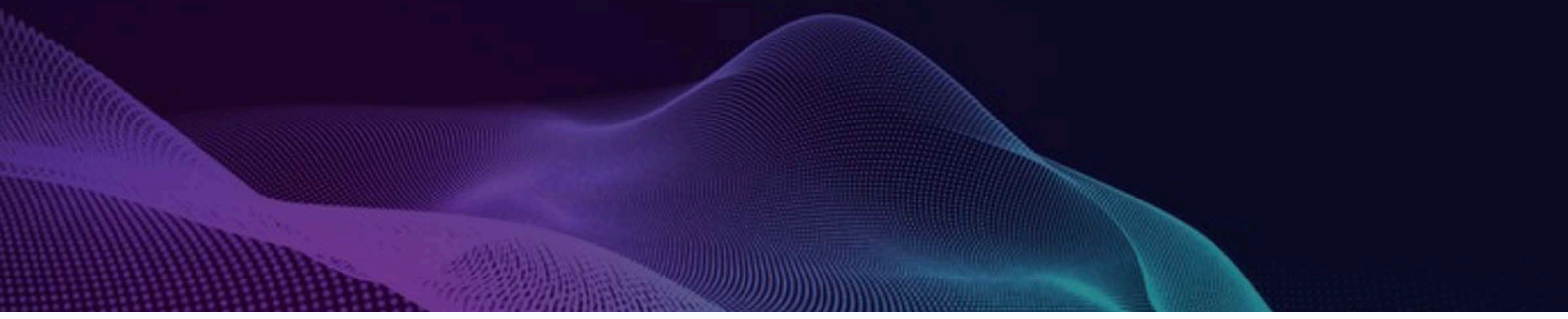
Cocoon Data

Ultra-secure, encrypted file sharing and collaboration platform.



Highly secure, end-to-end encrypted file storage.

Includes controlled access for external parties.

Cocoon Data 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 is inherently designed as quick to install and easy to use.

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.

When accessed by authorized individuals, 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, 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

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.

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 and Benefits

Features

US Data Sovereignty

- o Superior, end-to-end encryption with files encrypted at the user's device
- o Users can be internal or external to your organization
- o Access permission types for folders or files can be controlled directly by authorized users
- o Six user access permission types are available, ranging from view only through to full access
- o User permissions can be set for date/time windows
- o Easy to use with an intuitive user interface and click and drag operation
- o Use from a web browser, Apple/Android mobile app or Windows client
- o '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

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

Business Benefits

- ✓ Superior protection against unauthorized access to confidential files or network security breaches
- ✓ Reduce the potential for insider threats by blinding the Administrator from access to the encrypted files
- ✓ Enables secure collaboration with internal as well as external parties
- ✓ Overhead savings with centrally managed security policies that are easy to administer and can be managed within the business unit.

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
- ✓ Developed by Cocoon Data, a listed company that specializes in Data-Centric Security
- ✓ Satisfied Cocoon Data customers.

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.

Eclipse

- ✓ Enhances security for Microsoft SharePoint, OneDrive or Exchange files with encryption and centralized encryption management.

Data Security Console (DSC)

- ✓ A single management console for effective management of Cocoon Data's, 'Eclipse' and 'Discovery & Classification' from one place with a comprehensive security dashboard and reporting.

Customer Use Case

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 could access 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 submitted and accessed documents

Problem statement

An IT equipment service company required external field technicians to access and submit documents with secure client information that included log on credentials for the customer equipment. The field engineers included external subcontractors.

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 in a dedicated cloud environment as the file repository for all customer reports with end-to-end encryption security.

Folders were set up for customer groups which aligned to the supporting field technician teams. The customer service management team were able to directly control which external contactors had file access without the need to engage their IT department. Internal staff movements were automatically managed via AD processes.

During set up the company used Cocoon Data's 'Discovery and Classification' tool to scan all existing file directories for customer confidential information in text or images, classify these files, move them to the appropriate Cocoon Data directories and delete duplicate or outdated files.

Outcome

Authorized field technicians, whether staff or subcontractors, were able to view and upload customer files that were otherwise secured with encryption at the browser through to the secure file directories. When viewed online, the files were watermarked to identify the viewing individual to reduce the likelihood of data leakage by screenshot.

Existing file directories were cleansed of confidential client information which was either moved into Cocoon Data or deleted.

The company now operates with confidence that their confidential customer data is secured, which is also promoted to their clients.

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 of 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.

Regulated data sovereignty requirements

Cocoon Data can use accredited sovereign file storage platforms, such as Amazon's GovCloud, 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.

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 invitee 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 subfolder 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 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.

Implementation and Architecture

Easy one-click deployment using software defined networks

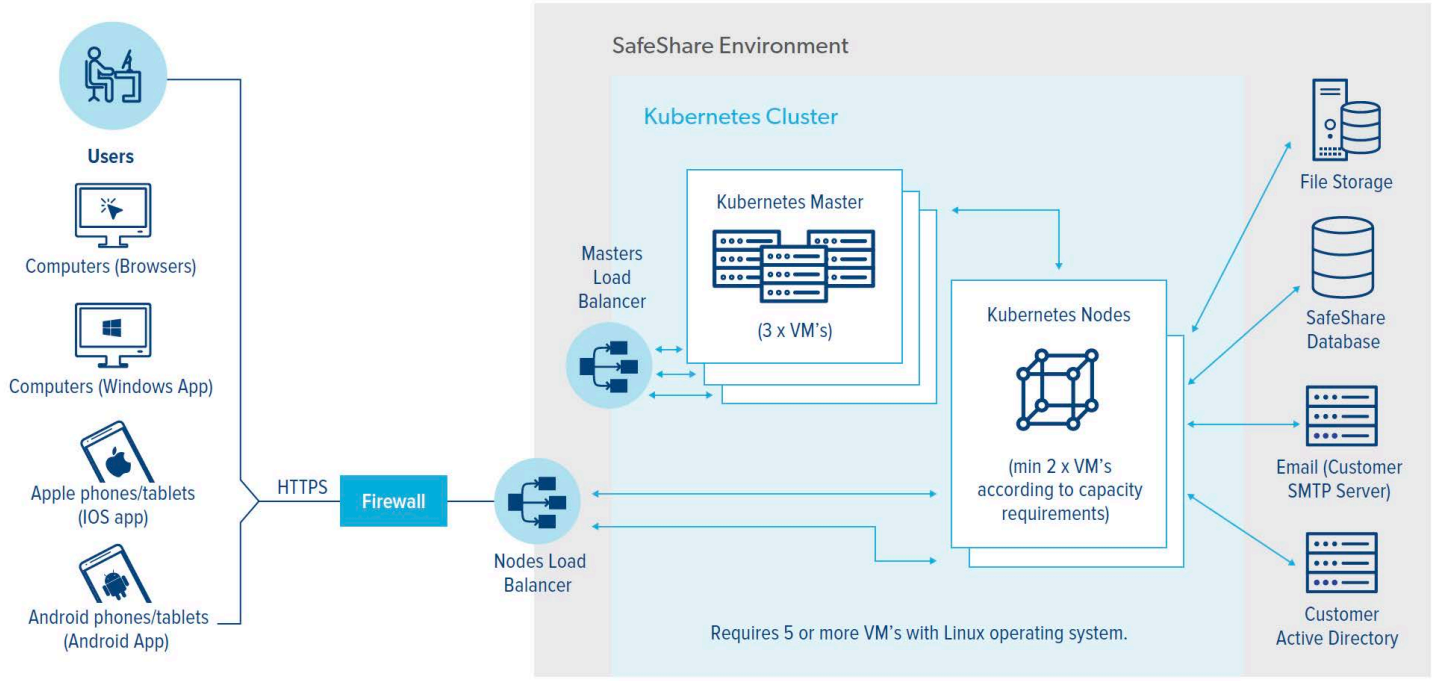
Cocoon Data is designed to be implemented with a one-click deployment using Kubernetes Software Defined Network (SDN) technology.

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 Data is designed for deployment as either a stand alone system on customer dedicated infrastructure, or for a multi-tenanted deployment.

Customer options are:

Dedicated Customer Deployment

Customers can purchase the Cocoon Data licenses and either self-implement or have it deployed on their behalf by a Cocoon Data Premier Partner.

The multi-tenanted capability can also be used to share an instance within the company, such as for separate business units or subsidiaries.

SaaS model from a cocoon data premier partner

Customers can purchase Cocoon Data as a SaaS model from the shared infrastructure of a Cocoon Data Premier Partner.

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 (US Region). This provides compliance with a number of US 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.

Data security console

Cocoon Data's Data Security Console (DSC) provides a single platform to centrally manage security policies across multiple applications and provides reporting aligned to business metrics with actionable intelligence.

IT administrators will be equipped with intuitively presented, actionable information and the means to centrally apply and control security polices across the range of applications, all from one portal.

- The Cocoon Data management portal is integrated into the DSC for convenient reporting and policy management.
- For SharePoint, OneDrive or Exchange, the integrated 'Eclipse' portal can set security policies for encryption and authorized access that are automatically pushed down to the applications for overriding security control.
- The 'Discovery and Classification' portal is also integrated into the DSC to scan document files in any storage directories for sensitive or confidential information, apply classification tags or migrate files according to scan results.

Mode	Description	Typical use case
Enterprise Customers		
Enterprise Customer License	Customers purchase Cocoon Data licenses from Cocoon Data for implementation and operation by their Systems Administrator. Cocoon Data provides support and can assist with the implementation.	Enterprise customers that currently self-manage their environment and seek to operate Cocoon Data with their own resources.
Service Providers		
Cocoon Data Premier Partners	Cocoon Data Premier Partners sell and support Cocoon Data to their customers as either a delivered solution or license for customers to self-implement.	Enterprise customers that have a business and support relationship with a Cocoon Data Premier Partner and wish to extend that relationship to include supply and support of Cocoon Data.

About Cocoon Data

Cocoon Data is an ultra-secure, ultra-simple file sharing and collaboration platform. Our intention is to make data security and compliance so simple, everyone can be part of it.

We are ISO 27001 certified and utilize patented technology to deliver the most powerful solution for secure file sharing and collaboration. We provide companies across a wide range of industries with the ability to simply and securely share files – both internally and externally.

Development of the Cocoon Data platform was driven by mission critical work for the intelligence and Defense Communities. Today, Cocoon Data is a preferred provider in the United States for ITAR compliant and CMMC ready file sharing for the defense industry. Our solution also provides globally compliant, secure file sharing and collaboration for business, government, education and healthcare organizations.

Contact

U.S
+1 303 536 1115
(Washington)

Australia
+61 2 8319 1919
(Sydney)

UK
+44 20 3488 0851
(London)

Email
info@cocoondata.com