Cocoon Data

Reg-Tech for Financial Services - to keep all stakeholders safe.

Cocoon Data for the financial services sector is a new approach for the Executive Office, Risk & Compliance Office, and Stakeholder Comms. Make sure what is sensitive and valuable stays that way.

Cocoon Data

Highly Secure, End-to-End Encrypted File Storage.

Includes controlled access for external parties.

Cocoon Data's is a highly secure, encrypted file storage and collaboration system that includes controlled, authorized access to external as well as internal parties.

Accessed using a browser, mobile app or Windows client, file encryption is done at the user's device for true end-to-end security.

Cocoon Data ties together Identity, Access Control and Encryption as one compliance ready system. It is truly unique, with global patents accordingly.

Data-centric security

Cocoon Data is a secure file storage system that encrypts files at the user's device before they are uploaded into the system. Access is controlled by authorized users who can allocate file or folder access permissions with a variety of options ranging from view only, to editing in browser, to full download access. Every step is securely logged for a full audit history. Access is logged against user ID and every unique encryption - there is no other audit like it.

When accessed by authorized individuals or staff using their bank ID credential, the encrypted document is either displayed on-screen as a watermarked pdf or downloaded and decrypted,depending on your access permissions.

This approach to high security data management is called 'Data-Centric Security', where the focus is on protecting the data itself, as the key asset, rather than reliance on traditional methods such as blocking intruders at the perimeter.

Sensitive data is protected

Because the files are encrypted end-to-end, one unique encryption key for each file, even if the system was to be compromised, your documents are protected from being read by anyone that you have not authorized.

Even your IT systems administrator cannot access the files within Cocoon Data, unless specifically authorized to do so by the document owner. The encryption keys are strictly managed by Cocoon Data to enforce access control according to the permissions.

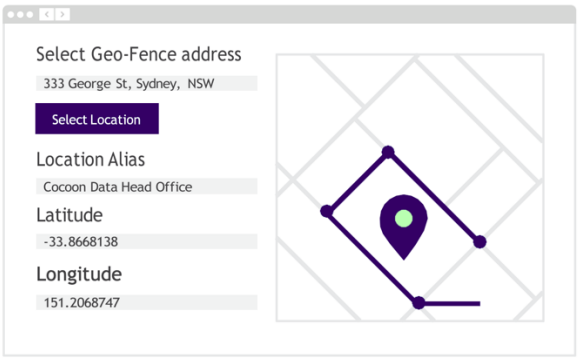
Internal and external users, fixed or mobile access

Now with Geo-Fence locking (see P4)

Cocoon Data users can be physically located anywhere, either within or external to your company network.

Authorized users can access the system from a web browser, mobile devices via an IOS or Android app, or Windows client.

User validation can be set to '2 Factor Authentication' (2FA)for additional security, where the logon includes verification from a mobile phone or computer app soft token or connected to company ID credentials.



Time-based access control for project documentation security

Document availability schedules can be set to manage secure document sharing within a date/time window.

Use cases can include restricting access to sensitive files for the duration of a project or controlling availability of confidential documents during a tender process.

All file types

Cocoon Data can encrypt files of any size or type.

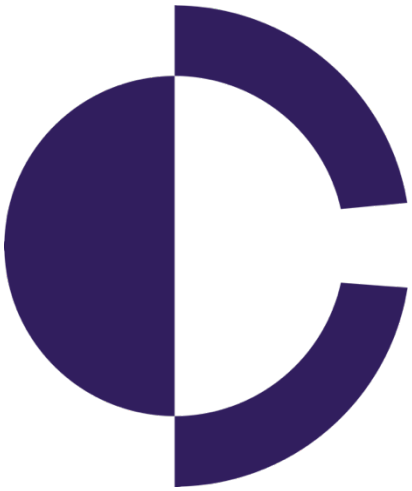
File types up to 15MB are encrypted at the user's device.

The 'view online' access permission is supported for 35 common file types, which Cocoon Data automatically converts to a watermarked pdf to enable this feature.

Key Features

Customer defined data sovereignty (choose your data center for SaaS from us)

- Superior, end-to-end encryption with files encrypted at the user's device
- Users can be internal or external to your organization
- Access permission types for folders or files can be controlled directly by authorized users
- Six user access permission types are available, ranging from view only through to full access
- User permissions can be set for date/time windows
- Easy to use with an intuitive user interface and click and drag operation
- Use from a web browser, Apple/Android mobile app or Windows client
- 'Cocoon Data Trust' license option based on private blockchain technology provides an immutable (cannot be changed) file history and additional key management security.



Technical and IT

- Operates on Linux for a lower cost operating system deploy on any cloud or on-premises infrastructure
- Supports large range of file types and sizes (> 1GB depending on connection speed)
- 2 Factor Authentication
- Reporting on usage and logging of all activities
- Active Directory or SAML integration.

aws partner network

Select Technology Partner

Cocoon Data is collaborating with AWS to deliver Cocoon Data for customers around the world.

Key Benefits

Compliance benefits

- Superior protection against unauthorized access to confidential files or network security breaches.
- Full audit trail - who attempted to access which files and when.
- Report on anyone who accessed any single file and what they did with it OR report on any user's complete activity - inside and outside the organization firewall.
- Each file is encrypted with a unique encryption key - meaning cryptographic functions are associated with each activity – this means a highly reliant audit log vastly superior to normal file server logs.
- Not even the administrator can access file or see content - any attempt to change access controls is broadcast to users - vastly superior to standard internal file servers or cloud services.
- Version control - between v1 and v2 Cocoon Data creates a new encryption key and stores a hash (algorithm 'fingerprint' that immutable) of the change - no more fiddling with versions or logs.

Credentials

- Originating from a military requirement, Cocoon Data was designed from the ground up as a secure vault with controlled collaboration
- 'Data-Centric Security' approach for superior protection of sensitive data
- Complies with many accreditation requirements for sensitive and confidential data - GDPR, ITAR, EAR, Aus Data Privacy Act
- Satisfied Cocoon Data customers – Cocoon Data software is trusted by over 26 federal government agencies in Australia to protect sensitive data.

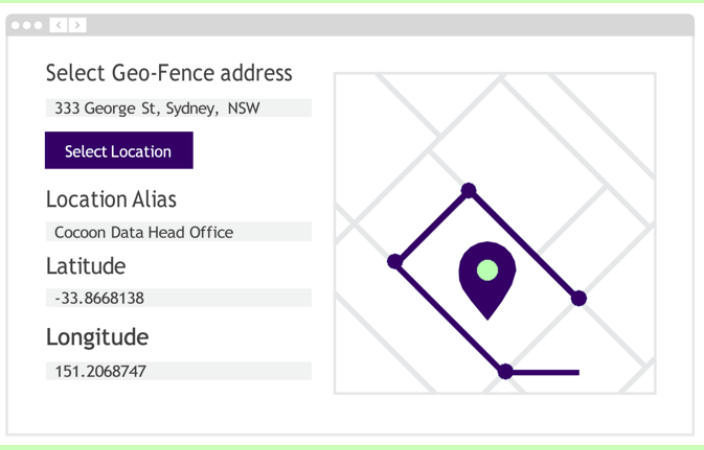
Additional security options with cocoon data companion products

- Discovery and Classification
  Scans your directories for documents containing sensitive or confidential data and classify or move files based on scan results. Features include automatic classification which is done in memory as files are ingested into Cocoon data.

Brand new Geo-Fencing

Lock files anywhere by managed encryption key service - 'you only get the keys if you are inside the fence - like your office address'.

For the first time in the world, access control, tied to ID, tied to encryption keys for content is now governed by where in the world you are - from locking content to a single tower to blocking access in a foreign country - data security has never looked like this for compliance. Dramatically reduces unauthorized leeks in financial services and lock data to authorized executives. A new paradigm shift from email attachments.



Customer Use Cases

Time-based secure external access to confidential files

Problem Statement

A project company required secure sharing of confidential documents with external contractor organizations and needed to control the time windows that external organizations couldaccess certain project documents.

The company's industry required strong security accreditation and was susceptible to significant commercial and reputational damage if confidential documents were viewed by unauthorized individuals or outside certain time windows.

Solution

The customer deployed Cocoon Data as an end-to-end secure file repository for project documents. With a preference towards cloud infrastructure, they chose to deploy Cocoon Data on the AWS GovCloud platform for its accreditation credentials.

Folders were set up for each project. The project administrators were able to directly set Cocoon Data folder access permission for internal and external individuals with nominated date/time windows. Moreover, they were able to differentiate individual access permissions to restrict certain individuals to view only online, edit online, or download access.

For added security the IT administrators were, by default, blocked from viewing encrypted project files unless specifically authorized by the project administrators.

Outcome

The company was able to operate with the convenience that external parties had controlled access to the required files within the authorized time windows, and the confidence that the encrypted documents were protected from unauthorized viewing or read access from intruders if access to their environment was compromised.

Importantly, access authorization was directly and easily managed by project administrators for self-managed, absolute control over access permissions.

Security for externally contributed security and operations data - an inter-bank organization

Problem Statement

A group of top-tier banks needed to share data dailyon security threats/breaches and other sensitive reporting related to this banking service.

The risk of unauthorized access to this information could be catastrophic to their business and that of their clients.

Solution

The customer deployed Cocoon Data AWS UK for a highly secure webfacing solution with GDPR/UK data sovereignty regulations being met.

Folders were set up for customer groups which aligned to the supporting business reporting categories. The executives and authorized operational people of each bank were able to shareand collaborate whilst maintaining full control and audit over who touched what and when whilst meeting financial services regulation and GDPR.

Security Features

True end-to-end encryption (file-encryption-in-motion)

For optimum security, the actual file is encrypted on the user's device for protection against unauthorized access to files in transit, such as could occur with a Man-In-The-Middle attack. This is a default setting for files less than 15MB, or as otherwise configured with consideration of browser capacity.

Called 'file-encryption-in-motion', this design offers strengthened security compared to 'encryption-at-rest' or other 'encryption-in-motion' techniques that use encryption to create a tunnel but do not actually encrypt the file until it is saved into the file storage directory, which leaves it vulnerable to a Man-In-The-Middle attack.

Comprehensive range of file access permissions

Cocoon Data can accommodate a wide range of use case requirements for access control to folders or files.

Six access permission types support access controls to view online only, edit in the browser (without downloading), download, upload, rename or remove files, set new access permissions and the ability to share files with internal or external individuals.

Classified files can also be restricted to named individuals as an overriding control and to prevent accidental bulk sharing.

Watermarks for additional protection with document forwarding

Documents that are restricted to 'online view only' for certain users can be configured to automatically insert a watermark when viewed.

The watermark includes the user ID and time/location when the file was viewed. This ensures that any forwarding of screenshots to other parties will identify the originating user.

Easy-to-use system for compliant record keeping

Cocoon Data provides a secure, structured records storage system for record keeping requirements that complies with most accreditation requirements.

These include for example, the US 'Office of Export Compliance' and 'e-CFR' (Electronic Code of Federal Regulations) record keeping requirements for all relevant shipping documents to be securely stored and organized for quick retrieval during audits.

Cocoon offers comprehensive dashboard style reporting of ALL activities as a standard to SaaS offering - with new SIEM connectors like Splunk coming soon - this means granular reporting and alerts on user activity anywhere in the world at any time.

In Australia Cocoon Data is now in the AWS Aus Gov Cloud and can be deployed at scale for large banks on private cloud infrastructure.

Regulated data sovereignty requirements

Cocoon Data can use accredited sovereign file storage platforms, such as Amazon's Gov Cloud, which is Amazon's isolated cloud region where accounts are only granted to US Persons working for US organizations.

Typical requirements for this include ITAR (International Traffic in Arms Regulations) and the EAR (Export Administration Regulations) regulations.

Enhanced security with private blockchain technology option

'Cocoon Data Trust' is a licensed option based on private Blockchain technology to provide industry-leading file security and an immutable history (cannot be changed) of all file activity over the life of the file.

The enhanced security results from file access encryption keys and access permissions are stored as encrypted data on a private blockchain, with the chain encryption key split into multiple pieces and each fragment stored on a different node, making it virtually impossible to compromise.

The immutable history is enabled with a data chain that is flexible in size to accommodate through-life history and stored on multiple nodes across the network in a way that blocks any tampering attempts.

Security How it Works – User Perspective

User registration

Cocoon Data users can be created by the Organizational Administrator or document Owners or Co-owners as follows:

The Organizational Administrator has options to:

1) Create a whitelist of email domain names or individual emails, which can then become registered users through the actions of Owners or Co-owners sending file share invitations with appropriate permissions. Share invitees not on the whitelist will be blocked from registration by this process.
2) Directly register users that are not on the whitelist.
3) Choose not to create a whitelist, in which case Owners or Co-owners can enable the automatic registration of any user through the action of sending a share invite to an email address.

File encryption and access control

All files are encrypted with user access permissions allocated at the sub-folder or file.

Creating folders and authorizing access permissions

When a new folder is created, the person creating that folder becomes the Owner, who can also add other users as Co- owners to have the same access permissions as the Owner.

The Owner or Co-owners can share files or the folder, giving access permission types from the following list, with any registered users or individuals that have emails or email domain names on the Organizational Administrators whitelist, or unrestricted if a whitelist has not been created.

This is done by simply clicking on the folder or file, select 'share', select the permission types and add the emails or email groups of selected individuals. An optional date/time window for the permitted access can also be selected.

When subfolders are created, they inherit the same access permissions as the parent folder by default. However, Owners or Co-owners can authorize different permissions at the level of any subfolder of file.

Access permissions would normally be set up as groups that can comprise:

- Individual emails
- Cocoon Data global groups
- Cocoon Data Individual contact groups.

Access Permission Types

Permissions	Description
'View' online	On screen view in PDF format with watermark (but can't download, copy/paste or print).
'Edit' online	Ability to edit files (but not download) in Office Online, plus 'View' permissions.
'Download'	Can download and print, plus 'Edit' permissions.
'Create'	Upload a new file as well as 'Download' permissions.
'Manage'	Can delete, rename, or move files plus the 'Create' permissions.
'Co-owner'	Ability to share files, set or change access permissions, classify files, appoint new Co-Owners plus all the above permissions. Co-owner permissions are the same as Owner permissions.

Receiving an invitation to share a file or folder

When a share invitation with access permissions is sent by an Owner or Co-owner, the recipient is alerted as follows:

- Registered users receive an email with the link and have ongoing access according to their permissions.
- Non-registered external users will receive a registration email with one-time-use password first, followed by an email with the file link.

Registered users, including administrators, will not be able to see files to which they do not have any access permissions.

Overriding file classification access control

As an overriding access permission, the Organizational Administrator can set Classification Permission lists of individuals or groups that are permitted to access documents with a certain classification.

Security Implementation and Architecture

Easy one-click deployment using software defined networks

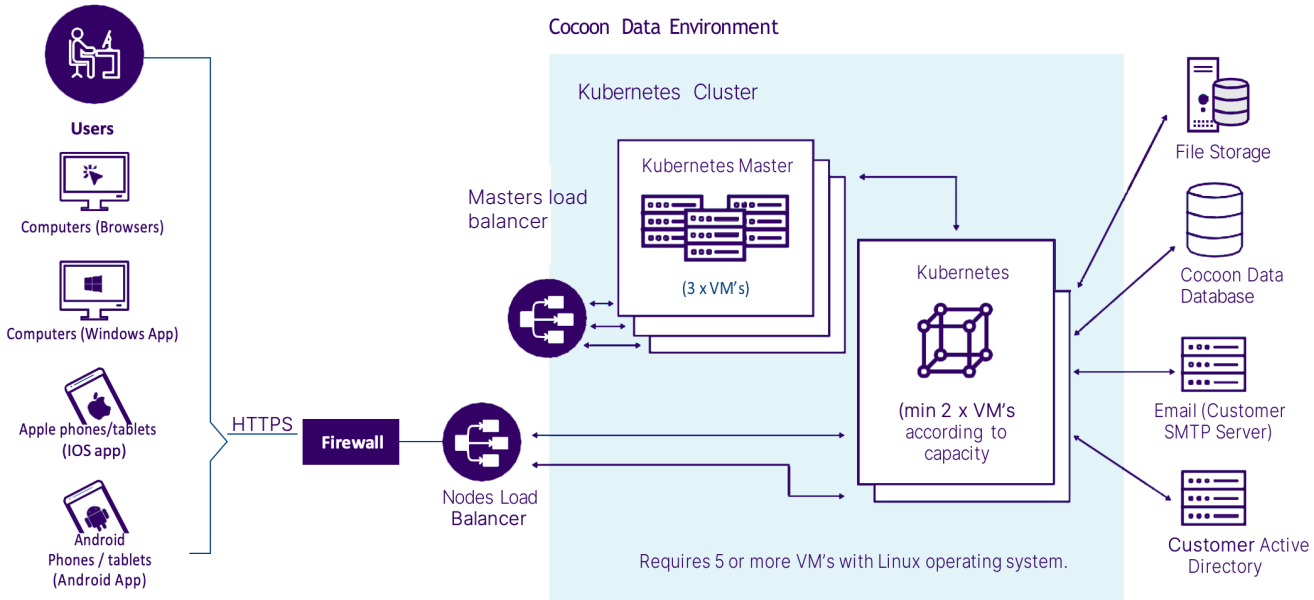
Cocoon Data is designed to be implemented with a one-click deployment using Kubernetes Software Defined Network (SDN) technology.

Just trigger the deployment and the system automatically sets up connectivity with the required servers, deploys the Cocoon Data application and is then ready to use.

Kubernetes also manages ongoing capacity requirements, such as automatically deploying or removing additional Cocoon Data Node VM as required.

This deployment method avoids the complexity and resources that would alternatively be required to install the Operating System, set up network connectivity and configure the applications for operation.

Cocoon Data System Architecture



Cocoon Data deployment models

Cocoon Custom Cloud

Customers can purchase Cocoon Data as a SaaS model and be deployed on private cloud infrastructure for large scale regulatory cases – i.e. large bank.

Cocoon Data SaaS Service

Customers can purchase Cocoon Data as a service from Cocoon Data's shared cloud infrastructure.

Options include infrastructure based in USA, UK, Australia or other countries upon request.

We can also provide service hosted on the AWS GovCloud (USand Australia). This provides compliance with a number of US and Australian regimes*.

*Includes: DOJ's Criminal Justice Information Systems (CJIS) Security Policy, U.S. International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5, FIPS 140-2, IRS-1075, and more.