COUCHDROP

COUCHDROP SECURITY OVERVIEW

A Couchdrop Whitepaper

COUCHDROP

Contents

COUCHDROP

Overview

Couchdrop is a cloud native SFTP server with support for FTP, SCP and limited Rsync support. Couchdrop is hosted in the cloud and built to work with cloud native storage like Dropbox and Amazon S3.

Couchdrop is provided to customers as a SAAS solution, whereby most of Couchdrop's customers pay a monthly fee for access to the platform. The enterprise subscription provides a platform for customers to pay for dedicated and isolated resources, but the majority of our customers utilise our shared platform.

The platform architecture is split into several microservices, of which a detailed breakdown is beyond the scope of this document as it's proprietary, but what is important to note for the reader is that these services are architectured to scale with load requirements and support Couchdrop's customers geographically.

Under the Hood

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

Web Application Front End
Couchdrop has several web application front ends that are customer facing and are used for both interaction with files and for management of the service. These front ends use HTTPS and interact with our API to service requests.

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/SCP and Rsync Service

The SFTP service provides the access layer for most of Couchdrop's customers using the service. This service is a lightweight implementation of the file transfer protocols and interacts with cloud storage via the FileIO service detailed above.

FTP Service

The FTP service is identical to the SFTP service, but supports native FTP instead.

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.

Movebot Worker Nodes

The Movebot product uses Couchdrop's VFS provided by the FileIO service and several other components. Move worker nodes are migration workers temporarily launched as virtual machines to perform a data transfer task as part of a migration. These worker nodes run a version of the FileIO service and a number of other subprocesses that perform the migration and interact with the API.

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.

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

COUCHDROP

Data Storage

Couchdrop SFTP provides two different models of data storage. The most common model and the one which the platform was designed for is that of BYOS (bring your own storage). With such a dramatic move to the cloud underway, Couchdrop saw an opportunity to add support for SFTP/FTP and Rsync with cloud storage like Dropbox, bridging the gap between the old and the new. As an additional offering, Couchdrop offers "hosted storage" whereby Couchdrop provides the storage component and charge based on utilisation (per GB).

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

In the case of BYOS, a Couchdrop customer provides their own storage and simply connects it to the Couchdrop cloud platform. 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.

Couchdrop does not store or retain any of the user's data on its own servers. This is the distinct difference between Couchdrop and other SFTP providers. This abstraction means that Couchdrop is impartial and is a convenient service for interacting with data while it resides with a trusted third party. Storage redundancy, encryption and to some extent security responsibility then resides with the third party and Couchdrop's access to this data can be controlled at a very granular level.

In the case of hosted storage, Couchdrop utilises Wasabi S3 storage and Amazon S3 storage. In both cases, each customer has their own set of unique storage buckets in a region that can be specified by the user. Both Wasabi and Amazon S3 are SOC2 compliant and conform to the highest security standards. On request, Couchdrop customers can choose to change ownership of the bucket and move it to their billing account instead of having Couchdrop on-charge it.

Data Encryption in Transit

As outlined in the last section, Couchdrop does not store customer data, rather it acts as a virtual layer to provide convenient access mechanisms.

To provide this layer, Couchdrop must interact via APIs provided by cloud storage providers to upload, download and list/retrieve metadata on files. In servicing user requests via the web portal, SFTP or other protocols Couchdrop has temporary access to files as they transfer between the cloud storage provider and the customer.

At all times during the transfer, the file is encrypted. Communication between Couchdrop servers and the cloud storage provider 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 a SSH tunnel. SSH utilises secure asymmetric SSL encryption that is well regarded and defacto. The only exception to this is FTP, which is an unencrypted protocol by design and not enabled by default in Couchdrop.

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.

Data Encryption at Rest

As outlined above, Couchdrop does not store customer data and so has no remit to encrypt customer data. Most customers using Couchdrop access their data directly with other services and Couchdrop is not the only service working on their data so encrypting it in rest would provide a deterrent for customers.

Data Locality

Couchdrop has servers located in several regions as outlined below. When it comes to data locality, there are two different considerations.

San Francisco	Frankfurt
New York	London
Toronto	Singapore
Amsterdam	Bangalore

Customer Storage Data

When customers download, upload or list data with our platform through the SFTP or other protocols, one of Couchdrop's servers is interacting 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

The second type of data access is customer metadata. This is specific to Couchdrop and includes usernames, OAUTH and other credential sets for cloud storage, billing information and other metadata used to provide the Couchdrop service.

Customer metadata is housed in the USA and may be temporarily transferred to other regions via encrypted APIs to service requests.

Customer Metadata

To provide our service, Couchdrop must store metadata for its customers. This metadata includes account information, security credentials and other information that is used 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.

Cloud Storage Credentials

Couchdrop is dependent on external cloud storage; customers must grant Couchdrop access. Storage access is generally granted with two methods.

OAUTH Tokens

OAUTH is a process in which customers follow a cycle of requests and redirects to the remote platform to enter their credentials and grant access to Couchdrop. The remote platform then provides Couchdrop with an access token and in some cases a refresh token.

These tokens then allow Couchdrop to access files and folders and normally is temporary in nature. At any point, the customer can revoke Couchdrop's access by visiting the administrator section of their cloud storage provider and choosing to revoke Couchdrop.

An example of OAUTH-based access would be Dropbox.

Credentials and Access Keys

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

Couchdrop highly recommends not reusing access keys and credentials and restricting access where possible. After the migration is complete, Couchdrop also recommends deleting and revoking the access keys and credential at the storage endpoint. This renders them useless in the unlikely event that they are compromised.

Storage of Credentials

Third party storage credentials are stored in a separate database to 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 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.

COUCHDROP

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 practise, Couchdrop does not store actual passwords, rather Couchdrop stores a SHA-512 salted hash of the password.

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

Movebot

Movebot is a sister product built by Couchdrop to provide easy, cost-effective and fast data migrations. Movebot harnesses the Couchdrop platform and is deeply integrated, using the same infrastructure, sharing several microservices, and storing and collecting customer information in the same database ecosystem.

Use of the Movebot product is governed by the same terms and conditions as Couchdrop and customers can use both products interchangeably.

For more information on security in Movebot, please refer to the Movebot Security Overview Whitepaper.

Security Features within Platform

Couchdrop offers several security features to our customers to help them manage security requirements.

Two-Factor Authentication (2FA)
An authentication method in which a user is granted access to Couchdrop's portal through both username and password, as well as a token or code that is received by a designated mobile number via SMS.

IP Access/Whitelisting
Access to the web portal, SFTP or another chosen protocol is restricted strictly to the IP addresses or networks specified under the specific users account. Could also be seen as a method of firewalling.

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 to add further 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 access permissions to folders within a users directory.

Disabling of Access Methods
With Couchdrop, customers can disable access methods that aren't required or are insecure. For example, a customer may permit some users to use FTP and SFTP while others may explicitly only be allowed to use SFTP.

Support for RSA Keys
Instead of symmetric username and password authentication, customers can opt for asymmetric authentication through RSA keys where customers provide the public key under a user and the user can authenticate to Couchdrop without requiring a username and password.

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.

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. If a region is not available, then please reach out to Couchdrop's support team and they will endeavour to make it possible. This removes shared resources and ensures customers have a presence closer to where they need it for performance.

Secure File Transfer
Couchdrop offers secure protocols to transfer files into its customers chosen cloud storage, whether it's through an SSH tunnel or via HTTPS.

Password Protected and Temporary Shared Links
When using Couchdrop's web portal, customers have the ability to create password protected shared links to files and folders that can also be configured with an expiry timer to ensure that data is only shared to those who need it and for as long as they need it.

COUCHDROP

API Access

Along with SFTP, FTP, Rsync and web-based access, Couchdrop provides customers with API access to the platform.

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.

API access is only provided to customers who request it and subscribe to the business or enterprise plans. A token is required 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.

Documentation can be found at https://couchdrop-1.gitbook.io/couchdrop-api/.

Network and Infrastructure Security

Infrastructure Security

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

Docker provides an immutable, scalable and secure way to deploy our 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 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.

Server and SSH access is restricted to specific engineering staff and is locked down to particular static IP addresses. SSH keys are encrypted and passwords are stored in the 1Password product.

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

Couchdrop uses a centralised configuration management system to store deployment configuration and configuration is always compartmentalised 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.

Firewall and Network Access

Where relevant and possible, Couchdrop uses firewall and network access technology to restrict access to sensitive infrastructure components.

For example, management access to servers is provided on a random port chosen internally and only available to certain IP addresses. Database access is also restricted behind firewalls and changes to these firewalls must be approved by the CTO as part of our internal security policy.

Dedicated Customer POP

Enterprise customers can opt to utilise dedicated infrastructure. Dedicated infrastructure allows Couchdrop to support higher than normal load requirements originating from a single customer, offering a more performant and reliable service.

Dedicated infrastructure also comes with added security features. Customers are provided with dedicated IP addresses and resources are secured with different configuration sets, firewall rules, and security keys.

There are several different tiers available for Dedicated infrastructure, ranging from a single SFTP service in our main data centers, to a completely independent version of our application cluster, including databases and web front ends, being run in a customer's own datacenter.

Infrastructure Providers

Couchdrop uses several infrastructure providers. They are listed below:

Provider	Purpose	Regions
Digital Ocean	Main Infrastructure	All Regions
Amazon AWS	Hosted Storage, DNS	All Regions
Azure	Dedicated POPs	All Regions
Google Cloud	Dedicated POPs	All Regions
Wasabi	Hosted Storage	All Regions

Physical Security

At this time, Couchdrop operates remotely. Staff are working from home or from co-working spaces such as Regus.

The nature of Couchdrop's business makes this possible with very little downside. Since Couchdrop is not managing physical server infrastructure and the company is cloud native, Couchdrop has very little physical security requirements.

Staff are provided with computer equipment and are prohibited from accessing Couchdrop resources from personal computers.

Privacy Policy

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

COUCHDROP

Compliance

GDPR

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 USA.

Couchdrop follows the HIPAA guidelines 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 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 its platform.

COUCHDROP

Disclosure

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

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. "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.

To report a vulnerability, please email security@couchdrop.io