Couchdrop

A COUCHDROP WHITE PAPER

# Couchdrop Security Overview

V2.0

# Contents

# Overview

With many organizations taking advantage of the benefits of cloud storage platforms, data that was once stored in highly controlled on-premise environments can now be safely stored on scalable remote servers with redundancy, encryption, and data loss prevention policies.

However, getting data to and from these platforms securely had been a challenge. Transferring files while adhering to organizational security requirements was a major obstacle, especially when trying to connect multiple systems or when needing to transfer to or from legacy or proprietary systems with limited protocol support. Regularly doing such transfers continued to be difficult, time-consuming, and manual.

Couchdrop was built to solve these issues.

Couchdrop is a cloud-native secure file transfer platform that integrates with modern cloud storage platforms like Dropbox, SharePoint, Google Drive, OneDrive, Amazon S3, and more, offering protocol support for SFTP, FTP, SCP, HTTPS, AS2, and mailbox-based transfers with these platforms.

Couchdrop is delivered as a multi-tenant SaaS platform, with 99% of customers using the shared hosted infrastructure. Enterprise customers can optionally choose a dedicated environment, including private IP ranges, dedicated compute, and isolated storage.

The platform is composed of several microservices designed to scale dynamically and operate across multiple geographies, with safeguards and security measures that ensure the protection of user files and data at all times.

This whitepaper is designed to provide a high-level overview of Couchdrop's security measures. For more details and specifics on Couchdrop security, we highly recommend reading the FAQs or other resources on our trust center.

# Under the Hood

Couchdrop's infrastructure may appear simple and straightforward from the front end, but there are many interconnected components under the hood that work together to safeguard user information and files.

Couchdrop has a distributed architecture, which means microservices are deployed in different cloud environments to service customers' needs in the most performant, secure, and cost-effective manner.

### Core Components

Couchdrop's infrastructure consists of multiple microservices and managed services provided by reputable third parties.

### Web Front Ends

Couchdrop has several secure HTTPS applications for end-users and admins to manage storage, users, and file access. These front ends use HTTPS and interact with the Couchdrop API to service requests. Web services sit behind reverse proxies and load balancers. These proxies and load balancers distribute load and provide a first line of defense.

### FileIO Service

The Couchdrop Virtual File System (VFS) is provided by the FileIO service. Couchdrop's FileIO service is a standalone web application that provides a virtualization layer to upload, download, list, and set permissions on files and folders stored in cloud storage providers. It provides a single API to access cloud storage. Customers do not normally interact natively with this service; rather, the SFTP/FTP or web front ends provide the user layer and pass requests to the FileIO service where needed.

### SFTP/FTP/AS2 and Mailbox Service

These services are lightweight protocol handlers built in-house that pass file operations to the FileIO service. Each protocol handler supports protocol-specific security and compatibility layers.

### API Service

The API is an HTTPS service that provides customer information, metadata, storage details, and authentication for the majority of the customer-facing applications in Couchdrop. It interacts with Couchdrop's distributed databases to retrieve information and forms the fabric piecing together the Couchdrop platform.

### Database Systems

Several database systems are employed in the Couchdrop platform. These include but are not limited to Postgres, MongoDB, and Redis. Where possible and advantageous, Couchdrop chooses to utilise managed database systems to provide a redundant and scalable platform.

## Data Storage

With the majority of organizations offloading some or all of their storage to the cloud, Couchdrop saw an opportunity to add support for SFTP/FTP, AS2, and secure uploads with cloud storage, bridging the gap between platforms and organizational boundaries.

Couchdrop provides two different models of data storage. The most common model–and the one that the platform was designed for— is that users bring their own storage. Users choose their platform from over 20 integrations, fill in authentication details, and connect the platform to Couchdrop. Couchdrop then utilises the mainstream and public APIs of the third-party storage provider (such as Dropbox or Amazon AWS) to upload, download, and list content information in response to SFTP (or other protocol) commands.

The second option is Couchdrop "hosted storage", which is included in all plans. With this option, Couchdrop utilizes Amazon S3 for storage. Customer data stored in hosted storage is encrypted using AES-256 via SSE-C from Amazon S3, which facilitates client-side key-based encryption. In the Couchdrop environment, each customer has their own set of keys used to encrypt data stored in S3. Using client-side key-based encryption ensures that data is locally separated between customers.

Both storage options are cloud native and utilise mainstream third-party storage and cloud providers for the actual data storage itself. Couchdrop is simply a virtualisation layer on top of cloud storage APIs and a front end SFTP/FTP/AS2 and web endpoint.

# Data Encryption

### Data Encryption in Transit

One of the primary reasons for using the SFTP protocol is due to its encrypted nature, and it was essential to ensure encryption applied to all points of the transfer process with Couchdrop.

Communication between Couchdrop servers and the cloud storage provider destination (or source) is normally encrypted with HTTPS/TLS 1.2 as provided by the third-party SDKs. Couchdrop ensures that all certificate validation is enabled and that we utilise trusted SDKs and frequently update them.

Between Couchdrop servers and the customer's network, data is encrypted by the utilised protocol. In the case of SFTP and SCP, this is over an SSH tunnel, which utilizes secure asymmetric SSL encryption that is well-regarded and de facto.

The only exception to encryption at all points is when using the FTP protocol, as it is unencrypted by design. Unencrypted FTP connections are disabled by default but can be enabled if needed, and **we highly recommend using the more secure FTPS protocol when possible.**

Internally, data in transit is stored in memory and normally in a chunked form. In some cases, if the servers are under exceptional load, data is paged out to disk in a chunked form. Couchdrop's servers employ AES encryption on disk to provide an additional security layer and ensure that data is always encrypted at rest.

### Data Encryption at Rest

Couchdrop does not store customer data directly. Instead, we integrate with other platforms and use S3 for hosted storage.

Data being transferred can be stored empirically during transit. When data is stored empirically, it is encrypted. Couchdrop also ensures that all metadata and configuration is encrypted at rest and only accessed via secure channels in our internal infrastructure.

# Data Locality

Couchdrop has servers located in multiple regions as outlined below:

- San Francisco
- New York
- Toronto
- Amsterdam
- Frankfurt
- London
- Singapore
- Bangalore

When it comes to data locality, there are two types of data to consider: Customer Storage Data and Customer Metadata.

### Customer Storage Data

When customers download, upload, or list data with Couchdrop, one of our servers interacts with the underlying storage provider. This interaction is geo-fenced and local to a particular region. To guarantee geo-fencing of data, customers can request specific IP pools from Couchdrop's support team and connect directly with the region they wish to utilise.

### Customer Metadata

Customer metadata is specific to Couchdrop and includes usernames, OAUTH, and other credential sets for cloud storage, billing information, and other metadata required to provide the Couchdrop service.

Customer metadata is stored in encrypted databases located in SOC2-compliant data centers in the USA. This data is only accessible via Couchdrop's secure API and stored, backed up, and managed in keeping with industry standards. Customer metadata may be temporarily transferred to other regions via encrypted APIs in order to service requests.

# Cloud Storage Credentials

Nearly all customers use Couchdrop for connecting to external cloud storage in some form. Connections are configured in the web interface, but in order to connect storage, customers must grant Couchdrop access through some method for the services to function.

Storage access is generally granted either through OAUTH Tokens or through Credentials and Access Keys.

### OAUTH Tokens

OAUTH is a process in which users follow a cycle of requests that involve redirecting them to the remote platform to enter their credentials and grant access to a requesting service, in this case, Couchdrop. The remote platform then provides the service with an access token and in some cases, a refresh token.

With Couchdrop, these tokens allow Couchdrop to access files and folders. Normally, this is temporary, and at any point, the customer can revoke Couchdrop's access by visiting the administrator section of their cloud storage provider and choosing to revoke access.

### Credentials and Access Keys

The less common approach to grant storage access is by providing Couchdrop with access keys or a username and password combination. Couchdrop then utilises these credentials to access the underlying storage.

**We highly recommend not reusing access keys and credentials and restricting access where possible.** If no longer required, we recommend deleting and revoking the access keys and credentials at the storage endpoint. This renders them useless in the unlikely event that they are compromised.

### How credentials are stored with Couchdrop

Third-party storage credentials are stored in a separate database from other customer metadata and demarcated from our normal environment. Couchdrop employs a TTL-based eviction process to ensure that Couchdrop is not retaining credentials for extended periods of time, such as when customers are no longer using the storage through Couchdrop's service.

An additional level of encryption is applied to sensitive storage credential data so that cloud storage data is never stored in an unencrypted, clear-text form.

## User Accounts and Credentials

Couchdrop provides the ability to create multiple additional user accounts under an organization. Along with the owner account, passwords must be stored for these accounts. Following industry best practice, Couchdrop does not store actual passwords; rather, we store a SHA-512 salted hash of the password instead.

More details on how this data is stored can be provided on enquiry with an NDA.

## Security Features within the Platform

Couchdrop offers several security features to help customers manage security requirements. Since Couchdrop is an evolving platform under active development, new security features are added frequently, or when requested by a significant portion of our customer base.

This list is a segment of some of Couchdrop's security features. See our website for the most up-to-date feature set.

### Two-Factor Authentication (2FA)

2FA is an authentication method in which a user logs in to Couchdrop with a username/password combination, and then must provide a specific token or code that is received by a designated mobile number via SMS.

### Firewall

Access to Couchdrop can be restricted strictly to the IP addresses or networks specified. In addition, protocols and features can be enabled/disabled globally for all users.

### Standard Permissions

Couchdrop enables administrators to restrict access permissions to strictly read-only, write-only, or read/write access. These standard permission sets can be built on further by using granular permissions (see below).

### Granular Permissions

Couchdrop provides the ability for granular permissions on specific folders within a directory that a user has access to. These range from the ability to upload, download, list files, get properties, and delete content. This could be used to provide different permissions to folders that a user has access to.

### User Folder Isolation

A major security method that prevents unauthorized access is the principle of least privilege. Within Couchdrop, customers can set a user's root folder to be any subfolder within their storage infrastructure and apply standard or granular permissions to ensure the user only has access to the folders they need.

### Disabling Access Methods

With Couchdrop, customers can disable access methods that aren't required or are insecure. For example, an admin may permit some users to use FTP and SFTP, while others may be restricted to SFTP only. Customers with sensitive data can also disable Support Team access that would allow support members to log in to the account for troubleshooting purposes.

### Support for RSA Keys

Instead of symmetric username and password authentication, customers can opt for asymmetric authentication through RSA keys. With this method, customers provide the public key under a user which allows the user to authenticate to Couchdrop without requiring a username and password.

### Dedicated Geo-Located Private Nodes

As part of Couchdrop's enterprise offering, customers can have their own private dedicated instance established in a region of their choice. This removes shared resources and ensures customers have a presence closer to where they need it for performance.

If you require a region that is not currently available, please reach out to us at sales@couchdrop.io

### Password-Protected and Temporary Shared Links

Customers have the ability to create Shared Links to files and folders. These links can be configured with security parameters like an expiration timer or one-time use to ensure that data is only shared with those who need it and for as long as they need it.

### Automatic lockout on accounts

When enabled, Couchdrop will automatically block a user for 15 minutes and send notifications to the account owner after 5 failed login attempts within 5 minutes. We also have other mechanisms in place to protect against brute force attacks.

### Single Sign-on (SSO) and User Provisioning

Customers can configure SSO and handle user management through their identity provider. Couchdrop can also be configured to connect to a SAML IDP for single sign-on via the web portal.

# API Access

In order to seamlessly integrate Couchdrop into workflows and normal operations, we can provide customers on Business and Enterprise plans with API access to the platform by request.

With API access, Couchdrop customers can create new user accounts, manage access and authentication, and utilise our virtual file system to upload, download, and interact with their cloud storage.

A token is required for API access and may be revoked at any time. Tokens are tied to a particular account and are limited in what they can do.

Accessing the API is done via HTTPS TLS 1.2. Couchdrop rejects access via unencrypted HTTP.

API Documentation can be found at https://developers.couchdrop.io/

# Network and Infrastructure Security

Couchdrop uses several clusters of virtual machines provided by Digital Ocean and Amazon AWS, normally running LTS versions of Ubuntu to host its infrastructure. Software is never deployed directly on servers. Instead, Couchdrop uses Docker containerisation for all microservices in its deployment.

Docker provides an immutable, scalable, and secure way to deploy services in a predictable fashion. Docker containers are scanned for updates and vulnerabilities as part of the service provided by its container registry, and containers are updated and deployed frequently as part of our continuous deployment process.

Servers have logging and monitoring agents deployed on them, which provide full audit logging and monitoring. This includes security and access monitoring.

Couchdrop also utilises some managed services provided by Digital Ocean and Amazon AWS. These services are updated, secured, and backed up by the respective providers, and connectivity with them is via SSL and restricted to certain IP pools.

Infrastructure access is governed by Couchdrop's internal security policy and is limited to critical Engineering and Support staff. Access is logged, audited, and 2FA is enforced on all accounts and infrastructure is via a secure VPN with 2FA.

Server and SSH access is restricted to specific Engineering staff and is locked down to particular static IP addresses. SSH keys are encrypted and stored in a secure vault in 1Password.

1Password is also used to store all company passwords. Strict policies around access and reuse are enforced and audited using 1Password.

Couchdrop uses a centralized configuration management system to store deployment configuration, and configuration is always compartmentalized for the infrastructure it is being deployed on. In most cases, configuration is not stored on Couchdrop's cloud infrastructure, and Couchdrop uses remote orchestration technologies to deploy and update its nodes.

Keys and sensitive configuration are managed by a vendor-independent KMS system. Access to this KMS is limited and regularly audited.

## Firewall and Network Access

Couchdrop enforces strict network access policies across all environments, combining cloud-level firewalling with infrastructure-level hardening.

Key practices include:

- Access to management services and ports is restricted to traffic originating from our production VPNs
- SSH and admin interfaces are locked down to a small set of static IPs via our VPN gateways
- All non-essential ports and services are disabled by default
- Management ports are randomized and inaccessible outside approved IP ranges
- Databases and internal services are only accessible within our internal private networks

Firewall rules and access configurations are reviewed every 90 days and follow a least-use, least-privilege policy, ensuring only strictly necessary access is maintained.

All firewall and network access changes are subject to **CTO approval** and logged for auditing.

## Infrastructure Providers

Couchdrop uses the infrastructure providers listed below.

| Infrastructure Provider | Use Case | Region |
|---|---|---|
| Digital Ocean | Main Infrastructure/Data Pane Pops | All regions except HIPAA |
| Amazon Web Services (AWS) | Main Infrastructure/ Databases | All regions |
| AWS S3 | Hosted Storage | All regions |

For a comprehensive list of third parties used to support the Couchdrop platform, please visit our trust center.

## Physical Security

Since Couchdrop is not managing physical server infrastructure and the company is cloud native, Couchdrop has very few physical security requirements. However, there are still safeguards in place for physical security.

Staff are provided with computers and other equipment used for accessing Couchdrop resources. All staff are prohibited from accessing Couchdrop resources from personal computers.

At this time, Couchdrop operates in a hybrid/office/remote model. Team members may work remotely or from our office in Christchurch, New Zealand. The office is equipped with multiple secure locking mechanisms and an alarm system. Every team member has a unique alarm code traceable to the specific individual.

## Privacy Policy

Couchdrop's privacy policy and terms of service can be located at https://www.couchdrop.io/legal/privacy-policy

# Compliance

### GDPR

Couchdrop can be configured to meet GDPR requirements. Further information on Couchdrop's GDPR can be located at https://couchdrop.io/privacy/gdpr

### HIPAA

Couchdrop and its partners often service the healthcare and insurance industry and fall under the HIPAA remit in the United States of America. While there is no HIPAA compliance certification, Couchdrop follows guidelines as put forth by HIPAA and will provide customers with a BAA if requested.

Further information on Couchdrop and HIPAA can be located at https://couchdrop.io/privacy/hipaa

### SOC2

Couchdrop is a SOC2-compliant organization. Please visit our trust center or email sales@couchdrop.io for a copy of Couchdrop's latest SOC2 report.

### Security Audit and Penetration Testing

If requested, Couchdrop can provide the results of various penetration tests performed by security companies on the platform.

# Security Incident Disclosure

Couchdrop will promptly, and without undue delay, notify the Customer if a Security Incident occurs, so long as applicable law allows this notice.

“Security Incident” means any actual Couchdrop disclosure of or access to customer data, or compromise of Couchdrop systems that Couchdrop determines is reasonably likely to result in such disclosure or access, caused by failure of Couchdrop’s Security Measures and excluding any unauthorized disclosure or access that is caused by Customer or its End Users, including Customer or its End Users’ failure to adequately secure equipment or accounts.

We may limit the scope of, or refrain from delivering, any disclosures to the extent reasonably necessary to avoid compromising the integrity of our platform, an ongoing investigation, or any customer’s or end user’s data. To report a vulnerability, please email security@couchdrop.io

## Conclusion – Keeping Security at the Forefront

Couchdrop's unique architecture allows the platform to be secure enough for enterprises while remaining simple, intuitive, and easy to use. Data resides within user storage platforms and is simply "streamed" between them with end-to-end encryption, with data only stored at rest when using the S3-based hosted storage. Features like firewalling, granular permissions, automatic lockout, and dedicated geo-located private nodes allow for additional security configurations to meet the needs of specific organizations.

While Couchdrop is a leader in security in the managed file transfer space, the platform is in active development and continuing to improve. As modern attacks and exploits in tech become more sophisticated and new security concerns arise, Couchdrop will continue to work to stay ahead and ensure user data and files are protected. Patches and updates are automatically delivered to users as soon as they're available, and the team will continue to keep security at the forefront for all product evolutions.

For more information about Couchdrop security, visit the Couchdrop trust center or contact us at sales@couchdrop.io

### Versions

| Version Number | Date |
|---|---|
| Version 1 | 2022 |
| Version 2 | 19 June 2025 |