ORIENTATION

The AI Revolution *Starts Here*

A beginner-friendly guide with real-world analogies.

No tech background needed — just curiosity.

Based on the Agent Factory Thesis
agentfactory.panaversity.org

What We'll Cover Today

01 What is AI, Really?

02 What is Agentic AI?

03 The Agent Is the Operating Layer

04 The 10-80-10 Rhythm

05 From 'Smart Tool' to 'Smart Worker'

06 The Agent Factory Idea

07 Your Personal AI Delegate

08 The 7 Principles of General Agent Problem Solving

09 The 7 Golden Rules of an AI-Native Company (Invariants)

10 A Real Example: Ecomm Mart

PART 01

What is AI, Really?

ANALOGY

The Smart Kitchen Appliance

A normal microwave follows fixed rules.
A smart one can look, recognize, and decide what to do.

1. **Input food**
   You place food inside

2. **Reads what it sees**
   Figures out what the food is

3. **Chooses the best settings**
   Picks time & temperature automatically

Working with AI is the same

Information in
AI looks at the input

→

Pattern recognition
It figures out what it is

→

Decision
It chooses what to do

AI doesn't follow every step from you. It figures things out from the information it sees.

Breaking Down "Artificial Intelligence"

Artificial

Made by humans, not by nature.

A plastic flower is artificial.

AI is intelligence built from software.

Intelligence

The ability to learn, understand,

and make decisions.

Humans have natural intelligence.

AI has a version built from data.

Everyday Examples You Already Use

Voice Assistant

Alexa, Siri

YouTube Recs

Spots patterns in what you like

Auto-correct

Predicts the word you meant

ChatGPT / Claude

Writes answers from questions

KEY TAKEAWAY

AI is software that can learn from data and make decisions on its own — without a human giving it step-by-step instructions every time.

It's not magic. It's math, data, and clever programming.

And it's already everywhere in your daily life.

PART 02

What is Agentic AI?

Normal AI vs Agentic AI

Both are smart — but only one does the job for you.

Normal AI

You ask: "How do I make a sandwich?"

It tells you the steps to follow...
but YOU do all the work!

You get the bread, add the filling, and build the whole sandwich yourself.

VS

Agentic AI

You say: "Please make me a sandwich."

It makes a plan and does each step...
the whole job, all by itself!

It goes to the kitchen, gets the bread, makes the sandwich, and brings it to you.

Game: "Get Ready for the Playground!"

It's a holiday — the class is free to go play outside!

The Goal You Give

"Get everyone ready to go play in the playground."
That's it — just the goal, nothing more. Don't tell them the steps; the kids figure it out on their own!

What the Kids Might Do (their own plan!)

Wear shoes

Put on sports shoes and caps for the sun.

Grab the ball

Pick a ball, skipping rope, or favorite game.

Line up

Make a line and walk out together safely.

"You just acted like an AGENT! Nobody told you each step — you had a goal and made your own plan. That is exactly what agentic AI does!"

What is "Agentic AI"?

Normal AI

You ask: "How do I make a sandwich?"

It tells you the steps to follow...
but YOU do all the work yourself.

Agentic AI

You say: "Please make me a sandwich."

It makes a plan and does each step...
the whole job, all by itself!

An Agent Does 3 Things

1. THINK

Makes a plan to reach the goal.

"First I need bread, then filling."

2. ACT

Actually does the steps.

Goes and builds the sandwich.

3. CHECK

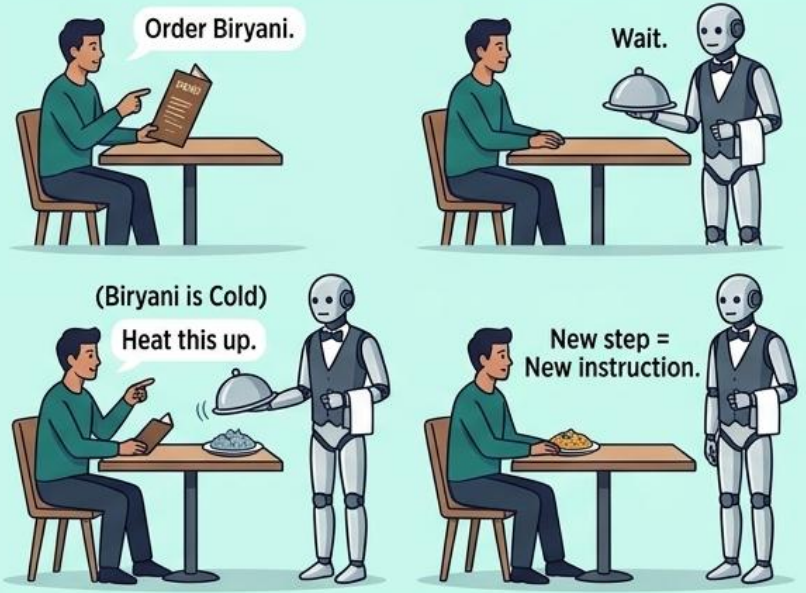
Sees if it worked.

Tries again if something is wrong.

AI EXPLAINED:

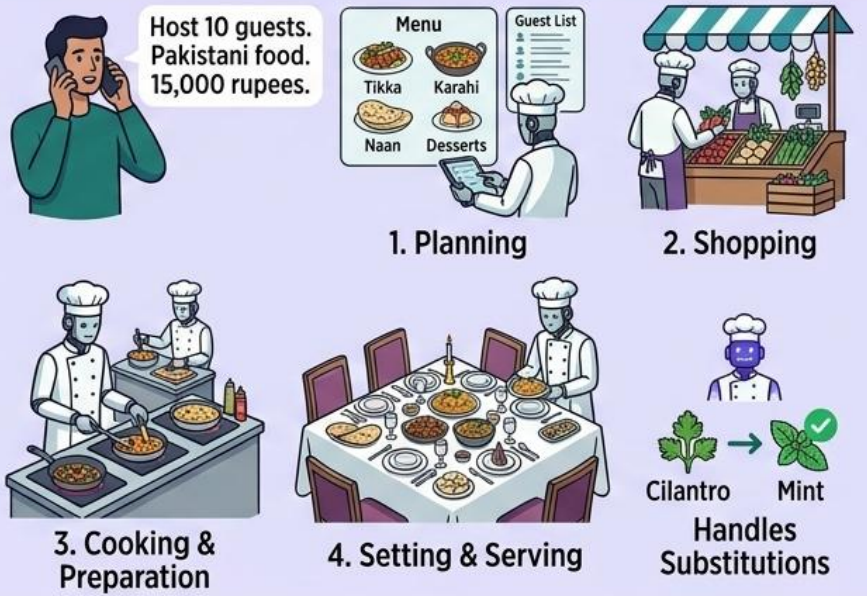
THE RESTAURANT ANALOGY

REGULAR AI: THE WAITER (REACTIVE)



- Explicit Orders Only
- New Step, New Command
- No Proactivity

AGENTIC AI: THE PERSONAL CHEF (PROACTIVE)



- Goal-Oriented
- Self-Directing
- End-to-End Execution
- No Hand-Holding

Three Levels of AI

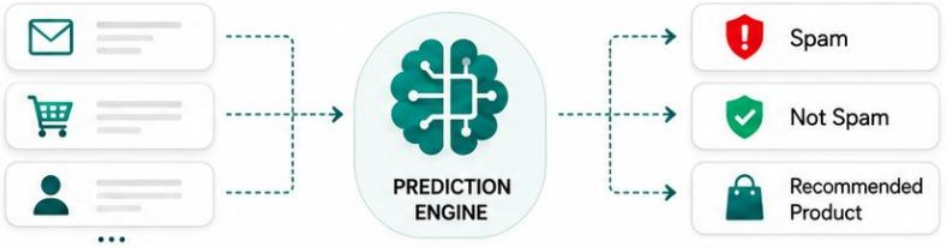
LEVEL 1

Level 1 — Predictive AI

(The Smart Filter)

You give it data. It gives one prediction.

Spam or not spam? What product to recommend? No conversation, no memory.



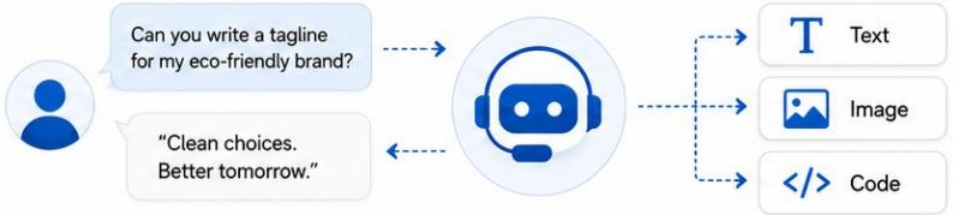
LEVEL 2

Level 2 — Generative AI

(The Chat Partner)

You have a conversation. It remembers context.

Creates text, images, and code. Still waits for your next instruction.



LEVEL 3

Level 3 — Agentic AI

(The Worker)

You give it a goal. It does the work.

It plans, uses tools, fixes mistakes, and finishes the job — without you guiding every step.

Level 1 predicts.

Level 2 creates and chats.

Level 3 plans and delivers.

What Makes AI "Agentic"?

Four abilities that turn a chatbot into a worker:

Planning

Breaks a big goal into smaller steps and decides the order

Tool Use

Browses the web, writes code, reads files, sends messages

Self-Correction

Notices mistakes and tries a different approach on its own

Goal Completion

Works until the job is done, not just one answer

Bakery Email Marketing: Two Paths

Regular AI: The Single-Task Tool

"Write a marketing email for my bakery."

Writes ONE generic email. *Then it is done.*

Your manual tasks:

1. Send the email manually
2. Track opens and clicks
3. Follow up with interested customers

Agentic AI: Your Intelligent Partner

"Run my email marketing this month."

Manages the *entire* campaign.

1. Segments customers
2. Writes targeted personalized emails
3. Schedules automatic sending
4. Tracks performance and improves the next batch

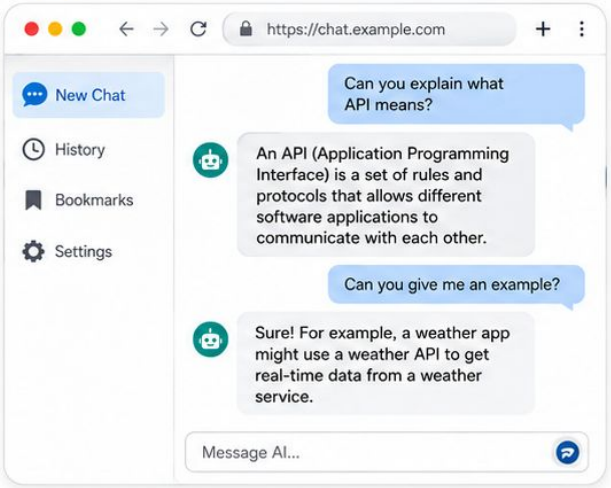
Regular AI helps with one task. **Agentic AI** handles the full goal.

Tool = one step | Agent = end-to-end work

From Browser Chat to General Agents

How most readers first meet AI — and what comes next

1. Browser Chat

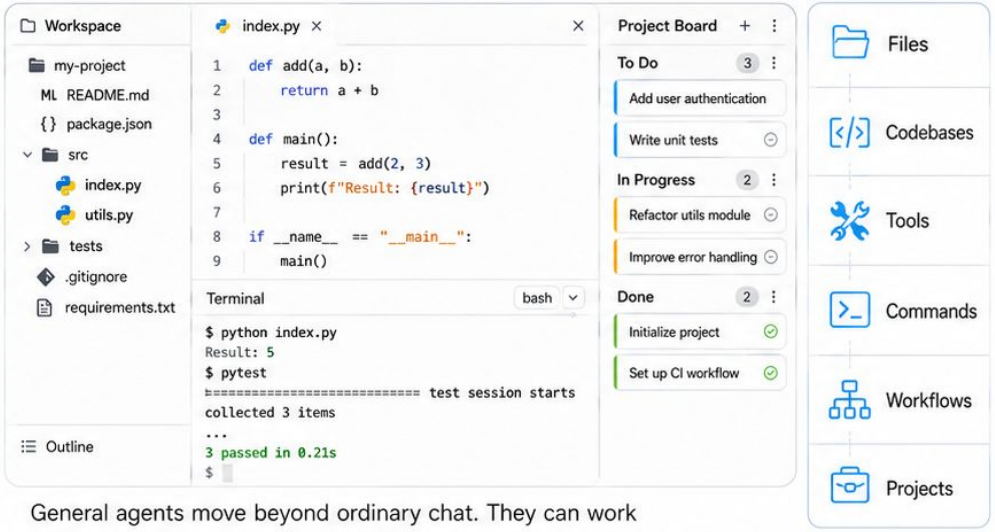


Most readers first meet AI through a browser-based LLM. They log into ChatGPT, Claude, Gemini, or another model and start typing in a chat window.

ChatGPT | Claude | Gemini | Other LLMs

Move Beyond Chat

2. General Agents



General agents move beyond ordinary chat. They can work inside an environment: files, codebases, tools, commands, workflows, and projects.

Claude Code | OpenCode | Claude Cowork | OpenWork

Chat: conversation in a browser

Ask questions. Get answers. Stay in the chat.

VS

General agents: work inside an environment

Take actions. Use tools. Complete real work.

PART 03

The New AI Era

The Agent Is the *Operating Layer*

The new era of computing: from app-centric PCs to agent-native PCs.

Why the agentic era ends the app, SaaS, and the PC as we know it.

PART 03-A

Two Deaths, Not One

JUNE 1, 2026

“For forty years, you launched apps. Click. Type. With RTX Spark and Microsoft Windows, you ask — and the PC does the work.”

— Jensen Huang, NVIDIA · GTC Taipei

NVIDIA and Microsoft unveiled a petaflop-class chip to run agents locally on Windows.

Two Deaths, Not One

The agentic era takes two casualties — one smaller, one larger.

1. SaaS dies

The agent replaces the app. The login, the navigation, the seat-based UI — unbundled into capabilities an agent calls and never names to you.

The smaller event: the app dissolves into a function call.

2. The PC dies — as we know it

The agent replaces you at the controls. The app-on-OS model, driven by hand through a graphical shell, becomes obsolete.

The larger event: you stop operating the machine.

Not the silicon — the operating model. It begins with digital, bounded, recoverable work.

The SaaSpocalypse, Unbundled

A SaaS app is three things welded together. The agent pulls them apart.

Workflow UI

Dies first. It existed only so a human could operate the capabilities. An agent operating them directly bypasses the screens entirely.

Capabilities

Survive — demoted from product to function call. A tool the agent reaches for via API or MCP, then sets down.

System of record

The prize. The authoritative data an agent must read to act becomes the most strategic layer in the stack.

SaaS gets unbundled — and the bundle was the business.

Old model:

humans use apps directly

AI-native model:

humans delegate work
through general agents

PART 03-B

The AI Operating Layer

The AI Operating Layer

Not the operating system itself — the layer that connects human intent to real work.

WORK ENVIRONMENT

Where the work actually lives — the agents reach up into it.

Files • **Codebases** • **Documents** • **Apps** • **Tools** • **Commands** • **Workflows** • **Projects**

AI OPERATING LAYER

← humans interact here

GENERAL AGENTS — operators that do the work

FOR DEVELOPERS
Claude Code • **OpenCode**

FOR KNOWLEDGE WORK
Claude Cowork • **OpenWork**

PERSONAL AGENTS — companions that know you, always on

OpenClaw • **Hermes**

proactive • persistent memory of you • works across all your apps & files

HUMAN INTERFACE LAYER LEGACY

The screens a human used to drive by hand — now demoted to a surface.

IDE • **Terminal** • **Browser** • **Docs** • **Email** • **Spreadsheets**

TRADITIONAL OPERATING SYSTEM PLUMBING

Windows • **macOS** • **Linux**

Manages files, memory, processes, devices, and security — the human never touches it again.

Human intent

AI operating layer

Action inside an environment

The reversal: the OS sinks to the basement; the AI Operating Layer becomes the floor the human stands on.

You build and manage your personal agents using general agents — and your personal agent, in turn, dispatches general agents to do the work.

The Reversal

The forty-year stack flips: the OS sinks, the agent layer rises.

The OS becomes plumbing

Windows, macOS, and Linux survive as invisible infrastructure — like TCP/IP or the BIOS. The human never touches them again.

The shell dies as the interface

The desktop, the dock, the app grid, the window-shuffling — demoted to legacy surfaces behind the agent layer.

The agent layer becomes the floor

You state the goal. The agent reaches down through the old interface and operates the machine on your behalf.

PART 03-C

General vs Personal Agents

Two Kinds of Agents

Both live in the operating layer. One is oriented toward the work, the other toward you.

	General agents	Personal agents
Oriented toward	the task / the work	the person — you
Examples	Claude Code, OpenCode; Claude Cowork, OpenWork	OpenClaw, Hermes
Lifespan	summoned per job; sessional	always-on; persistent
Memory	task-scoped context	long-term — it knows you
Initiative	directed — you invoke it	proactive — it anticipates
Role in the stack	your workforce / operators	your delegate / interface

AI Personal Agents vs General Agents

Two different AI roles in the age of AI-native computing

AI Personal Agents

OpenClaw

Also: **Hermes**

- Works for one person
- Knows your context, preferences, and goals
- Helps with everyday tasks and personal workflows
- Stays close to your files, apps, and routines
- Acts like a proactive personal AI companion

Best for

Personal productivity | Reminders | Planning | Research assistance | Life organization

VS

General Agents

Claude Code

Developer-focused agent for building and engineering

Claude Cowork

Collaborative agent for teams and organizations

- Works inside a broader environment
- Uses tools, files, and workflows to complete real tasks
- Can support developers and domain experts
- More task-oriented than personally intimate
- Designed for work across projects and organizations

Best for

Coding | Building | Testing | Research | Analysis | Writing | Coordination

Key Difference

Personal agents are centered on one individual and their daily life.
General agents are centered on getting broader work done across tools, projects, and professional environments.

Example framing: **OpenClaw = personal agent** | **Claude Code and Claude Cowork = general agents**

Build the Delegate; the Delegate Runs the Rest

The layer is recursive — you manage personal agents using general agents.

You → General agents

You build and configure your personal agent — its memory, permissions, and skills — with developer-grade general agents like Claude Code and OpenCode.

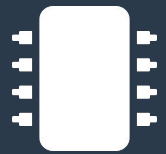
Personal agent → General agents

At runtime, your delegate knows your intent and dispatches general agents and AI Workers to carry out the work, then reports back to you.

The personal agent is your chief of staff. The general agents are the staff.

PART 03-D

The Computer That Controls Itself



RTX Spark: The Personal Agent PC

A petaflop-class chip puts frontier-model agents on the device — no cloud round-trip.

≈1 PF	128 GB	20	Local
AI performance, on-device	unified memory	Arm CPU cores	private — your data stays

NVIDIA’s OpenShell governs what an agent may touch and what may leave the machine. **The interesting engineering is not the petaflop — it is governed capability.**

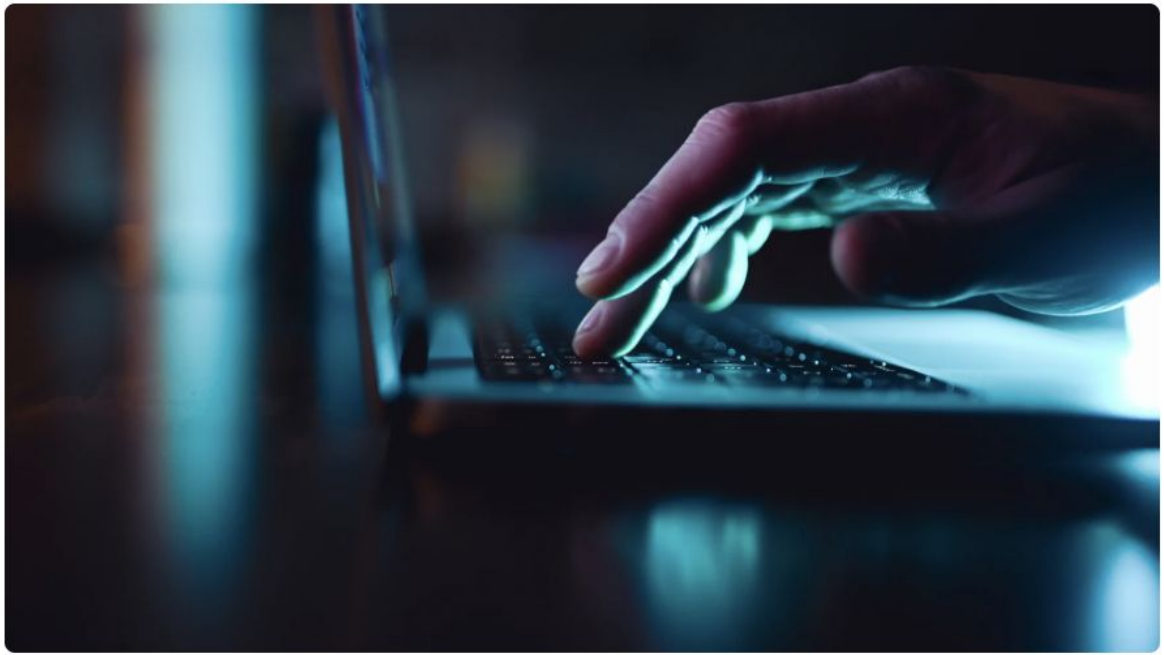
FROM TOOL TO TEAMMATE

The machine stops being an instrument you play and becomes an actor you direct.

A computer that controls itself — given your intent.

You ask; the PC does the work.

BUSINESS & TECH



The world’s biggest tech companies are betting big on computers that control themselves

NVIDIA | Windows

NVIDIA RTX SPARK

A POWERFUL NEW CHAPTER FOR WINDOWS PCs

BUILT FOR THE AGE OF AI

- UP TO **1 PETAFLOP** AI PERFORMANCE
- UP TO **20 ARM** CPU CORES
- UP TO **6,144** RTX CORES
- UP TO **128GB** UNIFIED MEMORY
- **INDUSTRY-LEADING PERFORMANCE PER WATT**

THE NEW ERA OF COMPUTING: BUILT FOR AGENTS

From App-Centric PCs to Agent-Native PCs

OLD PC MODEL

App-Centric

Humans use apps directly

You open the apps.
You do the work.

VS

AI-NATIVE PC MODEL

Agent-Centric

Humans delegate to agents

You ask.
The agent gets work done.

A NEW CLASS OF PC: THE PERSONAL AGENT PC

Purpose-built for personal agents and general agents

Example: Microsoft Surface Laptop Ultra

Powered by NVIDIA RTX Spark

RTX NVIDIA SPARK

Up to 1 petaflop of AI performance
Up to 128GB unified memory

Built for Windows
Optimized for a new era of AI experiences

Runs locally, under your control
Your data stays with you.
Private, secure, and powerful.

BUILT TO RUN PERSONAL AGENTS AND GENERAL AGENTS

Understand · Reason · Plan · Act · Use Your Apps · Access Your Files · Execute Workflows

DEVELOPER MODE (Mode 2)

We use general agents
(Claude Code, OpenCode)
to manufacture AI Workers

Claude Code
OpenCode

OUTPUT: AI WORKERS

Specialized AI agents that can think, use tools, and complete real work

Research Worker · Analysis Worker · Content Worker · Ops Worker · ...

AGENT FACTORY

The process that manufactures AI Workers and composes them into an AI Native Company

1. DESIGN
Define roles, goals, skills, and workflows

2. BUILD
Use general agents (Mode 2) to build AI Workers

3. TEST
Validate capabilities, safety, and performance in real scenarios

4. COMPOSE
Combine AI Workers into teams and multi-agent systems

5. DEPLOY
Put AI Workers to work and iterate continuously

AI NATIVE COMPANY

An organization where AI Workers operate together to create extraordinary results

PERSONAL AGENTS

Always with you.
Working for you.

Examples of Personal Agents

OpenClaw
Your personal AI assistant.
Knows you. Works for you.
Helps across all your tasks.

Hermes
Your proactive AI companion.
Plans ahead. Takes action.
Gets things done for you.

Private & Local · Knows Your Context · Proactive & Helpful · Works Across Apps & Files

THE FUTURE: People set direction. Agents do the work. Companies scale intelligence.

Built for the Age of AI

NVIDIA RTX Spark Laptop vs MacBook Pro with M5 Max

Two Arm-based laptops. Built for AI. Designed for the future.

NVIDIA RTX Spark Laptop

Windows AI Laptop
Powered by NVIDIA RTX Spark

- Up to 1 petaflop AI performance
- Up to 128GB unified memory
- Windows 11 AI PC
- Built for personal & general agents

Arm CPU	Up to 20 cores (Performance + Efficiency)	NVIDIA Blackwell GPU with Tensor Cores

VS

MacBook Pro with M5 Max

macOS

- 16-core Neural Engine for on-device AI
- Up to 128GB unified memory
- macOS Optimized for on-device AI
- Built for creators, developers and professionals

Arm CPU	Up to 16 cores (Performance + Efficiency)	Up to 40-core GPU

KEY DIFFERENCES

- **Higher AI Performance** — Up to 1 petaflop of AI performance with NVIDIA RTX Spark.
- **More Memory for AI** — Up to 128GB unified memory optimized for AI workloads.
- **Windows AI Ecosystem** — Access to a broad range of AI apps, tools, and enterprise workflows.
- **NVIDIA Software Stack** — CUDA, TensorRT, AI libraries, and enterprise-grade support.

BENCHMARK COMPARISON

Higher is better

NVIDIA RTX Spark Laptop		MacBook Pro with M5 Max
11,420	**Geekbench 6** (Multi-Core) Overall CPU performance	10,745
1,659,321	**Geekbench AI (Quantized Score)** On-device AI performance	1,243,876
8,341	**UL Procyon AI Computer Vision** Image generation (SD 1.5)	6,452
14,280	**UL Procyon AI Text Generation** LLM inference (Phi-3.5-Mini)	9,105
120.4	**Stable Diffusion XL** (fp16) Images per minute (faster is better)	78.6
82.1	**Token Generation Speed** (fp16) Tokens per second (Llama 3 8B)	58.7
98.7	**Blender 4.2.0** (CPU) Classroom (samples per minute)	85.9
31.2	**Battery Life** (Video Playback) Hours (longer is better)	24.0

KEY STRENGTHS

- **macOS Optimization** — Deeply integrated software and hardware for efficiency.
- **Industry-Leading Battery Life** — Up to 24+ hours of video playback for all-day productivity.
- **Privacy by Design** — On-device AI with advanced privacy and security protections.
- **Premium Build & Display** — Exceptional build quality and stunning Liquid Retina XDR display.

BOTH ARE BUILT FOR THE AGE OF AI

- **Run Powerful AI Locally** — Execute large models, generate content, and automate tasks on-device.
- **Private & Secure** — Your data stays with you. AI on your device, on your terms.
- **Built for Developers** — Tools, frameworks, and SDKs to build the next generation of AI experiences.
- **The Future is Agentic** — From personal assistants to autonomous agents—both are ready.

Benchmarks are approximate and may vary based on model configuration, software version, and testing conditions. Source: NVIDIA, Apple, Primate Labs, UL Procyon, Stable Diffusion Benchmarks (May 2025)

PART 03-E

Why This Time Is Different

Three Things Changed — Together

Models crossed a threshold

On OSWorld — real desktops, no partial credit — agent success jumped from ~12% to ~66% in a year, crossing the human baseline.

66%

Compute came to the device

A local petaflop with 128GB makes always-available, private, unmetered agent compute native to the machine — not a cloud subscription.

The OS vendors rebuilt

Microsoft wired agents into Windows behind every surface; eight makers ship RTX Spark PCs this fall. The change is the platform, not an app.

When all three land together, doing it yourself stops being the default — the gap the Siri decade never closed.

The Honest Objections

These set the pace and the scope — not the direction.

Cost

Petaflop laptops are a premium category; the installed base of human-operated machines persists for years.

Trust & governance

An agent with broad access can be misled. The platform that wins solves governed capability, not the most FLOPs.

The hybrid

For now, high-stakes work stays human + UI + agent — the thesis in its transitional phase, not an alternative to it.

Reliability

~66% average means roughly one task in three still fails. Bounded, recoverable tasks go first.

PART 03-F

What Dies, What Survives

What Dies, What Survives

WHAT DIES

- The app as the unit of human work
- The graphical shell as the place you live
- SaaS as a destination
- The human as operator

WHAT SURVIVES

- The OS as invisible plumbing
- Software capabilities, as tools agents call
- The human as the source of intent
- Judgment: what to want, and whether it’s good

The PC as hardware does not die — it becomes more essential. What dies is the human’s job of driving it.

What It Means for Builders

The strategic ground shifts — the agent has no eyes for your interface.

The moat moves

Be the layer the agent lives in, the capability it must call, or the governance it must obey. A beautiful, sticky UI is no longer the defense.

The firm that orchestrates agents out-produces the firm that buys more seats of the old software.

700 FTEs

≈ $40M profit lift

Klarna's customer-service agent did the work of ~700 full-time staff — "scale intelligence, not headcount." (Humans were re-added for complex cases: bounded tasks first.)

THE BOTTOM LINE

People set direction. Agents do the work. *The interface is the agent.*

The era is no longer “humans use apps.” It is “humans delegate work.”

PART 03-G

Two Ways to Use AI (General Agents)

Our main AI agents are general agents

General agents adapt across many tasks instead of being limited to one narrow workflow.

For Developers

Claude Code
OpenCode

General agents for developers

Used for coding, building, debugging, and software problem-solving.

For Domain Specialists

Claude Cowork
OpenWork

General agents for domain specialists solving problems

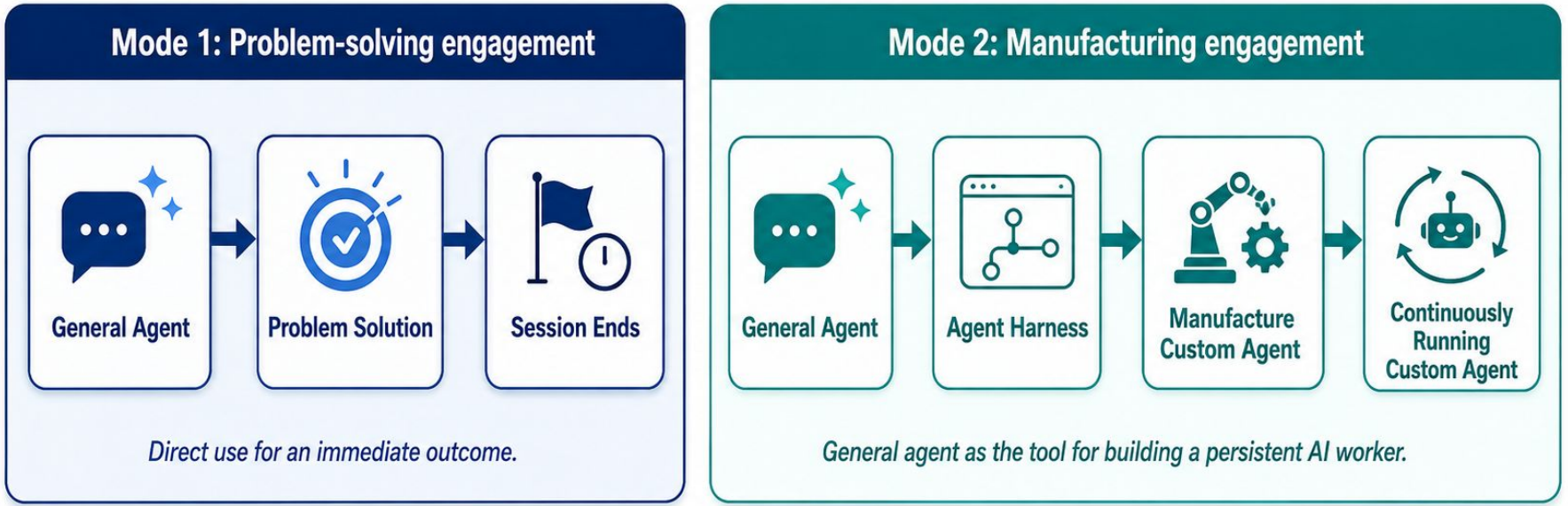
Used for analysis, research, planning, writing, and business-domain problem-solving.

Both are general agents

Different audiences, same core idea: flexible agents that help people solve real work problems.

Two Modes of General Agent Use

Mode 1 uses a general agent to solve an immediate problem.
Mode 2 uses a general agent to help build and deploy a custom agent that can keep running.



Refinement: in Mode 2, the continuously running custom agent is typically deployed through an agent harness or runtime, rather than the general agent itself running continuously.

ANALOGY

Fish vs. Fishing Net

Two Modes. Two Outcomes.

MODE 1

PROBLEM-SOLVING

Catch a fish. Solve today's problem.

Solves today.

BOTH ARE VALUABLE

MODE 2

MANUFACTURING

Build a net. Catch fish every day.

Builds tomorrow.

Start with Mode 1
Solve today's problem.

Move to Mode 2
Build tomorrow's solution.

Learn both. Use both. Grow beyond both.

Two Modes Side by Side

Mode 1 — Problem-Solving

"Help me do this thing right now."

You have a problem. You use AI to solve it. The session ends. Nothing permanent is built.

Example: "Help me analyze this spreadsheet" or "Write me an email to my client."

Mode 2 — Manufacturing

"Help me build a worker that does this job forever."

You use AI to build a new AI worker that will keep running long after you close your laptop.

Example: "Build me a customer support bot that runs 24/7 and answers common questions."

The Roles This Book Trains

1. THE CORE PIPELINE · INTENT → PRODUCTION

WHAT — Outcome Architect → **BUILD** — Digital FTE Builder → **SYSTEM** — AI-Native Company Architect → **RUN** — Cloud AI Engineer

2. EXTENDS IT · THE TWO ROLES ONLY THIS BOOK TRAINS

- **Subject Matter Expert as Skill Author**
  encodes domain judgment — the Worker's knowledge engine
- **Forward Deployed Engineer**
  the whole pipeline, run inside a client's company

3. SUPPORTS IT

- **Evals Engineer**
  the verification standard
- **AI Governance Officer**
  authors the workforce's rules
- **Digital FTE Supervisor**
  accountable, Worker by Worker

4. WHERE THE BOOK STOPS

- **LLMOps Engineer**
  ops & fine-tuning, not models
- **Harness Engineer**
  uses runtimes, doesn't build them
- **AI Data Engineer**
  agent-facing data only

5. THE BASELINE EVERYONE STARTS FROM

- **Mode 1 Practitioner**
  use a general agent to do your own work faster — a proficiency, not a title

PART 04

The 10-80-10 Rhythm

ANALOGY

The Film Director

A director doesn't do every task.
They **guide** the work.

1. **Set the vision**
   What should it look like?
2. **Let the team work**
   They do the work
3. **Review the final cut**
   Check and approve

Working with AI is the same

First 10%
You set direction

Middle 80%
AI does the work

Last 10%
You review & approve

START — IN PROGRESS — FINISH

The 10-80-10 Split

10%
Human sets direction

80%
AI does the work

10%
Human checks & approves

Three Things That Always Stay With Humans

Intent

Knowing what you want

Verification

Checking if the work is good

Ownership

Being responsible for the result

You're Promoted, Not Replaced

The Human Role

You are promoted, not replaced. From typist to editor. From coder to architect. From worker to director. AI takes over the middle 80%. You keep the parts that matter most — direction and judgment.

REAL EXAMPLE

Old Way

You spend 4 hours writing a business report yourself.

New Way

20 min writing clear instructions. AI writes the report in 5 min. 20 min reviewing and fixing. Same quality. One-tenth the time.

PART 05

From "Smart Tool" to "Smart Worker"

ANALOGY

The Carpenter's Drill vs. Hiring a Contractor

OLD WAY

You hold it.
You decide.
You do the work.

AI as a **TOOL**

- You control every step
- Tool makes one part faster
- You still do the job

NEW WAY

You give the job.
It does the work.
You check the result.

AI as a **WORKER**

- You define the outcome
- Worker handles the task
- You review the result

Working with AI is the same

Give the job
Define what you want

→

AI does the work
It handles the task

→

Check the result
Review and approve

Tool = You do the work | **Worker = AI does the work**

KEY TAKEAWAY

The biggest shift in AI right now isn't about making smarter tools. It's about turning AI from a tool you use into a worker you hire.

You stop paying for access to software.

You start paying for finished results.

Mode 2: Using General Agents to Manufacture AI Workers

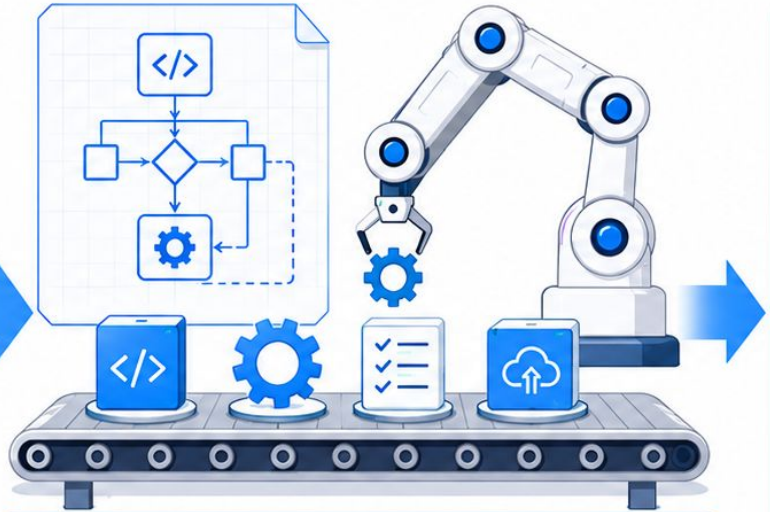
General agents such as Claude Code and OpenCode are used to build, configure, and deploy AI Workers.

Mode 2

General Agents

- Claude Code
- OpenCode

Work inside files, tools, commands, workflows, and projects.



Build • Configure • Test • Deploy

Manufacturing AI Workers

Output

AI Workers

Digital FTEs

- Research Worker
- Coding Worker
- Support Worker
- Analyst Worker

Specialized workers created for real tasks.

Browser chat answers questions. | Mode 2 general agents create the workers that do the work.

PART 06

The Agent Factory Idea

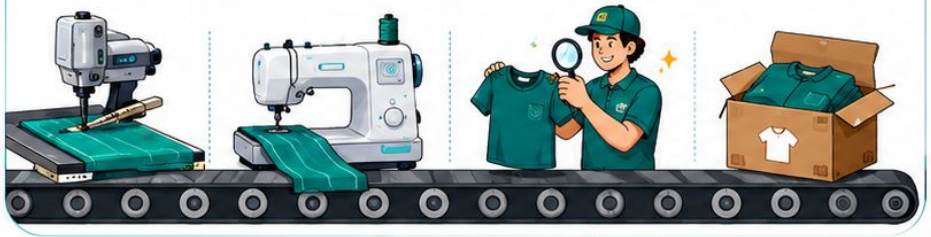
The Agent Factory

Analogy: A Garment Factory

GARMENT FACTORY

A garment factory doesn't make one shirt by accident.
It has a system.

1. Cutting → 2. Stitching → 3. Quality Check → 4. Packing



AGENT FACTORY

The same idea — but for AI workers.

1. Design AI Workers → 2. Train Them → 3. Put Them to Work → 4. Check the Results

REPEATABLE PROCESS

Design → Train → Deploy → Verify

NOT a product
Not something you buy.

A practice you learn
A repeatable way to build and manage AI workers.

AI-Native Company
A company where most workers are AI.

Agent Factory = a repeatable process for building AI workers.

The Company With Invisible Employees

Old World

200
Humans

Phones + emails

VS

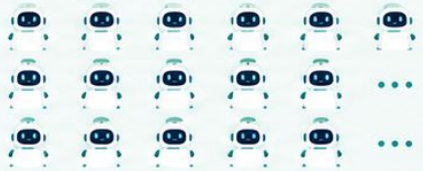
New World

10
Humans

+

190
AI Workers

10 human supervisors
handle tricky cases and oversee AI



190 AI workers
handle routine questions 24/7

Routine questions → AI handles instantly → Complex cases → Humans review

Fast service
Instant answers most of the time

Lower cost
Fewer humans to do the work

24/7
Always on, day and night

Most workers are AI. Humans handle the tricky cases.

Customers barely notice the difference — they just get fast, good service.

AI-Native Company

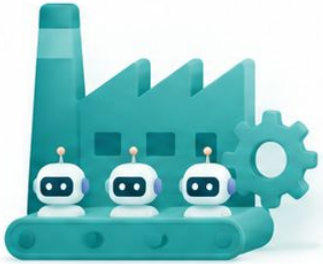
A company where most of the workers are AI, not human.

The Agent Factory Flow

1

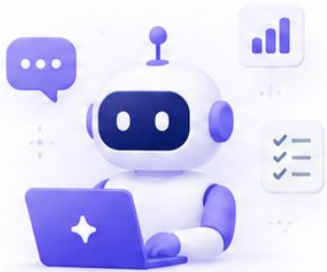
Human sets the goal

2



Factory builds workers

3



Workers do the jobs

4

Results delivered

Human gives direction → system builds AI workers → workers do the work → results return for human review

Agent Factory

The process that manufactures AI Workers and composes them into an AI-Native Company

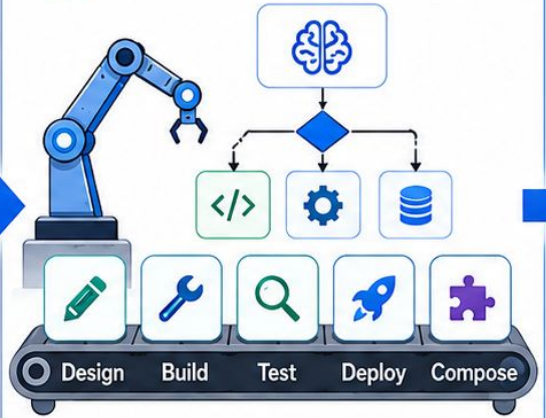
1 General Agents

Claude Code

OpenCode

Used in Mode 2 to build and orchestrate AI Workers

2 Agent Factory Process



Transforms general-agent capability into specialized AI Workers

3 AI Workers

- Research Worker
- Coding Worker
- Support Worker
- Analyst Worker
- Operations Worker

Specialized Digital FTEs created for real tasks

4 AI-Native Company

AI Workers are composed into a coordinated company system

General agents create AI Workers. | **Agent Factory** organizes them into an AI-Native Company.

PART 07

Your Personal AI Delegate

ANALOGY

The Executive Assistant

Intent → Delegate → AI workforce → Approval

You set direction. Your **AI delegate** manages the work. You review the result.

1 You set direction

You provide goals + guardrails

2 Your AI delegate

Understands your intent

3 Delegate coordinates specialist AI workers

Behind the scenes

Secure • Private • Always on

4 You review & approve

You review the final cut

You approve the result

You do not manage 20 AI workers directly.

Your one delegate manages them for you.

The Two-Layer Model

EDGE LAYER

You

Your Delegate

Your personal AI that knows your preferences, carries your authority, and manages workers.

AI WORKFORCE LAYER

Support Worker

Finance Worker

Sales Worker

Legal Worker

PART 08

The 7 Principles of General Agent Problem Solving

The Seven Principles, at a glance

Five core disciplines, wrapped by two operational principles.

P6 — CONSTRAINTS & SAFETY

scope what the agent is allowed to touch

P 1
Bash is the Key

ACTION OVER TALK

The agent has hands, not just a mouth.

Failure mode:
"It keeps narrating instead of doing."

P 2
Code as Interface

SHAPE OVER PROSE

Specify the shape before the content.

Failure mode:
"My prose request keeps getting misread."

P 3
Verification

VERIFY, DON'T TRUST

"Looks right" is the precise failure mode.

Failure mode:
"It looked right but broke in production."

P 4
Decomposition

SMALL, REVERSIBLE

Each step is cheap to undo. Atomic units.

Failure mode:
"One big change just nuked an afternoon."

P 5
Persistence

FILES ARE MEMORY

The chat is volatile. The filesystem isn't.

Failure mode:
"It forgot what we decided yesterday."

P7 — OBSERVABILITY

see what the agent did, when, and why

Build P1–P5 inward. Wrap them with P6 (Constraints) and P7 (Observability).

PART 09

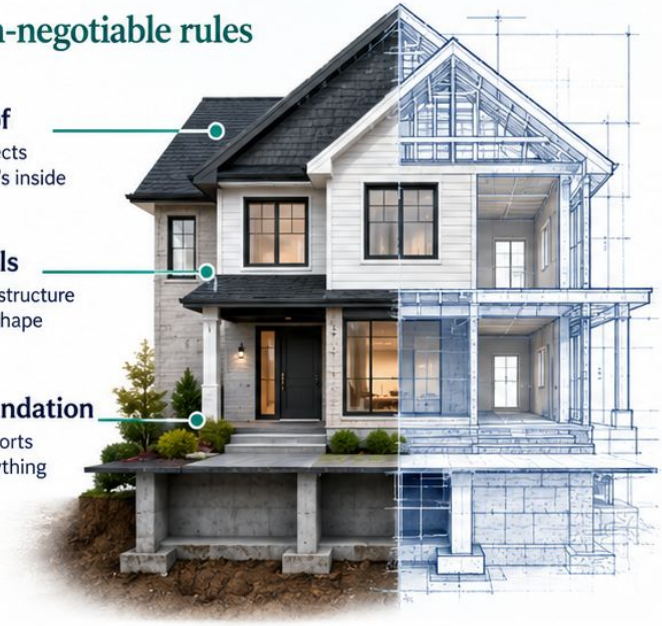
The 7 Golden Rules of an AI-Native Company (Invariants)

ANALOGY

Building Rules That Never Change

Tools change. **Structural rules don't.**

Non-negotiable rules



Roof
Protects what's inside

Walls
Give structure and shape

Foundation
Supports everything

Choices can vary

Bricks or concrete

Flat or sloped roof

For AI companies:

7 rules = your building code

Tools change every year

Structural principles stay the same

Tools change → Rules stay

Build on timeless rules, not temporary tools.

The 7 Golden Rules (1–4)

1 **Human is always in charge**

Every action traces back to a human. AI never sets its own goals.

2 **Every human gets a delegate (identic AI)**

You can't manage 20 workers by hand. Your delegate coordinates.

3 **Workforce needs a management layer**

Someone hires, assigns tasks, controls budgets, fires underperformers.

4 **Each worker uses the right engine**

Important work = reliable engine. Simple work = cheap engine.

The 7 Golden Rules (5–7)

5 **Every worker uses a system of record**

AI workers read/write the company's official memory. Without it, AI makes things up.

6 **Workforce can grow under rules**

When a gap appears, the system hires a new worker automatically — within human-set limits.

7 **Company runs on a nervous system**

Just like your body sends signals automatically,"hand touched something hot, pull back!" the AI company sends work between workers automatically. No human needed to pass tasks along. And if something breaks, the system recovers on its own.

Tools change. Rules stay.

PART 10

A Real Example: Ecomm Mart

Building the Support Worker (Steps 1–3)

Step 1

Write Clear Instructions

Define the goal: read tickets, classify them, write replies, escalate hard cases. Set budget: $200/month max.

Step 2

Connect to Company Records

Link to Shopify orders, customer database, and ticket system so the AI can look up real data.

Step 3

Give It Skills

Teach it: how to write professional replies, how to classify tickets, when to escalate. Like a training manual.

Building the Support Worker (Steps 4–5)

Step 4

Set the Guardrails

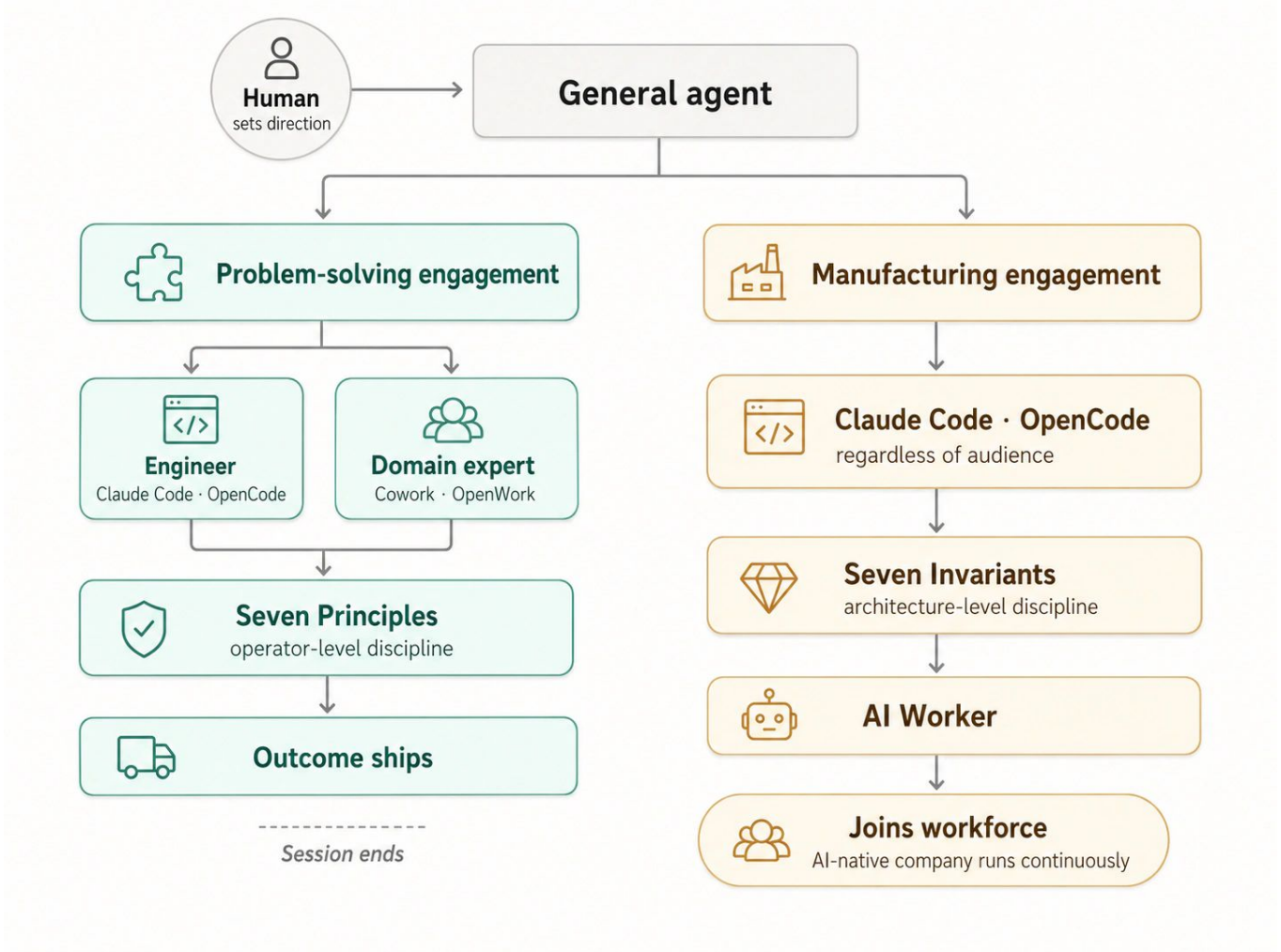
Budget cap, approval for big refunds, audit trail of every action. The AI can never go outside these limits, all will be define in specs

Step 5

Test, Then Deploy

Run on 100 old tickets first. Check results. Fix problems. Only then let it handle real customers.

Result: You just built a Digital FTE — a Full-Time Employee made of software. It works 24/7, stays within rules, and handles 80% of support tickets automatically.


Human
sets direction
General agent
Problem-solving engagement
Engineer
Claude Code · OpenCode
Domain expert
Cowork · OpenWork
Seven Principles
operator-level discipline
Outcome ships
Session ends
Manufacturing engagement
Claude Code · OpenCode
regardless of audience
Seven Invariants
architecture-level discipline
AI Worker
Joins workforce
AI-native company runs continuously

PART 11

Key Vocabulary & What's Next

Essential Vocabulary (1/2)

`AI`	Software that learns from data and makes decisions
`Agentic AI`	AI that plans, uses tools, fixes mistakes, completes jobs
`AI Worker / Digital FTE`	AI built to do one specific job, like a human employee
`Agent Factory`	The method for building AI workers (a practice, not a product)
`AI-Native Company`	Company where most workers are AI, selling results not tools

Essential Vocabulary (2/2)

`Delegate`	Your personal AI that manages the workforce for you
`System of Record`	Company's official memory — the single source of truth
`Spec`	Clear written instruction: goal, limits, budget, success criteria
`10-80-10 Rule`	Human direction (10%) + AI work (80%) + Human check (10%)

TODAY'S BIG IDEAS — IN ONE BREATH

AI is software that learns and makes decisions. Agentic AI takes this further — it plans, uses tools, and completes entire jobs.

The Agent Factory is the method for building AI workers and organizing them into AI-Native Companies where AI does the work and humans set direction and check quality.

You're not being replaced — you're being promoted from worker to director.

The future belongs to people who can clearly tell AI what to do, connect it to real data, and verify the results are correct.

That's what this program will teach you. Welcome aboard.

Thank You

Your journey into Agentic AI starts now.

Based on the Agent Factory Thesis
agentfactory.panaversity.org