>_ AgentRails

Enterprise Architecture Guide

Copilot Studio, MCP Servers, Power Platform, and x402 Payments

February 2026

www.agentrails.io

Architecture Overview

AgentRails enterprise deployments integrate across the full Microsoft 365 stack. The architecture connects Copilot Studio agents to internal systems via MCP (Model Context Protocol) servers, orchestrates workflows through Power Automate, stores governance data in Dataverse, and enables autonomous payments via the x402 protocol.

Core Components

- **Copilot Studio** -- Build and deploy custom AI agents with governed capabilities in Microsoft Teams
- **MCP Servers** -- Model Context Protocol servers provide scoped, secure access to internal data and APIs
- **Power Automate** -- Orchestrate approval workflows, escalation paths, and compliance reporting
- **Dataverse** -- Central store for agent state, policies, audit logs, and security roles
- **x402 Payment Layer** -- Autonomous USDC payments with enterprise spending controls
- **Admin Dashboard** -- Next.js management console for agents, transactions, policies, and audit logs

Copilot Studio Integration

AgentRails provides two pre-built Copilot Studio action sets that can be imported directly:

FinanceOps Actions

Revenue queries, transaction search, payment analytics, and spending reports. Finance teams ask natural-language questions in Teams: "What's our x402 revenue this month?" The copilot calls the AgentRails API and returns formatted results with charts.

Agent Executor Actions

Agent management, policy enforcement, kill switches, and status monitoring. Operators manage agents conversationally: "Pause research-agent-01" or "Show agents over their spending limit."

MCP Server Architecture

Model Context Protocol servers act as secure bridges between Copilot Studio agents and your internal systems. Each MCP server exposes a scoped set of tools that agents can invoke, with authentication, rate limiting, and audit logging built in.

- **Data access** -- Query internal databases, CRMs, ERPs without exposing connection strings
- **API orchestration** -- Compose multi-step API calls into single agent-friendly tools
- **File operations** -- Read/write documents in SharePoint, OneDrive with proper permissions
- **Custom logic** -- Business rules, calculations, validations specific to your domain

Governance Framework

AgentRails enforces governance at every layer:

Spending Policies

- Per-agent budget limits (daily, weekly, monthly)
- Per-transaction caps
- Destination address whitelists
- Rate controls (max transactions per minute/hour)

Security Roles (Dataverse)

- **System Admin** -- Full access to all agent and payment operations
- **Finance Manager** -- Revenue reports, spending policies, transaction queries
- **Agent Operator** -- Agent lifecycle management, status monitoring, kill switches
- **Auditor** -- Read-only access to audit logs, transaction history, policy changes
- **Read-Only Viewer** -- Dashboard viewing only

Audit Trail

Every agent action, payment, and policy change is logged with timestamps, user identity, and on-chain transaction hashes. Logs are stored in Dataverse and can be surfaced via Power BI dashboards or queried through the Copilot Studio FinanceOps actions.

Deployment Options

Hosted (Pro Tier)

AgentRails runs the x402 facilitator, API server, and admin dashboard. You connect your Copilot Studio agents via the OpenAPI connector. Best for teams that want fast time-to-value without infrastructure management.

Self-Hosted (Enterprise Tier)

Full source code deployed on your own infrastructure. ASP.NET Core 8.0 API with PostgreSQL, deployed to Azure App Service, Azure Container Apps, or any Docker host. Includes policy engine, admin dashboard, and all Copilot Studio integrations. Best for regulated industries or organizations requiring full data sovereignty.

Open Source Repositories

- agentrails-powerplatform-demo -- Custom connector (24 ops), Power Automate flows, solution package
- agentrails-copilot-actions -- FinanceOps + Agent Executor Copilot Studio actions
- agentrails-dataverse-integration -- Table definitions, sync flows, security roles

Book an Architecture Review

We offer 2-week assessment engagements to audit your M365 environment, map agent use cases, and design the governance framework. Contact sales@agentrails.io