MCP Dev Summit Mumbai

Building an Enterprise MCP Registry

Secure Discovery, Governance, Reuse at Scale

Presented By:
Kushagra Mittal, Dhruv Agarwal

MOTOROLA SOLUTIONS

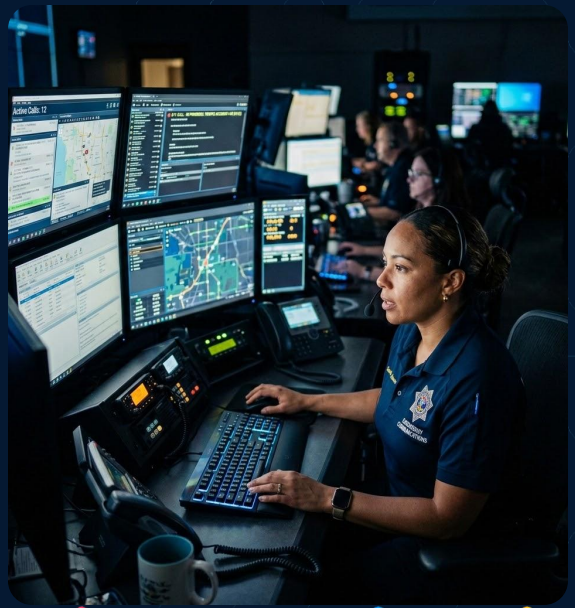
Hello Moto? (Not That One)

Mission Critical, Not Cellular

You’re thinking of the Razr. We’re thinking of the 911 Dispatcher. We don't build phones; we build the last line of defense.

From body-worn cameras to CommandCentral, we provide the mission-critical foundation for public safety across the globe.

"If your phone drops a call, you're annoyed. If our tech drops a call, the consequences are life-critical."



Case : Reinventing the Wheel

01

Waste

Three incompatible Jira MCP servers developed in parallel.

02

Redundancy

Triple the cloud compute and maintenance debt.

03

Discovery Gap

Zero central visibility on existing tool capabilities.

Case : The "Ghost" Admin

01

The Action

Dev hardcodes an admin bearer token in local config for "quick testing."

02

The Share

Config is shared over Slack for cross-team collaboration.

03

The Breach

An agent, acting for a junior user, pulls sensitive payroll data using the ghost token.

Case : The Silent App Crash

01

The Change

Team A tweaks a formatted SQL prompt embedded in their repo.

02

The Sprawl

Team B and C had already copy-pasted that prompt into their microservices.

03

The Break

Reasoning logic shifts subtly; Team B's agent starts returning unparseable schemas.

Question jungle

"The agent just triggered a destructive DELETE call on a production database—who allowed write-level scopes?"

"Why do we have six engineering teams building six variations of the exact same Jira tool?"

"Compliance needs a complete audit trail of exactly which raw user prompt triggered which query last Tuesday."

"Our orchestrator is hitting 12-second latency due to brute-force string matching. How do we route dynamically?"

"How do we safely propagate a real user's OAuth identity context down to an autonomous background tool?"

"Who actually owns the 'SQL-Generation' prompt? It's hardcoded directly inside a private repo!"

"How do we prevent sensitive PII from leaking straight into an external public model's training context?"

"An agent got caught in an infinite loop, making 500 tool calls in three minutes—how do we throttle?"

"Did a low-privilege employee just leak payroll data because they inherited an over-privileged dev token?"

"We upgraded our model, and now legacy tool calls fail—how do we enforce SemVer on prompts?"

"Can a rogue user trick our agent into calling an admin endpoint simply by typing an adversarial instruction?"

"What happens to stability when an API schema changes, but the agent's description isn't updated?"

Structural Obstacles in Enterprise Agentic System Adoption

ORGANIZATIONAL FRICTION

Siloed Development

Developers duplicate effort due to a lack of visibility across separate business units, asking: "Who has developed what?".

COMPLIANCE FRICTION

Security Blind Spots

Rogue, unvalidated agentic setups expose sensitive data boundaries to leakage.

ORGANIZATIONAL FRICTION

Slow to Scale

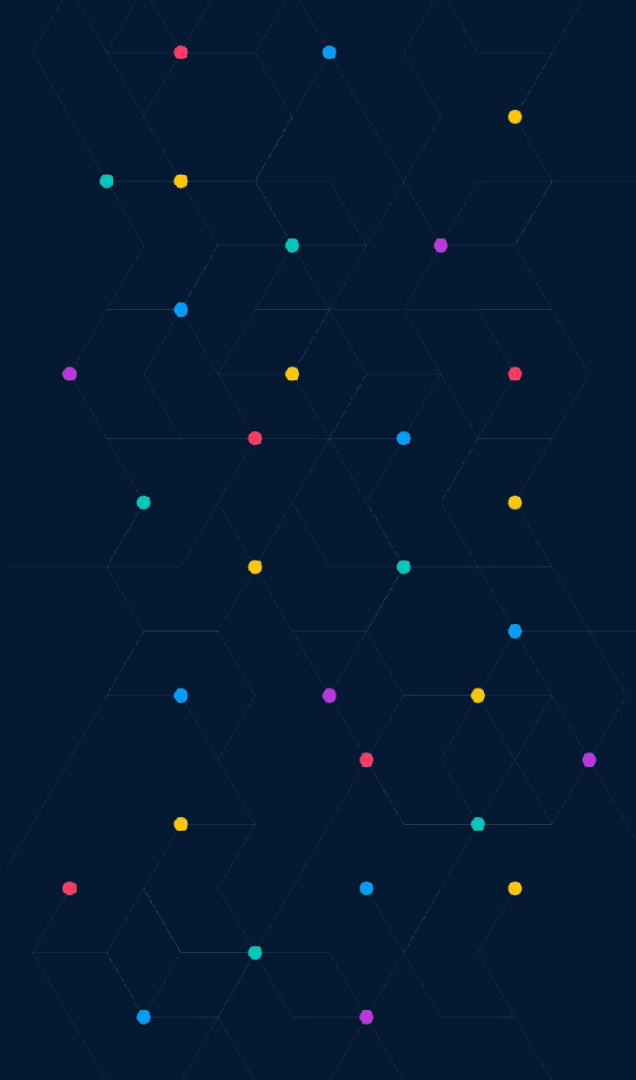
Failing to cleanly reuse validated code components drives up redundant cloud compute costs.

COMPLIANCE FRICTION

Fragmented Governance

Deployed tools operating without centralized observability cause disjointed testing and non-compliant audit logs.

MSI's Solution



Introducing MSI's Strategy

THE CORE THESIS

Agent-First Communication

At Motorola Solutions, we treat Model Context Protocol (MCP) and Agent-to-Agent (A2A) communication channels as first-class citizens.

ELIMINATING SILOS

Cognitive Decoupling

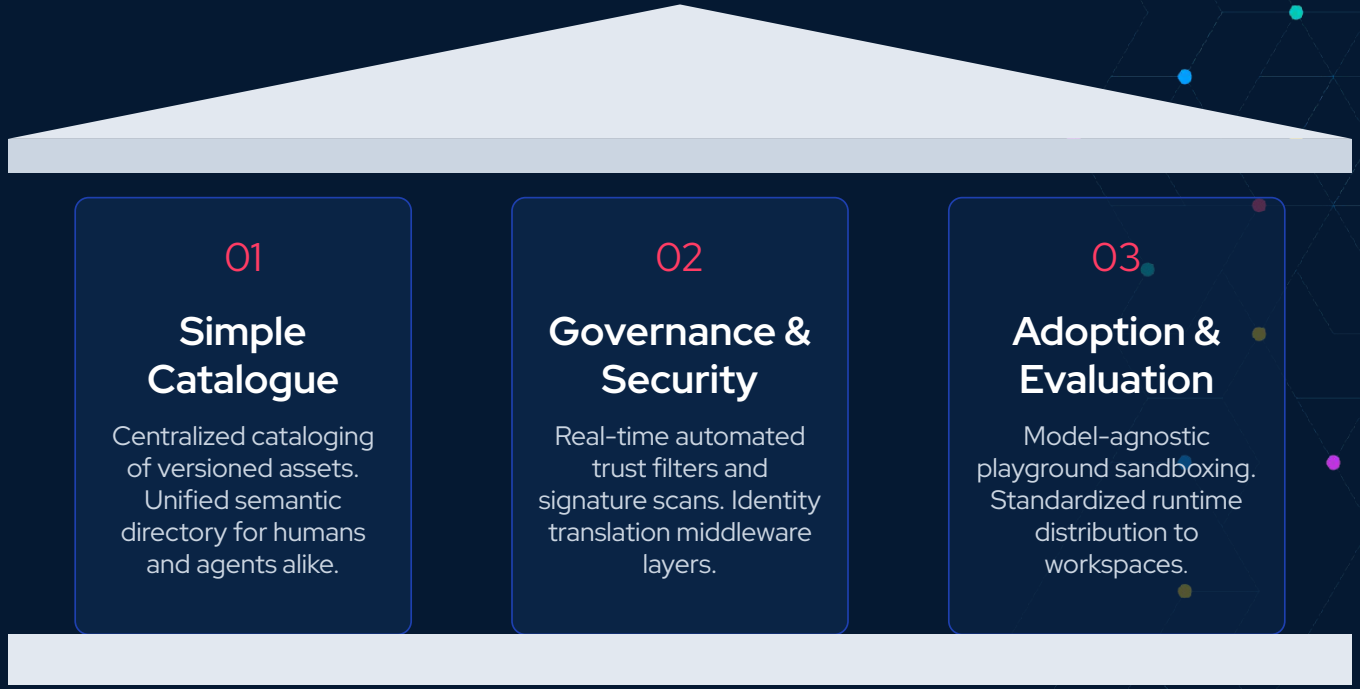
By decoupling model cognition from data access, we transition from proprietary, vendor-locked stacks to modular, interoperable agentic systems.

AI FOUNDRY

Enterprise Gateway

The unified, standardized corporate platform engineered for enterprise AI discovery, absolute governance, and secure infrastructure reuse.

The Philosophy



01

Simple Catalogue

Centralized cataloging of versioned assets. Unified semantic directory for humans and agents alike.

02

Governance & Security

Real-time automated trust filters and signature scans. Identity translation middleware layers.

03

Adoption & Evaluation

Model-agnostic playground sandboxing. Standardized runtime distribution to workspaces.

The Foundation: Simple Cataloging & Versioned Assets

AI Registries Component

Governed Discovery & Interoperability

A highly available, stateful catalog for remote MCP servers and pre-vetted corporate AI agents. Mandates strict operational interoperability via standardized MCP and A2A interfaces.

AI Assets Component

Versioned Templates & Soft Logic

A fully version-controlled, audited repository for peer-reviewed templates—encompassing system prompts, gems, and specialized NotebookLMs—optimized for custom, repeatable enterprise use cases.

The Governance Gate: Automated Asset Vetting

THE EXPOSURE RISK

Malicious Injection Path

In an open developer ecosystem, prompt repositories and live tool schemas are heavily exposed to malicious code injections and structural anomalies.

SHIFT-LEFT GATING

The AI Foundry mandates a compliance pipeline—the AI Scanner—that validates registered assets before deployment.

THE SHIELD

Parses text configurations against custom YARA signature rules to intercept prompt injections, verifies JSON-RPC compliance, and rejects over-privileged API scopes.

The Security Gate: Runtime Identity Propagation

THE CORE PROBLEM

Unified Auth Maze

Standardizing and maintaining dynamic authentication protocols for agents across hundreds of completely diverse corporate servers.

THE PLATFORM SOLUTION

Deploying an in-house middle-auth routing proxy utilizing dynamic OAuth scope mapping.

SECURITY BOUNDARY

Ensures raw user credentials never touch non-deterministic LLM paths, generating short-lived, ephemeral scoped credentials at execution runtime.

Architectural Shift: Decentralized AI Gateways

THE MARKET EVALUATION

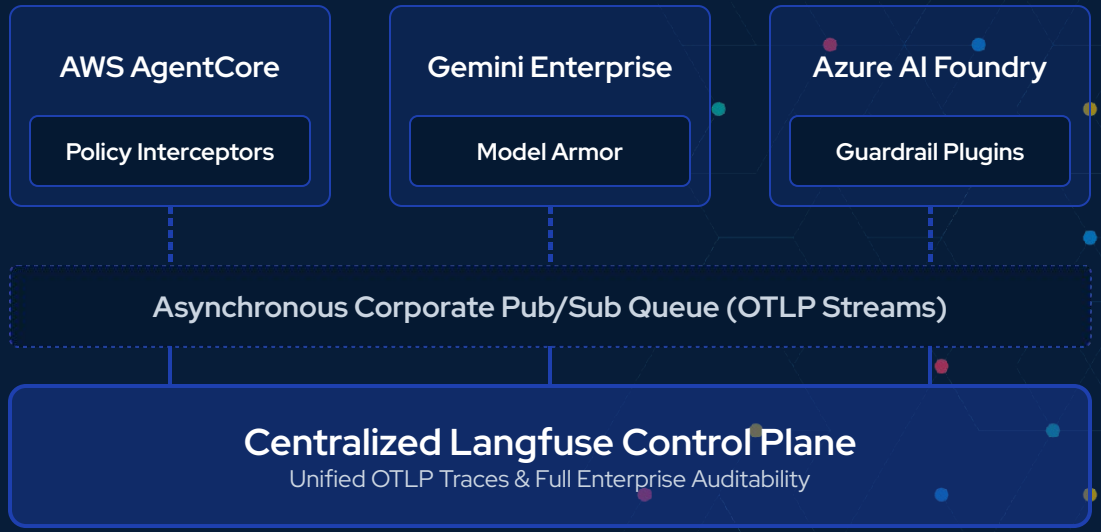
The Wall: Monolithic Failures

Blocker 01: Single Point of Failure (SPOF) risks for public safety.

Blocker 02: High HA Infrastructure Costs across isolated environments.

THE MSI SOVEREIGN APPROACH

Decentralized topologies replacing the monolith with flexible, on-demand gateways natively embedded into CSP landing zones.



The Adoption Gate: Capturing the Chain of Thought

THE CORE PROBLEM

Silent Observability

Gaining complete execution transparency over multi-step, non-deterministic agent tool execution calls.

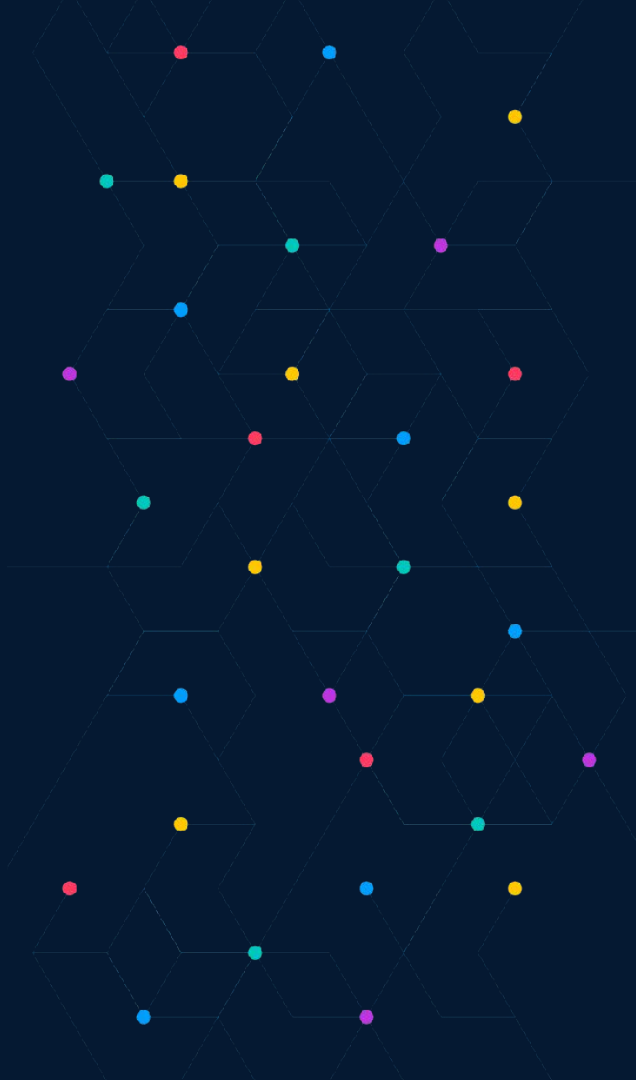
THE PLATFORM SOLUTION

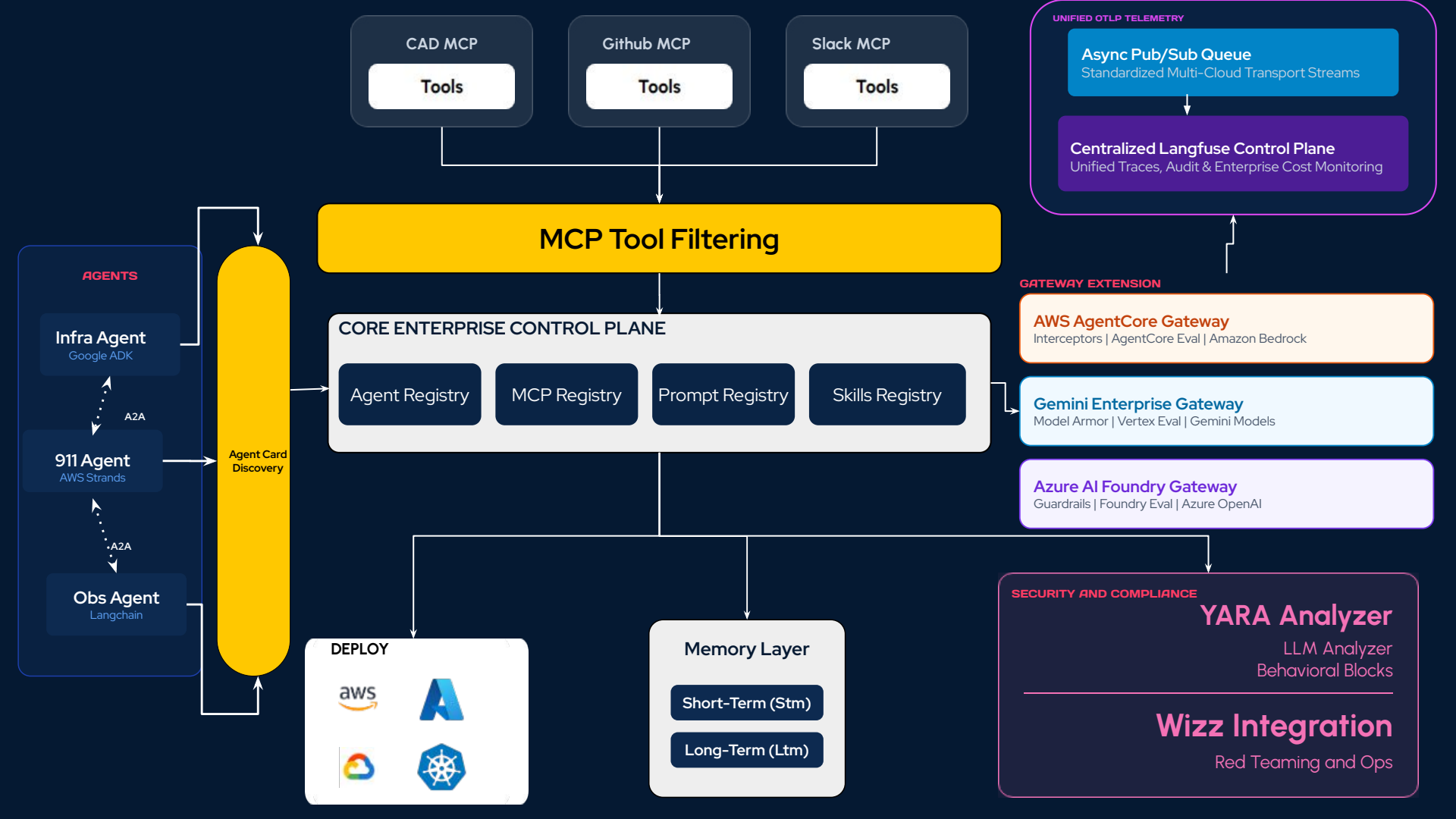
Wiring end-to-end distributed tracing spans using OpenLLMetry and Langfuse straight into the registry proxy layer.

SYSTEM BENEFIT

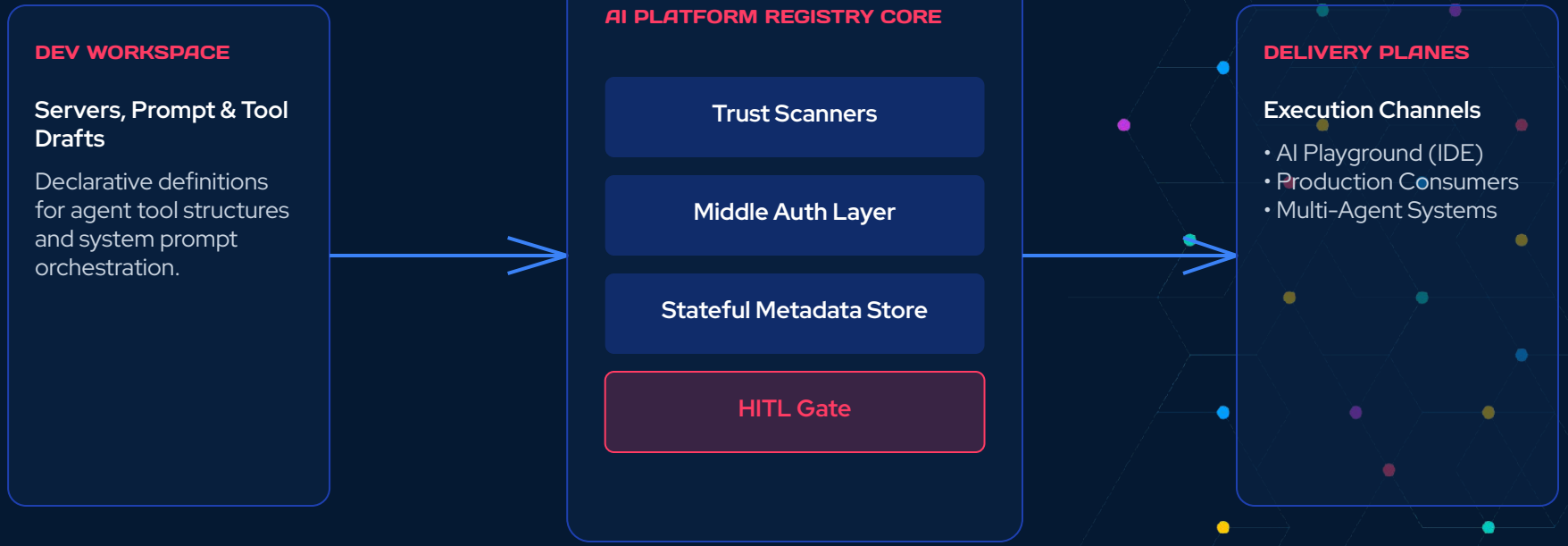
Resolves the compliance audit imperative by tracking execution latency, input token structures, and raw tool payloads transparently.

Enterprise AI Orchestration Architecture




CAD MCP
Tools
Github MCP
Tools
Slack MCP
Tools
UNIFIED OTLP TELEMETRY
Async Pub/Sub Queue
Standardized Multi-Cloud Transport Streams
Centralized Langfuse Control Plane
Unified Traces, Audit & Enterprise Cost Monitoring
MCP Tool Filtering
AGENTS
Infra Agent
Google ADK
A2A
911 Agent
AWS Strands
A2A
Obs Agent
Langchain
Agent Card Discovery
CORE ENTERPRISE CONTROL PLANE
Agent Registry
MCP Registry
Prompt Registry
Skills Registry
GATEWAY EXTENSION
AWS AgentCore Gateway
Interceptors | AgentCore Eval | Amazon Bedrock
Gemini Enterprise Gateway
Model Armor | Vertex Eval | Gemini Models
Azure AI Foundry Gateway
Guardrails | Foundry Eval | Azure OpenAI
DEPLOY
aws
Memory Layer
Short-Term (Stm)
Long-Term (Ltm)
SECURITY AND COMPLIANCE
YARA Analyzer
LLM Analyzer
Behavioral Blocks
Wizz Integration
Red Teaming and Ops

MSI's Strategy System Architecture Blueprint



Data Flow: Governance Pipeline and Schema Asset Ingestion

STEP 01

Commit Update

Developer commits an updated tool schema definition or system prompt text to a verified corporate repository branch.

STEP 02

Ecosystem Ingest

Registry takes the event, formatting the incoming JSON configuration payload for processing.

STEP 03

Trust Scanning

Payload hits Trust Scanners, checking signatures against YARA databases and running LLM adversarial simulations.

STEP 04

Registry Update

Upon clear verification, the asset state is written to the persistent Metadata Store and made instantly discoverable.

Data Flow: Live Runtime Execution & Identity Proxy

01 | REQUEST

Agent Trigger

Active agent fires an execution call targeting a secure internal API endpoint.

02 | INTERCEPTION

Context Capture

The Middle Auth abstraction engine intercepts the runtime request, pulling the primary user's profile context.

03 | RESOLUTION

Scope Mapping

The wrapper engine connects to the corporate Identity Provider, executing dynamic OAuth scope mapping to generate a restricted token.

04 | FORWARDING

Secure Proxy

The proxy appends the scoped token to the tool call header for safe downstream execution.

Data Flow: Safe Playground Isolation and Trace Collection

STEP 01

Sandbox Boundary

Playground initializes an ephemeral, zero-retention developer execution session.

STEP 02

Model Selection

Developer selects Claude, Gemini, or GPT-4 foundations to test against internal data sets.

STEP 03

Payload Intercept

Output content passes through security filters to catch unintended structural variations or PII leakage.

STEP 04

Telemetry Stream

Runtime telemetry blocks stream step-by-step reasoning spans straight to Langfuse endpoints.

Architecture Evolution: Comparative Reality Matrix

ENGINEERING VECTORS	LEGACY ENVIRONMENT	SOVEREIGN MSI's Strategy ARCHITECTURE
Tool Secrets	Hardcoded inside loose, config.json configurations.	Dynamically Brokered (Vault & Middle Auth Tokens).
Governance	Manual, ad-hoc, or inconsistent repository code reviews.	Automated Scanner Gates, LLM Audits, & YARA Signatures.
Discovery	Scattered "Copy-Paste" file strings over communication channels.	Dynamic Semantic Registry Catalogs and Indexing Searches.
Observability	Siloed, detached, and disconnected terminal logs.	Unified OpenTelemetry, OpenLLMetry, and Langfuse Spans.

Enterprise Value Realization: Key Adoption & Impact Metrics

METRIC 01 | VELOCITY

80% Reduction

Time-to-Market: Manual reviews (6 weeks) to automated gates (2 week).

METRIC 02 | EFFICIENCY

75% Reuse

Code Component Reuse: Eliminating duplicate wrappers across 15+ product groups.

METRIC 03 | SECURITY

0 Critical/High Violations

100% Assurance: 42 injection variants intercepted before deployment.

METRIC 04 | OBSERVABILITY

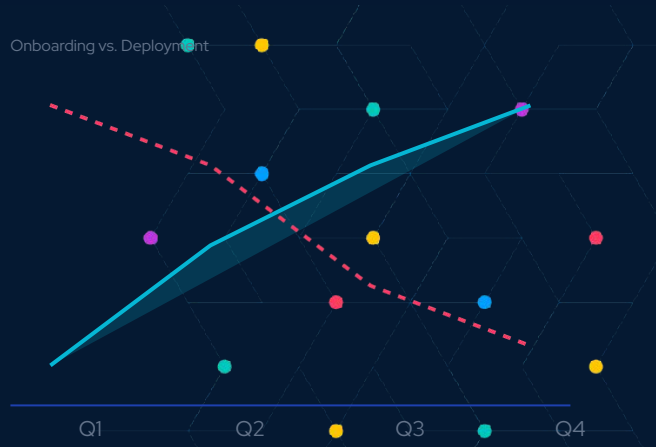
100% Coverage

Trace Coverage: End-to-end OTLP tracking via decentralized pipelines.

METRIC 05 | ADOPTION

3.5x Growth

Scale: 250% MoM increase in safe agentic workload routing.



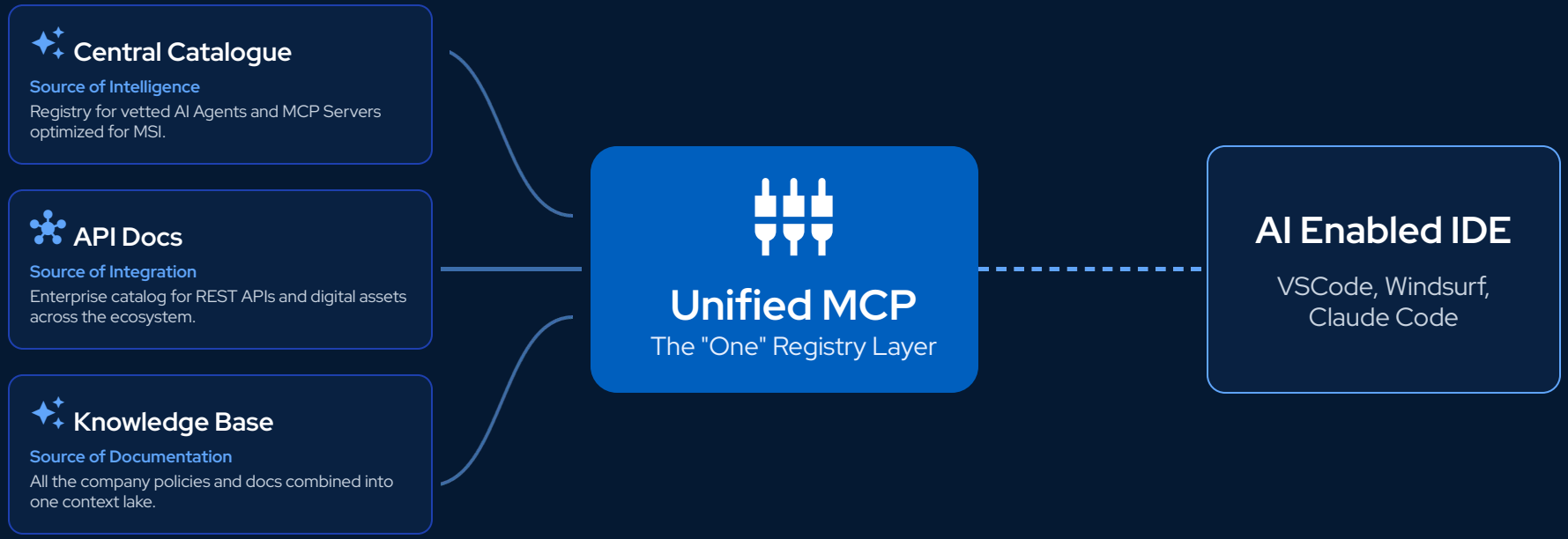
80% Faster Shipping

65% Less Duplication

Zero Trust Compliance

MCP Dev Summit Mumbai

The Unified IDE Gateway



Enterprise AI Infrastructure Teams

Kushagra Mittal

AI Platform Engineer

Motorola Solutions

SCAN TO CONNECT

kushagra.mittal@motorolasolutions.com

Dhruv Agarwal

AI Software Engineer

Motorola Solutions

SCAN TO CONNECT

dhruv.agarwal@motorolasolutions.com

MCP Dev Summit Mumbai

MCP Dev Summit Mumbai