your Digital file®

SMARTER SECURITY

Security Technology Whitepaper

Security Technology

Whitepaper

www.yourdigitalfile.com

E: info@yourdigitalfile.com

P: 1300 791 915 (Australia)

+61 7 3839 0387 (International)

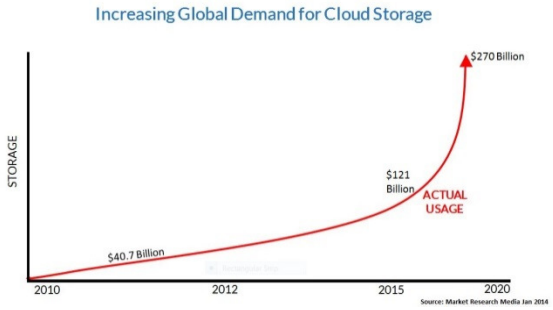
October 2015

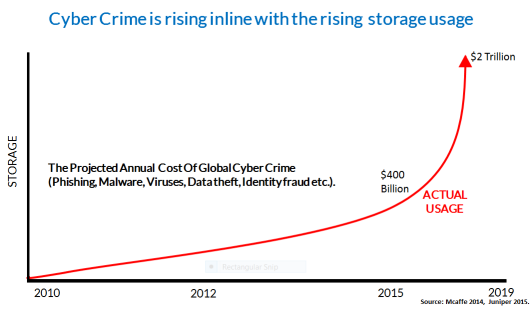
The cloud is not risk-free

All cloud storage solutions promise security.

The real question is — how secure is 'secure' ?

The escalation of cybercrime globally indicates cloud storage 'security' is greatly overstated by most providers. Several popular services continue to incur significant data breaches, with often the only defence offered to users is a reminder to 'frequently change your password'.





How can you decide which cloud services truly deliver what everyone wants?

That is — guaranteed document confidentiality and integrity.

Your Digital File, with its patented Cryptoloc security technology, is at the forefront of secure digital document management.

If information privacy, confidentiality and integrity matter to you, then Your Digital File is the solution.

Our security advantage explained…

What does patented security mean?

- It means Your Digital File has developed a custom process employing advanced encryption algorithms to uniquely secure each and every file

What does this mean for you and your clients?

- Your Digital File can never view the contents of any files
- The contents of all files are always protected
- Only you, and the people you authorise, can access your files
- Once uploaded to Your Digital File, your files are always securely recoverable, even if you delete them or lose your private key, password or login credentials
- *Information privacy and document integrity are guaranteed for each and every file. No compromises. Ever.*

How does Your Digital File deliver superior security?

- Your Digital File is the leading global cloud solution for the secure management of confidential documents online. It ensures that files are never compromised by employing a unique combination of advanced security features:

1. Strong User Identity Binding to Client-side Encryption Keys

- On registration, in addition to a username and password, the user creates a cryptographic key pair:
- A Private Key which is generated and stored on your device and is used for decryption and digital signing of files, and
- A Public Key which is stored within Your Digital File and is used by the user, the system and other users for encryption and to verify digital signatures
- To sign and share documents, users must successfully complete Your Digital File's rigorous identity verification process. This provides a high level of assurance for all verified users

2. Cryptoloc Security — Our Advanced, Patented Key Management System

- Cryptoloc technology generates three unique encryption keys for each document and combines these keys to create a Document Encryption Key
- This key (the Document Encryption Key) is used to encrypt and decrypt documents on the user's device
- Cryptoloc technology gives the user complete document control and confidentiality, as the user must use their private key to grant other users access to their documents.
- The three components of a Document's Encryption Key are stored in a manner which prohibits decryption by a single entity
- This ensures your documents remain completely confidential and protected, unable to be accessed by both Your Digital File or any malicious intruders in the unlikely event of a breach of our systems
- *In most other cloud storage solutions, such as Dropbox, the user's document encryption keys are always available to the service provider*
- *If these cloud services are compromised, all document encryption keys are exposed and the user's information is accessible*
- *In many highly secure cloud storage solutions the key is only stored client-side, and if the client loses their encryption keys, their documents are lost and unrecoverable*

3. Client-side encryption

- All file encryption (and decryption) takes place on the user's device, before being uploaded to Your Digital File
- Client-side encryption ensures all users' data is protected 'in transit' and 'at rest'

- All communications with Your Digital File (including transmission of the encrypted documents, encrypted key material and any metadata) are conducted via high-strength encrypted TLS tunnels

4. Escrow Model

- YDF provides an Escrow model for secure account recovery and access following a data legacy 'trigger event'
- The escrow is a trusted, neutral third party which does not have access to encrypted documents and can never view the user's files

How are the encryption keys distributed and protected?

- Three pairwise combinations of these keys are distributed to the user, the system and the escrow and encrypted by each party's Public Key

User	YDF	Escrow
Keys 1 & 2	Keys 2 & 3	Keys 1 & 3

- To decrypt the original document, two parties must successfully cooperate to recreate the original Document Encryption Key
- The user decrypts these key components using their Private Key and then recreates the original Document Encryption Key and decrypts the document client-side (on the user's device)

What happens in the background

Here's the technical reason why Your Digital File's advanced patented security technology is the leading cloud solution for the secure management of documents and files online….

When you sign up to Your Digital File ...

Along with creating a username and password, you create a (2048-bit RSA) cryptographic key pair:

a. **A Private key** which is stored only on your device, is password protected using your login password, and is used to digitally sign documents and decrypt document encryption keys; and

b. **A Public key** which is stored by Your Digital File and is used by the system, escrow and other users to encrypt and securely share document encryption keys (that only your Private Key can decrypt) and to verify digital signatures created using your Private Key.

As well as successfully authenticating to Your Digital File using your username and password, your Private Key must be present (and decrypted using your password) before any document can be downloaded, shared or signed. Your Private Key is stored only by you and must never be shared with anyone.

When you upload a document to Your Digital File, here's what happens …

All documents are encrypted pre-upload, transmission and rest.

Uploading documents…

1. Once your Private Key has proven your identity to Your Digital File, you calculate a unique "fingerprint" (SHA-512) on your computer for the unencrypted document.
2. Using your Private Key, you then digitally sign the "fingerprint" and a timestamp (which represents the current date and time), creating a (SHA-512 with RSA) digital signature of the unencrypted file.
    - This digital signature provides non-repudiation of origin, proving you uploaded this document at a specific date and time, and is used to verify the integrity of the document upon download from Your Digital File after being decrypted by authorised users.
3. Your computer then creates three unique, randomly generated (AES-256) symmetric encryption keys (*Primary* Document Encryption Keys, $DEK_1/DEK_2/DEK_3$) which, when combined, create the unique Document Encryption Key ($DEK_1+DEK_{2+}DEK_3=DEK$).
4. The Document Encryption Key (DEK) is then used to encrypt your document.
5. Next your computer encrypts the Primary Document Encryption Keys using Public Key Cryptography.
    - The Primary Document Encryption Keys are distributed between the different parties in the system (User, System, Escrow/Other), with no single Private Key protecting all three of a document's Primary Document Encryption Keys.
    - Two of these three keys are allocated to you, the User (DEK_1^u/DEK_2^u), two to Your Digital File, the System (DEK_2^s/DEK_3^s) and two to your Escrow Agent or Business Recovery Account and any other users with whom you shared the document (Escrow–DEK_1^e/DEK_3^e and Other–DEK_1^o/DEK_3^o) and encrypted using the Public Keys of each authorised party.
    - This patented process ensures your documents remain completely confidential and protected, unable to be accessed by both Your Digital File or any malicious intruders in the unlikely event of a breach of our systems.
6. A second digital signature is created, using the procedure outlined above, based on the *encrypted form* of the original document.
    - This is to ensure the document's integrity from its point of origin (your computer), prior to being uploaded to Your Digital File and protects against corruption both during transmission to and from Your Digital File and while stored ("at rest") on our servers.
7. Both digital signatures, including "fingerprints" (based on the unencrypted and encrypted document), the encrypted document and the encrypted Primary Document Encryption Keys (a minimum of 6–two for each authorised party) are securely uploaded to Your Digital File using high-strength SSL technology.

- The system then verifies the digital signatures of encrypted document and all keys before storing the (encrypted) Primary Document Encryption Keys, the encrypted document, its "fingerprints" and associated digital signatures on our servers.

Here's what happens when you download, share, sign or update documents…

Downloading documents…

1. When downloading your documents from Your Digital File, the system decrypts the Primary Document Encryption Key you are missing (not stored encrypted with your Public Key–DEK_3) and re-encrypts it with your Public Key
2. The system then sends all three encryption keys (protected by your Private Key–DEK_1^u/DEK_2^u/DEK_3^u), the encrypted document and its "fingerprints" (created in uploading steps 1-6) to your computer.
3. Your Private Key is used to decrypt the encrypted Primary Document Encryption Keys and rebuild the Document Encryption Key.
4. The document is then decrypted on your computer using the Document Encryption Key and its integrity verified using the original "fingerprint" created when originally uploaded.

Sharing documents…

1. If you share a document with another party, the system sends one of your Primary Document Encryption Keys and the Public Key of the other user to your computer.
    - The Primary Document Encryption Key sent is the one the system can not access – DEK_1^u, which was created protected when the document was uploaded (see Uploading steps 3 & 5.
2. Your Private Key is used to decrypt this key, then re-encrypt this key using the Public Key of the other user.
    - This creates a encrypted Primary Document Encryption Key the other user can later decrypt (DEK_1^o).
3. This new key is then uploaded to the system using high-strength SSL technology and stored in the system, allowing the other person to download and access the document.
    - On Your Digital File's servers, the system performs the same process for the Primary Document Encryption Key which is not stored protected with your Public Key and re-encrypts it with the Public Key of the other user.
    - This creates a second encrypted Primary Document Encryption Key the other user requires when accessing the shared document (DEK_3^o).

Signing documents…

1. When a user legally signs a document, the system sends the unique "fingerprint" of the original document to their computer.
2. They use their Private Key to create a digital signature (of the received fingerprint and a timestamp), confirming their agreement to the content of the document.

3. This signature is then uploaded to Your Digital File and stored along with the document in the system.

Updating documents…

- If a document is modified (a new version uploaded), the system stores the new version of the document, as per the original upload process above, which includes a new "fingerprint", timestamp and author details.
    - You may be prompted to review and sign the revised version of the document (if required) as your previous signature no longer applies because the document has since been changed and a new document created.

When you lose your Private Key…

If you lose your Private Key, forget your password, or believe your Private Key has been compromised, you will need to use Your Digital File's Account Recovery facility.

1. During Account Recovery you will generate (on your computer) a new password and a new Public/Private Key pair, the same processes performed when you originally registered with Your Digital File.
    - After you have been contacted by Your Digital File staff and your identity and the request has been verified, your Account Recovery request is released to your Escrow Agent.
    - You must then contact your Escrow Agent directly and confirm your Account Recovery request before they will take any action.
2. Once your Escrow Agent has received positive confirmation of your request, they will login to Your Digital File and using functions only available to Escrow Agents, decrypt (on their computer) the required Primary Document Encryption Keys (one for each document–$DEK_1^e[1..n]$) which were previously encrypted using their Public Key and re-encrypt these document encryption keys using your new Public Key.
    - These re-encrypted document encryption keys are then uploaded to Your Digital File using high-strength SSL technology and can only be decrypted using your new Private Key.
3. Your Digital File follows the same process as the Escrow Agent for the each of the required document encryption keys protected with the system's Public Key ($DEK_2^s[1..n]$).
    - The end result is two document encryption keys per document, each encrypted with your new Public Key being stored by Your Digital File.
    - This allows you to download and decrypt all documents stored in Your Digital File using your username, your new password and your new Private Key without ever compromising the security of your documents.
4. At this stage, your old Private Key is no longer usable and will not decrypt any documents stored in Your Digital File.
    - If your key was compromised or accidentally made available to an unauthorised user, they will no longer be able to access your documents stored in Your Digital File, even if they know your username and password.

When a Data Legacy "trigger event" has occurred…

1. After the "trigger event" has been confirmed by Your Digital File staff, and once all Data Legacy "nominees" have been fully identified by Your Digital File, the user's Data Legacy is released to the Escrow Agent.
2. Both Your Digital File and the user's Escrow Agent perform the same technical process as when a user goes through the Account Recovery process to decrypts the document encryption keys for the each document authorised for release by the original user and re-encrypts these using the Public Keys of each verified "nominee", as instructed within the user's Data Legacy

Summary: Why choose Your Digital File?

- Complete confidentiality, privacy & non-repudiation when signing, sharing and storing documents and digital assets.
- Files are never compromised and always securely recoverable.
- Documents cannot be accessed by Your Digital File or any malicious intruders in the unlikely event of a breach of our systems.
- If the user forgets or loses their login credentials , they must activate the recovery process to verify their account and personal identity.
- Our secure Escrow model means that some components of each user's document encryption keys are stored encrypted with the public key of a trusted, neutral third party, which does not have access to view their files and can only perform secure account recovery when instructed by the end user.