BUILDWITHHQ PRODUCT WALKTHROUGH

CrewOS

AI Agent Workforce

A coordinated workforce of specialized AI operators — each with its own role, context, tools, authority, and approval rules.

CREWOS - WALKTHROUGH SCENARIO

Prepare the Monday operating briefing, identify exceptions, draft follow-ups, and pause anything customer-facing until approval.

View evidence | Start workflow

1	6	5	4
GOVERNED PRODUCT MODEL	CORE CAPABILITIES	WALKTHROUGH STAGES	SEPARATED DATA / CODE PLANES

EXECUTIVE SUMMARY

What CrewOS is

CrewOS packages reusable BuildWithHQ primitives into a focused ai agent workforce product experience.

01
Product layer
A branded application experience shaped around a specific operating job.

02
Governed intelligence
AI can analyze, retrieve, recommend, and prepare actions inside the same permission envelope as the application.

03
Operational actions
Workflows, approvals, APIs, webhooks, MCP tools, and custom services move from insight to controlled execution.

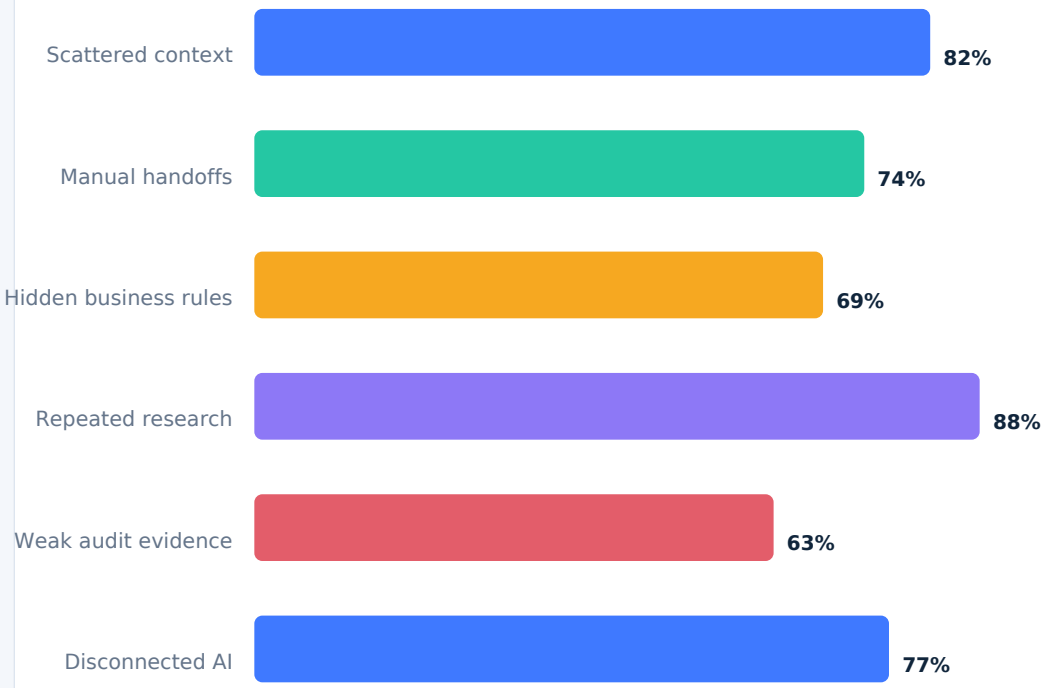
04
Platform leverage
Dedicated data planes, audit evidence, exports, and optional container services stay reusable under the product.

WHY THIS EXISTS

The operational problem

CrewOS is designed for work that becomes expensive when context, decisions, and actions are fragmented across tools and people.

Illustrative sources of operating friction



What changes

Instead of treating AI, records, workflows, permissions, and integrations as separate projects, the product keeps them inside one governed operating model.

Design goal

Reduce the distance between context, decision, and controlled action without flattening the business rules that make the workflow safe.

NOT JUST A FEATURE

A complete operating product

Run your business with an AI team , not a chatbot.

WHO IT SERVES

- Executive gets a purpose-built view, authority level, and workflow.
- Operations lead gets a purpose-built view, authority level, and workflow.
- Agent supervisor gets a purpo… authority level, and workflow.
- Department owner gets a pur… authority level, and workflow.
- Compliance reviewer gets a purpose-built view, authority level, and workflow.

WHAT MAKES IT DIFFERENT

- AI is attached to governed records and evidence.
- Actions are explicit contracts, not hidden autonomous behavior.
- Permissions remain server-side …creens, APIs, AI and exports.
- …code is optional - not the only …atch.

CORE CAPABILITIES

The six building blocks of CrewOS

A coordinated workforce of specialized AI operators — each with its own role, context, tools, authority, and approval rules.

01
Agent roles
Create specialized operators for research, sales, analytics, support, finance, or your own domain.

02
Shared operating records
Use normal BuildWithHQ records, relations, workflows, and knowledge as the team’s governed context.

03
Action contracts
Map agent recommendations to workflows, APIs, webhooks, and custom service endpoints.

04
Human approval
Stop financial, customer-facing, or high-risk actions until an authorized user approves them.

05
Agent memory
Store vectorized context and prior operating knowledge separately from runtime application records.

06
Execution evidence
Write retrievals, approvals, denials, and actions to the compliance trail for later review.

ARCHITECTURE

Separated by responsibility. One product to the user.

BuildWithHQ keeps runtime records, AI context, compliance evidence, and custom execution separate while the application presents one coherent experience.

1 **Runtime Database**

Users · product records · workflows · configuration

2 **AI / Vector Database**

Embeddings · knowledge · retrieval · AI configuration

3 **Compliance Database**

Reads · approvals · refusals · evidence · replay trail

4 **Isolated Code Container**

Custom APIs · SDKs · private logic · background services

Unified permissions, actions, APIs, exports, and audit boundaries across the product

DATA MODEL

Everything important becomes connected context

The product data model is not a set of isolated modules. Records can relate recursively so users and AI can traverse the real operating context.

Why relationships matter

A recommendation or workflow can bring in the right customer, document, task, history, approval, or related object without forcing the user to manually reconstruct context.

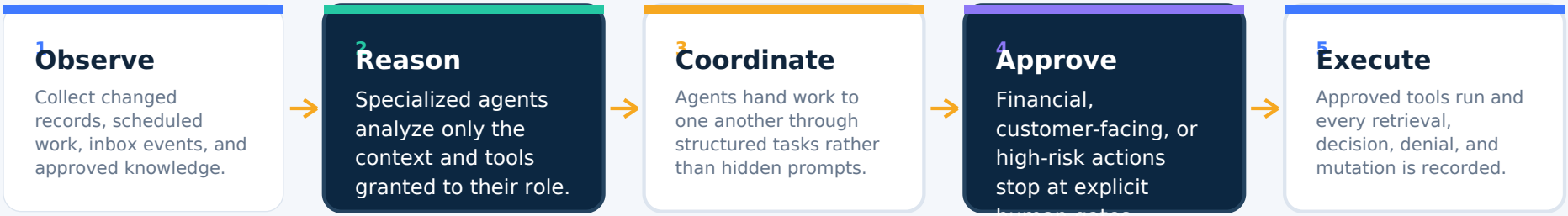
Security stays attached

Relationships expand context only when the current identity is allowed to traverse the connected record and field. More context does not mean broader access.

WALKTHROUGH

From input to governed outcome

Prepare the Monday operating briefing, identify exceptions, draft follow-ups, and pause anything customer-facing until approval.



The five stages are illustrative - each BuildWithHQ implementation can add branches, approvals, retries, SLAs, external systems, and custom services.

WALKTHROUGH 1/5

1. Observe

Collect changed records, scheduled work, inbox events, and approved knowledge.

INPUT

What enters this stage

Identity, permitted records, related context, workflow state, and any source-specific inputs required for observe.

EVIDENCE

Evidence produced

Store the records consulted, source versions, relevant model output, workflow transition, approvals/denials, and mutation result so the operation can be explained later.

ENGINE

What BuildWithHQ does

Collect changed records, scheduled work, inbox events, and approved knowledge. The runtime enforces tenant, role, record, field, rate-limit, and action boundaries before the stage can progress.

EXPERIENCE

What the user sees

A focused CrewOS screen should expose the result, why it happened, what remains unresolved, and the next safe action - without forcing the user to inspect raw infrastructure.

WALKTHROUGH 2/5

2. Reason

Specialized agents analyze only the context and tools granted to their role.

INPUT

What enters this stage

Identity, permitted records, related context, workflow state, and any source-specific inputs required for reason.

EVIDENCE

Evidence produced

Store the records consulted, source versions, relevant model output, workflow transition, approvals/denials, and mutation result so the operation can be explained later.

ENGINE

What BuildWithHQ does

Specialized agents analyze only the context and tools granted to their role. The runtime enforces tenant, role, record, field, rate-limit, and action boundaries before the stage can progress.

EXPERIENCE

What the user sees

A focused CrewOS screen should expose the result, why it happened, what remains unresolved, and the next safe action - without forcing the user to inspect raw infrastructure.

WALKTHROUGH 3/5

3. Coordinate

Agents hand work to one another through structured tasks rather than hidden prompts.

INPUT

What enters this stage

Identity, permitted records, related context, workflow state, and any source-specific inputs required for coordinate.

EVIDENCE

Evidence produced

Store the records consulted, source versions, relevant model output, workflow transition, approvals/denials, and mutation result so the operation can be explained later.

ENGINE

What BuildWithHQ does

Agents hand work to one another through structured tasks rather than hidden prompts. The runtime enforces tenant, role, record, field, rate-limit, and action boundaries before the stage can progress.

EXPERIENCE

What the user sees

A focused CrewOS screen should expose the result, why it happened, what remains unresolved, and the next safe action - without forcing the user to inspect raw infrastructure.

WALKTHROUGH 4/5

4. Approve

Financial, customer-facing, or high-risk actions stop at explicit human gates.

INPUT

What enters this stage

Identity, permitted records, related context, workflow state, and any source-specific inputs required for approve.

EVIDENCE

Evidence produced

Store the records consulted, source versions, relevant model output, workflow transition, approvals/denials, and mutation result so the operation can be explained later.

ENGINE

What BuildWithHQ does

Financial, customer-facing, or high-risk actions stop at explicit human gates. The runtime enforces tenant, role, record, field, rate-limit, and action boundaries before the stage can progress.

EXPERIENCE

What the user sees

A focused CrewOS screen should expose the result, why it happened, what remains unresolved, and the next safe action - without forcing the user to inspect raw infrastructure.

WALKTHROUGH 5/5

5. Execute

Approved tools run and every retrieval, decision, denial, and mutation is recorded.

INPUT

What enters this stage

Identity, permitted records, related context, workflow state, and any source-specific inputs required for execute.

EVIDENCE

Evidence produced

Store the records consulted, source versions, relevant model output, workflow transition, approvals/denials, and mutation result so the operation can be explained later.

ENGINE

What BuildWithHQ does

Approved tools run and every retrieval, decision, denial, and mutation is recorded. The runtime enforces tenant, role, record, field, rate-limit, and action boundaries before the stage can progress.

EXPERIENCE

What the user sees

A focused CrewOS screen should expose the result, why it happened, what remains unresolved, and the next safe action - without forcing the user to inspect raw infrastructure.

GOVERNANCE

Permissions follow the user into AI, APIs and actions

One authorization model should determine what each role can read, retrieve, export, approve, or mutate.

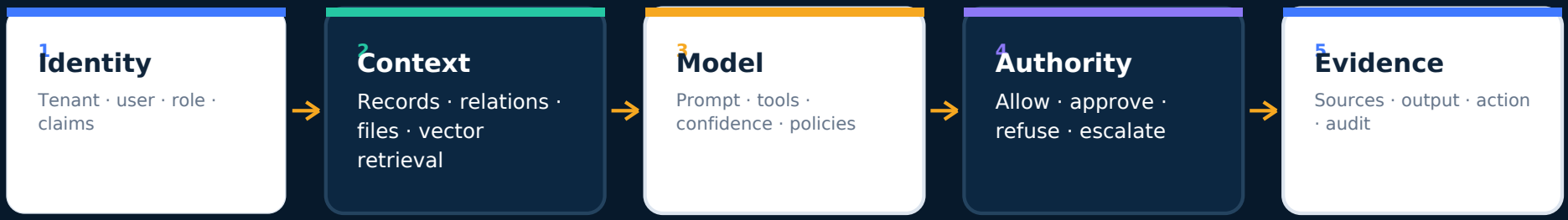
Illustrative authority matrix - 1 restricted to 5 broad

	Read	AI context	Recommend	Approve	Execute
Executive	5	4	2	5	1
Operations lead	5	4	4	5	4
Agent supervisor	5	4	4	2	4
Department owner	5	4	4	2	1
Compliance reviewer	5	3	2	5	1

AI OPERATING MODEL

AI is a participant in the workflow - not a bypass arou

The AI layer can retrieve, synthesize, rank, draft, and recommend. Server-side policies still decide what data and actions are actually available.

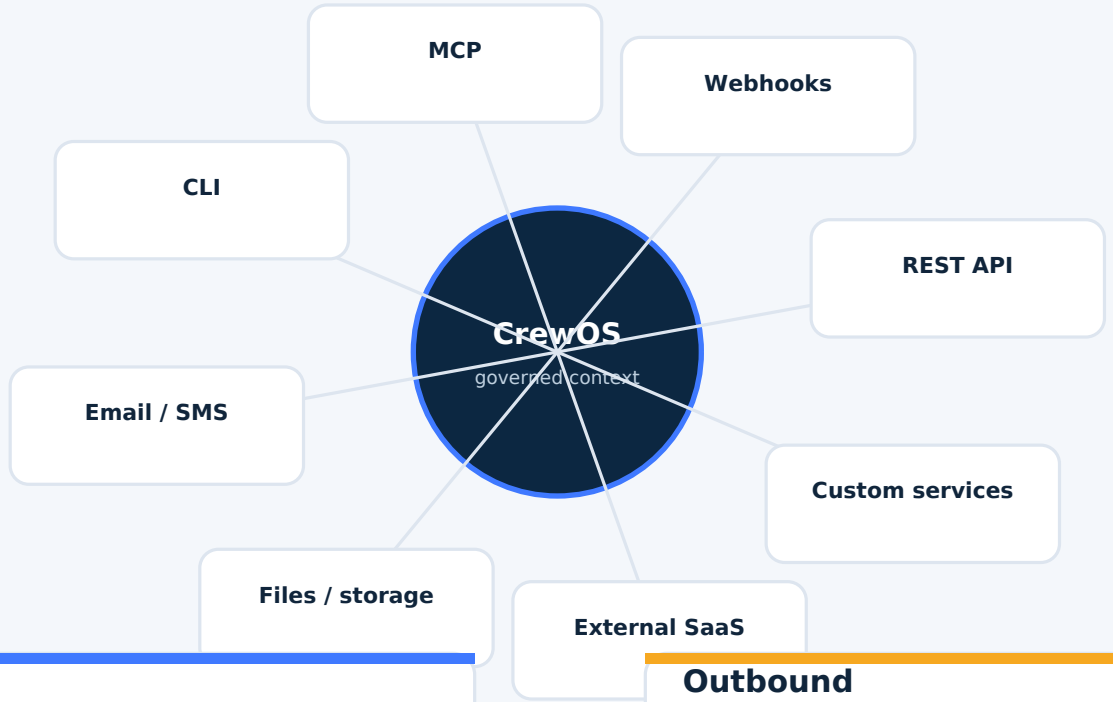


This pattern lets the same intelligence layer support employees, end customers, scheduled agents, MCP clients, and API-driven experiences.

INTEGRATION SURFACE

Connect to the systems already around the business

API, webhooks, MCP, CLI, file import/export, and optional private services let the product fit into an existing stack instead of becoming another isolated island.



Inbound

Events, imports, messages, usage data, customer records, documents, signals, or other domain-specific inputs.

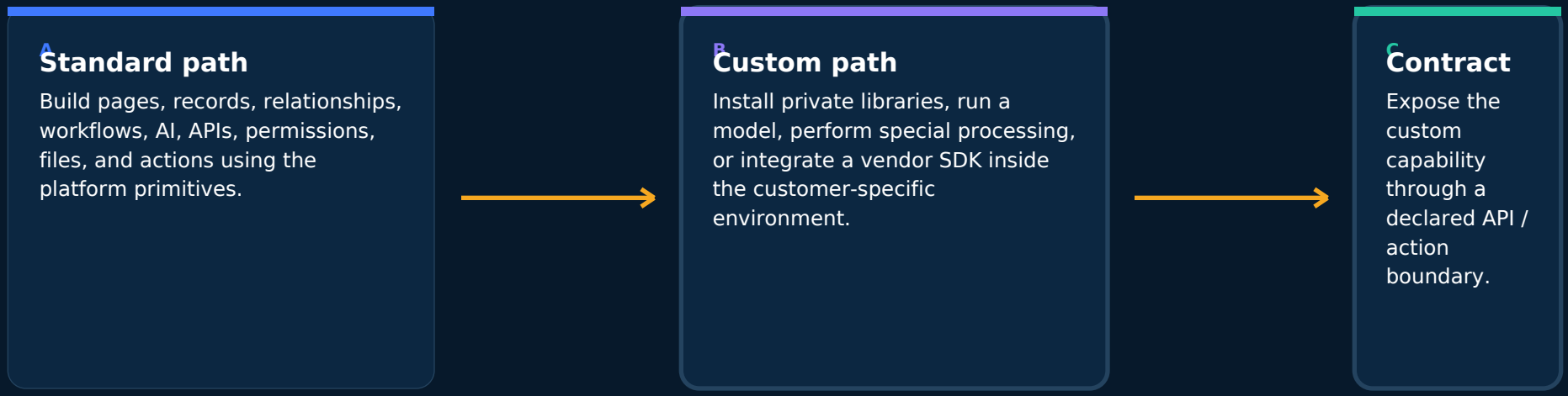
Outbound

Actions, notifications, record updates, webhooks, exports, generated files, MCP tools, or custom API calls.

ESCAPE HATCH

Optional isolated container when the product needs

Most of the application can remain schema-, workflow-, and API-driven. When a developer needs a special SDK, proprietary algorithm, or long-running service, the isolated container provides a controlled extension point.

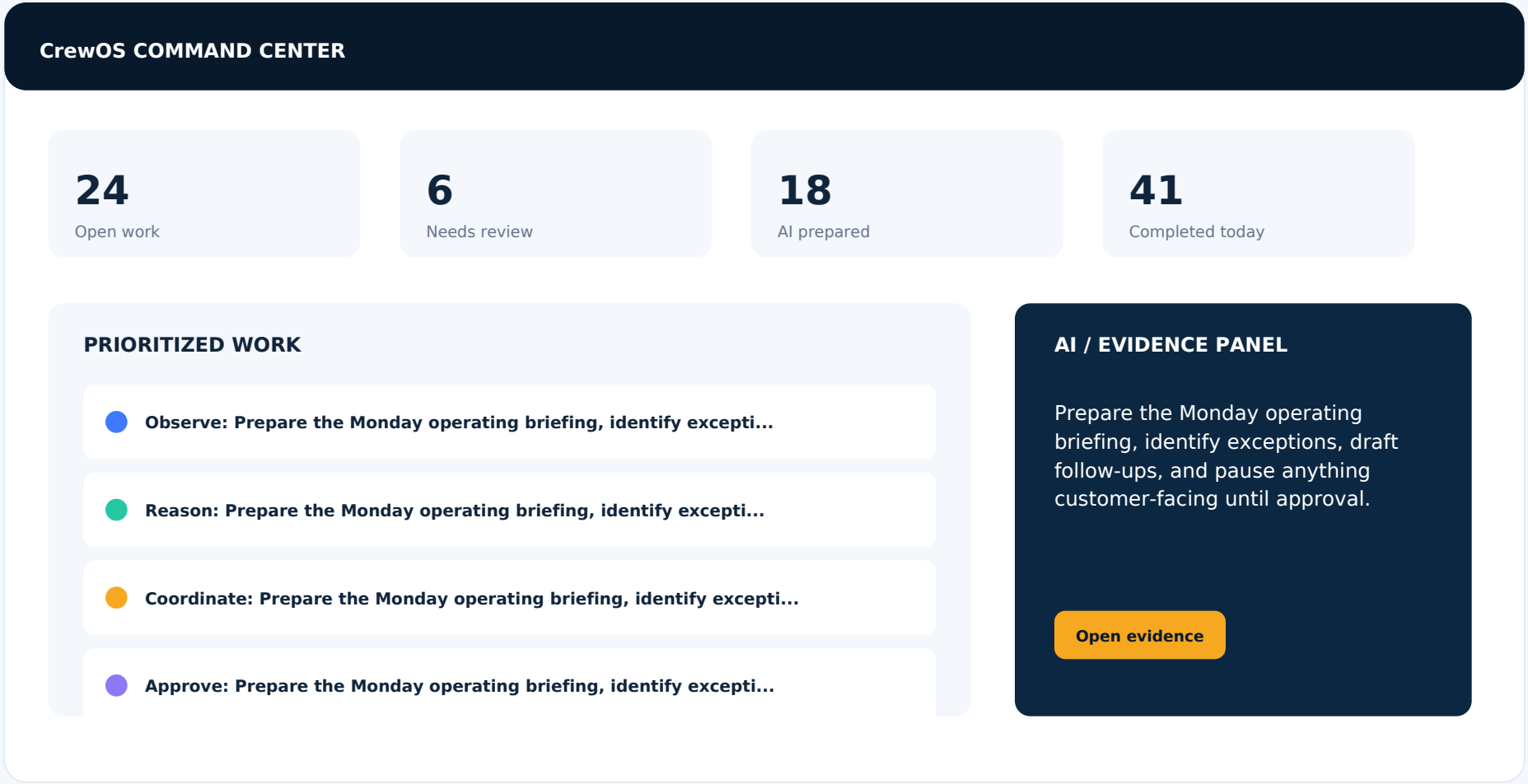


The central execution layer can call the declared service while the custom code remains isolated from the core platform and from other customers.

PRODUCT EXPERIENCE

What a CrewOS operating screen can look like

The point of the blueprint is to turn deep infrastructure into a focused daily workflow.



OPERATING FLYWHEEL

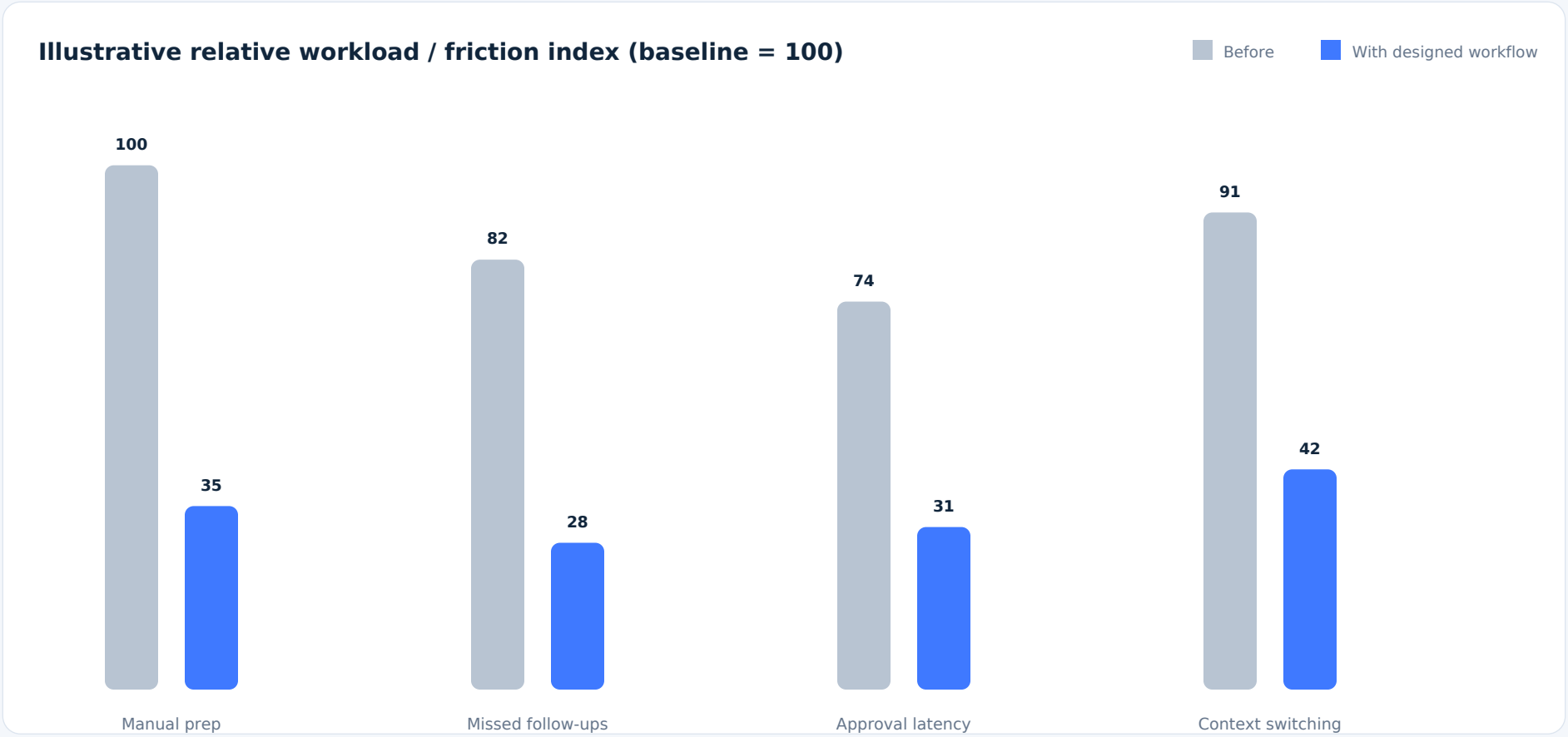
Every completed cycle can improve the next one

The product gets stronger when outcomes, approvals, exceptions, source quality, user corrections, and workflow performance are fed back into the operating model.

ILLUSTRATIVE IMPACT

Where operating leverage can show up

The numbers below are not measured BuildWithHQ customer results. They are an illustrative model showing the kinds of friction the product is designed to reduce.

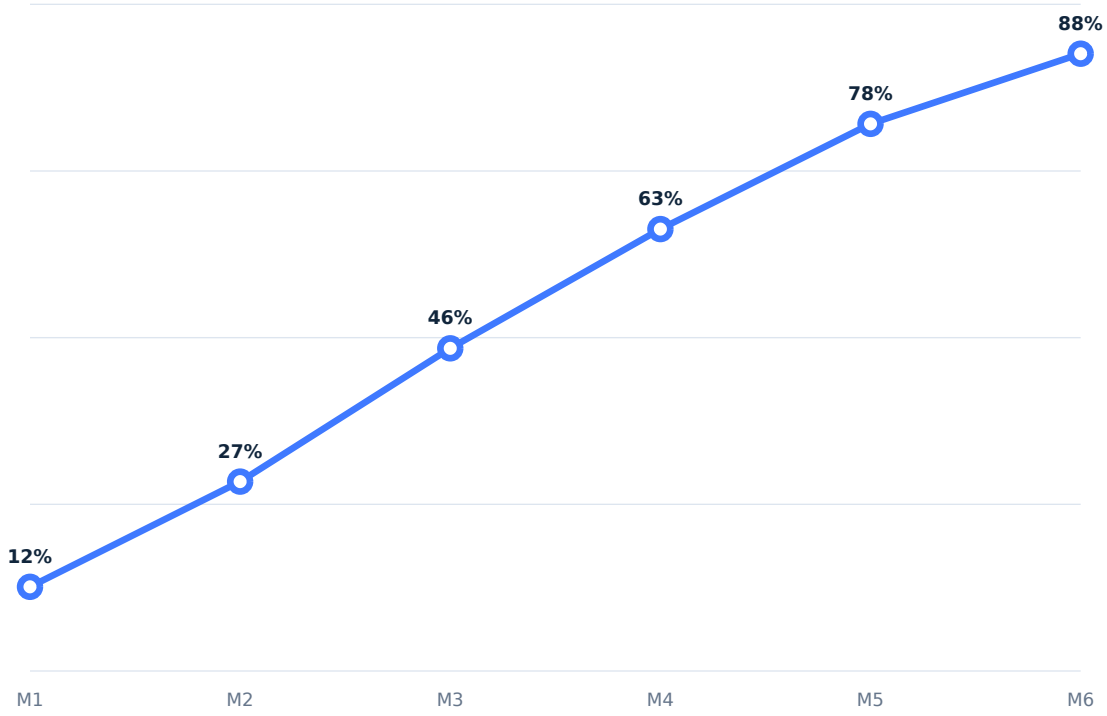


ILLUSTRATIVE ROLLOUT

Value compounds as more work enters the governed

A staged deployment lets the team prove retrieval, routing, approvals, and actions before widening automation authority.

Illustrative percent of target workflow running through the product



Phase 1 - Assist

Read-only context, search, summaries, classification, and drafts. Human users make every consequential decision.

Phase 2 - Governed action

Add explicit tools, approval thresholds, scheduled runs, and carefully bounded auto-actions where the evidence is strong.

PRODUCT DIRECTIONS

Six ways to package CrewOS

One BuildWithHQ blueprint can be narrowed to a vertical, customer segment, operating team, or recurring workflow and then branded as its own SaaS product.

01
Executive operating brief
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

02
AI sales development team
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

03
Support triage workforce
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

04
Finance close assistant
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

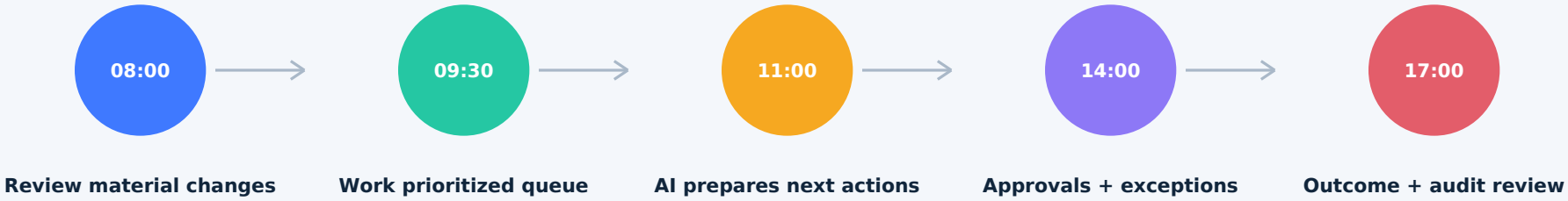
05
Compliance evidence assembly
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

06
Portfolio monitoring
Use the same core CrewOS architecture, then customize terminology, records, permissions, integrations, AI behavior, and workflows for this market.

DAILY OPERATION

A role-aware experience from morning to close

Different users can work on the same underlying records while seeing different queues, context, evidence, and action rights.



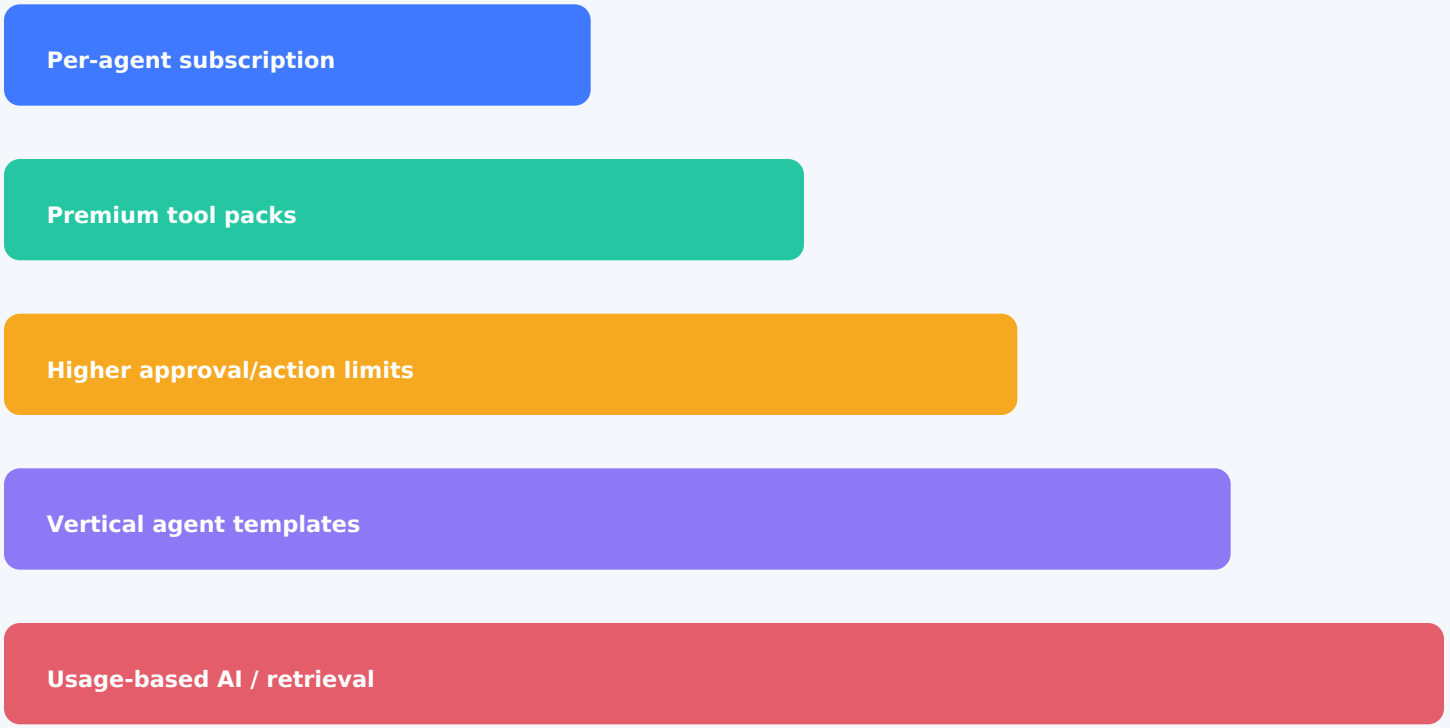
The important part

The application is not forcing every role into the same dashboard. The runtime can expose the same record with different fields, related context, actions, AI tools, and approval rights based on who is looking at it.

COMMERCIAL MODEL

Ways a builder could monetize the product

These are product packaging ideas, not fixed BuildWithHQ pricing. A builder can mix software subscriptions, usage, premium modules, infrastructure, and services.



Illustrative packaging ladder: start simple, then monetize the capabilities that scale with customer value or infrastructure consumption.

IMPLEMENTATION ROADMAP

A practical 90-day build sequence

The exact timeline depends on scope, but the safest pattern is to establish data + identity first, then intelligence, then actions, then expansion.

0-30

Foundation

Data model, identity, permissions, core screens, imports.

31-45

Context

Relationships, files, search, vector retrieval, evidence.

46-60

Workflow

Queues, SLAs, rules, approvals, notifications.

61-75

AI + MCP

Assistance, agents, MCP tools, bounded action contracts.

76-90

Production

Observability, exports, load tests, runbooks, launch controls.

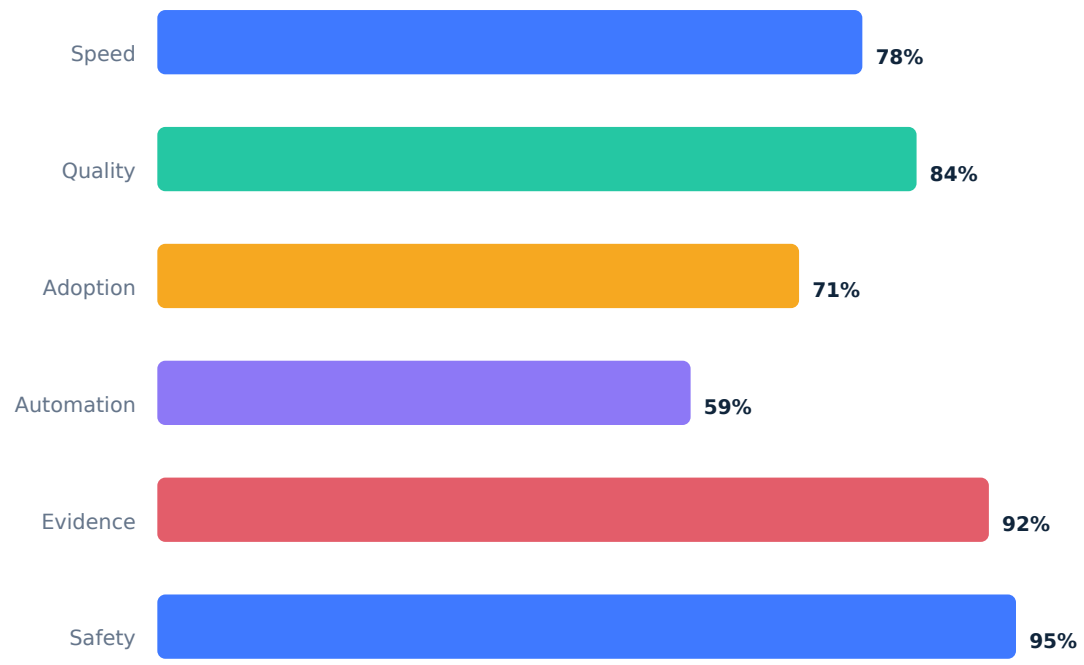
Launch authority should expand only after the evidence trail, failure handling, permission checks, and rollback path are tested.

MEASUREMENT

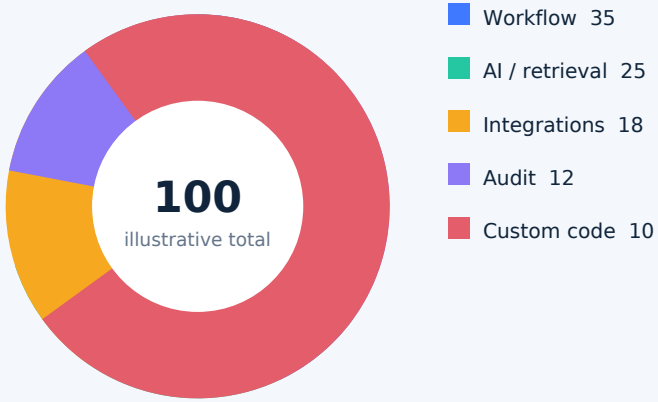
What to measure after launch

The product should be evaluated on operating outcomes, not just model usage. Track speed, quality, safety, adoption, and economic leverage together.

Illustrative maturity scorecard



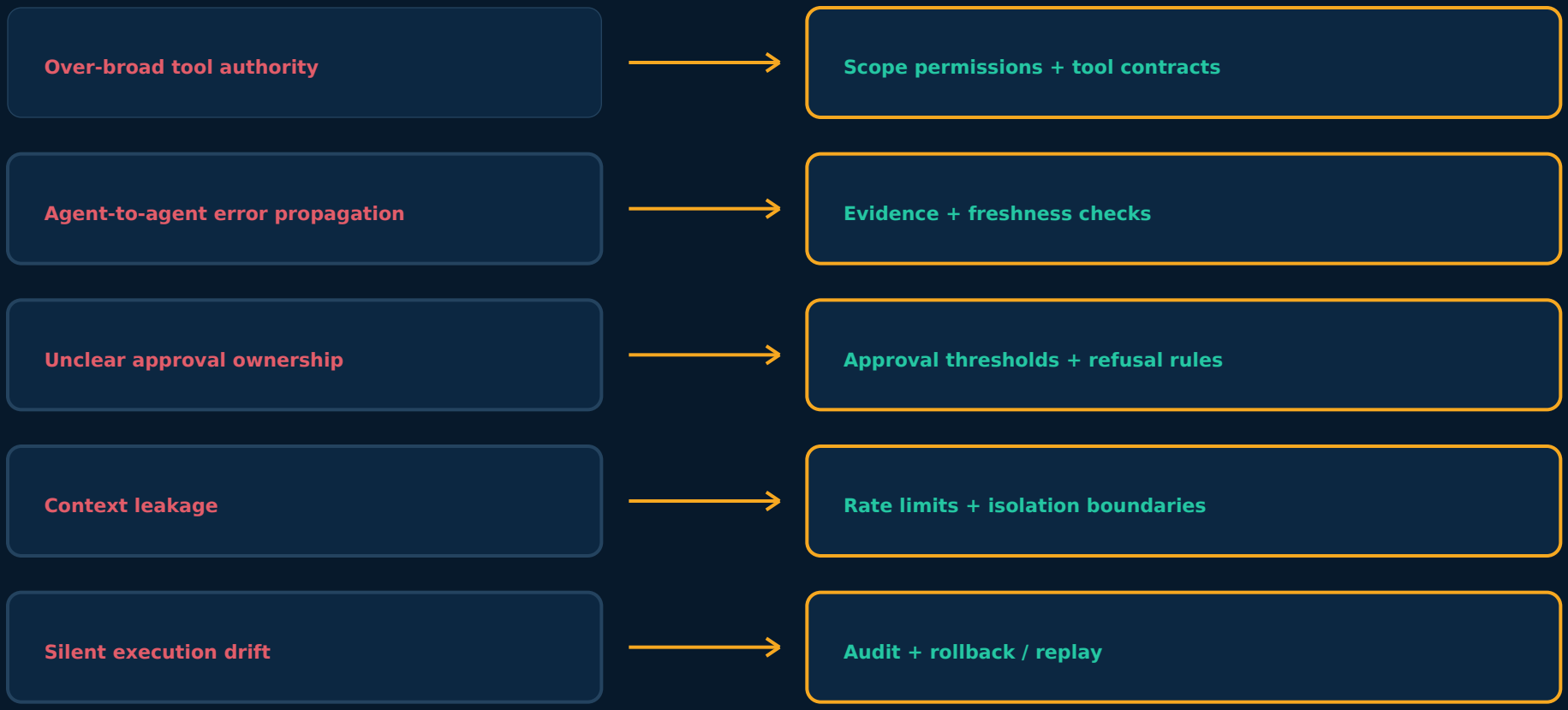
Illustrative implementation effort mix



RISK + CONTROL DESIGN

Make the dangerous path harder than the safe path

The goal is not to promise that AI or automation cannot fail. The goal is to constrain what failure can affect, surface evidence, and preserve a deterministic way to stop or reverse the operation.



DEVELOPER SURFACES

One backend, multiple ways to use it

The same product can support a visual SaaS interface, an external frontend, internal automation, developer tooling, and agent access without creating five disconnected permission models.

1
UI
Built-in product pages

2
REST
External apps + integrations

3
MCP
AI clients + agent tools

4
CLI
Developers + operations

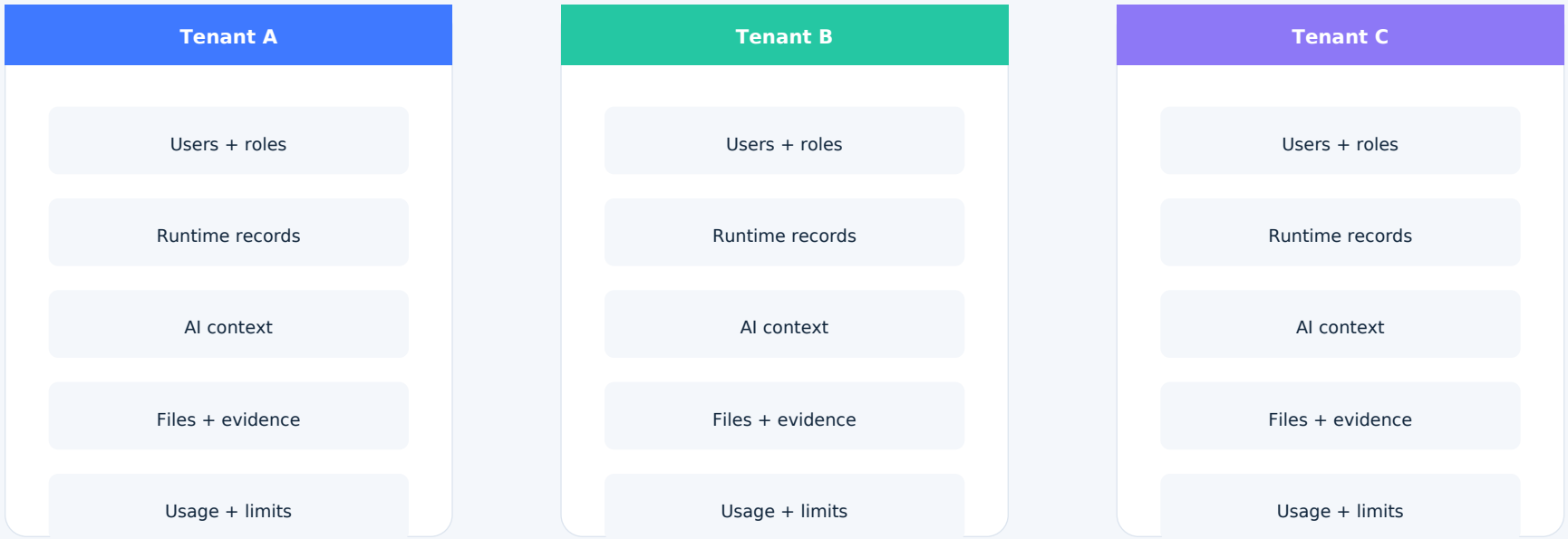
5
Webhooks
Event-driven systems

6
Export
Portability + reporting

SAAS OPERATIONS

Productize once. Isolate customers by design.

BuildWithHQ is intended to let a builder define the product experience while tenant, user, permission, data, AI, and optional service boundaries keep each customer context separated.



Shared platform primitives - isolated customer context - configurable product experience

BUILD THIS

Start with CrewOS. Make it yours.

CrewOS is a product direction, not a fixed template. Use the blueprint as a starting architecture, then shape the records, screens, AI behavior, integrations, permissions, workflows, container services, and commercial model around your market.

01

1. Define the job

Choose the recurring operating problem and the user roles that feel it most.

02

2. Map the system

Define records, relationships, evidence, permissions, workflows, and required integrations.

03

3. Add intelligence

Layer AI and agents into the governed operating loop instead of around it.

ldWithHQ turns reusable platform primitives into products you can brand, extend, and s

buildwithhq.com / Build This