Technology Overview

04.12.19

Contents

Introduction

Codat is a technology company building infrastructure that businesses can use as-a-service to reduce costs of integrating with financial software and data providers.

This document provides an overview of the business operations relevant to ensuring that Codat provides a secure, reliable and available solution to its clients.

This document is not exhaustive, for more information please contact the author David Hoare (d.hoare@codat.io) directly or find further contact details on the Codat website, www.codat.io.

Codat Terminology

The following definitions are used throughout the rest of this document.

Codat/We/Us – Refers to the Codat company, the directors, the employees and the products offered by the company.

Clients – Businesses that have a contract with Codat to use the service we provide.

Companies – Businesses that are served in some way by the Client and who will be authorising the Client to interact with their financial data.

Accounting Platform Providers – Third party suppliers of software businesses use to manage their finances. e.g. Sage, Xero, Intuit

Website – The website at https://www.codat.io used to market the Codat solution to the wider community.

Client Portal – The online platform used by Clients of Codat to manage integrations and interact with Companies' financial data.

Link Site – A Codat developed website that can be used by Companies to select their accounting software before beginning the process of authorising an integration.

Codat API – The API at https://api.codat.io used to enable the linking of a Company's accounting software, synchronisation of financial data and access of data by the Client.

Development Process

Codat are strong believers in Agile Software Development and have delivered many successful projects using this approach. We have adopted the Scrumban methodology, with two week iterations.

The steps in feature development at Codat are:

- Ideation
- Requirement gathering
- Design
- Estimation
- Development
- Testing
- Release

Tooling

Development work is managed through Microsoft Azure Devops a hosted solution that provides tooling to aid workflow and issue management. The solution is integrated with source control, continuous testing, build pipelines and release management allowing end-to-end auditing from feature requests to production releases.

Access to Azure DevOps is via a Microsoft Account (2 factor authentication is enforced for all users) with permissions and access controlled by the CTO - more information on user roles can be found here.

Codat engineers use the following software for software development:

1. Microsoft Visual Studio
2. JetBrains ReSharper
3. JetBrains WebStorm
4. Syntevo SmartGit
5. Microsoft SQL Server Management Studio

Development Environments

1. Engineers' local machines
2. Integration
3. UAT
4. Production

Source Control

Codat use private Git repositories hosted by Microsoft and integrated to Azure DevOps to store code and co-ordinate changes across the development team. Access to repositories is enabled by either enabling SSH public keys or using secure Personal Access Tokens, both can be added and revoked in Azure DevOps.

A feature-branch workflow is used, this workflow requires engineers to create a branch for each piece of functionality or issue they work on. When the functionality is complete, a pull request is created and

reviewed by at least one other engineer before being merged into the master code base. The reviewing engineer is required to be an expert in the area of the codebase being changed – in the case of changing affecting more than one area of the system, the pull request must be reviewed by more than one engineer, with a reviewer from each team.

Branch policies are used to control code changes and ensure a high quality of code in the master branch - more detail on Azure DevOps branch Policies can be found here. The pull request review policies detailed above are enforced through this mechanism.

The following controls provided by Azure DevOps Branch Policies have been enforced:

- No direct commit to master branch
- Pull requests must have a linked work item (User Story or Bug)
- All pull requests must be reviewed by at least one other Engineer

Two factor authentication for Azure DevOps access is enabled.

To limit access to production keys and database connection strings these sensitive settings are stored in Microsoft Azure and are therefore not visible in the codebase or in Azure DevOps.

Open Source

All Codat's code is proprietary and private except for language specific client libraries. These client libraries provide a "wrapper" around the publicly available API for a specific language, they are designed to be used as a tool by clients to speed up adoption of the API. Client libraries do not contain sensitive information (e.g. no Company data or personal data) and can therefore be made public to allow Clients to contribute to the scope and maintenance of each library.

To provide a distinct separation between private and open-source code, GitHub is used for open source repositories. The JavaScript client library can be found at https://github.com/codatio/codat-js.

Test Driven Development

Untested code is not permitted in the Codat codebase. Where sensible we practise a test-driven approach to development, writing tests first to ensure requirements are met. Tests are run at build time and the build will fail if all tests do not pass, preventing the code from being released. End-to-end tests which test user flows and the entire data pipeline are run multiple times a day on a schedule. The engineering team is alerted in the event of test failures by Slack and email notifications.

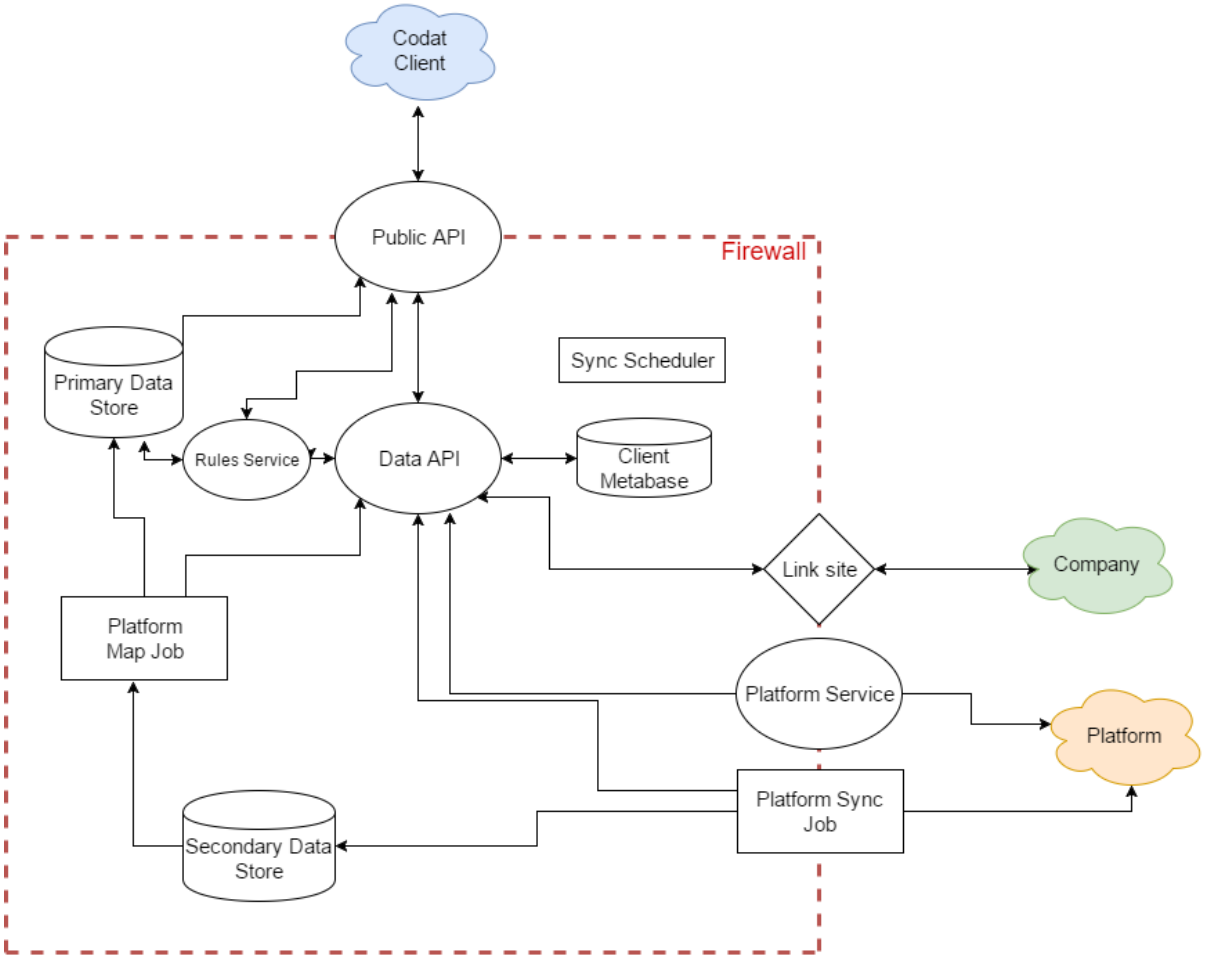
The testing frameworks NUnit, Machine.Specifications and Protractor are used; for current statistics on code coverage of our tests please contact David Hoare, CTO (d.hoare@codat.io).

Technical Architecture

The Codat technology system has a microservice architecture, this modular structure parallelizes software development and enables a scalable and robust system to be created.

There are currently 40 services that make up the Codat technology infrastructure, each with a separate instance for each of the three environments (integration, UAT, production). Most importantly, each connection to an external data source is a separate service with the responsibility of handling authentication, authorisation, data fetch and data mapping. Services are configured to automatically scale out to multiple instances in the event of increased load, thus ensuring high levels of availability

and performance. Load on instances is proactively monitored by Azure, and the engineering team is alerted via email in the event of unexpected spikes.



Public API

The Public API is the API Clients use to enable the linking of a Company's accounting software, synchronisation of financial data and access of data by the Client.

The API is an ASP.NET Web API, a Microsoft framework that enables the building of secure and scalable RESTful HTTP services.

The API endpoints are documented at https://docs.codat.io and developers can use the interactive Swagger documentation at https://api.codat.io/swagger.

Hosting and Data Storage

Codat uses the Microsoft Azure platform for all hosting and data storage. Codat has ensured that all hosting and data storage by Azure is located in the UK only.

Microsoft Azure is a growing collection of integrated cloud services that developers and IT professionals use to build, deploy and manage applications through a global network of data centres.

In particular Codat uses Azure's Platform-as-a-service (PaaS) offering rather than Infrastructure-as-a-service (IaaS). This means that the underlying application infrastructure is managed by Microsoft themselves, ensuring it is maintained to the highest standard. Operating System patching is carried out automatically by Microsoft.

Codat uses the following services provided by Microsoft Azure for hosting and data storage:

1. SQL Databases
2. Table Storage
3. Blob Storage
4. Storage Queues
5. Web Applications
6. Web Jobs
7. Managed Redis cache
8. Service Bus

All data is stored on Microsoft Azure architecture.

Azure Security

Codat utilises the following security offerings provided by Microsoft Azure:

Encryption at rest – SQL transparent data encryption, Storage Service Encryption, AES-256

Encryption in transit – TLS/SSL enforced for all data transit, HSTS, IPSec

Role level access – Azure RBAC, Active Directory

For a more detailed explanation of Microsoft Azure security and data protection features see https://www.microsoft.com/en-us/trustcenter/

Access

Microsoft Azure access is restricted to only senior engineers and two-factor authentication is enforced. Azure Active Directory is used to control access in a granular manner; Production infrastructure is separated out onto a dedicated Azure Subscription and therefore access can be restricted to only the CTO and Lead Engineers.

Security and Data Protection

Security is of vital importance to all Codat employees and shareholders. Codat ensures that it has appropriate technical and organisational security measures in place to protect personal data to the standards required by applicable law.

Data sensitivity classification

All data held at Codat must be classified in terms of its sensitivity:

- Confidential – all data passed through the Codat platform which is contributed by Companies who authorise Codat clients to access their data via the Codat platform. The security of this data is Codat's primary priority at all times.
- Metadata – all data relating to the transmission of Company data through the Codat platform. This data must be held internally to Codat, in line with the ISMS.
- Internal – all data relating to the internal workings of Codat and its clients. This data must be held internally to Codat, in line with the ISMS.
- Public – all data which has been made publicly available from Codat.

Security awareness training

All employees of Codat must go through security awareness training, both at the start of their employment and at least annually thereafter.

Classroom training is provided on a monthly basis by the CTO, covering phishing, physical security, desktop security, wireless networks, password security and malware.

The effectiveness of Codat's training programme is measured against the number of security incidents, managed and tracked by the CTO.

Continual Improvement

To ensure Codat continues to provide best-in-class security quarterly meetings of a Security Working Group are conducted. Codat commissions an annual penetration test using third-party providers against a copy of the production environment created for this purpose – not the live environment.

IP Security

Codat provides the option to enforce IP security in addition to the standard authentication offered; this means access to the API and Client Portal is restricted to a whitelist of allowed IP addresses. IP security is on a per-Client basis, allowing it to be turned on/off as per the Client's needs and ensuring separate whitelists between Clients.

Common Attack Types

Attack Type	Defence
Social Engineering	Custom IP security
Phishing	Two-factor authentication turned on for Email, VSTS and Microsoft Azure.
DoS/DDoS	CloudFlare, Azure auto-scaling
SQL Injection	Isolated data access services, no direct SQL access

XSS	ASP.NET request validation
Brute force	Invalid login limit, automated IP blocking

Physical machines

No Client or Company data is stored on physical machines and Codat does not own physical servers. The PCs and laptops of employees all have encrypted hard drives. The use of removable media (eg CDs, USB drives) is not permitted on company computers, the "All Removable Storage classes: Deny all access" Windows Group Policy is enforced to prevent any unauthorised use. All devices are registered in Codat's Azure Active Directory, and the Active Directory is regularly audited by the CTO to ensure operating system patches are being applied. As part of the documented offboarding process, all physical machines are retained by Codat when employees leave the business.

All hardware items that have the ability and capability to store Codat information and sensitive data must be disposed of securely at end-of-life, to minimise the risk of unauthorised access. Codat uses Data Eliminate Ltd's on premise solution for the purposes of asset disposal. All assets must be destroyed to the standards required by HMG's Secure Sanitisation Level 1.

Software licence management

Codat provides employees with licenses for approved software packages, including Microsoft Windows 10 (operating system), G Suite (email and calendar), Office 365 (productivity tools) and the tools used by the engineering team discussed above. These licenses are only permitted to be used on Codat hardware. Software licenses are managed centrally by the CTO. License management portals report installed versions of software products on each machine, this is regularly audited by the CTO to identify any unauthorised usage and to ensure that software patches are being applied. For licenses which require user login, compliance with security policies (eg password complexity, two-factor authentication enrolment) is likewise monitored centrally. As part of the documented offboarding process, all software licenses are revoked by Codat when employees leave the business.

Codat employees

To minimise risk of accidental or malicious activity that could lead to a security breach, access to production environments and settings is restricted. Only senior engineers with the required DevOps skillset are granted access and only after successful completion of their probationary period.

Resolving Issues

We strive to ensure that a high quality of software is produced, limiting the likelihood of errors in the systems we offer for clients. However, our 5-step process detailed below is in place to enable us to identify and resolve issues effectively should they occur.

1. Detection
2. Triage
3. Prioritisation
4. Resolution
5. Retrospective

Detection

As soon as an error is identified, a ticket is created in our issue tracking tool (Azure DevOps). There are three ways issues can surface:

Automated Monitoring

Multiple automated checks run 24/7 that alert Codat engineers if systems are un-responsive or show un-expected behaviour.

Third-party tooling from Pingdom, LogEntries and Application Insights is used to enable automated monitoring and alerting. Steps have been taken to ensure no Client or Company data is shared with these third-party suppliers.

Report from Codat employee

Codat engineers or support staff may spot unexpected behaviour in a system. In this instance they report the issue directly to the Head of Product (Peter Lord, CEO) who then takes responsibility for documenting and triaging the issue.

Report from Client

A client may report unexpected behaviour via the Codat technical support channel (support@codat.io). The Codat support team then communicates the issue directly to the Head of Product who then takes responsibility for documenting and triaging the issue as well as following up with the client who reported the issue directly.

Triage and Prioritisation

Issues are triaged into four main categories which reflect the severity of the issue and the response by Codat engineers.

Level	Description	Time to fix SLA*
Critical	Any security issue or any issue that has potential to expose Clients or Companies data.	< 30 mins
High	A major component of the system is not functioning correctly. The issue is impacting clients and there is no workaround.	< 4 hours
Medium	A major component of the system is not functioning correctly but there is a workaround or a minor component of the system is not functioning correctly.	< 1 business day
Low	There is a minor issue with very low impact to clients and there is a workaround.	< 30 days
False Alarm	Either an incorrect report or the system behaviour reported is as designed.	-

*time from incident detection to fix, SLA currently only covers UK business hours.

Resolution

Dependent on the level of issue, certain structure in resolution is enforced.

Required for Critical

CTO to be immediately informed of reported issue. Codat Security Incident Response Plan to be followed, and Codat will evaluate whether a personal data breach has occurred which will require notification to the relevant Client.

Required for Critical and High

Incident lead is assigned.

All engineers stop developing and a stand-up meeting is conducted to synchronise diagnosing and fixing the issue.

Notes on actions taken must be recorded throughout to allow an incident report to be written at a later date.

The following options are available for engineers when resolving an issue:

Take all systems offline – used only in extreme circumstances where there is a potential security or data breach threat.

“Rollback” changes – used when a recent version of code released contains a programming error.

Create and release a fix for the issue – updating the servers with new code that fixes the reported issue.

Retrospective

For all Critical, High and Medium issues a retrospective meeting of relevant parties must be conducted to minimise chances of similar issues occurring again.

Recommended actions should be noted and deadlines for actions should be recorded. Progress on action points should be tracked in Microsoft VSTS. A formal incident report must be filed with the CTO no longer than 2 weeks following the fixing of any Critical, High and Medium issues.

Business Continuity

In the event of a disaster or failure scenario the Business Continuity Manager will lead implement and lead the plan to ensure the best possible service is provided for Codat Clients. The business continuity manager is Peter Lord, CEO.

Loss of buildings

All key staff have portable devices, which can be removed quickly. All key functions can be delivered remotely, using the same, or replacement devices. In the case of a complete disaster which caused the building and all equipment inoperable immediately, purchase of new laptops for key staff would be authorised and purchased within 6 hours, allowing a 24 hour response time to set up all critical functions at a new location.

The Codat system is not hosted on-site, so platform operation would not be affected.

Key Personnel Loss

The engineering team at Codat currently contains 8 senior engineers with knowledge of the entire system, meaning that the loss of one engineer would not significantly harm the functioning of the Codat system.

Isolated Azure Failure

Some localised Azure failures may mean that services can be re-created in different UK Azure data centres. The estimated time to re-create a complete Codat infrastructure in a different UK Azure datacentre is 12-24 hours.

Total Azure Failure

In the unlikely event of a complete Azure failure in all datacentres Codat would not be able to operate for up to 7 business days whilst it re-deployed all systems to another cloud service provider. Amazon AWS would be the most likely choice in this unlikely scenario. In such case, Codat would be sure to restrict any location of data in AWS to the UK only.