Frontier Agent Platform

A new technology blueprint for companies that are AI-operated but human-led.

Dorian Groeger
Microsoft

A new organizational blueprint is emerging, one that blends machine intelligence with human judgment, building systems that are AI-operated but human-led.

Work Trend Index Annual Report
2025: The Year the Frontier Firm Is Born
https://aka.ms/wti

Microsoft

AI momentum is forcing organisations to think differently.

Business leaders told us:

AI Strategy

82%

think **this year is critical** to rethink strategy and operations for AI

AI Automation

46%

say their organization is already using agents to **fully automate** workstreams

Digital Labor

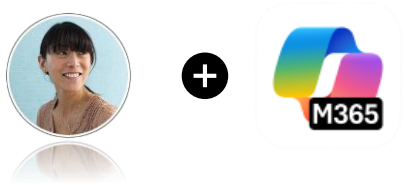
82%

expect to **use digital labor** to expand their workforce in the next 12 to 18 months

The three patterns of work

Pattern 1

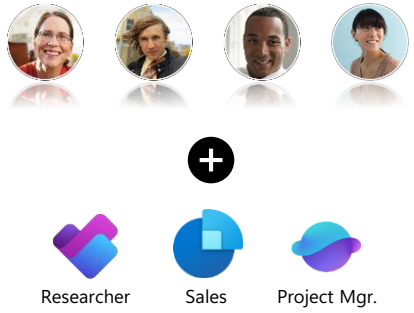
AI Assistants



Every employee has an AI assistant that helps them work better and faster

Pattern 2

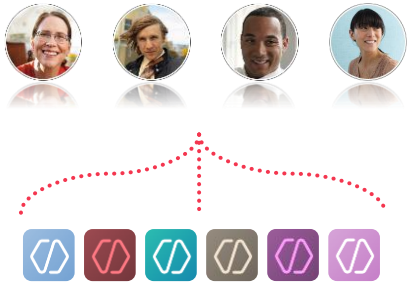
AI Teammates



Agents join teams as “digital colleagues”, taking on specific tasks at human direction

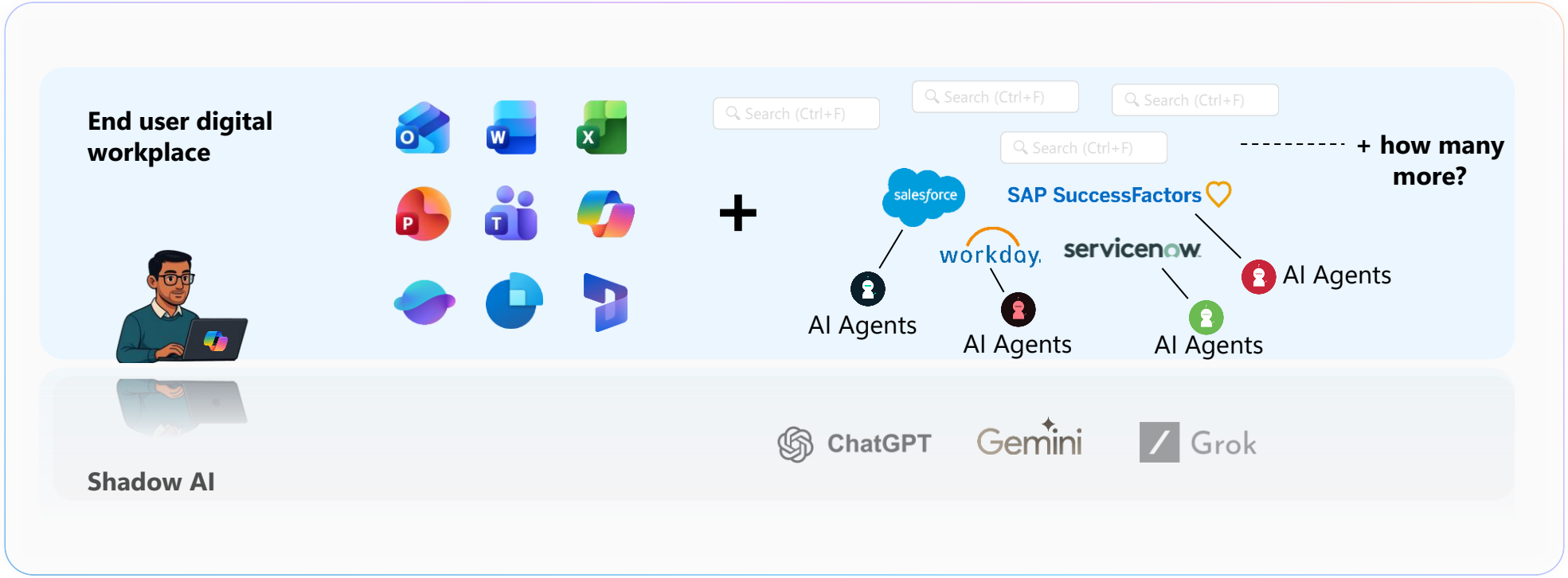
Pattern 3

AI Operators

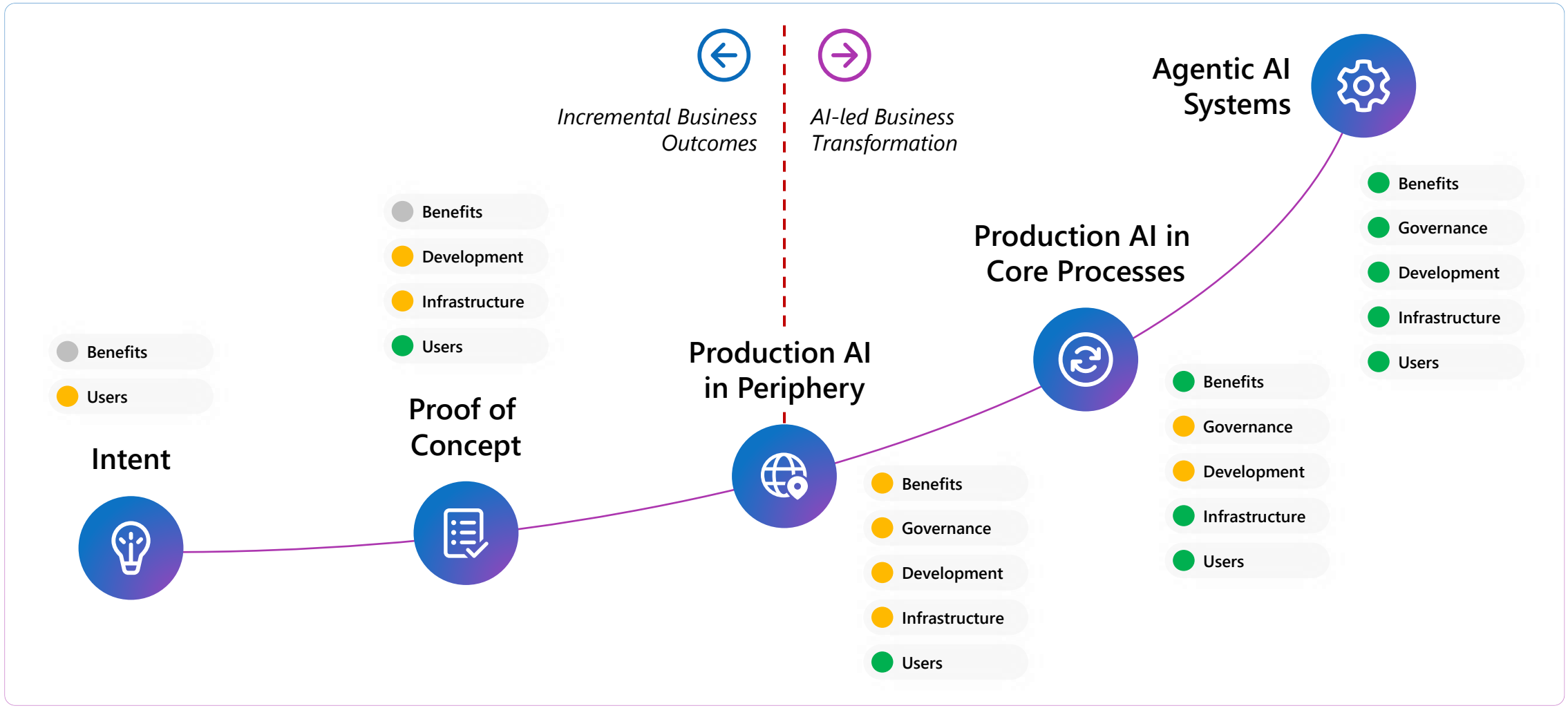


Humans set direction and agents run entire business processes and workflows, checking in as needed

AI everywhere does not make a platform

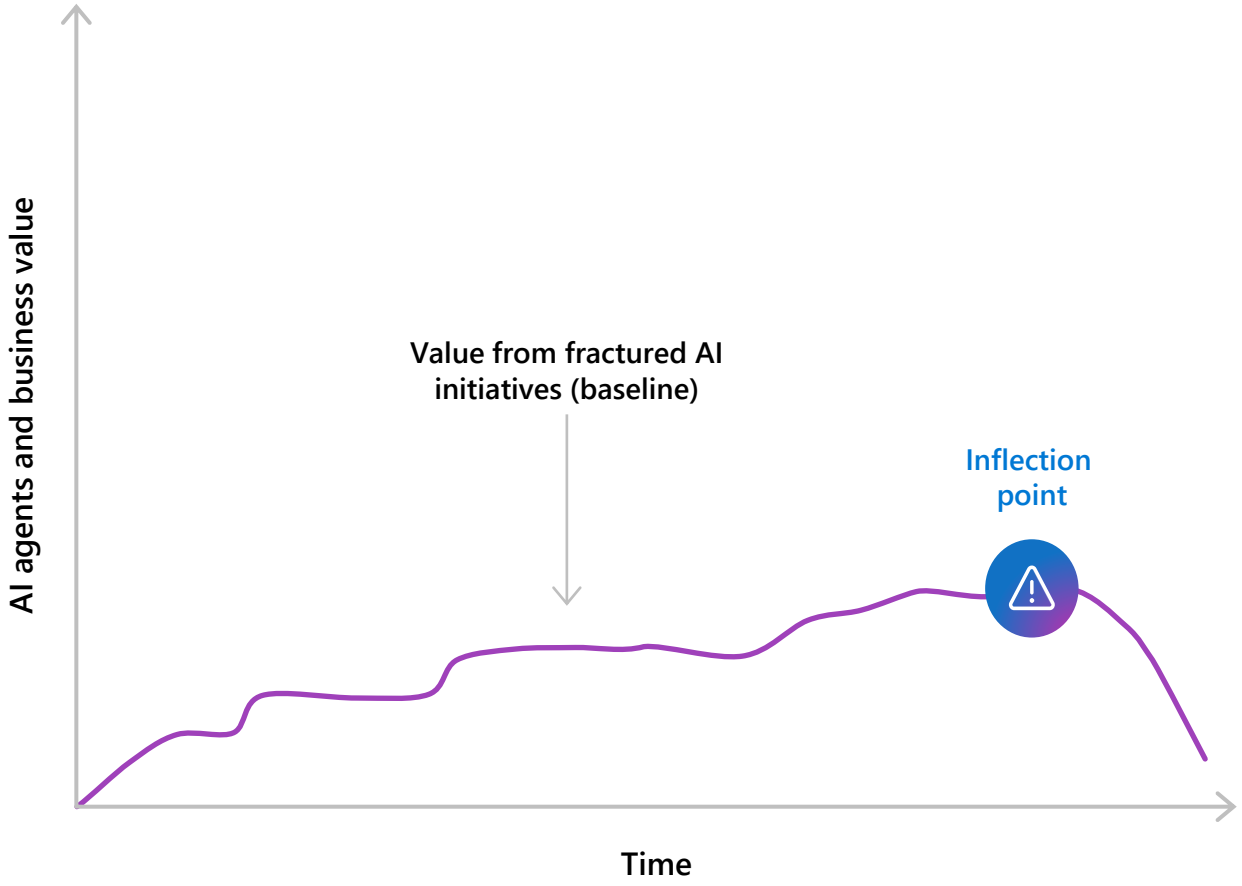


Where do organizations get stuck?

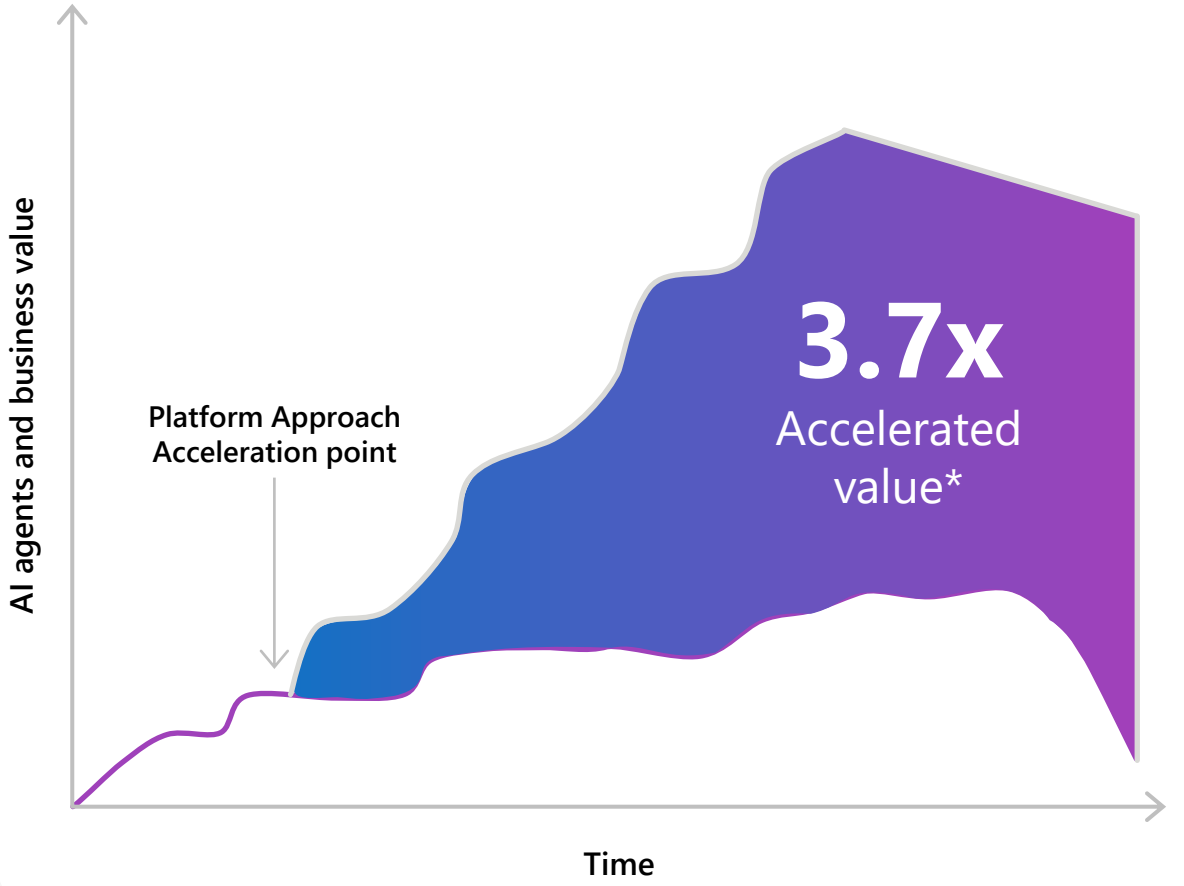


From AI fragmentation to AI acceleration

Limited impact from fractured AI initiatives



AI CoE: Unlock and accelerate business value



*IDC InfoBrief: Sponsored by Microsoft, 2024 Business Opportunity of AI, IDC# US52699124, November 2024

Non-negotiables of a Frontier Agent Platform

Scope the platform to your strategy — and each agent to the task, risk, and accountability.

Development

Build / Buy / Partner — without changing the operating model
Onboard into the same governance, identity, and lifecycle.

Enable every builder persona
From business makers to pro developers

Ship fast, stay safe
Speed from reusable patterns; safety from automatic guardrails

The UI for AI

One front door for humans and agents
not a patchwork of portals.

Agents, Data & Tools

Task-scoped autonomy
Use the *minimum autonomy* needed:
with human oversight where judgement matters.

Act on data where it lives
Retrieve and take actions at source, honouring permissions

Open tool and agent interoperability
Agents must invoke tools, APIs, and other agents through standard interfaces

Systems of Record

Enterprise Data, Wherever It Belongs
The platform must support operational systems, analytical platforms, and knowledge stores

Agent Control

Every agent has identity, owner, and purpose
with a human owner, defined role, and clear boundaries.

One governance plane
Policies, auditability, monitoring, and controls across all agents

Minimise attack surface by design
Least privilege, strict boundaries, continuous protection, and traceability

Microsoft Frontier Agent Platform

Agent Development

Power Platform

Build agents without code barriers.

Business users create, own, and govern agents, safely and at scale.

Azure AI

Engineer-grade agent development.
Full control of models, tools, and runtime.

Agents Toolkit

Developer tooling for enterprise agents.

Agent Framework + SDKs; host on or off Microsoft.

The UI for AI

Microsoft 365 Copilot | The front door for agents. Use agents in Teams, Outlook, Office apps & on any device. Chat, search, create, reason, and act in one experience.

Agent Store

3rd Party Agents
Install and use agents from Microsoft partners.

Microsoft Agents
Use a range of agents available from Microsoft, spanning personal productivity, task specific and role specific agents.

Custom Agents
Build your own agents and bring agents from other agent platforms.

Agent Hosting

Match hosting to who owns the agent. Zero-code to Azure-engineered, with complete control.

Intelligence

WORK MEMORY | PERSONALISATION | TUNING | INFERENCING | ORCHESTRATION

Open Protocols

Open access to tools and data.

MCP Servers

Prebuilt tools, instantly available.

Connectors

Prebuilt access to data and APIs.

Enterprise Data Platform

AI-ready data for agentic workloads. Fabric, Databricks, and Dataverse — with built-in MCP capabilities.

Enterprise Systems of Record & Applications

D365 CRM | D365 F&O | Salesforce | SAP | Workday | ServiceNow | SQL Databases | Storage

Agent Control System

Agent 365

Verified identity and least-privilege control

Detect and remediate risky behavior

Classify sensitive data and enforce controls

Copilot Analytics

Operations

Set guardrails for all Foundry agents.

Quotas, policies, and controls — across Microsoft and non-Microsoft runtimes.

All Agents

Govern and control agents from all platforms including OpenAI, Google and AWS.

Your unique intelligence is what powers agents

Unified view of your business

How your employees work

Your knowledge sources

Your business processes

Your data and apps