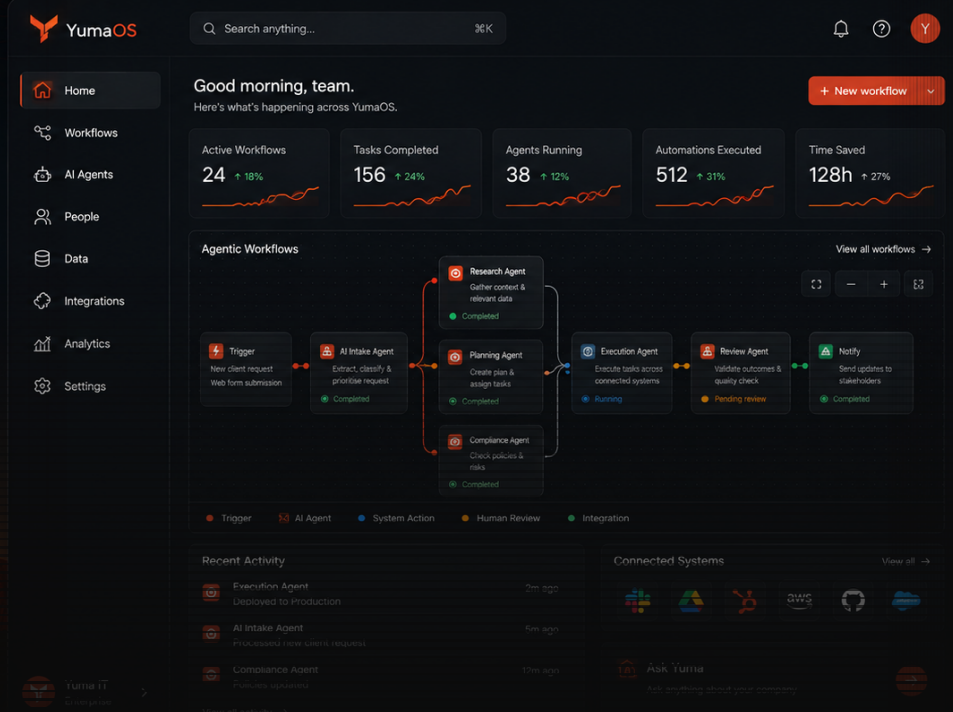




Say **Yuma** to simplified company management, driven by **agentic workflows**, everywhere you work.

People Workflows AI Agents Data Integrations

Intelligent agents. Connected systems.
Real work. Real results.



YumaOS

Say **Yuma** to simplified company management, driven by **agentic workflows**, everywhere you work.

Intelligent agents. Connected systems. Real work. Real results.

PRODUCT

CompanyOS · multi-tenant

FROM

Yuma IT Pty. Ltd.

STATUS

Private product

PAGES

20 · capabilities

FIVE CLUSTERS

People

Directory, CRM, workspaces.

Workflows

Projects, Pulse, risks.

AI Agents

Mastra, queue, Hermes.

Data

RAG, graph, vault.

Integrations

MCP, webhooks, comms.

Yuma IT Pty. Ltd.

A company operating system. White-label. Single deploy.

PRIVATE PRODUCT · AUSTRALIAN COMPANY · CAPABILITIES BRIEF

THE OPPORTUNITY

The work is already happening. The operating system is not.

Most organisations already run people, projects, money, and comms. They just run them in a pile of tools that do not share a directory, a permission model, or a memory. YumaOS is built for the organisations that are done paying that tax.

Yuma IT works with government, research, Indigenous organisations, and Australian businesses. Data residency in Australia is a hosting and delivery choice we make with you — Yuma IT positioning, not a stamp we put on every deploy.

Government

Program offices and agencies that need one picture of people, work, spend, and records — with roles, overrides, and an audit trail that can be shown.

Research organisations

Institutes that live on grants, tenders, documents, and collaboration. Knowledge has to be findable. Access has to be deliberate.

Indigenous organisations

Operators who need a system that can be branded as theirs, hosted with care, and run without a vendor maze. Yuma IT is Supply Nation Certified — that is the company, on the close page.

Australian businesses

Operators who want CRM, delivery, commercial, and comms in one white-label system — not another SaaS login for every function.

Who it is not for

Teams hunting a public app store listing will not find YumaOS on yumait.com.au/projects. It is a private product. This document is the capabilities brief.

CompanyOS. One deploy. Five clusters.

YumaOS is a multi-tenant company operating system: a single-deploy Next.js industry app starter. You white-label it, switch modules, and run it as the operating layer for a company — people, work, agents, data, and the systems already around them.

Intelligent agents. Connected systems. Real work. Real results.

People

Directory, users, workspaces, customers, leads, and the org chart. Who you work with is a first-class record.

Workflows

Projects, tasks, calendar, schedules, operations, Pulse, risks. The work, not another board.

AI Agents

Mastra agents with an action queue you cannot disable, auto-approve rules, traces, and Hermes.

Data

Postgres and pgvector, document RAG, Semantica knowledge graph, vaulted secrets, audit.

Integrations

MCP in and out, webhooks, external APIs, Slack, Teams, SMS, email, Entra, SCIM.

Stack, in one line

Next.js 16 · Better Auth · Drizzle · Postgres / pgvector · Mastra agents · Docker → Coolify

HOW IT WORKS

One codebase. Your brand. Your modules.

YumaOS is a single-deploy application, not a suite of products you stitch together. White-label branding, a module system, and skills sit on the same Next.js 16 app. You stand it up once. You decide what is on.

Local Docker for a first look. A homelab when the team is ready to live in it. Coolify and GHCR when it is production.

01 White-label shell

Brand, modules, and skills. The operating system ships as theirs — wordmark, colour, and the surfaces they actually open.

02 Company operating layer

People, work, commercial, comms, knowledge, agents. Multi-tenant. One Postgres. One permission story.

03 Platform & deploy

Better Auth, Drizzle, vault, MCP, webhooks, OpenAPI. Docker locally. Homelab next. Coolify + GHCR in production.

ON THE SAME DEPLOY

Modules

Skills

OpenAPI

White-label

Multi-tenant

Action queue

Roles first. Overrides when the work demands it.

Access in YumaOS is attribute-aware in a specific, honest sense: roles, user permission overrides, and resource-level document and form access. That is the model. Settings → Access / Roles is where it is administered. There is no invented policy engine in this brief.

MFA, Entra SSO, and SCIM sit on the same Better Auth foundation. The audit log is how you show who did what.

RBAC

Roles and permissions live in the product (lib/rbac, the RBAC schema). Assign a role. The default access follows.

Permission overrides

A person is not always their role. User-level overrides exist for the exception — the one officer, the one contractor.

Resource access

Documents and forms can be granted at the resource. The file, the form, the record — not only the role.

MFA

Multi-factor on the same auth stack. Not a bolt-on afterthought.

Entra SSO

Microsoft Entra for organisations that already live there.

SCIM

Provisioning that can follow the identity source, not a CSV ritual.

Audit

A trail of access and action. Evidence, not a slide.

Agents propose. The queue holds. People decide.

Mastra agents are part of the operating system: ops, risk, docs, quote, router, Slack, Teams. They do not silently mutate the company. Actions land on a queue. The queue is on. It cannot be disabled.

Auto-approve rules exist for the work you have already decided is safe. Traces exist for the work you need to explain. Hermes is chat and voice on top of the same roster.

Ops

Operational work routed into the queue — the day-to-day, not a demo agent.

Risk

Risk-aware actions, sitting next to the risk register rather than a side chat.

Docs

Document work: draft, retrieve, file. Knowledge is a first-class surface.

Quote

Commercial drafting that lands where estimates and quotes already live.

Router

The agent that decides which agent. Routing is a job, not a hope.

Slack

The same roster, in Slack. Actions still hit the queue.

Teams

The same roster, in Microsoft Teams. Same queue. Same rules.

Action queue — always on

Every agent action is queued. This is not a setting. You review, approve, or reject. The company does not drift because a model was confident.

Auto-approve & traces

Rules for the work you have already accepted. Traces for the work you will be asked about. Hermes for chat and voice when the keyboard is the wrong interface.

The directory is the system of record.

People in YumaOS are not a bolt-on contacts app. Customers, leads, the org, the directory, users, and workspaces share one multi-tenant picture. Import the customer book from CSV when you are migrating. Keep the living record in the operating system.

Workspaces keep a company from becoming one flat list. Users are people with roles — which is how access on the previous page actually attaches.

Customers

The book of who you serve. CSV import when you are coming from somewhere else.

Leads

The front of the funnel, in the same system that will quote and invoice them.

Organisation

Structure, not a spreadsheet of names. The org is a record.

Directory

Findable people. The difference between a company and a mailing list.

Users

Accounts, roles, overrides. The human side of RBAC.

Workspaces

Boundaries inside the tenant. Teams see the company they are in.

WORK

Projects, imported time, Pulse, and risk.

Work in YumaOS is projects, tasks and labels, wiki, calendar, schedules, operations, Pulse, and risks. Time is imported from the tools you already use to capture hours. YumaOS is not a time tracker. It is where those hours land next to the work they belong to.

Projects & tasks

The unit of delivery. Labels on tasks. The board is not the product — the project is.

Wiki

Operational writing next to the work, not a second wiki product.

Calendar & schedules

When the work happens. Schedules as a record, not a screenshot.

Time import

Hours come from existing tools. We do not pretend to replace the tracker you already run.

Operations & Pulse

The operating rhythm — what is moving, what is stuck, what needs a look.

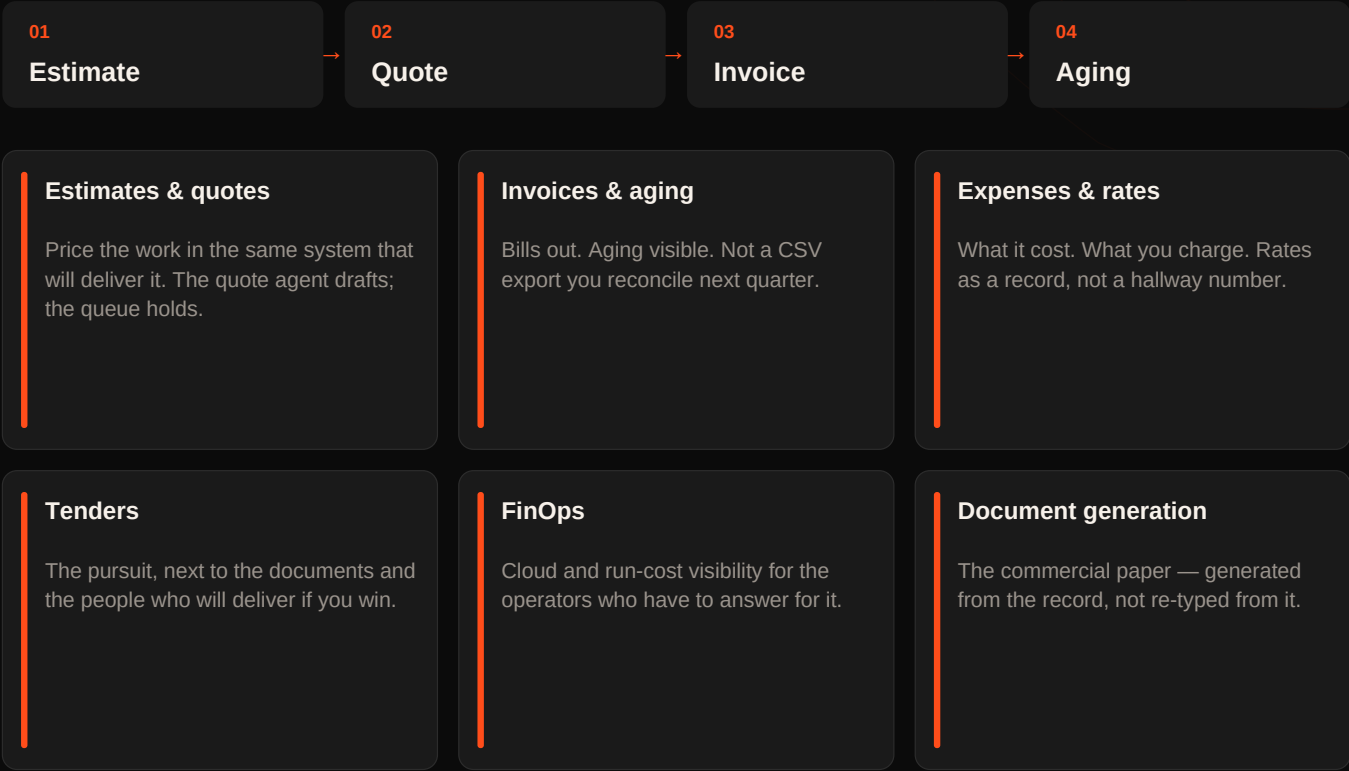
Risks

A register in the same system as the work. The risk agent sits beside it.

Time import is a deliberate non-feature: we take hours in. We do not ask teams to abandon the tracker they already trust.

Estimate, quote, invoice. Tenders and FinOps.

Commercial work should not live in a second finance silo. YumaOS carries estimates through quotes into invoices and aging, with expenses, rates, tenders, FinOps, and document generation on the same deploy.



Email and SMS that know the segment.

Outbound is campaigns with open and click tracking, segments, templates, and suppressions. SMS goes out through Twilio, AWS End User Messaging, or Azure Communication Services. Inbound email and mailboxes mean the conversation can come back. Social and notifications sit on the same comms surface.

Email campaigns

Send to a segment. Track open and click. Templates you can reuse. Suppressions you must honour.

SMS

Twilio, AWS End User Messaging, or Azure ACS. Pick the pipe the organisation already has.

Segments & templates

Who receives what. Written once. Applied with intent.

Suppressions

The list of people you do not contact. A control, not an afterthought.

Inbound & mailboxes

Replies and operational mail land in the system, not only in someone's personal inbox.

Social & notifications

The other surfaces people already look at. Notify from the same events.

Documents that answer. A graph that connects them.

Knowledge in YumaOS is retrieval, structure, and a place to write. Document RAG over what you have filed. Semantica as the knowledge graph — how records connect, not only how they search. A documents studio, public-token forms, media, search, and a command palette.

The wiki on the work page is the operational writing. This page is the knowledge layer those pages sit on.

Document RAG

Ask the corpus. Answers come from documents you actually hold, with the access model still in force.

Semantica graph

A knowledge graph of how things connect — people, records, documents — not a tag cloud.

Documents studio

Where documents are made and kept. Studio, not a dump folder.

Public-token forms

Forms that can be filled without a full login, on a token you issued. Resource access still applies.

Media & search

Files you can find. Search across the operating system, not one module.

Command palette

Go to the record. Run the action. Keyboard-first for people who live in the system.

VAULT & SECRETS

Secrets in the vault. Keys out of the repo.

The vault is AWS KMS and private S3. There are no static AWS keys in the product posture we ship. Secrets are retrieved, used, and not left in environment files you copy between laptops.

This is not a compliance certificate. It is an architecture choice: encrypt under KMS, store in a private bucket, keep long-lived keys out of the tree.

AWS KMS

Keys managed in KMS. Encryption is a service, not a passphrase in a wiki.

Private S3

Objects in a private bucket. The vault is not a public URL with a long name.

No static AWS keys

The posture is: do not ship long-lived keys. Credentials are assumed, not pasted.

What this is not

Not a listed certification. Not a promise that every customer deploy uses the same account. The mechanism is KMS + private S3.



Vault path

Application → KMS unwrap → private S3 object → use → forget

NO STATIC KEYS IN THE TREE

INTEGRATIONS

MCP in and out. The tools you already run.

YumaOS is built to sit in a landscape, not replace it on day one. MCP inbound and outbound, webhooks, external APIs, competitor monitoring, Slack and Teams agents. The operating system talks to what you already paid for.

MCP in

Other agents and tools can call YumaOS through MCP. The action queue still applies to work that mutates the company.

MCP out

YumaOS agents can call out over MCP. The roster is not trapped inside one chat window.

Webhooks

Events out. The rest of the estate can react without polling a UI.

External APIs

First-class outbound integrations for the systems that will not move.

Competitor monitoring

A watch on the landscape you sell against. Signal in, not a spreadsheet someone forgets to open.

Slack & Teams

The Slack and Teams agents from the roster. Same queue. Same auto-approve rules. Same traces.

Ship it as theirs. Keep the operating system.

YumaOS is an industry app starter you white-label. The wordmark, the colour, the surfaces — configured as the customer's system. Modules and skills decide what is on. You are not asking them to log into Yuma every morning. They are logging into their company.

White-label is a product capability, not a slide. Branding, modules, and skills live on the same single deploy.

White-label branding

Their name. Their colour. Their login wallpaper if they want one. The chrome is configurable.

Modules

Switch capability on for the organisations that need it. Not every tenant is every feature on day one.

Skills

Packaged capability on top of the module set — the difference between a starter and a finished industry app.

Multi-tenant

One deploy, many companies. Branding and modules are per tenant, not a fork per customer.

What stays yours

The operating system, the agents, the access model, the vault. You are not reselling a skin on someone else's SaaS.

What they see

A company system with their mark on it. People, work, money, comms, knowledge.

Control, evidence, and an Australian option.

What we can say honestly: RBAC with overrides and resource access, MFA, Entra SSO, SCIM, an audit trail, a KMS-backed vault with no static AWS keys, and an Australian hosting option when Yuma IT runs the deploy. That is the posture.

What we will not say: invented certifications, invented uptime, invented residency guarantees on every install. If a customer hosts it, their hosting is their hosting. If Yuma IT hosts it in Australia, that is a delivery choice we can make.

Access

Roles, user overrides, document and form access. Administered in Settings
→ Access / Roles.

Identity

Better Auth, MFA, Entra SSO, SCIM.
The identity source can be theirs.

Vault

AWS KMS + private S3. No static AWS keys in the tree.

Audit

A log you can show. Access and action, not a screenshot of a dashboard.

Australian hosting option

When Yuma IT delivers the environment, data can stay in Australia. That is us, not a product flag on every Docker run.

What is not claimed

No ISO number on this page. No SOC letter. No invented seal. Ask for the controls; we will show the controls.

USE CASES

Example positioning. Not case studies.

These are example placements for the product — how we would sit YumaOS in a conversation. They are not case studies, not named customers, and not results. If a number appeared on a banner in a screenshot, it was mock UI.

Agency program office

One directory of people, one view of programs and risks, comms that can be audited, documents that can be retrieved. Access by role, override, and resource.

Research institute

Grants and tenders next to the knowledge graph. RAG over the corpus. Forms with public tokens for contributors who should not get a full account.

Indigenous organisation

A system that can wear their brand, run their modules, and be hosted with an Australian option. Yuma IT as the company in the room — Supply Nation Certified.

Mid-market Australian operator

CRM, delivery, quotes to invoices, email and SMS, agents on a queue. Replace the pile without pretending one tool is twelve products.

DIFFERENTIATORS

One system. One deploy. One permission story.

Most 'platforms' are a logo over a pile. YumaOS is the opposite bet: a single Next.js application that already contains the company — and agents that are not allowed to skip the queue.

Single-deploy CompanyOS

Not a suite. People, work, commercial, comms, knowledge, agents — one app, one database, one auth.

Agents with a mandatory queue

Mastra is in the product. The action queue cannot be turned off. Auto-approve is a rule you wrote, not a vibe.

Honest access

RBAC, overrides, resource-level document and form access. We will not dress that up as a paper access-control standard.

White-label industry starter

Built to be shipped as theirs. Modules and skills, not a CSS file and a handshake.

Vaulted secrets

KMS and private S3. No static AWS keys. Architecture, not a sticker.

Private on purpose

Not listed on yumait.com.au/projects. Sold in the room, deployed with intent.

Australian company, optional AU host

Yuma IT can host in Australia. That is a delivery fact, not a claim we stamp on every self-host.

Companions, not a rewrite

YumaOS-iOS is YumaOS to go. YumaOS-Android carries Hermes and Android Auto. Same operating system, smaller glass.

ADOPTION

Laptop. Homelab. Then production.

You do not adopt YumaOS with a twelve-month integration program. You run Docker locally. You put it on a homelab when the team is ready to live in it. You put Coolify and GHCR in front of it when it is a real environment.

Companions stay light: YumaOS-iOS is YumaOS to go. YumaOS-Android is Hermes plus Android Auto. They are private companions, not a second product story.

01

Docker, local

The first look is a container on a laptop. Same app. Same modules. No theatre.

02

Homelab

When a team needs to live in it — directory, work, a real tenant — the homelab is the honest middle.

03

Coolify + GHCR

Production is Coolify and the GitHub Container Registry. The same image, run as an environment.

COMPANIONS · LIGHT TOUCH

YumaOS-iOS

YumaOS to go.

YumaOS-Android

Hermes + Android Auto.

The stack is specific because the product is real.

We will not print an uptime percentage we did not measure. We will name the stack. Next.js 16, Better Auth, Drizzle, Postgres with pgvector, Mastra agents. E2E coverage exists because a company operating system that cannot be tested cannot be shipped. OpenAPI exists because integrations should not be folklore.

Next.js 16

The application. App router, one deploy, the UI and the server in one tree.

Better Auth

Sessions, MFA, Entra SSO, SCIM. Auth is a library, not a side project.

Drizzle

The schema is code. RBAC tables included. Migrations you can read.

Postgres / pgvector

The company record and the vectors for RAG, in one database you can back up.

Mastra

The agent runtime. Ops, risk, docs, quote, router, Slack, Teams.

OpenAPI

A contract for the HTTP surface. Integrations against a spec, not a guess.

E2E

End-to-end tests on the paths that matter. Credibility is green runs, not a slide.

Docker → Coolify

The same image, three rooms: laptop, homelab, production.

No invented availability figure. No invented test count. If you want the suite, we run it. If you want the spec, we open OpenAPI.

NEXT STEP

// Say Yuma.

Say Yuma to simplified company management, driven by agentic workflows, everywhere you work.
Intelligent agents. Connected systems. Real work. Real results.

YUMA IT PTY. LTD.

A private product. A real next step.

YumaOS is not listed on yumait.com.au/projects. If this brief is in your hands, you are in the conversation.

Write to us. Tell us the organisation, the hosting preference, and whether this is a laptop look or a production intent.

EMAIL

hello@yumait.com.au

WEB

<https://www.yumait.com.au>

ADDRESS

49 Phillip Ave, Watson ACT 2602

CERTIFIED

Supply Nation Certified