TeraGo Cloud Drive

TERAGO CLOUD DRIVE SECURITY ARCHITECTURE

Integrating security into an enterprise-wide, cloud-based file sync and share

TeraGo Cloud Drive

Table of Contents

Introduction

The TeraGo Cloud Drive platform offers enterprises everything they need for a file sync and share service. It manages how files are stored, accessed, shared and governed across end points, remotes sites and the cloud. Security is a top consideration, and the Cloud Drive 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 Cloud Drive platform. For a complete list of "all things security", please review the product documentation and relevant release notes.

What needs to be secured?

Delivering a world-class Enterprise File Sync and Share service involves handling, storing and transferring sensitive corporate data, which needs to be secured and protected at all times. To understand the security aspects of the Cloud Drive platform, let's take a look at its high level architecture (*see Figure 1*). The key components of the architecture are:

- ***Portal***: the portal is a key component of the solution architecture. It handles file traffic to and from the TeraGo 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 Cloud Drive portal can be accessed from our TeraGo software agent, software agent or mobile app, and from any regular web browser.

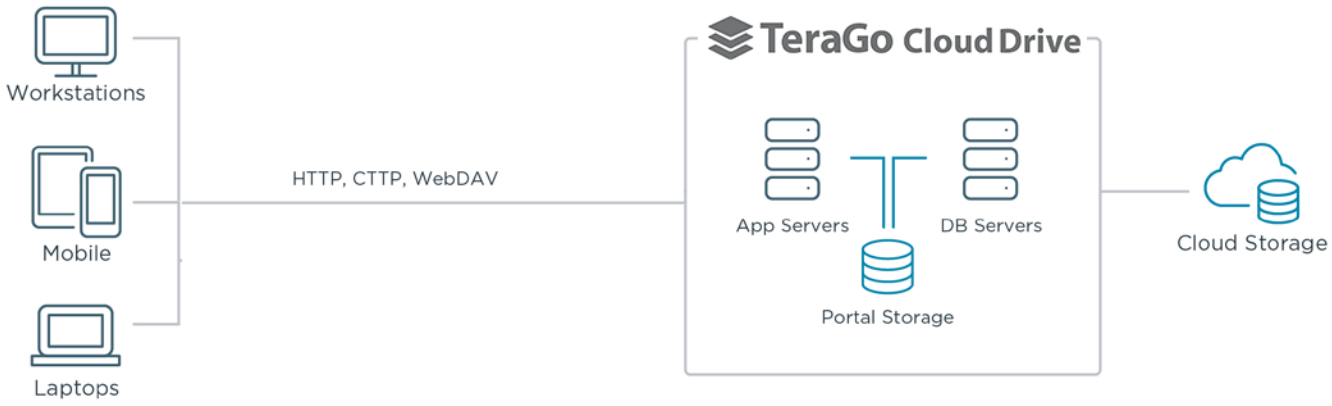


Figure 1 TeraGo Cloud Drive Platform Diagram

- ***Software Agents***: installed on users' laptops/desktops. These agents facilitate communication and file transfer to/from the Cloud Drive portal. The software agent establishes secure communication to the Cloud Drive portal, and encrypts files before they leave a user workstation.

- ***Mobile App***: installed on users' smartphones or tablets, and facilitates communication to/from the Cloud Drive 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.

Security considerations touch every aspect of the Cloud Drive platform, and can be discussed in any order. The one chosen for this whitepaper is:

- ***File data security:*** since files require protection throughout the platform, we start with a discussion about common mechanisms used for protecting files.
- ***Components security:*** each component of the platform has its own unique security requirements. We describe how security is applied to the Cloud Drive Portal, Software Agent and the Mobile App.
- ***File sharing security:*** each file sharing scenario, with co-workers, outside partners or customers, introduce its own security requirements. We describe how sharing is securely handled in each of these scenarios.
- ***Content security:*** files are susceptible to content related attacks, including viruses etc. We describe the measures taken to protect files against such attacks.
- ***System management***: the platform configuration and its attributes are set through management interfaces. Administrative tasks should be reserved to authorized users, and subject to auditing.
- ***Network security***: components of the Cloud Drive platform are interconnected via the corporate network and use its Internet access. Network security policies should be applied to Cloud Drive platform components as well.
- ***Development methodology***: security is more that 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.

With that order in mind, let's dive into the discussion about the platform security aspects.

File data security

Files are the main information that must be secured and protected. They must be protected 'at rest', that is when stored anywhere within the system; and files must also be protected 'in transit', when transferred between solution components (e.g. between an agent and the Portal). The general scheme for file data security is described in the adjoined diagram (see *Figure 2*). The specific details about the various encryption processes are outlined in the sections below.

At Rest

Files may be kept at different locations, for example: on a user laptop, the target cloud storage, or when downloaded to a mobile device. To protect files that are stored anywhere, Cloud Drive uses advanced encryption techniques:

- ***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 done by the client (e.g. Cloud Drive software agent) before the files are even sent across a network link. The source-based encryption approach ensures that sensitive data never leaves the customer environment before being fully protected.

In Transit

Files are sent across network links between different elements of the Cloud Drive solution architecture (*see Figure 1*). For example, between an end user laptop and the Cloud Drive Portal, or between the Cloud Drive Portal and a mobile device. 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:

- **Cloud Drive Transfer Protocol (CTTP):** is a secure protocol used between components of the solution, for example between an agent and the Portal. The protocol uses Transport Level Security (TLS), with support for versions 1.0, 1.1 and 1.2.

- **HTTPS:** where CTTP can't be used, for example between a web browser and the Cloud Drive Portal, a secured version of HTTP is used, using TLS encryption.

- **Fingerprinting**: to prevent tampering 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**: are used for verifying that only authorized solution components can communicate with each other. The Cloud Drive Portal uses X.509 2048bit certificates, signed by a Certificate Authority (CA). The certificates are used to verify connections between the Cloud Drive Portal and its clients, or with web browsers.

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 Cloud Drive solution architecture, metadata is kept in a metadata database, separated from the encrypted bulk data.

Encryption Key management

Encrypted files are impossible to decipher, unless of course one gains access to the encryption keys. In order to protect unauthorized access to encryption keys, Cloud Drive stored them in the metadata database, which is hosted behind TeraGo's best-in-class firewall and security architecture. Access to the Portal itself is guarded through a variety of security measures listed below.

Portal security

The Cloud Drive 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, storage quotas, file sharing policies, device administration, software updates, and many more.

Certificates

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

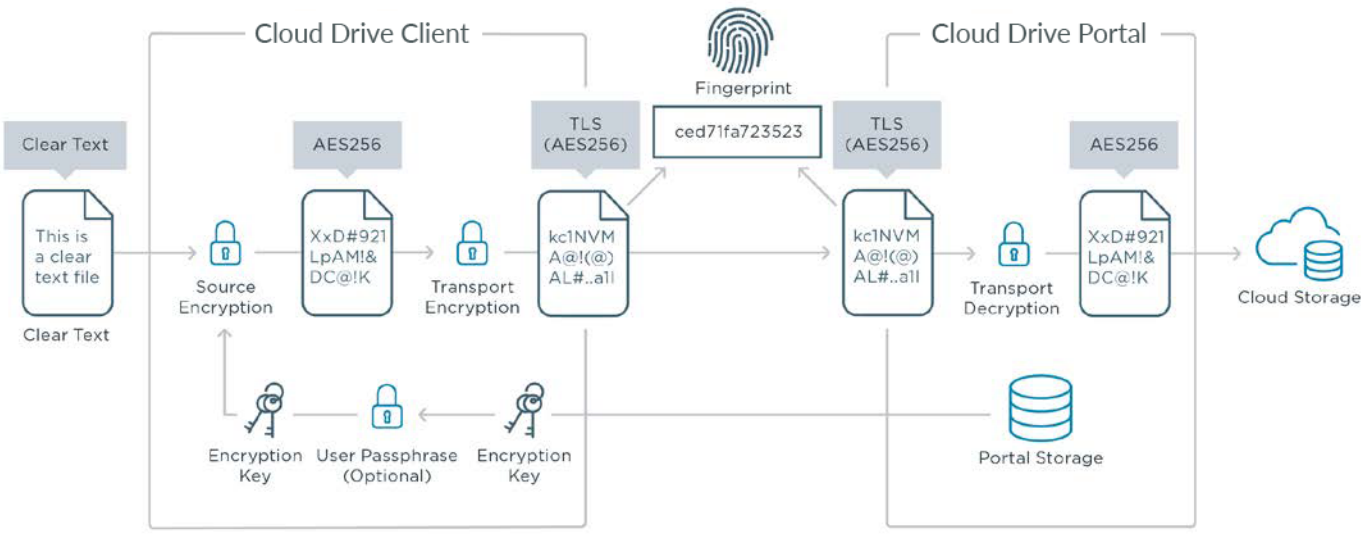


Figure 2 File protection scheme

Client enrollment

Cloud Drive clients must 'enroll' with the Portal before allowed to exchange data. The enrollment process applies to cloud software agents 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 that 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, OR uses 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), then the Portal can be easily configured to use these directory services for users' authentication, avoiding duplicate management of user credentials. The Cloud Drive 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).

Role-based Access

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

End users have access their own data and may configure only their own clients. Administrators have broader access rights, but those are based on their specific administrative role (see *Role-based Access*).

Agent security

The Cloud Drive Agent performs the task of file synchronization. The Agent connects directly to a Portal. When connected to a Portal, the Agent will synchronize files between the user workstation and designated 'cloud folders'. The Cloud Drive agent 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 the Agent and the 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 Cloud Drive Portal issues time-limited "tickets' to the Agent, and those used by the Agent-Portal SSO.

Source-based Encryption

Any data sent from Agent to the Portal and then 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 TeraGo Cloud Drive Mobile App can be installed on users' smartphones or tablets. The Mobile App 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 the Mobile App, users are required to enter their credentials or use SAML authentication in order to authenticate themselves to Cloud Drive Portal. Upon success, the portal "enrolls" the Mobile App (see *Client enrollment*). In addition, the Mobile 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 the Cloud Drive Mobile App automatically locks up and removes all the stored confidential data after several failed PIN code entry attempts.

Data encryption

The Mobile App 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 Mobile 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 and Android 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 the Mobile App, 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)

The Cloud Drive Mobile App 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" the Cloud Drive Mobile App 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. Cloud Drive 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

Cloud Drive supports secure, enterprise file sync & share (EFSS). This capability allows users to either synchronize their own files/folders across multiple devices they own, or 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 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: the Cloud Drive Agent, Mobile App, 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.

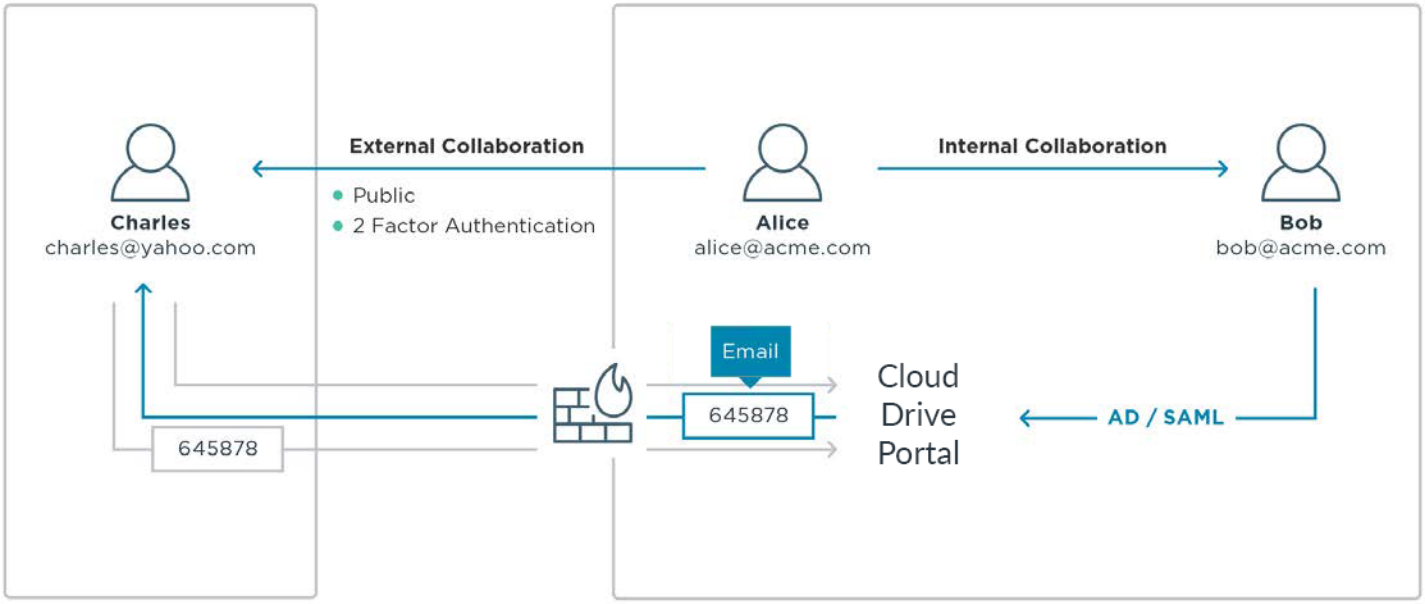


Figure 3 File sharing security

Cloud Drive 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 Cloud Drive Portal allows the organization to define which users are allowed to collaborate with external guests at the per-user or per-group level.

Cloud Drive Portal supports two-factor authentication for External user invitations, based on random numeric passcodes or "challenges" which are sent to the invitation recipient (by 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, so as 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.

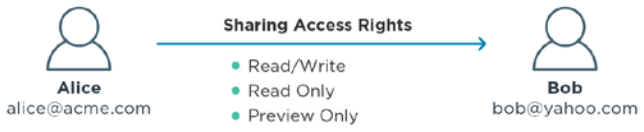
All accesses to invitations, as well as successful or failed two-factor authentication attempts, are logged.

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 it's IP address. In addition, content shared as 'preview only' cannot be synchronized for offline access by Cloud Drive Agents and Mobile App.

File-sharing permissions

Users are granted different permission levels to files which are 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 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.

Content security

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

Allow/Deny Policies

Cloud Drive 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.

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

Configuration and management of the Cloud Drive solution is performed through the Portal.

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

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

Logging & Auditing

The Cloud Drive Portal maintains extensive logging of all configuration and data changes. One of the log types displayed are Audit logs, which document various configuration changes. Audit logs include information on the action type, account name, date, timestamp, target, and more. The Cloud Drive Portal can also log all file changes and file accesses.

The Portal 'Audit Log Viewer' is available for portal administrators.

Cloud Drive audit logs can be automatically forwarded to an organizational Syslog server for log analysis, threat detection, protection against log tampering, and long-term storage. Log messages can be forwarded via the syslog protocol for long term safekeeping and analysis.

Network security

The Cloud Drive solution elements are deployed at various network locations. The Agent and the Mobile App are deployed on user devices (laptop, desktop or mobile) and therefore benefit from any network protection the device has.

Development methodology

Cloud Drive's development 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. Cloud Drive implements 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 regularly performs independent 3rd 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:

- *SQL Injection*: taking control over the Cloud Drive 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…

  Cloud Drive implements a vulnerabilites 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 Cloud Drive platform evolve as new functionalty is added and enhacements are made. For the latest security capabilities please review the Cloud Drive product documentation and the relevant release notes.

Summary

The Cloud Drive 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, so 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) 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 two-factor authentication for external file sharing to ensure only intended parties can access files
- Granular event logging: monitor and log security events such as user access and failed logins, and integrate with 3rd 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

The rich security capabilities described in this document ensure that files are protected by the Cloud Drive platform wherever they are stored (“at rest”), and whenever they are sent (“in transit”). Cloud Drive allows enterprises to deploy and manage Enterprise File Sync and Share with complete peace of mind and without any security compromises.