

Building Agents? Stop Re-creating the Wheel.



Enterprise IT teams are losing months of velocity attempting to rebuild foundational logic, security layers, and data context outside Workday just to make agents functional.

Re-creation traps that are slowing you down.

Identity & Permissions (Security):

Re-architecting fine-grained user access rules so agents don't expose sensitive employee, payroll, or financial data to unauthorized users.

Business Process Logic (Workflow):

Hardcoding approval workflows, routing rules, and validation logic into custom application code rather than triggering established enterprise processes.

Data Context & Schema Mapping (Data):

Manually exporting, cleaning, and feeding static data into LLMs, forcing agents to operate on outdated or incomplete operational context.

Audit Trails & Governance (Compliance):

Building custom logging pipelines to record every prompt, response, tool call, and system action for auditability.

API & Connector Maintenance (Integration):

Writing, testing, and maintaining brittle point-to-point integration scripts that break whenever data schemas update.

Human-in-the-Loop Controls (Trust):

Patching together custom UI prompts to halt autonomous execution for high-stakes decisions requiring manager or HR approval.

The Hidden Cost

Stop wasting developer velocity rebuilding security and governance infrastructure you already own.

Bridge to Solution:

Deploy Custom Agents with Workday Extend that automatically inherit your existing security, user permissions, data models, and business processes on day one.

The solution — Workday Extend.

Build with Speed:

✓

Force Multiply Your Builders:

Use Developer Agent to write code, wire components, and create agent skills from plain-language prompts.

✓

Deep domain expertise and native AI skills to build on Workday:

Accelerate builds with purpose-built developer skills across apps, orchestrations, and APIs.

✓

Bring Your Own Tools:

Allow engineering teams to build in their preferred IDEs (e.g., Claude, Cursor, Antigravity) or directly inside Workday.

✓

Choose Your Framework:

Build Custom Agents using Google ADK, TypeScript or your framework of choice.

Run with Trust:

✓

Grounded in live context:

Understanding organizational hierarchies, skills, and active business rules to increase confidence in agent outcomes.

✓

Always-On Enterprise Guardrails:

Execute agents on the Workday Trusted Agent Platform, inheriting live user permissions, business process controls, and audit logs.

✓

Reach Any System or Surface:

Deploy across your enterprise stack—natively in Workday or through external tools like Microsoft Copilot or Google Gemini.

Stop writing brittle APIs — use Workday Agent-Ready Tools.

Your engineers already know Model Context Protocol (MCP) standards are the future of agentic integration. Workday Extend brings enterprise guardrails to those open standards.

	Traditional APIs	Workday Agent-Ready Tools (MCP)
Architectural Purpose	Static point-to-point scripts that break when schemas update.	Built for Agentic Reasoning: Dynamic, low-latency access engineered specifically for autonomous AI execution & inter-agent communication.
Business Context	Raw data payloads that force LLMs to guess operational context and rules.	Injected World Context: Automatically passes relevant context information, such as org hierarchies, user permissions, and active approval chains - directly to the prompt.
Governance & Safety	Requires heavy custom code to prevent unapproved write actions.	Inherent Guardrails: Automatically separates read lookups from high-stakes write actions with full audit trails built in.
Identity & Trust	Shared API tokens or static keys that bypass user-level security.	Agent System User & Passport: Assigns unique agent identities with OWASP-verified security stamps and least-privilege scoping.

Stop Rebuilding Guardrails. Start Shipping Governed AI.

Explore Workday Extend

Schedule a Demo