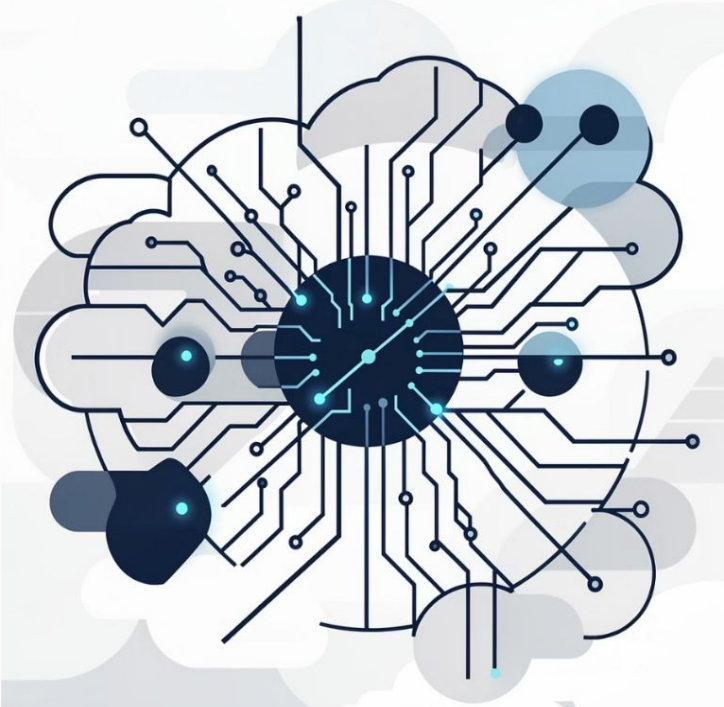
Agentic AI for Multi-Cloud Code Automation

Transform infrastructure intent into production-ready code across AWS, Azure, and GCP—automatically securing, optimizing, and deploying at enterprise scale.



The Multi-Cloud Infrastructure Challenge

Engineering teams face mounting complexity as organizations adopt multi-cloud strategies. Manual infrastructure-as-code development introduces inconsistencies, security gaps, and delays that compound across environments.

Delivery Bottlenecks

Multi-cloud complexity creates weeks of delay for infrastructure provisioning

Error-Prone Manual Code

Hand-written IaC leads to configuration drift and production incidents

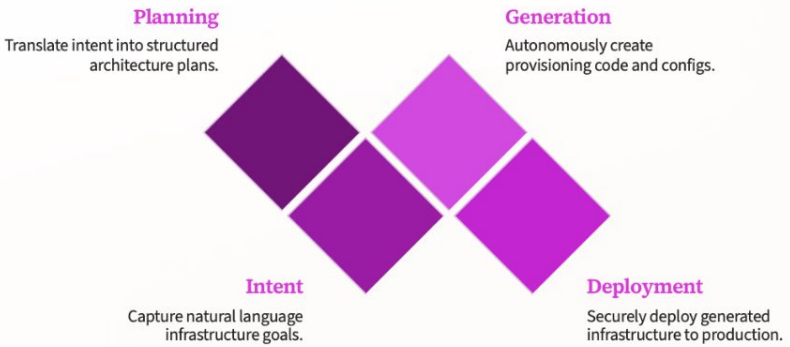
Security as an Afterthought

Compliance and security controls bolted on post-deployment

Runaway Cloud Costs

Over-provisioned resources and inefficient architectures drain budgets

Autonomous Infrastructure Generation



Intent Understanding

Natural language requirements translated into architectural decisions

Production-Ready Code

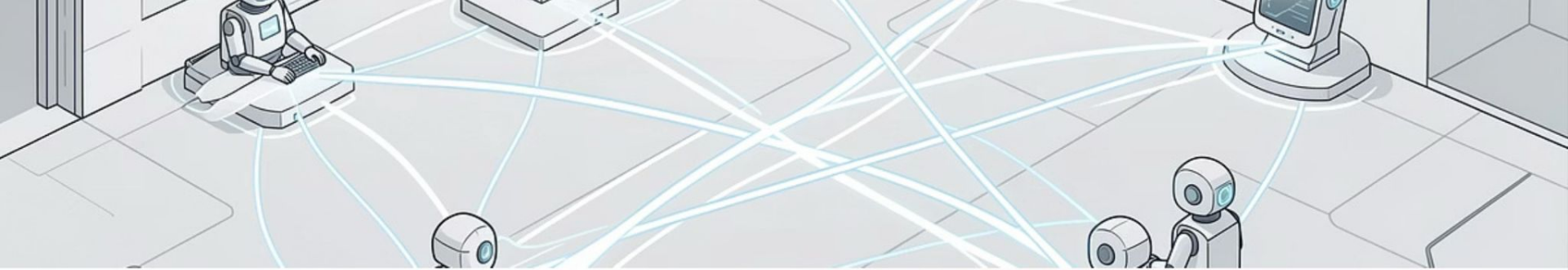
Enterprise-grade IaC with built-in best practices and patterns

Integrated Security

Policy-as-code validation ensuring compliance from day one

Automated Deployment

CI/CD pipelines generated and executed without manual intervention



Understanding Agentic AI

Unlike traditional automation, agentic AI systems operate with autonomy—planning multi-step workflows, selecting appropriate tools, and validating outputs before delivery. Each agent specializes in a domain while coordinating with others to achieve complex infrastructure goals.

01

Goal-Driven Planning

Agents decompose high-level objectives into executable tasks

02

Multi-Step Execution

Autonomous workflow orchestration across infrastructure domains

03

Tool Selection

Dynamic choice of IaC frameworks, SDKs, and deployment methods

04

Output Validation

Automated testing and compliance checks before code delivery

Intelligent Platform Architecture

Input Layer

Natural language requirements and existing repository analysis

Agent Orchestration

Intelligent coordination of specialized AI agents

Specialized Agents

Code generation, security scanning, cost optimization

Execution Layer

IaC provisioning and automated CI/CD workflows

Enterprise Integration

The platform seamlessly integrates with your existing toolchain, Git workflows, and cloud provider APIs. Agent collaboration happens transparently, delivering infrastructure code that follows your organization's standards and governance policies.

Unified Multi-Cloud Experience

Amazon Web Services

EKS orchestration, IAM policy generation, VPC networking, RDS databases, Lambda functions

Microsoft Azure

AKS deployments, Bicep templates, Virtual Networks, Azure SQL, managed identities

Google Cloud Platform

GKE clusters, IAM bindings, VPC design, Cloud SQL, Cloud Functions, GCS storage

Write infrastructure requirements once and deploy to any cloud provider with consistent patterns, security controls, and operational standards. The platform translates your intent into provider-specific best practices automatically.

Enterprise-Grade Code Generation

Modular Architecture

Generated infrastructure follows enterprise patterns with clear separation of concerns. Each module is independently testable, reusable, and maintainable.

Standardized structure ensures teams can navigate, modify, and scale infrastructure confidently across all environments.

Network Layer

VPCs, subnets, routing tables, security groups

Compute Resources

Kubernetes clusters, container services, serverless functions

Security Controls

IAM policies, encryption, secrets management, compliance

Comprehensive Tool Support

Infrastructure as Code

- Terraform HCL and modules
- Pulumi with TypeScript/Python
- Azure Bicep templates
- AWS CloudFormation

Scripting Languages

- Python automation
- Bash scripting
- PowerShell workflows
- Groovy for Jenkins

CI/CD & GitOps

- GitHub Actions workflows
- GitLab CI pipelines
- ArgoCD deployments
- Flux continuous delivery

Cloud Native SDKs

- AWS SDK integrations
- Azure CLI automation
- GCloud command suite
- Kubernetes API clients

Security and Compliance Built-In

1

Least-Privilege IAM

Granular permissions following zero-trust principles

2

Policy-as-Code

Automated compliance validation against industry standards

3

Secrets Management

Encrypted credential storage with rotation policies

4

Audit-Ready Output

Complete traceability and compliance documentation

Security isn't retrofitted—it's embedded in every generated resource. The platform continuously validates against CIS benchmarks, SOC2 requirements, and custom organizational policies before deployment.

Measurable Enterprise Impact

75%

Faster Delivery

Infrastructure provisioning accelerated from weeks to hours

60%

Cost Reduction

Optimized resource allocation and automated right-sizing

95%

Security Compliance

Policy violations caught before deployment

3x

Developer Velocity

Engineers focus on business logic instead of infrastructure

Build at the Speed of Thought

One natural language prompt. Any cloud provider. Production-ready infrastructure that's secure, compliant, and optimized—delivered automatically.

> *"Transform infrastructure intent into reality. Empower your teams to deploy with confidence across AWS, Azure, and GCP—without sacrificing security, compliance, or control."*

THANK YOU