Workato Enterprise MCP: Executive Positioning

November 11 2025

THE STRATEGIC IMPERATIVE

Workato will transform into an AI first company by establishing **Workato Enterprise MCP as the foundation for AI that works**—capturing AI spend by becoming the platform for enterprises to deliver AI agents—built on any agent toolkit – that are secure, scalable, and accurate.

This requires consistently positioning ourselves as the essential foundation for agentic transformation, winning CIO mindshare, and building the category we're defining: **Enterprise MCP as the modern orchestration infrastructure for the agentic era.**

THE MARKET OPPORTUNITY

Today's AI is stochastic, not systematic—confidently wrong when CIOs need predictably right. AI can't access most business data, doesn't understand context across systems, and can't take secure, governed actions in production.

MCP (Model Context Protocol) is emerging as the "TCP/IP of the agentic era"—16,000+ servers built, adopted by Anthropic, OpenAI, and Cursor. It's becoming the standard way agents discover and use tools. **But MCP alone can't make agents enterprise-ready.** Like early TCP, it provides communication primitives but lacks what enterprises actually need. Agents get raw database access instead of proven business processes. They can call individual APIs but can't orchestrate multi-system workflows with transactional integrity. And they operate without embedded security, governance, or compliance—exposing enterprises to security threats, data breaches, compliance violations, and operational failures.

The opportunity isn't to connect AI to systems—it's to govern how AI + agents interact with the enterprise. **It's the difference between "access" and governed action to act safely, predictably, and at scale.**

TAM: The iPaaS market exceeded $9 billion in 2024 and will reach $17 billion by 2028 (Gartner). The market for AI Orchestration is expected to be significantly larger, projected to reach $30 billion by 2030 from USD $11 billion in 2025, at a CAGR of 22.3%(Marketsandmarkets) Workato is well positioned to take significant share in both these large categories.

WHO WE ARE & WHAT WE'RE BUILDING

Workato delivers enterprise infrastructure for the agentic era, redefining iPaaS and helping enterprises unify data, applications, processes and AI into a single, governed platform. Trusted by 50% of the

Fortune 500, Workato's cloud-native architecture connects every application, data source, and process to power real-time orchestration at scale. With enterprise-grade security and continuous innovation at its core, Workato provides the trusted foundation for organizations to automate with confidence and operationalize AI across the business.

Key Platform Advantages

- **Universal connectivity:** Connect any data, system, file, or AI service—structured or unstructured, cloud or on-prem.
- **Deep orchestration:** Coordinate logic, data, and AI reasoning across end-to-end processes with transactional control.
- **One cloud-native runtime:** Serverless, decoupled architecture that upgrades in place with no downtime or rework.

Workato isn't just keeping up with the AI era—it's the infrastructure that makes **enterprise AI secure, scalable, and accurate.**

WORKATO ENTERPRISE MCP

The world's first platform purpose-built to deliver AI agents that are secure, scalable, and accurate.
We close the enterprise control gap by giving any agent or LLM governed, auditable access to real business context and workflows.

Agents need to be..	Secure	Scaleable	Accurate
What we offer	**Enterprise Trust** *Confidence and compliance*	**Enterprise Orchestration** *Coordination across systems*	**Enterprise Skills** *Execution you can trust*
What makes us different	Embeds *security, governance, and compliance* at every layer — ensuring every agent action is authenticated, authorized, and auditable. Security and governance aren't bolt-ons. Workato enforces scoped credentials, RBAC, PII obfuscation, encryption, and full audit trails across all agent	Gives agents *context and control* — the ability to act across multiple systems, data sources, and teams with full understanding of business logic and state. While basic MCP connects to individual APIs, Workato orchestrates complete business outcomes. One platform to orchestrate processes spanning Salesforce, NetSuite, Workday, and beyond.	Gives agents *repeatable, trusted actions* — proven business workflows that execute the same way every time. Instead of raw API calls, Workato enables thousands of tested Enterprise Skills (like "process refund" or "approve PTO"). Each Skill encapsulates logic, approvals, retries, and error handling so agents perform consistently. These are the building blocks of predictability that enable AI

	interactions. Compliance with SOC2, PCI, and ISO standards is built in — so every AI action is safe, explainable, and compliant by design.	Context is built in: data, real-time signals, and intent are all managed transactionally and auditable.	trust in enterprise environments.

COMPETITIVE POSITIONING

For enterprises seeking to become agentic, Workato Enterprise MCP is **the only platform** that transforms AI agents from experimental to essential by providing accurate business processes, secure enterprise orchestration, and scalable infrastructure—unlike basic MCP servers that expose the "Enterprise Control Gap."

- **vs. Traditional iPaaS:** "They bolt AI onto aging runtimes that create IT bottlenecks and maintenance debt. Enterprise MCP is built on a cloud-native, decoupled runtime that unifies integration, orchestration, and governance for the agentic era."
- **vs. Agent Platforms:** "They host agents. Enterprise MCP governs them — authentication, observability, and safe execution across every enterprise system."
- **s. Point Solutions (App-specific MCP):** Safe but shallow. No orchestration—just app access and limited context. Enterprise MCP ensures agents and apps act *together* across multiple systems, according to trusted, secure, and proven Enterprise Skills.
- **vs. Open Source (DIY MCP):** "DIY MCP runs code. Enterprise MCP runs enterprises — with audit, encryption, and compliance built in."

OUR VALUE BY PERSONA

For CIOs and IT Executives
Move AI from concept to control. Enterprise MCP gives you the governance framework to operationalize agents and AI across the business — safely, predictably, and at scale.

- End pilot purgatory with a platform built for production-AI and real ROI
- Standardize how every AI system connects, acts, and is audited
- Modernize legacy integration foundations for the agentic era

For AI, Innovation, and Transformation Leaders
Turn AI from experimentation into execution. Enterprise MCP provides the production backbone to bring LLMs, copilots, and agents into real business operations with trust and observability.

- Govern how AI accesses data and performs actions across systems
- Rapidly convert proven business processes into reusable, agent-ready skills
- Confidently move from prototype to enterprise deployment

For Line-of-Business Leaders
Build agents that move the business, not just productivity hacks. Enterprise MCP connects AI directly into the systems and processes that define your function — sales, finance, HR, operations — all under enterprise guardrails.

- Build meaningful, process-integrated agents with enterprise context
- Leverage governed Skills that safely access real data and actions
- Innovate faster without bypassing IT or security controls

For Developers and Technical Builders
Unblock innovation without losing trust. Enterprise MCP gives you full freedom to use any model, framework, or tool — within a governed, observable runtime built for production scale.

- More freedom to innovate, less friction to deploy — creativity and control in one platform.
- Build your way — low-code, pro-code, or vibe code — without being boxed in by platform constraints.
- Try new tools, models, or AI frameworks without infrastructure overhead or integration rewrites.
- Turn experiments into production-ready systems through built-in security, observability, and scalability.

For Security and Compliance Teams
Every action. Every identity. Fully governed. Enterprise MCP embeds zero-trust principles directly into AI orchestration — so agents, systems, and humans all operate within enforceable policy.

- Continuous authentication and least-privilege access at runtime
- Centralized audit trails, encryption, and key management
- Compliance aligned with SOC, ISO, PCI, HIPAA, and GDPR standards

---

THE PATH FORWARD

Strategic Imperative: Reposition from "iPaaS vendor" to "Enterprise AI infrastructure company"—unlocking premium pricing and CxO-level buying to drive AI revenue from $6M to $250M+ at 40-50% YoY growth.

Execution: Prove value with existing customers → Win new enterprise logos → Build ISV ecosystem → Drive mainstream adoption. **The platform where AI gets to work.**

Workato Enterprise MCP: Messaging Framework

Platform Overview

Platform	Workato Enterprise MCP
Who We Are	Workato, The Enterprise MCP Company
TL;DR	Enterprise MCP is the new iPaaS+/Enterprise Orchestration for the agentic era. Enterprise MCP allows us to not only serve our existing base (Orchestrate-first), but vastly expands our relevance to a new, Agentic-first buyer/market as well.
Category	PALO ALTO, Calif.--(BUSINESS WIRE)--Workato®, **the Enterprise MCP Company,** today announced… PALO ALTO, Calif.--(BUSINESS WIRE)--Workato®, **the leader in Enterprise MCP,** today announced… PALO ALTO, Calif.--(BUSINESS WIRE)--Workato®, **the industry's first Enterprise MCP company,** today announced…
Headline	Orchestration for the Agentic Era—Powered by the #1 iPaaS.
Tags	95% of GenAI projects fail. Join the 5% that don't. - Only Workato Enterprise MCP makes your AI agents **secure, scalable and accurate—**Built on the #1 iPaaS.
Short Description	

The Problem Enterprise MCP Solves

Universal Problem Statement:
AI agents cannot execute reliable business processes by calling raw APIs.

The Reality:
Resetting a password requires 8 API calls across 3 systems with conditional logic, retry handling, and audit trails. Processing a refund involves data validation, approval workflows, inventory updates, and financial reconciliation. AI calling these as individual API endpoints introduces unpredictability, security gaps, and operational risk.

What's Missing:
The orchestration layer that transforms API primitives into repeatable, governed business operations. Without it, AI remains experimental—incapable of automating core processes that run your business.

Two Go-To-Market Motions

Motion	Agentic-First	Orchestrate-First
Audience	**New AI-First Buyer - CIO, Chief AI Officer, VP, AI & Innovation** Executives and teams leading large-scale AI or agentic transformation initiatives who may not know iPaaS or orchestration at all**.**	**Existing IT Buyer - CIO, VP Engineering, CTO.** Our existing enterprise orchestration buyers—IT, integration, and platform teams already evaluating iPaaS, BPM, ETL, or APIM.

Narrative	**Lead with "Enterprise MCP" as the missing layer** connecting AI to real systems, context, and governance. Message interoperability with existing stack (MuleSoft, UiPath). Bridge LLM reasoning to business action..	**"Enterprise MCP"** is the next gen, AI-ready orchestration platform—the foundation for AI adoption even for teams integrating Salesforce, NetSuite, or Workday. Show how enterprise MCP makes Workato AI-relevant while maintaining IT infrastructure customers already value.
Description	**Workato Enterprise MCP is the platform that makes agents work.** It gives any AI the context, continuity, and control to act inside your enterprise systems with trust and precision. Built for interoperability, governance, and scale, Enterprise MCP bridges your existing stack with any AI framework—turning isolated intelligence into accurate enterprise actions.	**Workato Enterprise MCP is enterprise orchestration evolved for the modern era**—unifying integration, automation, and AI governance on cloud-native infrastructure. Transform brittle integrations into reusable Enterprise Skills, orchestrate with transactional integrity, and deploy with embedded security.

Two Entry Points

EMCP for Agentic-First

	What Workato EMCP Delivers
ed trust, visibility, or control e MCP servers and frameworks are —no identity, RBAC, observability, or With no governance, monitoring, or ctions become risky, opaque, and o approve for real business use	**Trust & Security** Observability and monitoring for every decision, action, and outcome—with audit logs, policy enforcement, and more.

erprise context and scale	**Orchestrated Context**
on't exist in any single app or ut often across multiple apps, ata sources, and real-time signals.	Connects data, apps, and processes across the enterprise, giving AI the context and coordination to reason, act, and deliver real outcomes.
ovise or hallucinate s their way through work—calling raw vering results that are often confidently sing context and real-time signals.	**Enterprise Skills** Trusted, pre-orchestrated business actions give agents accurate, reusable building blocks—grounded in enterprise truth instead of ad-hoc APIs.

Bridge to Orchestrate-First: When agents fail, it's rarely the AI model—it's the infrastructure underneath. The "agent problem" is actually an orchestration problem. Fragmented systems, brittle integrations, and ungoverned data flows make agents confidently wrong. Fix the orchestration layer, and agents become predictably right.

EMCP for Orchestrate-First

	What Workato EMCP Delivers
tions & legacy platforms aS, RPA, and ETL tools create silos, l rising technical debt.	**Unified Platform** Replace redundant integration, automation, and API tools with a modular, open platform—eliminating overlap, tech debt, and vendor lock-in.
costs & IT bottlenecks requirements, long release cycles, and enance and rework drive up costs and ty.	**Modernization & Agility** Cloud-native and serverless to cut cost and boost speed—no maintenance, downtime, or specialized developers required.
AI & agentic initiatives	**Foundation for AI & Agentic**

	Designed for the future—where AI and orchestration work together through a secure, governed orchestration fabric.
rapped in silos—88% cite data, governance gaps with only 5% seeing pact.	

Bridge to Agentic-First: Solve today's integration pain and be ready when agents arrive. Your integration stack wasn't built for intelligent workloads—when AI tries to orchestrate across your systems, it exposes every integration gap you've been working around.

Three Value Pillars

What Agents Need	What We Offer	Value
CONTEXT	Orchestrated Context	Agents get all required context: data, processes, and real-time signals from every relevant application.
TRUST	Trust & Security	xComplete observability and access control—with role-based permissions, audit logs, and policy enforcement built-in.
ACCURACY	Enterprise Skills	Accurate, predictable business actions agents can use to execute complete business actions.

TRUST: Trust & Security

Why It Matters

Problem: Open-source MCP servers lack identity, RBAC, observability, and auditability.

What It Is

Enterprise Trust is the comprehensive security, governance, and compliance architecture embedded at every layer of the platform—ensuring every agent action is authenticated, authorized, and auditable.

Impact: CISOs approve deployment, compliance is automatic, security scales with AI, breaches are preventable.

Technical Architecture:

- Runtime user authentication (patented) - Agents inherit user permissions
- Role-based access control (RBAC) - Least-privilege enforcement at platform level
- Automatic PII obfuscation - Sensitive data masked before agents see it
- Immutable audit trails - Every action logged with full forensic traceability
- Field-level security - Control what data crosses into LLM context
- Compliance certifications - SOC2, PCI, ISO standards built into infrastructure

Value Statements

- **Zero-Trust by Default**
  Every agent action is authenticated, authorized, and auditable with least-privilege access
- **Compliance That Scales**
  SOC2, PCI, ISO—pre-built and built-in. Every action leaves a traceable audit trail that satisfies regulators, boards, and CISOs alike.
- **Observable & Governed**
  Full visibility into every action and decision, with policies and permissions enforced at runtime to prevent unsafe behavior before it happens.

Proof Points

- 50% of Fortune 500 trust Workato
- Patented runtime user authentication
- RBAC at platform level
- Automatic PII obfuscation
- Immutable audit logs
- SOC2/PCI/ISO certified

CONTEXT: Orchestrated Context

Why It Matters

Problem: Agents see fragments—one app or database at a time—not a complete picture across systems, processes, data sources, and real-time signals. For example: quote generation requires Salesforce + NetSuite + approvals + contracts. Separate API calls = no completion awareness, no rollback, lost context, partial state.

What It Is

Enterprise Orchestration is the governed, stateful runtime that coordinates data, logic, and AI reasoning across every system, team, and process with transactional control and persistent context.

Technical Architecture:

- Stateful execution (agents don't lose context mid-workflow)
- Transactional integrity (all steps complete or roll back cleanly)
- Real-time signals (events, data changes, triggers coordinated)
- Multi-system coordination (one business outcome = many systems working together)
- Persistent memory (workflow state maintained across sessions, systems, outages)

Value Statements

Full Enterprise Context
Gives AI a real-time view of how data, decisions, and people connect—enabling multi-step reasoning across the business.

Process Coordination
Sync logic, status, and real-time data across systems—turning disconnected workflows into end-to-end business outcomes.

Coordinated Intelligence
Blends deterministic control with adaptive reasoning—so AI acts with precision and purpose.

Why It Matters

Problem: They see fragments—one app or database at a time—not a complete picture across systems, processes, data sources, and real-time signals. For example: quote generation requires Salesforce + NetSuite + approvals + contracts. Separate API calls = no completion awareness, no rollback, lost context, partial state.

Proof Points

- 50% of Fortune 500 trust Workato
- 12,000+ connectors to enterprise systems
- SentinelOne: 10x faster quote generation across CRM + ERP
- Production results across complete workflows
- Cloud-native runtime scales automatically

ACCURATE: Enterprise Skills

What It Is

An Enterprise MCP Skill is an atomic, indivisible unit of real work—complete, durable workflows that execute predictably every time. Unlike raw API calls, Skills encapsulate:

- Business logic (not just connectivity)
- Approval workflows (governance built-in)
- Error handling & retries (resilience)
- Transactional integrity (all-or-nothing)

Examples: process_refund, create_quote, onboard_employee, approve_purchase_order

Our Enterprise MCP offering includes:

- **Skill Builder:** A low-code designer for creating new Enterprise Skills—packaging logic, approvals, and error handling into reusable business actions.
- **Skills Library:** Governed catalog where teams can discover, share, and manage approved Enterprise Skills.
- **MCP Composition:** The ability to compose MCP servers from
- **MCP Gateway:** The secure bridge that exposes Enterprise Skills to any AI agent or framework—making them instantly callable through the Model Context Protocol.

Enterprise Skill Packs are curated collections of Enterprise Skills organized by industry vertical, business function, or common use case. They can be used by business users in AI tools like ChatGPT and Claude and also by Builders of custom agents. They will be sold as add-ons to Workato Enterprise MCP.

Pricing and Packaging:

Value Statements

- **The Atomic Building Block of Work**
  Each Enterprise Skill replaces multiple API calls, business logic, and error handling—packaged as a single, trusted business capability, like process refund, approve payment, and reset password.
- **From APIs to Accurate Enterprise Actions**
  Built-in retries, rollbacks, and state management ensure that outcomes are consistent across teams, agents, and systems—every time.
- **Security Built-In**
  Enforce access controls, data masking, regulatory requirements by design

Why It Matters

Problem: Today's AI is stochastic—confidently wrong, guessing through work, and reinventing new solutions every prompt instead of being accurate. **Impact**: Agents become reliable (same input = same output), trust becomes earnable, deployment becomes possible.

Proof Points

- SentinelOne: 10x faster quote generation
- Samsara: 40% autonomous helpdesk
- Complete business logic with consistent execution
- Access proven processes from Fortune 500

Competitive Positioning

Universal Statement: *For enterprises seeking to become agentic, Workato Enterprise MCP is the only platform that transforms AI agents from experimental to essential by providing accurate business processes, secure enterprise orchestration, and scalable infrastructure—unlike basic MCP servers that expose the "Enterprise Control Gap."*

Comparison	Them / The Challenge	Workato Positioning
vs. DIY/Open Source MCP (e.g. Self-hosted)	*"We can build this ourselves"* Community-driven; no SLA or vendor support, security unverified. DIY setup for auth, secrets, and logging; no unified SSO or RBAC. SOC 2 only on Enterprise Cloud; compliance and governance self-managed. Git-based deployment requires CI/CD and infra expertise	**"DIY MCP runs code. Enterprise MCP runs enterprises—with audit, encryption, and compliance built in."** You could build it—12-18 months. Workato has 12+ years of enterprise orchestration built in. Question is: spend a year building infrastructure, or deploy agents this quarter? **Discovery questions:** 1. "How many months are you planning to invest building auth, policy, audit, and Skills library before the first agent connects safely?" 2. "What's your plan for maintaining compliance certifications and security updates as MCP evolves?"
vs. App/Vendor MCP (e.g. Workday, ServiceNow)	*"We already have MCP from our vendor"*	**"Safe but shallow. No orchestration—just app access. Enterprise MCP ensures agents act together across multiple systems."**

	Vendor lock-in. Limited to their ecosystem. Can't orchestrate across your full stack. Security is policy-driven, but agent safety requires manual setup.	Vendor MCP gives you access to *their* app. Enterprise MCP orchestrates across *all* your systems—Salesforce, NetSuite, Workday, and beyond. **Discovery Questions:** 1. "How many systems beyond [Workday/ServiceNow] do your agents need to access?" 2. "What happens when you need agents to orchestrate across multiple vendor systems?"
vs. In-App Agents (Copilot, Joule, Rovo)	*"We already have an agent for that."* Sure, but you can't have 1,000 agents trapped inside single applications. No cross-system context or orchestration. Can't access enterprise data outside their native app.	**"They host agents. Enterprise MCP governs them—authentication, observability, and safe execution across every enterprise system."** In-app agents are productivity tools trapped in silos. When you need agents to orchestrate across Salesforce, finance systems, and support tools—that's where Enterprise MCP comes in. **Discovery Questions:** 1. "What happens when [Copilot] needs to access data in systems outside Microsoft 365?" 2. "How many in-app agents would you need to deploy to cover your entire enterprise stack?"

vs. LOB Point Solution Agents (Piper SDR) **Important Note:** this positioning is best suited for an IT audience (not LOB leader) as they tend to purchase deep point solutions that serve their business needs.	*"We already have [Piper/point solution] and it works for our team"* Expensive per-agent licensing. Limited to one function (e.g., SDR outreach only). No platform for reusability or building additional agents across functions. Cost multiplies as you add agents for other departments.	**"Point solutions solve one problem. Enterprise MCP solves the category."** Piper does SDR outreach. What happens when finance, support, HR, and operations all need agents? With Enterprise MCP, you build the foundation once and extend agents across every function—not buying separate point solutions for each department. **Discovery Questions:** 1. "Beyond [SDR/specific use case], what other functions are asking for agents?" 2. "What's your platform strategy when you need agents in finance, support, HR, and operations?"
vs. Agentic Platforms (Agentforce, N8n)	*"We're already using [Agentic Platform]"* No pre-built MCP servers/tools—must generate from existing APIs. High developer dependency. Limited enterprise governance and security controls.	**"They build agents. Enterprise MCP makes agents enterprise-ready."** Perfect—we're not replacing them. We're the orchestration and trust layer underneath. You keep your agents; we make them safe to deploy with governance, context, and proven Skills **Discovery Questions:** 1. "Who's responsible for ensuring agents can only access appropriate data across systems?" 2. "How do you audit what agents are doing across your enterprise?"

vs. iPaaS MCP (Boomi, Mule)	*"We already have an iPaaS"* MCP Server connector announced but not GA. High developer dependency for agent access. Governance is manual. Security setup is hands-on. Legacy architectures slow to adapt to MCP.	**"They bolt AI onto aging runtimes that create IT bottlenecks. Enterprise MCP is built on cloud-native infrastructure for the agentic era."** Boomi and Mule were built for yesterday's integration challenges. When MCP emerged, Workato rapidly delivered 100+ pre-built, enterprise-ready MCP servers. Legacy platforms force customers to build and maintain their own MCP infrastructure. **Discovery Questions:** 1. "How long has [Boomi/Mule] been promising MCP support versus having production-ready servers?" 2. "Are you managing the infrastructure for [Boomi/Mule] or is it fully serverless?"

Social Proof Topic Source Quotes

Company + Messanger	Quote	Resources
.monks Laurent Farci, Chief Information Officer	"MCP is quickly becoming the standard for how AI works with corporate applications. With Workato Enterprise MCP, organizations can instantly unlock business capabilities with AI in a secure way from	LINKEDIN

	day one," said Laurent Farci, Chief Information Officer at .monks. "Workato already orchestrates critical processes across our business — from sales opportunity management to employee onboarding and IT project management. With Enterprise MCP, we can now transform our business processes into AI-ready services at speed and scale, giving us the confidence to use AI to move faster than ever."	
Anthropic Theo Chu, Product Manager	"We're excited to see the Model Context Protocol (MCP) transforming Workato's approach to enterprise workflow automation. With Workato's Enterprise MCP offering, Claude brings more intelligent, context-aware automation to the enterprise," said Theo Chu, Product Manager at Anthropic.	Press Release

Nasdaq Angela Stewart, VP	"MCP is the universal bridge between AI and enterprise action-unlocking secure, governed, and instant access to business capabilities. Workato is leading the charge in MCP by creating a standard for organizations to turn their systems, data, and processes into AI-ready services with limitless innovation."	LINKEDIN