willow vs Archestra.AI

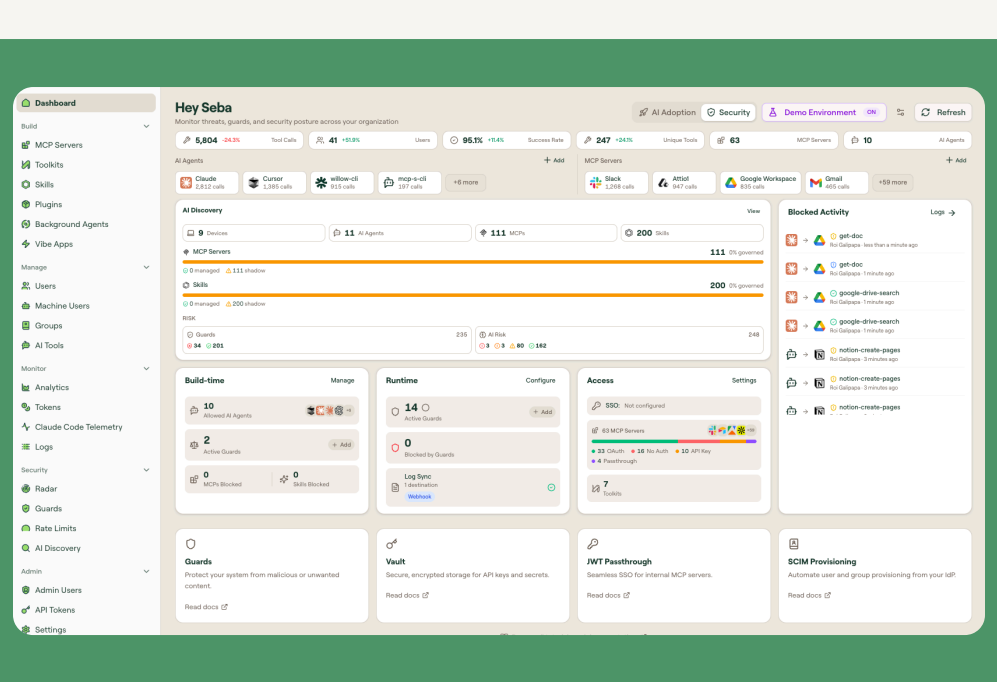
Willow vs. Archestra: Managed Platform vs. K8s-Native Open Source

Archestra is open-source with Kubernetes orchestration and Dual LLM security. Willow is a managed access control plane with employee self-service, machine users, and IT workflows proven at 5,000+ employees.

Get Started → Book a Demo

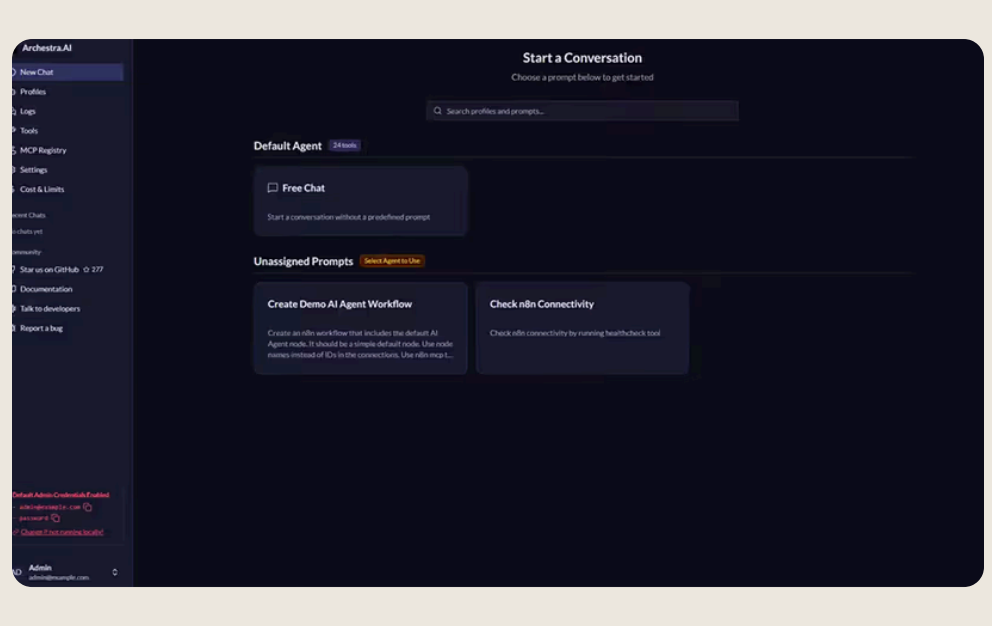
Trusted by

WIX agora papaya global innovi



Willow Admin Console

Managed access control plane. Employee self-service, machine users, IT approval workflows, and 5,000+ employee deployments.



Archestra Control Plane

Open-source K8s-native platform. 858+ MCP servers, Dual LLM prompt injection protection, Prometheus/OpenTelemetry observability.

The Bottom Line

Archestra is open-source with 858+ MCPs and innovative AI security (Dual LLM, Dynamic Tools). Willow is a managed platform with employee self-service, machine users, and IT workflows battle-tested at scale.

Best for Willow

Enterprises needing managed deployment with employee enablement and machine users.

Best for Archestra

K8s teams wanting open-source with extensive MCP catalog and advanced AI security.

Key Differentiator

Willow offers managed deployment with employee self-service and machine users. Archestra provides open-source K8s infrastructure with Dual LLM security.

Feature Comparison

Feature	Willow Access Platform	Archestra.ai
Architecture	Access Control Layer—manages deployment for you	MCP Pipe—self-managed K8s infrastructure
Deployment	SaaS, on-prem, or air-gapped	Docker (dev), Kubernetes + Helm (prod)
Licensing	Commercial	Open source (free)
Authentication	OAuth2, OIDC, SAML, JWT, SSO (Okta/Entra/JumpCloud)	OAuth 2.0 + PKCE
Identity & Access	RBAC, SCIM, Groups, Auto-provisioning	RBAC, tool policies, per-identity rate limits
Machine Users	Service accounts for automation	Not supported
MCP Catalog	100+ curated MCPs + API-to-MCP	858+ built-in MCP servers
Employee Portal	Self-service + toolkit creation	ChatGPT-like chat interface
IT Approval Workflows	CISO approval, sandboxed testing	Not supported
Observability	Splunk/Loki/Grafana integrations	Prometheus + OpenTelemetry native
AI Security	Policy guardrails, 3rd party integrations	Dual LLM, Dynamic Tools for prompt injection
Compliance	SOC 2 certified	SOC 2 certified

Get Started → Book a Demo

Fit Check

Who Each Solution Is Best For

Willow is Best For

Enterprises needing managed deployment with employee enablement. Ideal if you:

- Need production-proven deployments at 5,000+ scale
- Require employee self-service for faster adoption
- Need machine users for automated AI workflows
- Want quick SSO/SCIM setup with Okta, Entra, JumpCloud
- Prefer managed infrastructure without K8s expertise

Best for Archestra

K8s teams wanting open-source with extensive MCP catalog and advanced AI security.

- Prefer open-source with full source access
- Have DevOps comfortable with Kubernetes and Helm
- Need 858+ built-in MCP servers
- Want Dual LLM and Dynamic Tools prompt injection protection
- Need Prometheus/OpenTelemetry observability

Deployment & Infrastructure

Managed platform vs. self-hosted K8s infrastructure.

Willow offers managed deployment:

- **SaaS or On-Prem:** SOC 2 compliant, no K8s required
- **Air-Gapped:** Fully isolated environments supported
- **Rapid Setup:** Deployments completed in days
- **Managed Updates:** Vendor handles infrastructure

Archestra provides K8s-native deployment:

- **Kubernetes Production:** Helm charts, 45ms p95 latency
- **Terraform Provider:** Infrastructure-as-code automation
- **Open Source:** Full source code access
- **Self-Managed:** You handle cluster ops and updates

Bottom Line

Both let you run agents, but they optimize for different things. Runlayer optimizes for building agents quickly. Willow optimizes for governing autonomous agents, giving each one its own scoped identity, least-privilege access, and full audit, so security can say yes to unattended work.

Security & Access Control

Enterprise identity vs. AI-specific security features.

Willow delivers enterprise identity:

- **Quick-Start SSO:** Okta, Entra, JumpCloud guided setup
- **SCIM Provisioning:** Automated user lifecycle
- **Machine Users:** Service accounts for CI/CD
- **IT Workflows:** CISO approval, sandboxed testing

Archestra provides AI-specific security:

- **Dual LLM Protection:** Two-agent prompt injection defense
- **Dynamic Tools:** Auto-restricts capabilities on untrusted content
- **Tool-Call Policies:** Per-tool access control
- **HashiCorp Vault:** Secrets with auto-rotation

Bottom Line

Both let you run agents, but they optimize for different things. Runlayer optimizes for building agents quickly. Willow optimizes for governing autonomous agents, giving each one its own scoped identity, least-privilege access, and full audit, so security can say yes to unattended work.

Connectors & MCP Library

Catalog size and customization approaches differ.

Willow provides curated connectors:

- **100+ MCPs:** Slack, Jira, GitHub, Notion, Linear
- **API-to-MCP:** Convert any REST API instantly
- **Employee-Driven:** Teams propose new MCPs
- **Version Control:** Track with rollback

Archestra provides extensive catalog:

- **858+ MCPs:** Largest open-source catalog
- **Private Registry:** Add third-party MCPs
- **Private Registry:** Add third-party MCPs
- **Trust Levels:** IT-verified indicators
- **Version Control:** Full rollback capabilities

Bottom Line

Both let you run agents, but they optimize for different things. Runlayer optimizes for building agents quickly. Willow optimizes for governing autonomous agents, giving each one its own scoped identity, least-privilege access, and full audit, so security can say yes to unattended work.

Employee Experience

Self-service adoption vs. chat-centric interface.

Willow enables self-service:

- **Employee Portal:** Browse MCPs, toolkits, prompts
- **One-Click Connect:** Cursor, Claude, VS Code **instantly**
- **Machine Users:** Agent-to-agent automation
- **No IT Bottleneck:** Self-service discovery

Archestra provides chat interface:

- **ChatGPT-like UI:** Intuitive for all users
- **Multi-Model:** Claude, GPT-4, Gemini, open-source
- **Prompt Registry:** Share prompts org-wide
- **Built-in Chat:** No external AI clients needed

Bottom Line

Both let you run agents, but they optimize for different things. Runlayer optimizes for building agents quickly. Willow optimizes for governing autonomous agents, giving each one its own scoped identity, least-privilege access, and full audit, so security can say yes to unattended work.

Management & Observability

Enterprise analytics vs. cloud-native observability.

Willow delivers enterprise management:

- **Usage Analytics:** Track by team, tool, use case
- **Audit Trails:** Complete compliance logs
- **Cost Visibility:** Token usage monitoring
- **Policy Management:** Per-agent, per-MCP guardrails

Archestra provides cloud-native observability:

- **Prometheus Metrics:** LLM tokens, request duration
- **OpenTelemetry:** Distributed tracing per call
- **Grafana Dashboards:** Pre-configured monitoring
- **Cost Optimization:** Auto model switching (96% savings)

Bottom Line

Both let you run agents, but they optimize for different things. Runlayer optimizes for building agents quickly. Willow optimizes for governing autonomous agents, giving each one its own scoped identity, least-privilege access, and full audit, so security can say yes to unattended work.

Why enterprises pick Willow

We are six to ten months ahead of most companies in AI adoption. More code to production, fewer incidents, real outcomes. Willow is what made it possible to move that fast without slowing down our security posture.

Asaf Yonay
Head of AI Core, Wix

WIX

Wix needed a secure, governed way to connect employees and agents to internal tools, documentation, and workflows. With Willow, the AI Core team built the enterprise MCP infrastructure that now supports nearly 600 tools and 300,000+ weekly tool calls across engineering, product, design, HR, finance, legal, and business teams.

60%
of enterprise AI rollouts stall on security review
Source: Gartner, 2025

84% / 91%
of developers use AI coding tools, with up to 91% of these tools unmanaged or unapproved by IT and security teams
Source: European Cyber Security Organization

Most
enterprises have no visibility into shadow AI usage
Source: IDC, 2025