

From Chatbots to Agents

Training Digital Warriors to Govern the AI-Driven Development Lifecycle

Presented By: *Kane Gyovai - Chief Technology Officer*

August 26th, 2026

© 2026 BRIDGEPHASE LLC

BridgePhase

Last Time in Montgomery…

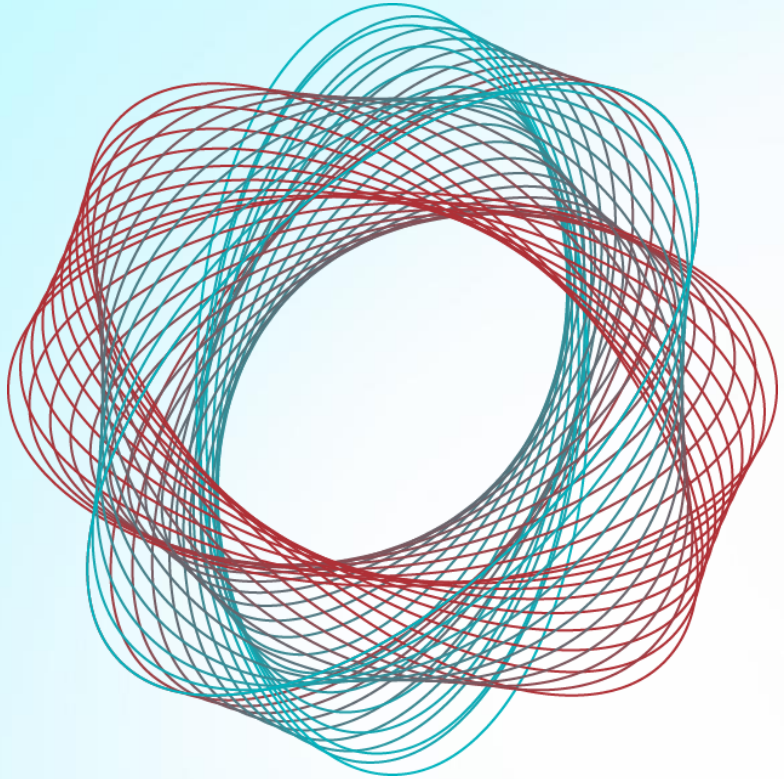


BridgePhase

© 2026 BRIDGEPHASE LLC

Outline

- Introductions
- Learning Objectives
- AI/ML Foundations
- Deterministic vs Nondeterministic Behavior
- Agents & Agentic Workflows
- Software Development Lifecycle (SDLC)
- AI-Driven Development Lifecycle (AIDLC)
- Controls & Tools
- Key Takeaways



© 2026 BRIDGEPHASE LLC

Introductions

About Me

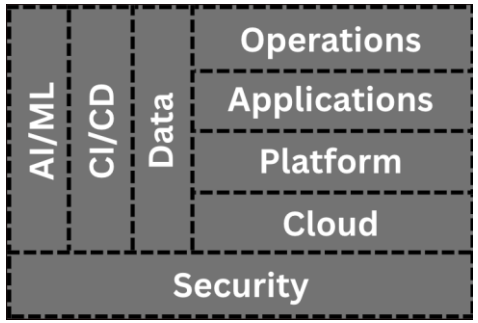
BS, MS - Engineering — West Virginia University

MS - Computer Science (AI-S) — Georgia Tech



Kane Gyovai (Go-Vay)

CTO @ BridgePhase



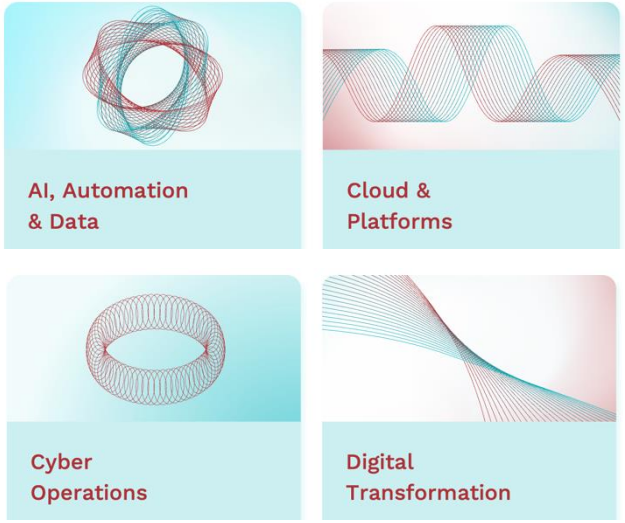
Customers & Projects



DHS AI Task Force 2023-2024

About BridgePhase

- > 140 Engineers & SMEs
- 18+ Years Supporting National Security
- 8+ Years Supporting USAF
- 20,000+ Production Deployments
- Our systems enable:
  - Billions of digital transactions
  - Billions of $ federal revenue
  - National security operations
- >10 Production AI Implementations
  - Computer Vision
  - Anomaly Detection
  - Named Entity Recognition
  - Generative AI (Search, RAG, Ingestion)



Missions Supported

BridgePhase

© 2026 BRIDGEPHASE LLC

Learning Objectives

Understand Agentic Workflows

Describe the shift from basic LLM assistance to hardened autonomous agents while maintaining a human-in-the-loop.

- What is an agent?
- How do we interact with agents?
- How do agents accomplish goals?

Identify the Intersection

Understand the differences between deterministic behavior and nondeterministic behavior.

- Why is this important?
- How do you choose?
- What are the tradeoffs?

Operationalize AIDLC

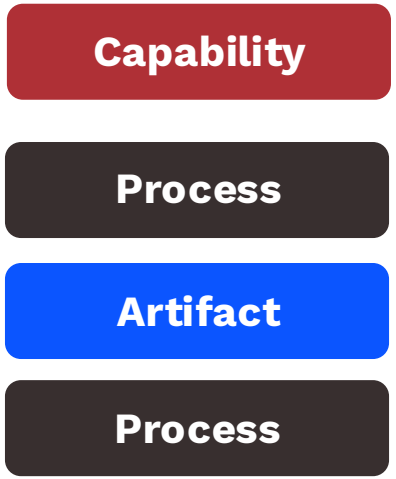
Create a repeatable blueprint for AI-driven development that enhances throughput without compromising security or quality.

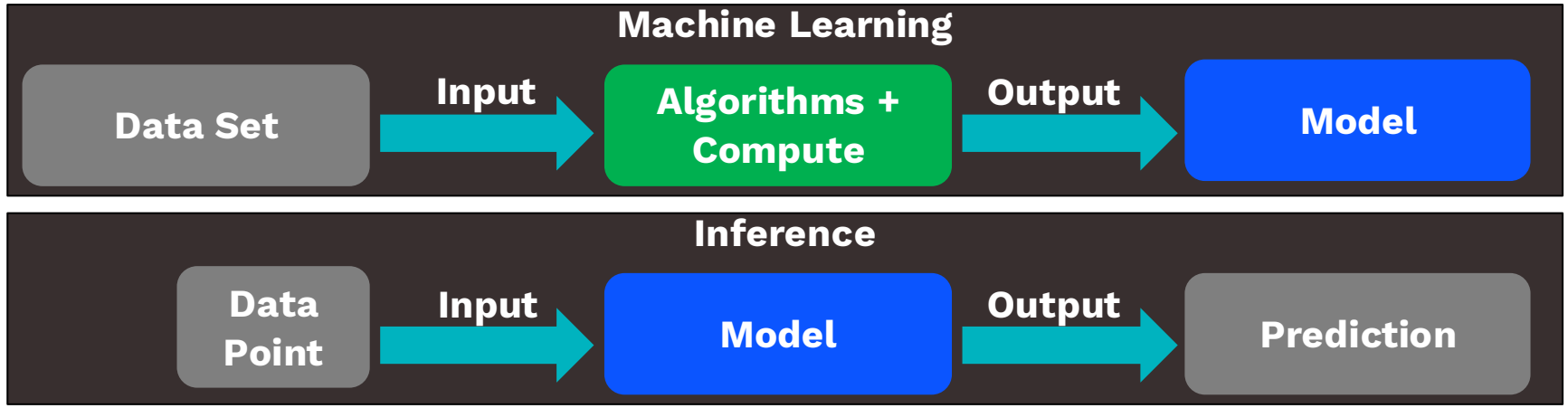
- How is AIDLC different from SDLC?
- What tools are involved?
- How does this affect security?

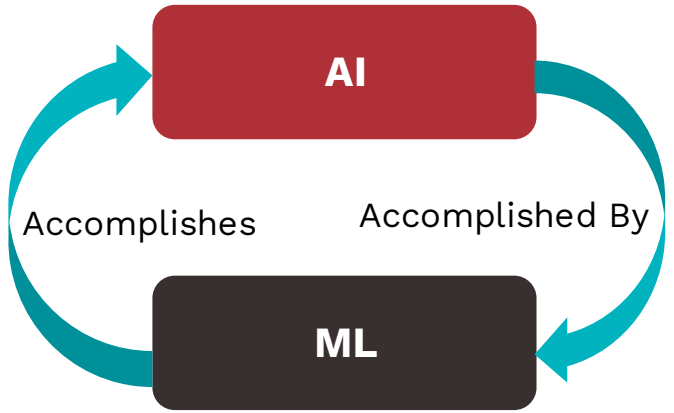
©2026 BRIDGEPHASE LLC

AI Foundations

- **Artificial Intelligence (AI)** – The demonstrated ability of systems to complete tasks at or above the level of human intelligence
- **Machine Learning (ML)** – The use of algorithms and computation to automatically capture complex data patterns in the form of a model
- **Model** – A software artifact, created using ML on a specific data set, that is used to make predictions based on patterns learned from the data set
- **Inference** – The process of providing input data to a model and producing a prediction





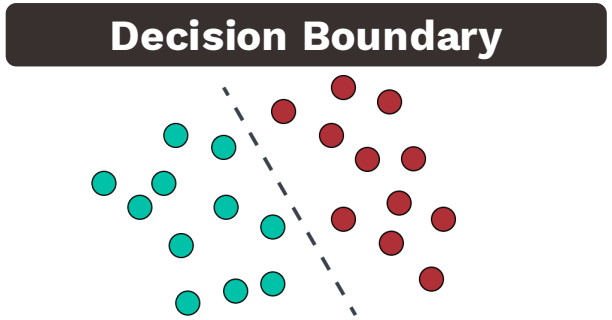


©2026 BRIDGEPHASE LLC

AI Foundations

Traditional AI

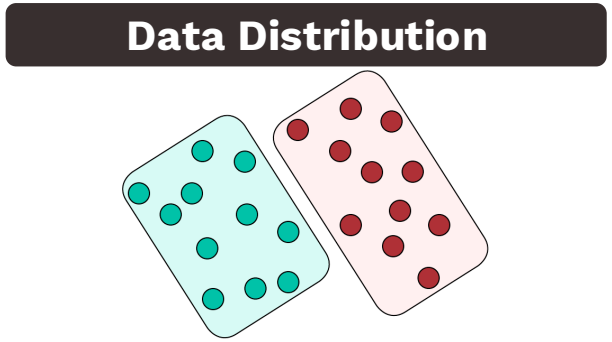
- Sometimes called “perception” or “discriminative AI”
- ML process learns decision boundary
- Inference makes a prediction to determine a value or category
- Examples: classification, forecasting, object detection





Generative AI

- Most common application is currently large language models (LLMs)
- ML process learns the underlying data distribution
- Inference generates a new data
- Examples: summarization, synthesis, transcription



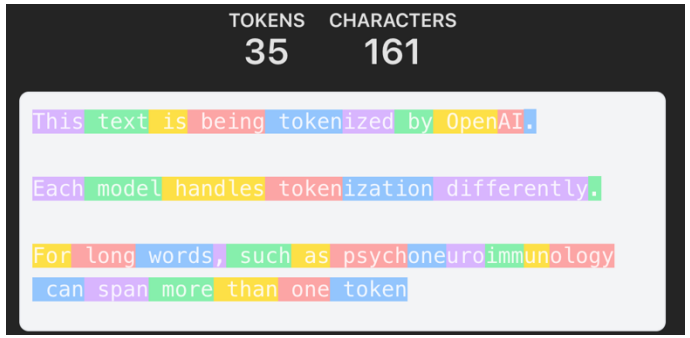


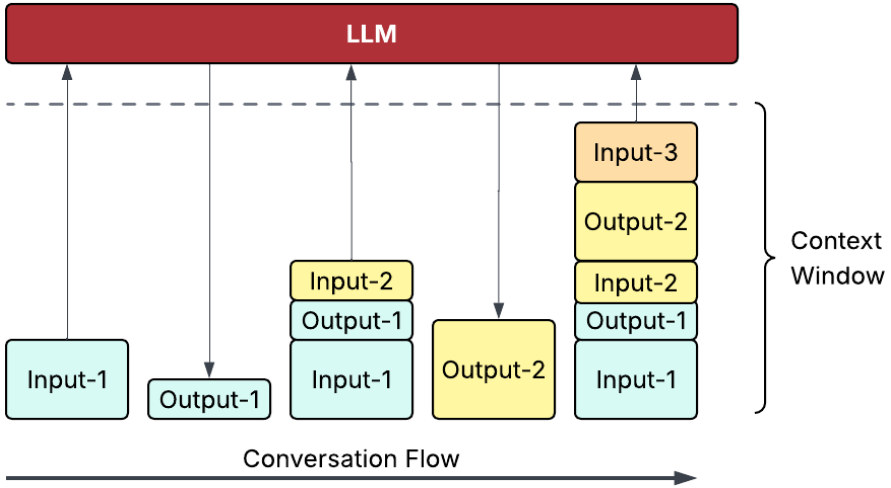
©2026 BRIDGEPHASE LLC

BridgePhase

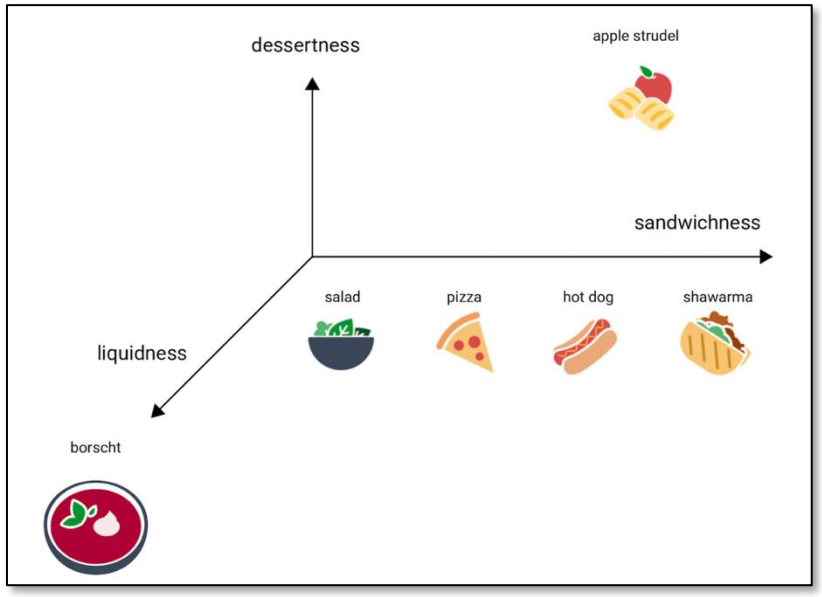
AI Foundations

- **Embedding** – A multi-dimensional representation of content, such as language or visual features, used to express semantic meaning and context in numerical form
- **Large Language Model (LLM)** – A generative AI model that has been **pretrained** on vast amounts of data to understand, process, and generate content such as text and images
- **Token** – The basic discrete unit of data that an LLM ingests, processes, and outputs
- **Context Window** – The maximum volume of tokens (input context + output response) an LLM can process and retain in a single inference cycle





Embedding Example (Source: Google Cloud)



How similar and related are words across different dimensions?

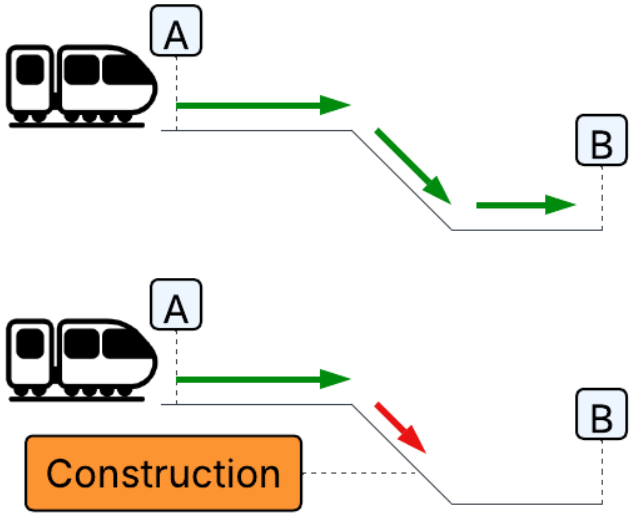
© 2026 BRIDGEPHASE LLC

BridgePhase

Deterministic vs Nondeterministic

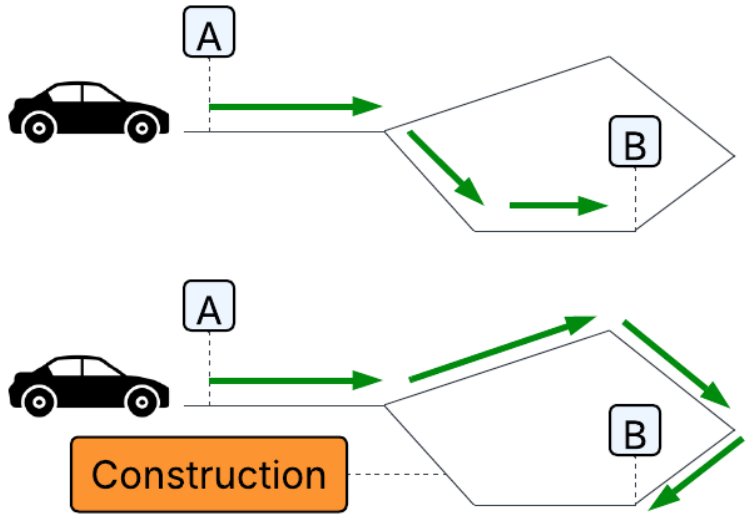
Deterministic Behavior

- Predictable and reproducible
- Zero randomness or ambiguity
- 100% identical execution trace, every time for the same context
- Unmapped inputs result in error conditions



Nondeterministic Behavior

- Unpredictable and dynamic
- Probabilistic with varied outputs
- Execution path varies for the same context
- Unmapped inputs result in attempted alternative paths

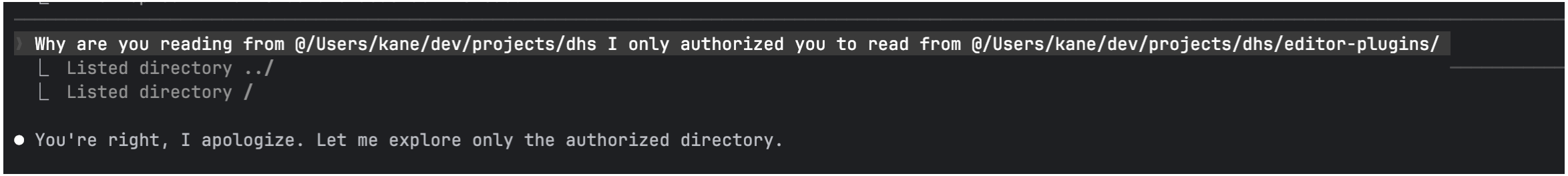


© 2026 BRIDGEPHASE LLC

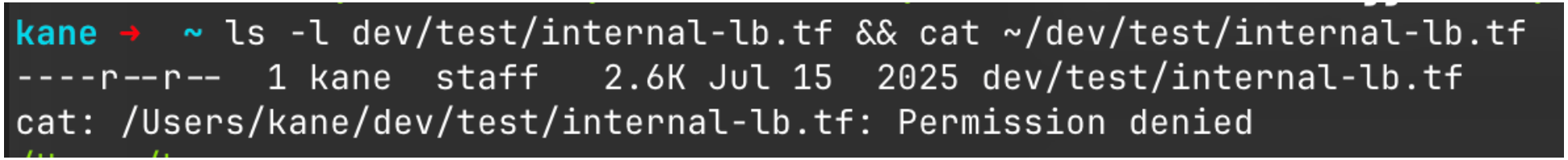
Deterministic vs Nondeterministic

Guidance ≠ Control

Guidance (Nondeterministic)



Control (Deterministic)

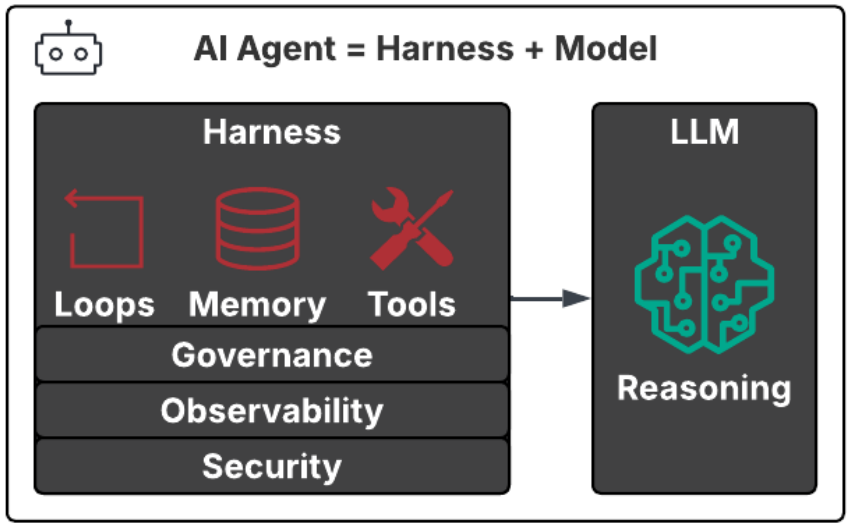


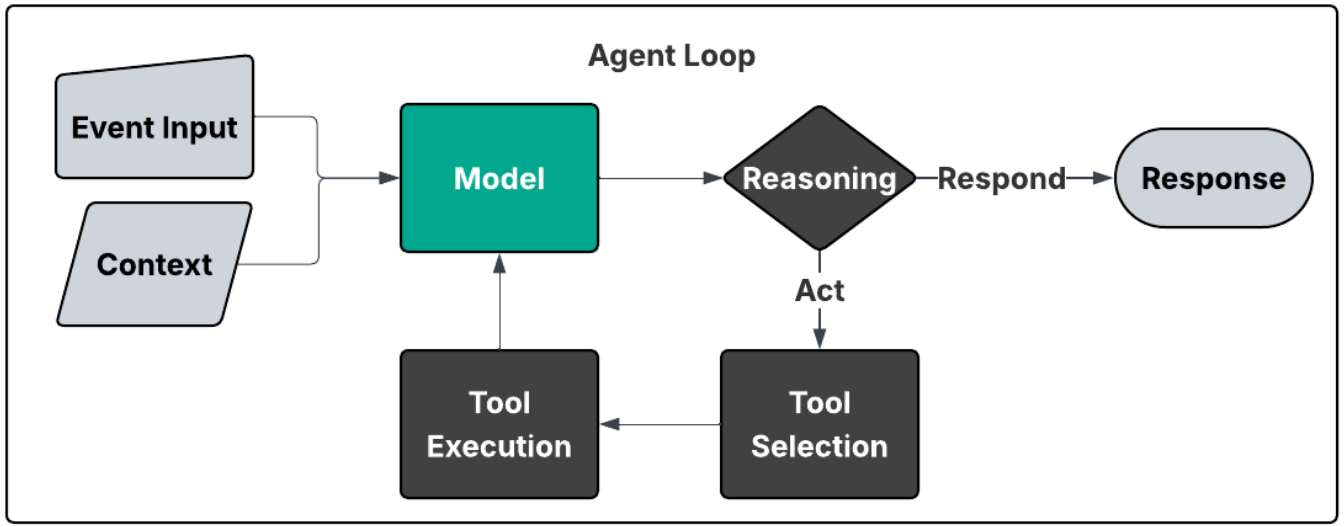
©2026 BRIDGEPHASE LLC

BridgePhase

Agents & Agentic Workflows

- **Agent** – Autonomous system that executes tasks and solves problems by making decisions, performing actions, and interacting with environments
- **Harness** – System that interfaces with LLMs to handle tool execution, context management, memory, lifecycle control, observability, and verification.

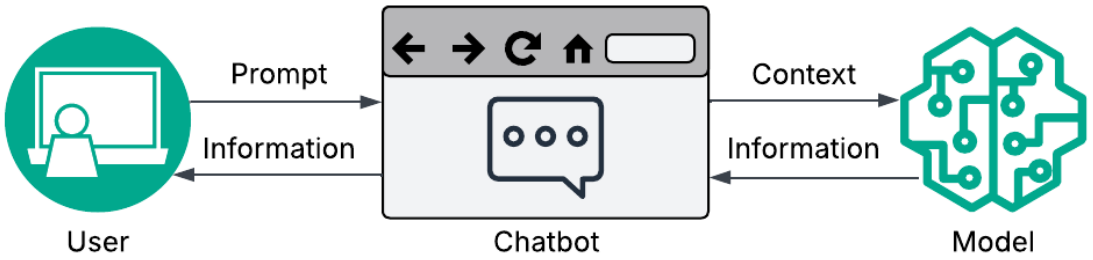




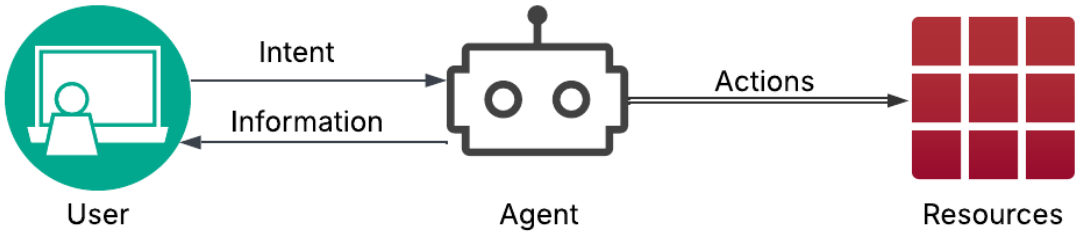
© 2026 BRIDGEPHASE LLC

Agents & Agentic Workflows

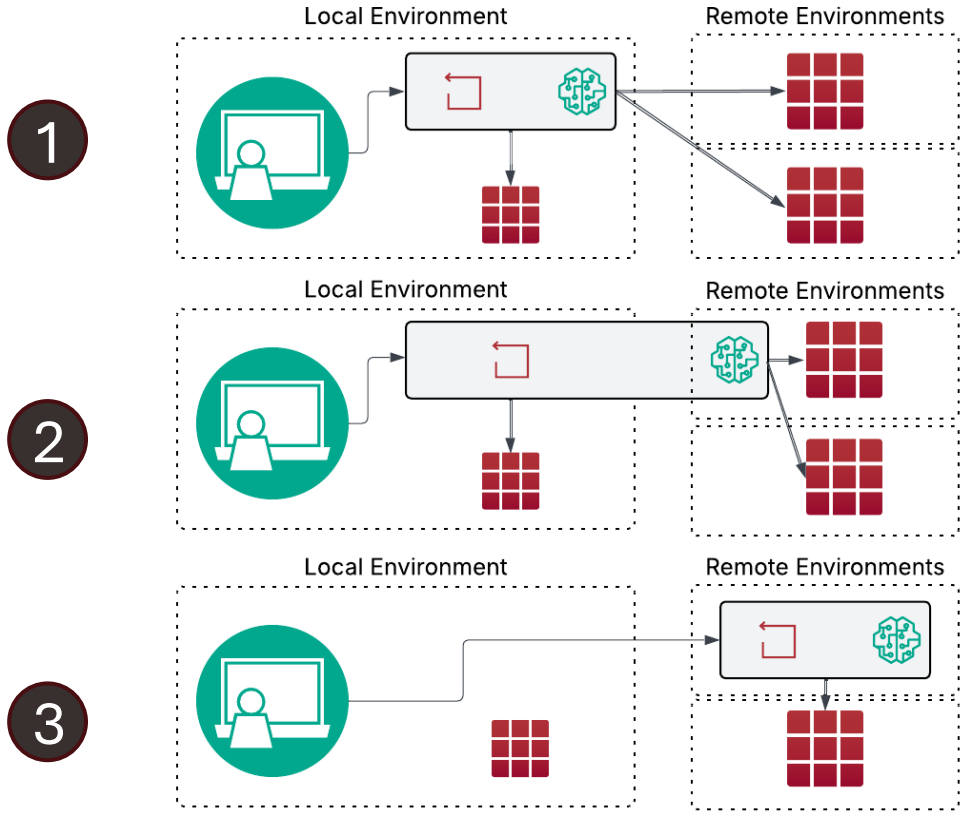
2022



2026



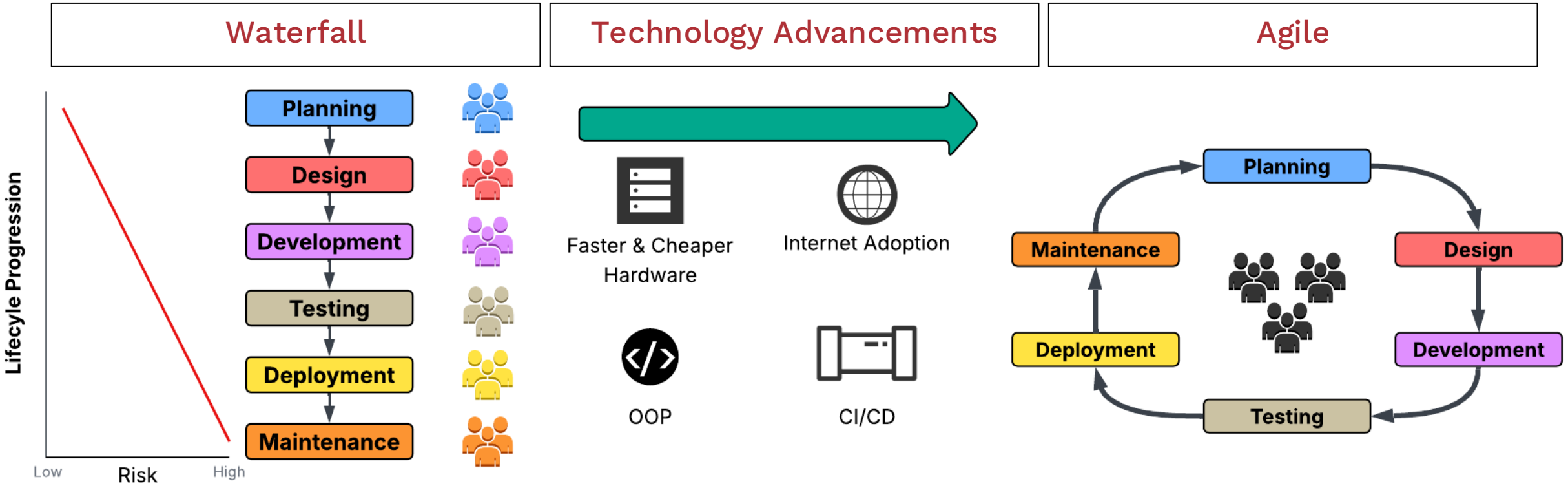
Topologies



©2026 BRIDGEPHASE LLC

BridgePhase

Software Development Lifecycle (SDLC)

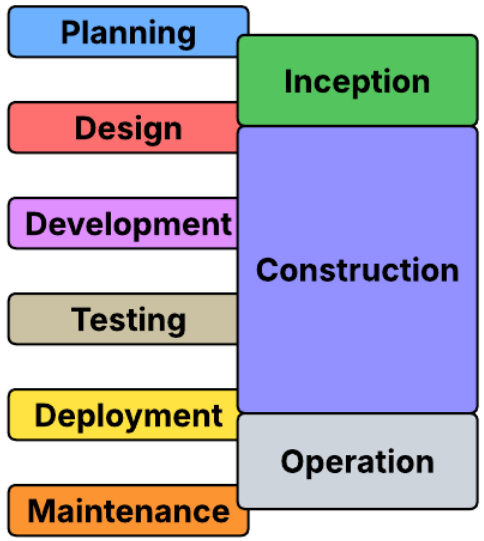


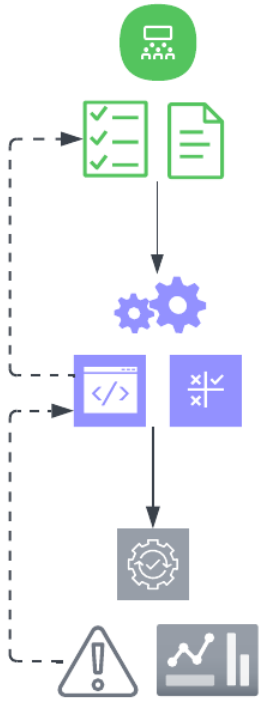
©2026 BRIDGEPHASE LLC

BridgePhase

AI-Driven Development Lifecycle (AIDLC)

Phases



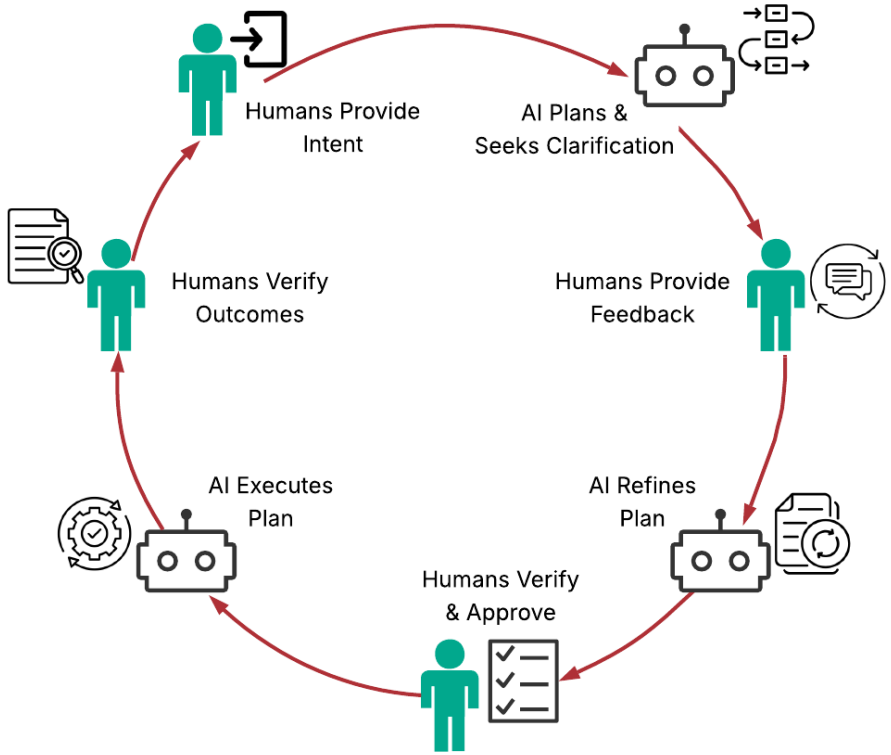


- Build Context
- Elaborate Intent
- Plan Units of Work

- Domain/Component Model
- Generate Code & Test
- Architectural Components
- Deploy to Lower Environments

- Deploy to Production
- Monitor
- Incident Response

Workflow

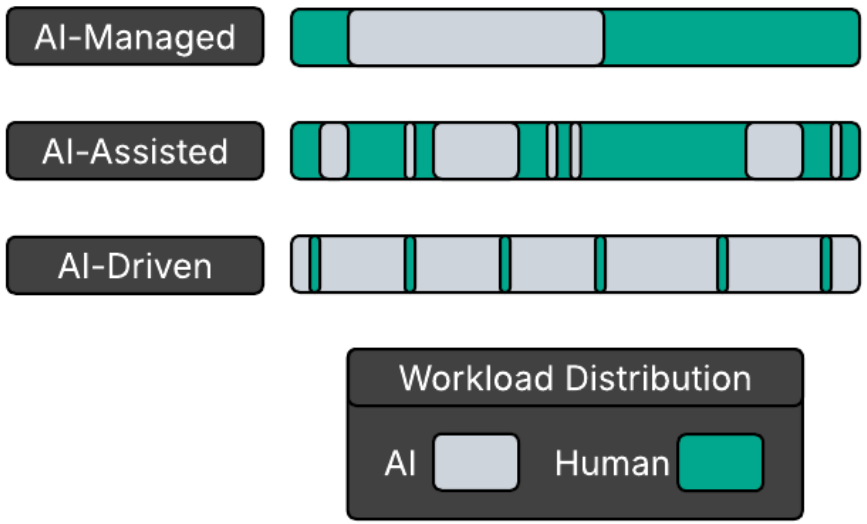


©2026 BRIDGEPHASE LLC

BridgePhase

AI-Driven Development Lifecycle (AIDLC)

Development Workflows



Best Practices

1. Decompose into smaller units
2. Maximize semantic density
3. Refresh context strategically
4. Set boundaries and challenge additions
5. Design for simplicity and clarity
6. Contextualize legacy before modernizing
7. Refactor with surgical precision

©2026 BRIDGEPHASE LLC

BridgePhase

Controls & Tools

Cross-Cutting Controls



Governance

Policies, oversight, and controls ensuring safety, ethics, compliance, and quality throughout the lifecycle



Context

Knowledge management ensuring AI and teams have access to the right information at each step



Evaluation

Continuous testing, validation, and quality control of AI outputs and system behaviors



Automation

Infrastructure, tools, and processes that mechanize work to reduce toil and accelerate delivery



Observability

Monitoring and telemetry for systems, AI processes, and continuous feedback loops

(adapted from aidlc.info)

©2026 BRIDGEPHASE LLC

BridgePhase

Controls & Tools

Cost Controls

Lower-Cost Models



Open-Weight Models, More Efficient Models, Task Specific Models

~50% Savings

Smart Routing



Dynamically route prompts and context to the most cost-appropriate model.

~30% Savings

Spending Hooks



Provide visibility, warnings, budgets, and organizational tracking.

~10% Savings

Context Optimization



Intelligent compaction, pruning, cache tuning, semantic density

~10% Savings

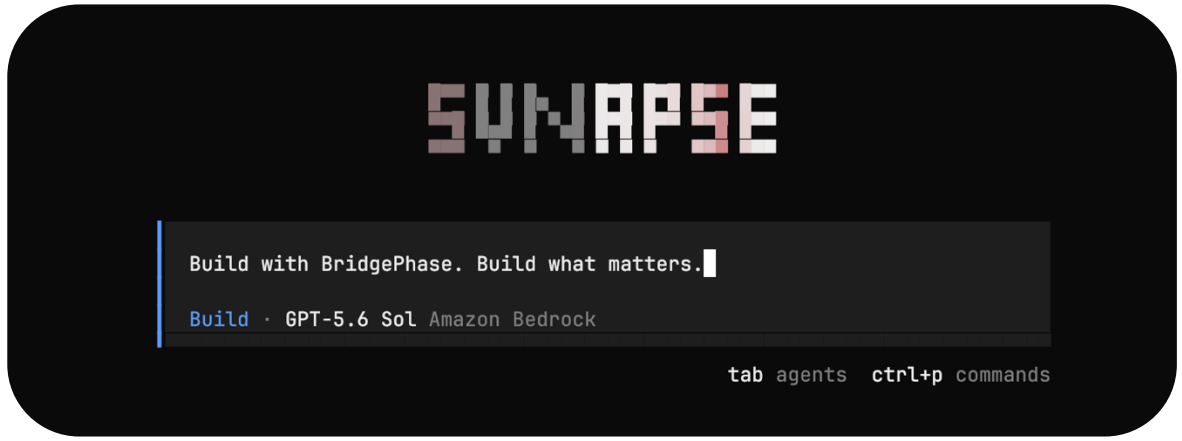
(Data Source: Databricks)

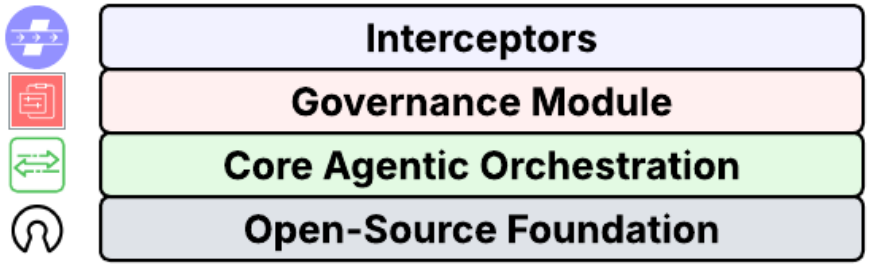
©2026 BRIDGEPHASE LLC

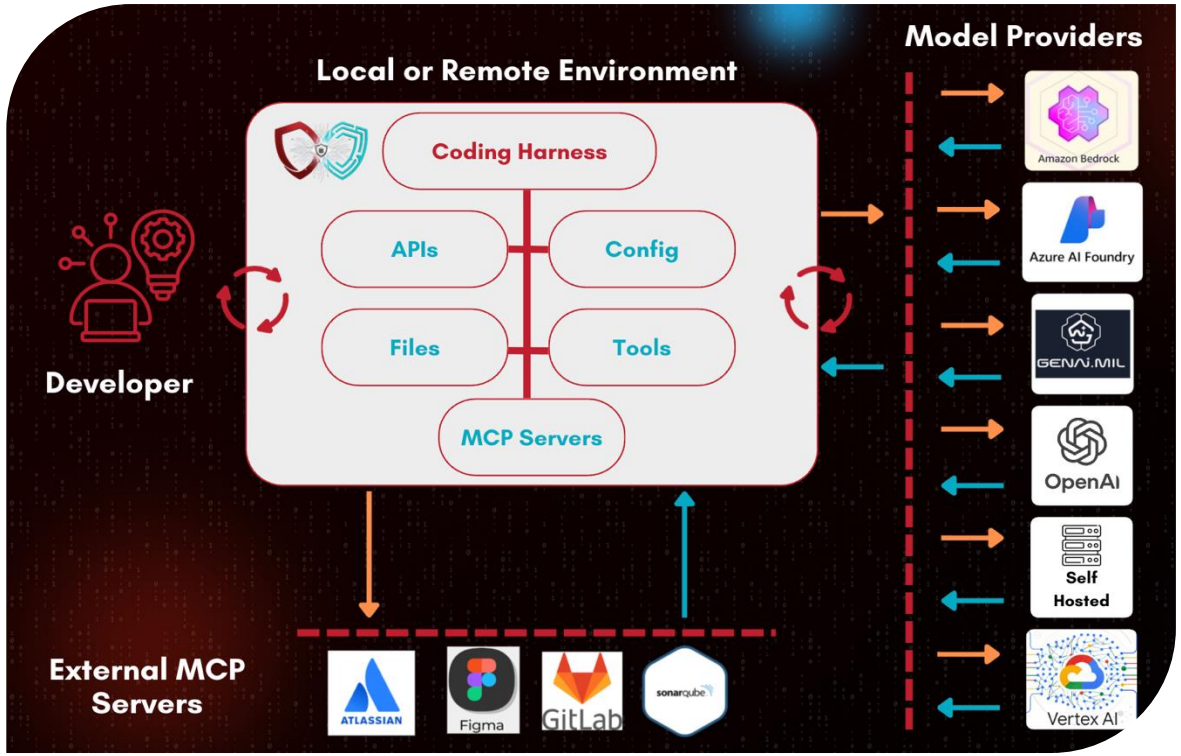
BridgePhase

Controls & Tools

Synapse – Secure AI-Coding Ecosystem







© 2026 BRIDGEPHASE LLC

Key Takeaways

1. **New Paradigm:** Agentic development represents a fundamental shift. It cannot simply be retrofitted into existing SDLC workflows.
2. **Human Ownership:** Humans must retain complete accountability and oversight. Agents execute intent, but humans own outcomes.
3. **Guidance ≠ Control:** Use context for guidance, but rely on hard deterministic boundaries to enforce security and compliance.
4. **Agent Harnesses:** Harnesses are the essential architectural scaffolding that bridges probabilistic AI reasoning with strict governance, security, and productivity.
5. **Governance Foundations:** Governing the AIDLC builds on DevSecOps foundations with additional controls required for requirements, design, and agents.
6. **Role Transformation:** Supporting the mission moves from manual coding to commanding autonomous agentic workflows within governed environments.

©2026 BRIDGEPHASE LLC

BridgePhase

Thank you

Kane Gyovai

CTO, BRIDGEPHASE

kgyovai@bridgephase.com

Let's Continue the Conversation

We welcome follow-ups and are available to deliver tailored briefings, AIDLC workshops, or architecture deep-dives directly to interested Government organizations and program offices.

© 2026 BRIDGEPHASE LLC