A THOUGHT LEADERSHIP PAPER

# The Autonomous Workforce

*Why Every Enterprise Now Has Two Workforces*

**Pat Calhoun**
Chief Commercial Officer, XOPS
August 2026

For decades, every major technology wave, from mainframes to cloud computing, changed how work was performed without changing who performed it. Technology remained a tool: it amplified human capability, but people still did the work. Artificial intelligence is the first technology wave to break that pattern.

AI does not simply make existing workers more productive. It performs work itself, analyzing, recommending, negotiating, monitoring, creating, and executing with delegated authority rather than direct human instruction. Enterprises are deploying autonomous agents that reconcile invoices, triage security events, optimize supply chains, generate software, negotiate procurement decisions, and coordinate with other agents. These systems are no longer waiting for someone to click a button. They perform work continuously on behalf of the organization.

> *That distinction changes how enterprises must think about management.*

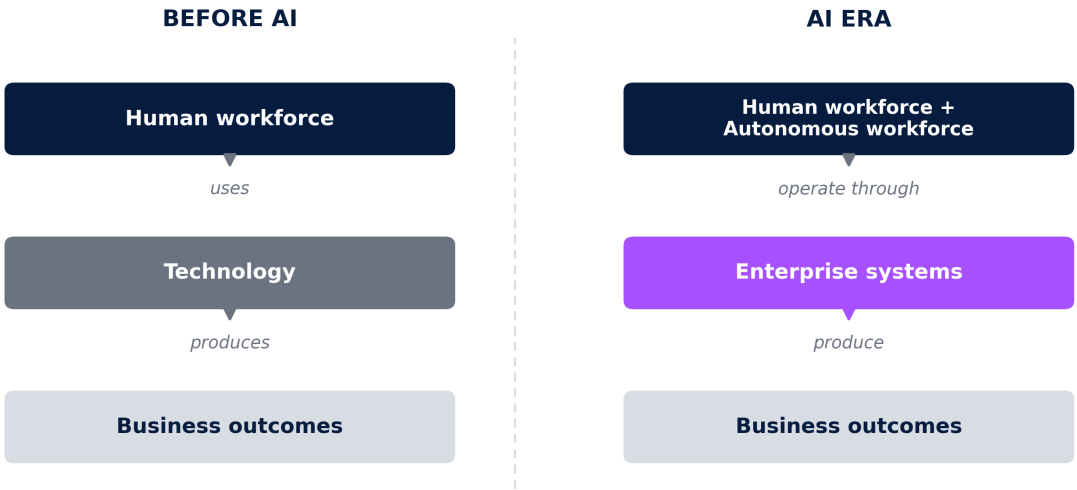



*Figure 1. AI creates a second workforce.*

## From Technology Assets to Autonomous Workers

For decades, CIOs have managed technology as an asset: hardware has owners, software has licenses, infrastructure has administrators. Workers, by contrast, have identities, managers, budgets, and lifecycles. They are hired, onboarded, transferred, and offboarded through disciplines built because unmanaged workers create operational, financial, and security risk.

Throughout this paper, I use the term autonomous worker to describe an AI agent delegated authority to perform work on behalf of the enterprise — not an argument for personhood, but an operational distinction. A chatbot that answers questions on demand remains a productivity tool; an autonomous worker operates independently and continuously, with delegated authority to act. It authenticates into enterprise systems, consumes budget through model usage, performs work within delegated

authority, and can trigger downstream actions across business systems without human intervention. It can be reassigned, granted additional authority, suspended, or retired. In every operational sense that matters to enterprise leadership, these systems increasingly resemble workers more than software — yet most organizations continue to manage them as though they were simply another application. That mismatch is becoming one of the defining operational challenges of enterprise AI.

| Human workforce | Autonomous workforce |
|---|---|
| Employee identity | Agent identity |
| Manager | Accountable owner |
| Role | Declared scope |
| Budget | Budget |
| Approval authority | Delegated authority |
| Onboarding | Provisioning |
| Transfer | Reassignment |
| Offboarding | Suspension or retirement |
| Performance | Cost and business value |

*Figure 2. Two workforces require one operating model.*

## The Enterprise Already Has Two Workforces

Today, responsibility for autonomous workers is fragmented. Finance monitors AI spending through invoices and token dashboards. Security inventories identities and API keys. Infrastructure teams track compute. Architecture sets standards. Procurement negotiates agreements. Individual business units deploy assistants and agents to solve local problems. Every function sees a fragment of the picture, but almost nobody owns the workforce as a whole.

Consider an employee who leaves the company on Friday. Their identity is disabled, their laptop reclaimed, their access to Microsoft 365, Salesforce, and Workday revoked — a lifecycle that enterprises have spent decades refining. Now imagine that employee also created three autonomous workers responsible for customer support, contract analysis, and executive reporting. The employee is gone, but those workers keep operating: their credentials stay active, their budgets keep funding model consumption, and they keep making decisions within authority no one remembers delegating.

Nothing is technically broken. Identity management works as designed, the AI platforms remain available, finance still receives accurate invoices. The operating model, however, has failed, because no enterprise system was built to answer what has suddenly become the most important question:

> *Who is accountable for this autonomous worker?*

The result is two workforces governed by entirely different management models. Human workers exist inside mature operating disciplines refined over decades. Autonomous workers exist inside provider consoles, cloud accounts, and departmental experiments — consuming budgets and exercising increasing autonomy while rarely participating in the same governance as the humans alongside whom they work. This is not fundamentally a technology problem. It is a management problem.

## Every Strategic Asset Creates a New Management Discipline

Enterprise history follows a consistent pattern: whenever a new class of strategic asset becomes essential to the business, a management discipline eventually emerges to govern it — usually only once the scale, value, and risk of the new capability become too great to manage informally.

Software followed this path, and Software Asset Management emerged to govern licensing, compliance, and lifecycle. Cloud computing followed a similar trajectory, and FinOps emerged to provide continuous governance over elastic, consumption-based economics. Cybersecurity evolved from an infrastructure concern into a board-level discipline as digital risk became business risk.

Autonomous workers represent the next step — not because AI is inherently more complex than previous technologies, but because autonomous workers occupy a different role: they do not simply enable work, they perform it. The question is no longer whether organizations need AI governance. Most already know they do. The real question is whether they have an operating discipline capable of managing an autonomous workforce.

## The Questions Boards Will Ask

During the past decade, boards wanted to understand cloud strategy, cybersecurity posture, and digital transformation — conversations focused on technology investment. The next set of questions will be different. Boards are unlikely to spend time debating which foundation model the enterprise has standardized on; that is an implementation decision.

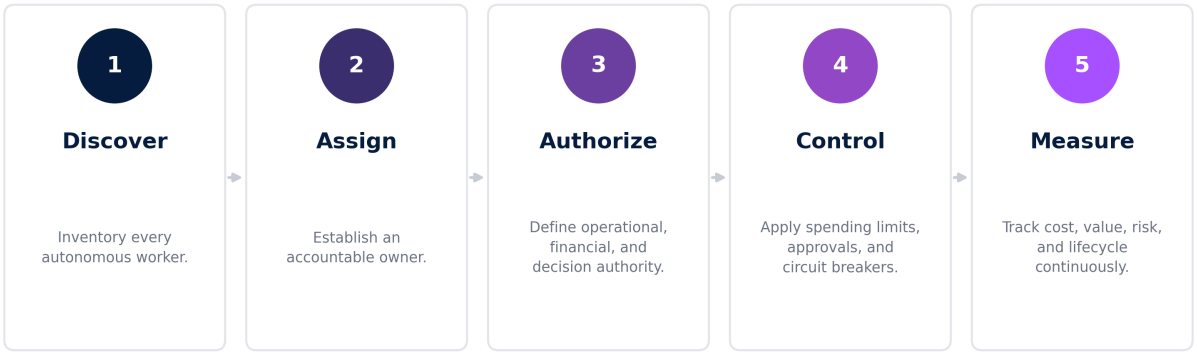
Boards care about accountability, delegated authority, and operational control. They will ask how many autonomous workers operate across the enterprise, who owns them, what decisions they are authorized to make, what financial authority they hold, what prevents uncontrolled spending, what they cost, and whether they create measurable value. They will also ask a question few organizations can answer today: what is the maximum financial exposure of any autonomous worker?

Human employees operate within defined approval limits and spending authorities. Autonomous workers will require the same controls — or organizations risk a workforce capable of consuming enterprise resources continuously without meaningful guardrails.

## The Five Foundations

For CIOs, the practical implication is straightforward: autonomous workers require an operating model, not simply another technology platform. That model rests on five foundations.

> *Every autonomous worker should be discoverable, accountable, authorized, bounded, and continuously evaluated.*




*Autonomous workers should not merely be visible. They should be owned, bounded, controlled, and continuously evaluated.*

These are not purely technical actions. They require collaboration across identity, security, finance, architecture, procurement, legal, risk, and business leadership — and CIOs are uniquely positioned to lead the effort because they already operate at the intersection of enterprise technology, governance, and business transformation.

## From Governance to Operations

Recognizing that every enterprise now has two workforces is only the beginning. The larger challenge is operational: how should an enterprise continuously discover autonomous workers, establish ownership, manage delegated authority, control lifecycle events, and connect operational cost to business value?

Existing enterprise platforms each solve part of the problem. Identity systems govern credentials and access. AI platforms manage models and execution. FinOps monitors consumption. Security evaluates risk. Together they provide important capabilities, but none was designed to operate an autonomous workforce as a coherent enterprise system.

> *This gap marks the emergence of a new enterprise operating discipline: Autonomous Workforce Operations.*

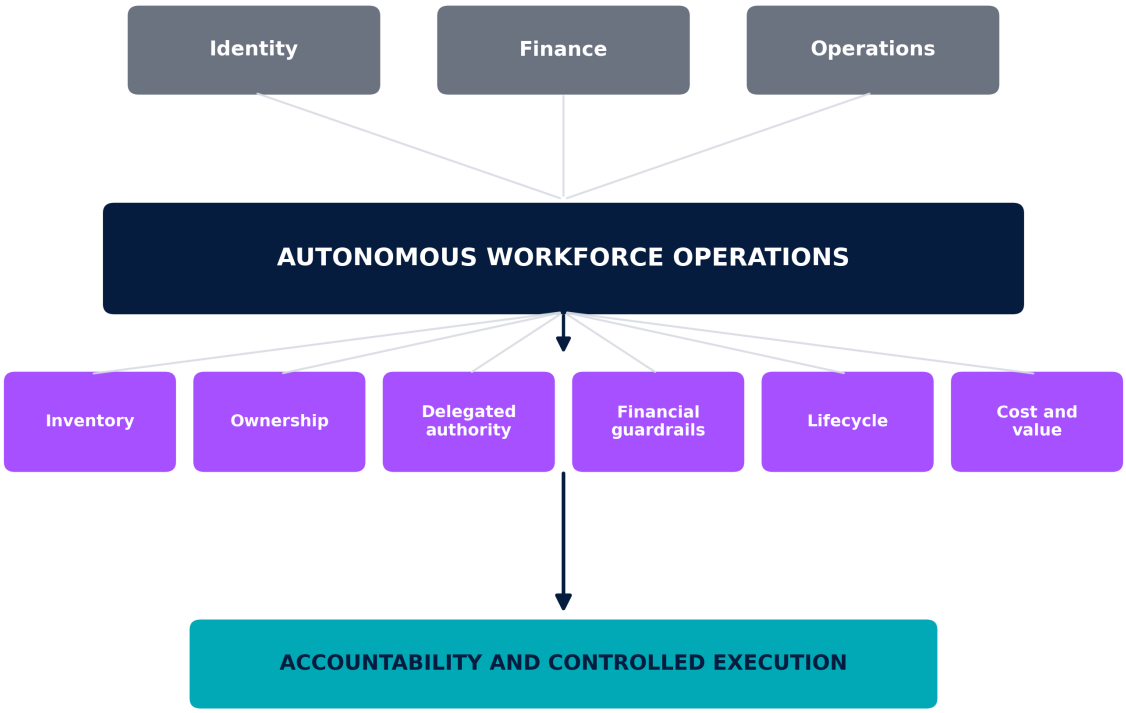



*Figure 3. Existing platforms govern fragments. Autonomous Workforce Operations governs the workforce.*

## The Next Enterprise Operating Discipline

Just as Software Asset Management became essential when software evolved into a strategic asset, and FinOps emerged when cloud economics became too dynamic to govern manually, Autonomous Workforce Operations is the operational layer required for the enterprise's second workforce. Its purpose is not simply to provide visibility into AI, but to establish continuous operational control over autonomous workers throughout their lifecycle.

At XOPS, this belief has shaped our platform from the beginning. Rather than treating AI as another technology estate to govern, XOPS manages autonomous workers as operational entities — continuously connecting identity, ownership, delegated authority, lifecycle, execution, cost, and business value into a single system of accountability.

The organizations that succeed over the coming decade will not necessarily be those that deploy the most AI. They will be the ones that build the operating model capable of managing it. The CIOs who recognize this shift first will define the next generation of enterprise operations.

> *The autonomous workforce is coming. The only question is whether enterprises will manage it as software or as a workforce.*