etc.

CTERA supports extensive, military-grade logging. For example, system log files include the following:

- All actions performed by an administrator are logged. This includes for example: changes in portal's settings, roles, plans, share policy, etc.
- All login/logout attempts, along with start/end time for user access to the system
- Concurrent login attempts from different workstations
- Application shutdown events
- The identity of individuals or processes associated with a logged event, along with the event time and outcome.

The CTERA-generated logs can be processed other systems. The audit log messages are formatted using JSON, allowing external system to easily parse and analyze them.

The system continuously monitors the logging process to ensure its successful operation:

- An immediate warning is provided when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity.
- Administrators are immediately notified on any failure in the logging system
- The system can be optionally configured to trigger a device shutdown upon logging failure.

Access by CTERA Personnel

CTERA Portal runs entirely within the customer premises (behind the firewall). CTERA personnel do not require any access to the customer Portal, and providing remote access is not a precondition for CTERA's support services. In case a remote support session is desired, the Portal owner may provide CTERA support with temporary access.

Network Security

The CTERA solution elements are deployed at various network locations. CTERA Drive and CTERA Mobile are deployed on user devices (laptop, desktop or mobile) and therefore benefit from any network protection the device has. CTERA Edge filers are deployed at remote sites, and benefit from each site's network protection services. The Portal on the other hand is deployed either on the customer's datacenter network (i.e. private cloud), on a hosted yet isolated network (i.e. virtual private cloud - VPC), or on a hosted and shared network (i.e. public cloud).

Firewall

CTERA Edge appliances sit behind the remote site firewall and enjoy its protection. A Portal deployed inside a datacenter benefits from customer-defined firewall services. The same applies to a Portal deployed inside a VPC, which is isolated and protected by customer-defined firewalls.

It is possible to place the Portal application servers and database servers each in their own separate networks, with

different firewall policies. This means that only the application servers need to face the Internet, shielding the sensitive database servers from the hazards of unsecured networks.

Port Configuration

The Portal and the Edge appliance utilize network connections that must cross the firewall. These connections include both standard protocols and ports (e.g. HTTP, HTTPS) and the CTERA transfer protocol (CTTP). It is therefore important to consult the CTERA documentation for protocols and ports used, and to configure the firewall rules to allow operation of these protocols/ports.

Intrusion Detection

Much like firewall services, CTERA Edge and CTERA Portal benefit from any intrusion detection and prevention services (IDS/IPS) that apply to the rest of the customer network – at the remote site, the datacenter, or the virtual private cloud.

CTERA Portal allows HTTPS traffic to be offloaded to a load balancer (e.g. F5). In such configuration it is possible to place IDS/IPS solutions or WAF (Web Application Firewall) on the network between the load balancer and the Portal servers in

IP Whitelisting

The CTERA Portal supports configuring a list of specific IP address ranges, from which administrators can access the CTERA Portal's web interface. This ensures that administrative functions of the Portal are accessible only from approved network locations.

Development methodology

CTERA's development lifecycle for software and hardware is highly methodical and includes specific provisions for code reviews and inspections, as well as thorough automatic and manual testing procedures. All designed to minimize security vulnerabilities and other defects. CTERA implements internal security validation processes which are based on industry best practices and standards, such as the Open Web Application Security Project (OWASP) "Top Ten Projects" and others.

In addition to internal code reviews, a well-known third- party certification lab retained by CTERA regularly performs independent third-party code review for security-critical code segments. Penetration testing is performed through use of automated and manual tools in combination with security review of critical code sections as recommended by the OWASP and WASC methodologies. Following is a partial list of vulnerabilities tested by CTERA:

- SQL Injection: taking control over the CTERA Portal database
- Hidden Backdoors: used by attackers to easily infiltrate the system over and over
- Cross-Site Scripting (XSS): injecting malicious code into innocent user's browsers
- Cross-Site Request Forgery (CSRF): impersonate a user and perform actions in his name
- Bypassing Authentication: taking over users and administrators accounts
- Authorization Breaches: performing unauthorized actions and accessing unauthorized information
- Bypassing Crypto: viewing of confidential and private info by unauthorized people
- Command Injection: injecting commands to a remote server and taking over
- Denial of Service: making the application unavailable to remote users
- And more...

CTERA implements a vulnerabilities patching policy, which involves periodic issuance of images with up-to-date vulnerability patches. Customers get access to updated software images for critical vulnerabilities.

The security aspects of the CTERA platform evolve as new functionality is added and enhancements are made. For the latest security capabilities please review the CTERA product documentation and the relevant release notes.

Summary

The CTERA Enterprise File Services Platform was designed from the ground up to fully protect the files it handles. Advanced encryption techniques along with strong authentication mechanisms ensure that files are accessible only to authorized users. This paper described numerous platform security features; let's just recap the highlights:

Source-based AES-256 encryption:

Data is encrypted before it is sent to the cloud and remains encrypted as it is stored.

In-Transit TLS encryption:

All network transfers use Transport Level Security (TLS) 1.2 protocol, preventing unauthorized interception of data.

SHA-1 data fingerprinting:

Ensures data integrity as it travels between locations, prevents man-in-the-middle attacks and transfer errors.

Private encryption key management:

Manage your own encryption keys or use personal passphrases per user to prevent privileged admins from accessing data.

Single Sign-On (SSO):

Use your SSO and ID management tools of choice to provide seamless user authentication and avoid duplicate credentials.

Role-based access control:

Define Active Directory or LDAP roles and groups to control access to data and set up administrator roles.

2-Factor authentication for file sharing:

Use email and SMS-based two-factor authentication for external file sharing to ensure only intended parties can access files

Deploy at your cloud of choice:

Deploy on-premises or in a virtual private cloud (VPC) to keep your data within your network and 100% behind your firewall.

Granular event logging:

Monitor and log security events such as user access and failed logins and integrate with third-party audit trail retention and reporting.

Restricted content policies:

Define rules based on file size, name, or type that deny or allow files to be shared externally or uploaded to your network

3rd party security tools:

Integration with third-party security tools (e.g. Anti-Virus and MDM) extends the CTERA platform security capabilities.

The rich security capabilities described in this document ensure that files are protected by the CTERA platform wherever they are stored ("at rest") and whenever they are sent ("in transit"). CTERA allows enterprises to deploy and manage cloud-based file services with complete peace of mind and without any security compromises.