Security and Architecture
Overview

dazychain

Access control

Assigned roles and groups govern user access to functions within Dazychain. Individual projects are further protected via an access list of allowed 'collaborators'. All roles are assigned by the organization administrator. An organization can appoint one or more users to an Organization Administrator role.

Users are verified by login and password pair over a TLS 1.3 encrypted link. Passwords are always encrypted before storing.

Dazychain can configure Single-Sign On (SSO) for an organization, using Secure Assertion Markup Language (SAML). Organizations can choose to apply an additional two-factor authentication using their own access process.

Intake forms and the external portal can be accessed with non Dazychain users. These are authenticated using a Microsoft account. Organization administrators can restrict access to specific domains to ensure only their own organization has access – or turn this off entirely.

Application security

Penetration testing

Penetration tests are conducted internally prior to each release of Dazychain. External third-party penetration tests are performed annually.

Vulnerability protection and monitoring

Our application runs on Amazon Web Services (AWS). We utilize AWS Shield, Amazon Inspector, Amazon CloudFront, Amazon Guard Duty and AWS's Web Application Firewall to monitor, identify and log vulnerabilities for remediation.

Data security

The database, including documents, are encrypted at rest using AES-256 algorithm. All communications in transit between the application and the database are encrypted using HTTPS with TLS 1.3 protocol.

We use a shared, multi-tenanted database with data tagged as owned by a specific company. No company can view another's information unless permission has been provided, such as in the case when companies are collaborating with their law firms.

Dazychain shares limited data with third parties, only as required for the operation of the platform. For example, we share limited data to produce notification emails, aggregate logs and edit documents.

Yarris engineers and system administrators have access to Dazychain only on an as-required basis with an audit trail. Yarris makes use of cloud services to host our databases and application servers, as such we have no physical access or data stored on-premises. The system retains a complete history of access to the system, including each data change on business entities such as matters and deliverables.

All administrator accounts are personnel specific. Passwords are encrypted and cannot be viewed.

Compliance and privacy

ISO27001
Our ISO 27001:2013 controls and wider Information Security Management System (ISMS) internally and externally audited annually.

SOC 2
Annually undertaken and externally audited, we produce type 2 reports.

Privacy Act

We comply with the Privacy Act 1988 (Privacy Act) and related Australian privacy and data laws.

Employee security

All staff undertake police checks before they join the organization and again once every two years. Confidentiality agreements are signed by all employees, third parties and contractors.

During orientation, employees are briefed in detail on the organization's ISMS policies. The policies are
updated frequently, shared with employees and acceptance is documented. Security awareness refresher training is undertaken by all employees each year.

Backups and recovery

Client data is backed up by cloud providers hosting our databases and file systems daily:

- MongoDB (Database): Backup retention - two weeks
- S3 (Document store): Backup retention - unlimited

On termination, our policy is to retain client data for the period requested by the client, usually one month. After that time, the data is deleted. Yarris can assist with data migration arrangements for an additional professional services fee.

Yarris has fully developed Disaster Recovery and Business Continuity plans included in our ISMS that are ISO 27001 certified.

User support

Telephone, ticket, and email support are available during business hours, Monday to Friday (8am to 6pm AEST/AEDT excluding Australian national public holidays)

Our online Help Centre has a full collection of help guides which are available 24/7 at dazychainsupport.zendesk.com

Ticketing Support requests are logged by support tickets within Dazychain or help centre (accessed from website: https://dazychainsupport.zendesk.com/hc/en-us). The Client can log tickets to Yarris and create an account to monitor and review all submitted tickets and resolutions. Clients can create support tickets by:

- Emailing the request to: help@dazychain.com
- Logging in through the help center and logging a ticket
- Calling our office on 1300 927 747

Clients are also assigned a dedicated Account Manager who provides additional support services including:

- Continuing business analysis check-ins to improve your workflow, templates, and reporting
- Complimentary training on an ongoing basis covering new improvements and features of the system or existing features
- Assistance in applying any configuration changes to the organization account

Software updates

Development releases are typically rolling releases but when system downtime is required this is performed outside of business hours.

Scheduled system maintenance or development releases take place at 9pm AEST/AEDT and users will receive notice via email, at least 24 hours before scheduled maintenance.

Release notifications on product updates are communicated to users via email, and release notes are made available in the Dazychain Help Centre.

All software development to production systems is developed according to the Yarris Software Development Lifecycle (SDLC) Standards. The SDLC phases are:

- Initial phase
- Feasibility phase
- Requirements analysis phase
- Design phase
- Development phase
- Testing:
    - Business review
    - Code review and functional testing
    - Integration testing
    - User acceptance
- Implementation phase
- Operations and maintenance phase
- Security vulnerabilities testing and remediation

Service Level Agreement

Yarris will use commercially reasonable efforts to make Service available to Dazychain, customers. Failure to achieve the minimum scheduled uptime over a quarter will result in Yarris refunding a portion of the monthly license fees. Yarris commits to host, support and maintain the application.

At Risk Amount: means a sum equal to one third of the monthly licence fees for the Quarter. The At Risk Amount is further broken into portions for Availability (one third) and Page Performance (two thirds).

Key performance indicators

Our customers expect the following KPIs to be achieved. Failure to successfully achieve these KPIs may result in Yarris refunding a portion of the monthly licence fees.

Availability

Should Availability for a Quarter fall within the following ranges, a portion of the At Risk Amount for Availability will be forfeit:

Level	Measure	Penalty
Acceptable	Greater than or equal to 99.7%	Nil
Failure, mild	Between 99.69% and 98.01% (inclusive)	One third of At Risk Amount for Availability
Failure, moderate	Between 98.0% and 97.01% (inclusive)	Two thirds of At Risk Amount for Availability
Failure, high	Less than 97.01%	Full amount of At Risk Amount for Availability

Page Performance

Should Page Performance for a Quarter fall within the following ranges, a portion of the At Risk Amount for Page Performance will be forfeit:

Level	Measure	Penalty
Acceptable	Greater than or equal to 95%	Nil
Failure, mild	Between 94.99% and 90.01% (inclusive)	One third of At Risk Amount for Page Performance
Failure, moderate	Between 90.0% and 85.01% (inclusive)	Two thirds of At Risk Amount for Page Performance
Failure, high	Less than 85.01%	Full amount of At Risk Amount for Page Performance

Scheduled maintenance and upgrades

Should Yarris fail to provide sufficient notice for upgrades or maintenance occurring without 24 hours' notice to customers, this is viewed as a KPI failure without financial penalty.

Client IT implementation requirements

A client's IT team assistance will be required in the implementation of Dazychain for the following activities.

Whitelisting

Whitelisting may be required for the Dazychain.com domain and depending on your environment, port 443.

When our domains are added to a client's whitelist, it means they are explicitly allowing traffic from our domains to pass through their network or security measures, ensuring that Dazychain and associated services (Outlook, DocuSign) can function without being blocked or restricted. This helps enhance security by restricting access only to trusted sources.

Whitelisting requirements

Single Sign On

Dazychain uses Secure Assertion Markup Language (SAML) via Cognito as our single sign-on (SSO) authentication method. This is supported by many identity provider services, such as Azure AD / Entra ID, Okta and OneLogin. IDP Initiated / Entra Azure Dashboard is available. SSO is an additional function that can be configured for your organization and will require the client IT team's participation.

Single Sign-On configuration guide

Outlook add-in installation

Dazychain users can use the application via an Outlook add-in, this can be added to their Outlook via the App Store. Depending on your environment, users may need the application enabled for installation.

Installation instructions

My Portal

Dazychain enables users without a license to access features such as intake forms, contract automation and, matter and document sharing via 'My Portal'. All users will require access authorization via your active directory.

Off-platform user log in

Additional Dazychain feature information

Microsoft Online / WOPI

Dazychain implements the Web Application Open Platform Interface (WOPI) protocol to integrate Office for the web with Dazychain documents. The WOPI protocol lets Office for web access and change files that are stored in the Dazychain cloud.

The following office formats are supported:

- Word: Docx format - files ending in .docx
- Excel: Xlsx format - files ending in .xlsx
- PowerPoint: Pptx format - files ending in .pptx

Older formats such as .doc, .ppt and .xls are not supported.
Dazychain has a minimal implementation of WOPI. Functionality is limited to editing the document types listed above. Additional functionality such as document type conversion, renaming and moving documents is not currently available.

WOPI overview

DocuSign integration

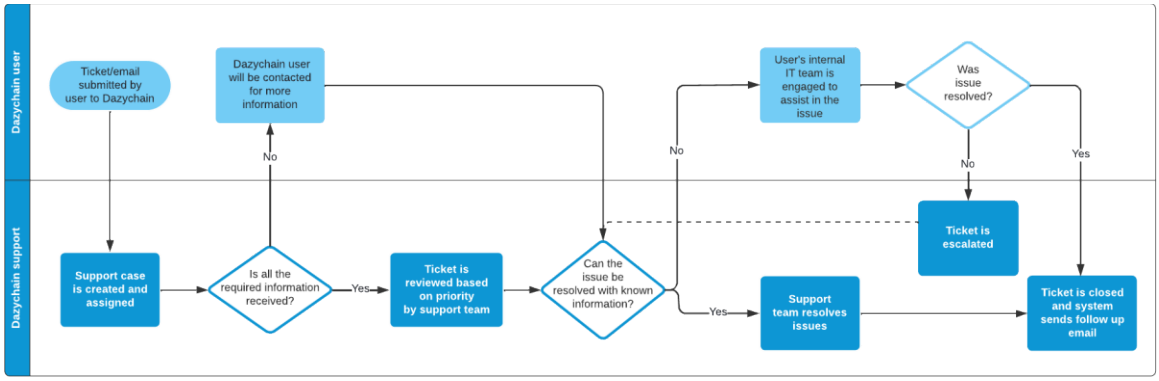
Dazychain integrates with DocuSign, additional configuration is not required. Users when initiating “Send to DocuSign”, are prompted to login with their DocuSign credentials if a valid session is not already running.

Post implementation

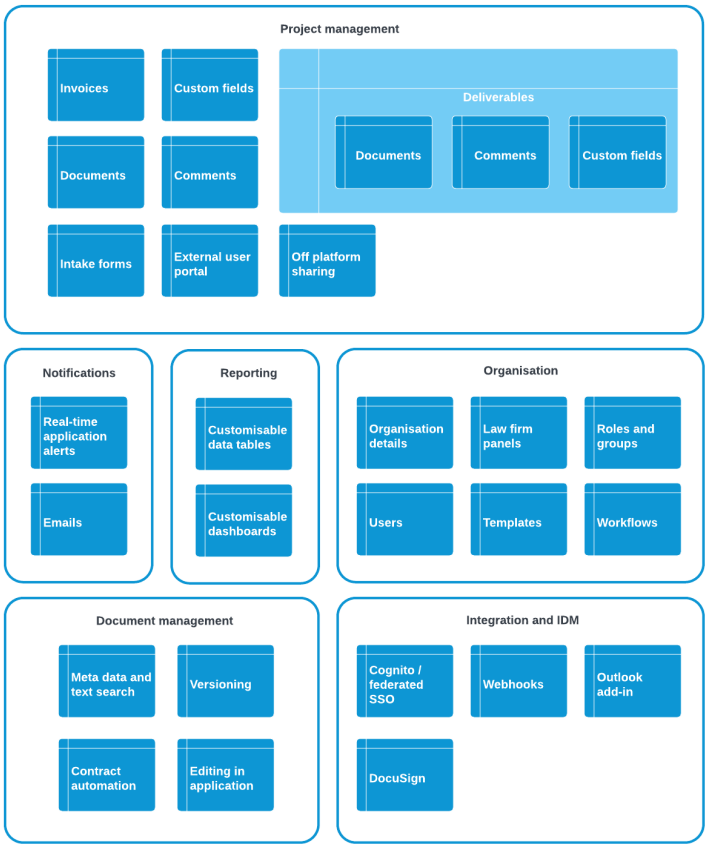
Once implemented Dazychain requires minimal work from the client IT team:

- Configuration changes are simple and require no code changes and the account manager assists at no additional charge.
- Yarris provides full technical support as part of the Dazychain platform.
- Where SSO is enabled, client IT may be required to add new users to the directory.

Any user support requests should be submitted directly to Dazychain by users. When investigation is required on the client side Dazychain will contact the client IT team to collaborate on a resolution.

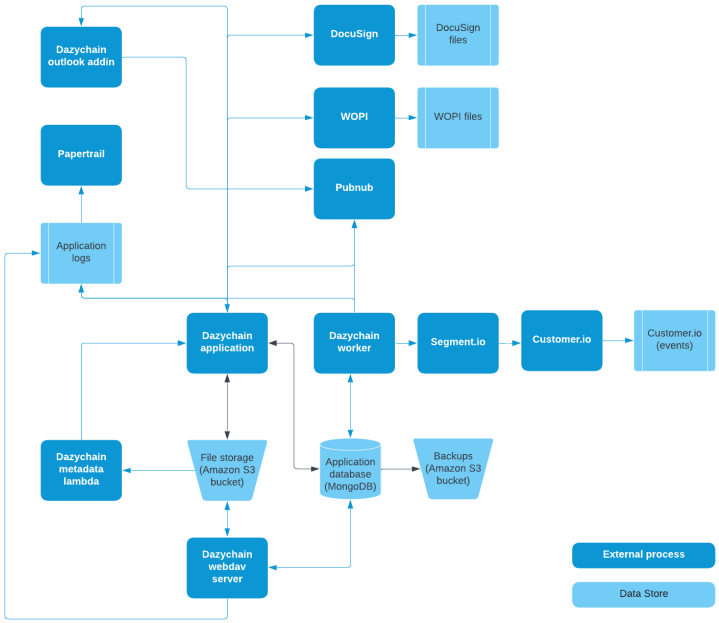


Application modules overview

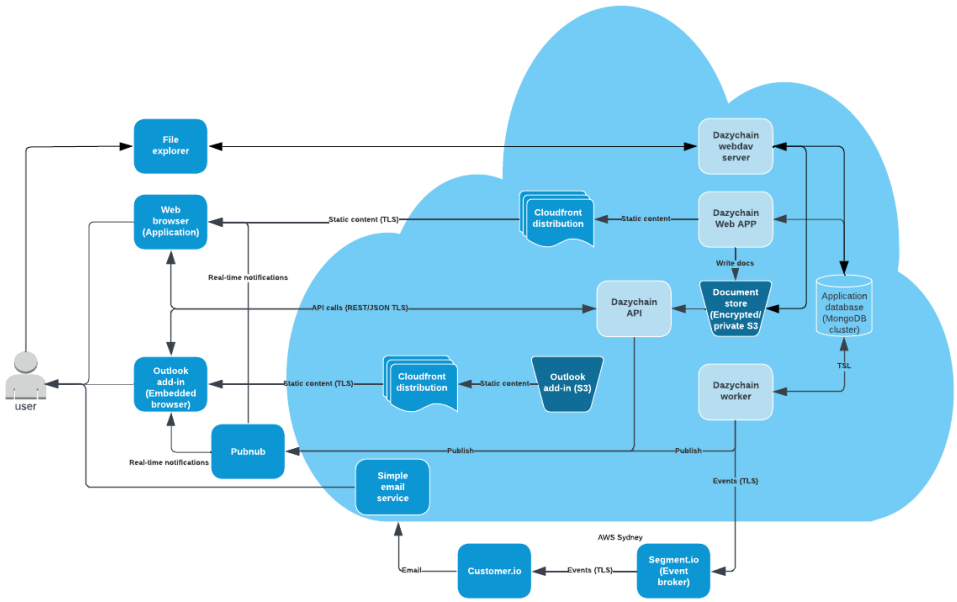


Data stores

Application data and client-stored documents are hosted in Amazon S3 buckets, located either in the Sydney (Australia) or North Virginia (United States) AWS regions, depending on customer preference. All data is stored in highly redundant storage environments. The application's database is hosted by MongoDB Atlas in Australia, ensuring performance, security, and compliance with local data residency requirements.

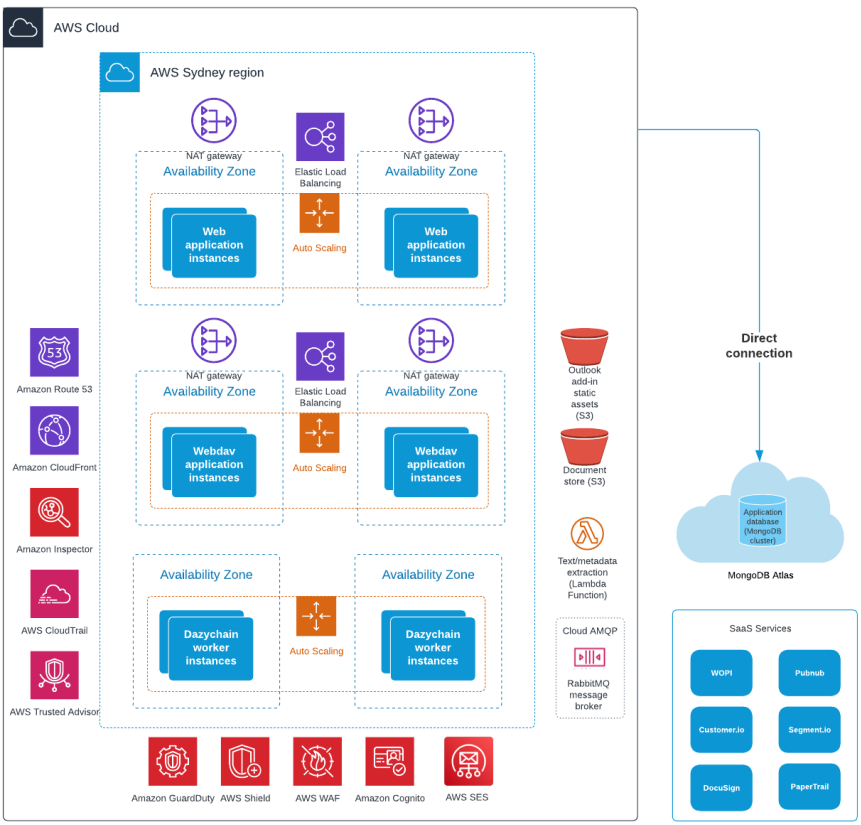


Simplified system architecture



Technology architecture

Our application stack runs on AWS, fully utilizing the multi availability zones for High Availability and redundancy. The application sits behind Elastic Load Balancers. We also make full use of AWS Shield to combat denial of service attacks. The application is tightly controlled during high load scenarios, with new instances created as required to combat the load.



InfoSec Policies

Information Security Policies (Summary Info)

Acceptable Use
Acceptable use policy is a document stipulating constraints and practices that a user must agree to for access to a corporate network and other organizational assets.

Access Control
Access Control Policy defines high-level requirements and guidelines on user account management, access enforcement and monitoring, separation of duties, and remote access.

Backup and Restoration
The organization actively manages risks associated with data loss by defining a sound backup regime for all the data services.

Bring Your Own Device (BYOD)
This policy is intended to protect the security and integrity of organization's data and technology infrastructure when employees are using their personal device(s) to connect to organization's corporate network.

Business Continuity and Disaster Recovery
Yarris has a Business Continuity and Disaster Recovery Policy that ensures that the organization can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

Change Management
A formal change management policy governs changes to the applications and supporting infrastructure and aid in minimizing the impact that changes have on organization processes and systems.

Clean Desk and Clear Screen
A clear desk and clear screen policy ensures that all sensitive/confidential materials are removed from workspaces and locked away when the items are not in use or an employee leaves their workstation.

Corporate Ethics
The organization values ethics, trust and integrity throughout its business practices.

Customer Support and SLA
Customers are important to Yarris by providing Customer Support and a Service Level Agreement (SLA) to support its customers.

Data Retention and Disposal
This policy is about the organization's approach for data retention and secure disposal.

Disciplinary Policy
The organization has implemented a disciplinary process in order to deal with instance(s) of indiscipline including (but not limited to) non-compliance to information security policies and procedures by users.

Incident Management
It is critical to the organization that security incidents that threaten the security or confidentiality of information assets are properly identified, contained, investigated, and remediated.

Information Classification
Information classification is the process of assigning value to information in order to organize it according to its risk to loss or harm from disclosure.

Information Security
Yarris utilizes the "Tugboat Logic Platform" to manage InfoSec policies, provide security awareness training, implement and document security controls, and track compliance with customers, third-party vendors, independent auditors and regulatory agencies.

Internal Audit
The organization conducts Internal Audits on its existing policies and controls to ensure the best level of service to its customers.

IT Asset Management
The organization closely manages IT systems and the data that they contain from purchase to disposal.

Key Management and Cryptography
The organization utilizes the latest commercially accepted encryption protocols.

Mobile Device Management
This policy defines procedures and restrictions for connecting mobile devices to organization's corporate network.

Network Security
Yarris provides a protected, interconnected computing environment through the use of securely configured network devices to meet organizational missions, goals, and initiatives.

Personnel Security
Organization members understand their roles and responsibilities around security and privacy.

Physical and Environmental Security
The organization protects managed systems and personnel from unauthorized access and from natural and human caused damage or destruction.

Remote Access
Access to organization resources from outside organization networks for business purposes is closely managed and protected.

Risk Assessment and Risk Treatment Methodology
The organization provides a foundation for the effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified.

Server Security
The organization manages, configures and protects organization servers and hosts based on industry best practices.

Software Development
The organization designs and builds software with security and privacy as design principles.

Technology Equipment Handling and Disposal
The organization appropriately disposes of equipment that contains sensitive information.

Vendor Management
The organization actively manages risks around 3rd party vendors and their access to Yarris data.

Vulnerability Management
The organization conducts scheduled application/network scanning and penetration tests

ISO/IEC 27001:2022 Certificate

SOC 2 Type 2 Attestation Status