

AI & SECURITY ENGINEERING PRACTICE

Agile AI

Corporate Core Architecture — one accountable practice across network, AI systems, software delivery, and offensive security.

NETWORK & SECURITY DIRECTOR

Kshitij Pawar

AI AUTOMATION DIRECTOR

Niraj Joshi

OFFICIAL DOMAIN

AGILEAI.CO.IN



INDEX

Contents

02	Document Index	CONTENTS
03	Vision & Mission	STRATEGIC INTENT
04	Founders	LEADERSHIP PROFILE
05	Company Story	ORIGIN & TRAJECTORY
06	Five Technology Pillars	CAPABILITY OVERVIEW
07	Network Solutions	INFRASTRUCTURE ENGINEERING
08	AI Engineering	APPLIED INTELLIGENCE SYSTEMS
09	Web & API Architecture	SOFTWARE ENGINEERING
10	Security & VAPT	OFFENSIVE VALIDATION
11	Cloud & DevOps	PLATFORM ENGINEERING

12	Zero Trust Architecture	BLUEPRINT DIAGRAM
13	Security Fundamentals	PROTECT · DETECT · RESPOND
14	Secure Development Lifecycle	SIX-STAGE PIPELINE
15	DevSecOps Delivery Pipeline	CI/CD BLUEPRINT
16	AI Development Lifecycle	MODEL & RETRIEVAL ARCHITECTURE
17	Technology Ecosystem	PLATFORM & TOOLING MATRIX
18	Docker & Kubernetes	CONTAINER ORCHESTRATION
19	Client Engagement Journey	DELIVERY FRAMEWORK
20	Innovation Roadmap	FY26 – FY28
21	Contact	ENGAGEMENT CHANNELS

STRATEGIC SYNTHESIS

Vision & Mission

01 - VISION

A single, accountable engineering practice for enterprise infrastructure.

We believe the modern enterprise stack has become fractured by design — one vendor builds, another audits, a third maintains, and no one owns the outcome. Agile AI exists to close that gap: to be the one technical partner capable of designing, building, automating, and defending an organization's entire digital core, end to end.

02 - MISSION

Eliminate structural friction across network, software, AI, and security layers.

We unify systems architecture, secure software delivery, applied AI automation, and offensive security validation inside one continuous lifecycle — so every system we ship is provisioned for scale, engineered for resilience, and proven under attack before it reaches production.

GOVERNING PRINCIPLES

01

Architectural Scale

Systems provisioned natively for peak load and long-term technical debt reduction.

02

Secure by Construction

Cryptographic and vulnerability controls embedded inside the build cycle, not appended after.

03

Offensive Validation

Continuous manual threat simulation — we attack our own systems before anyone else can.

CORPORATE IDENTITY PORTFOLIO

Founders

Agile AI is engineered and led by two practitioners who build the systems they secure — not separately, but as one continuous discipline.



Kshitij Pawar

CO-FOUNDER & NETWORK / SECURITY DIRECTOR

Leads architectural strategy across network infrastructure and enterprise security — designing resilient, low-latency network foundations and directing offensive security operations and VAPT.



Niraj Joshi

CO-FOUNDER & AI AUTOMATION DIRECTOR

Directs AI engineering, automation, and software delivery — building production-ready ML systems, RAG pipelines, and intelligent process automation embedded into every engineering milestone.

"We started Agile AI on a simple premise — the people who build a system should be capable of breaking it too. That's the only way accountability survives contact with a live production environment."

COMPANY STORY

Built from the friction of fragmented technology delivery.

Agile AI was founded on a direct observation from the field: enterprise technology teams were routinely hiring one vendor to build systems, another to secure them, and a third to keep them running — with no single point of accountability when something broke. We built a practice designed to remove that fragmentation entirely.

ONE ACCOUNTABLE TEAM, ACROSS THE ENTIRE TECHNOLOGY LIFECYCLE

DIGITAL TRANSFORMATION MANDATE

01

Assess

Audit existing infrastructure, code, and security posture against enterprise-grade benchmarks.

02

Modernize

Re-architect legacy systems into cloud-native, microservice-based, API-first platforms.

03

Automate

Layer applied AI and intelligent automation across operational and data workflows.

04

Harden

Validate every layer through continuous manual VAPT and compliance-readiness cycles.

CAPABILITY MATRIX

The Five Technology Pillars

01

Network Solutions

High-performance enterprise topologies — routing and switching optimization, multi-cloud provisioning, and load distribution engineered for maximum uptime.

02

AI Engineering

Production-ready machine learning models and context-aware NLP pipelines. LLM fine-tuning, applied RAG architectures, intelligent process automation.

03

Software Engineering

Advanced web applications and custom logic layers. Fast REST/GraphQL APIs, scalable backend architectures, microservice communication pathways.

04

Security & VAPT

Aggressive vulnerability assessment and penetration testing. Automated infrastructure scans blended with deep manual exploitation validation.

05

Cloud & DevOps

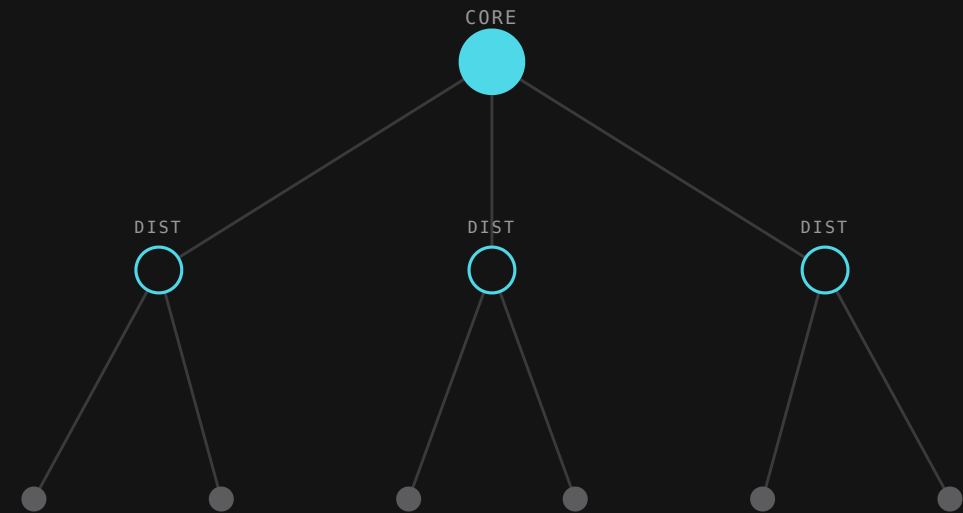
Continuous integration and delivery pipelines, container orchestration, infrastructure-as-code, and observability across hybrid, multi-cloud estates.

PILLAR DEEP-DIVE - 01

Network Solutions

Designing and deploying high-performance enterprise network topologies — routing, switching, cloud provisioning, and load distribution engineered for maximum operational uptime.

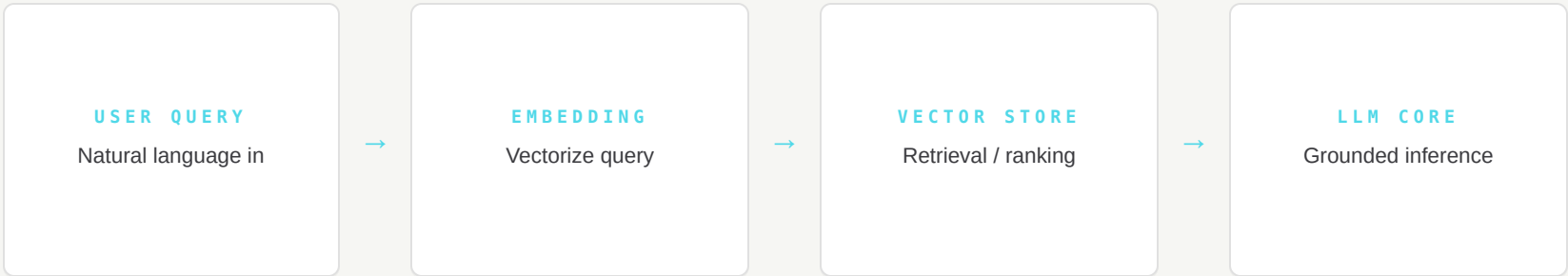
- Routing Matrix Design
- Switching Optimization
- Multi-Cloud Provisioning
- Load Distribution Management



PILLAR DEEP-DIVE - 02

AI Engineering

Production-ready machine learning models and context-aware natural language pipelines — automating unstructured data, manual operations, and business intelligence at enterprise scale.



- LLM Fine-Tuning Arrays
- Applied RAG Pipelines

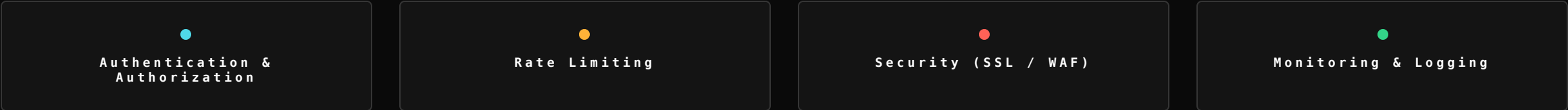
- Intelligent Automations
- AI Agent Orchestration (MCP)

PILLAR DEEP-DIVE - 03

Web & API Architecture

Scalable, secure, reliable service architecture — from client surface to data layer, with authentication, rate limiting, and monitoring enforced at the gateway.

COMMON LAYERS



→ REST & GraphQL API Design

→ Microservice Communication

→ Scalable Backend Architectures

→ Defensive Web Layouts

PILLAR DEEP-DIVE - 04

Security & VAPT

Aggressive vulnerability assessment and penetration testing — blending automated scans with deep manual validation across web, API, and network surfaces.

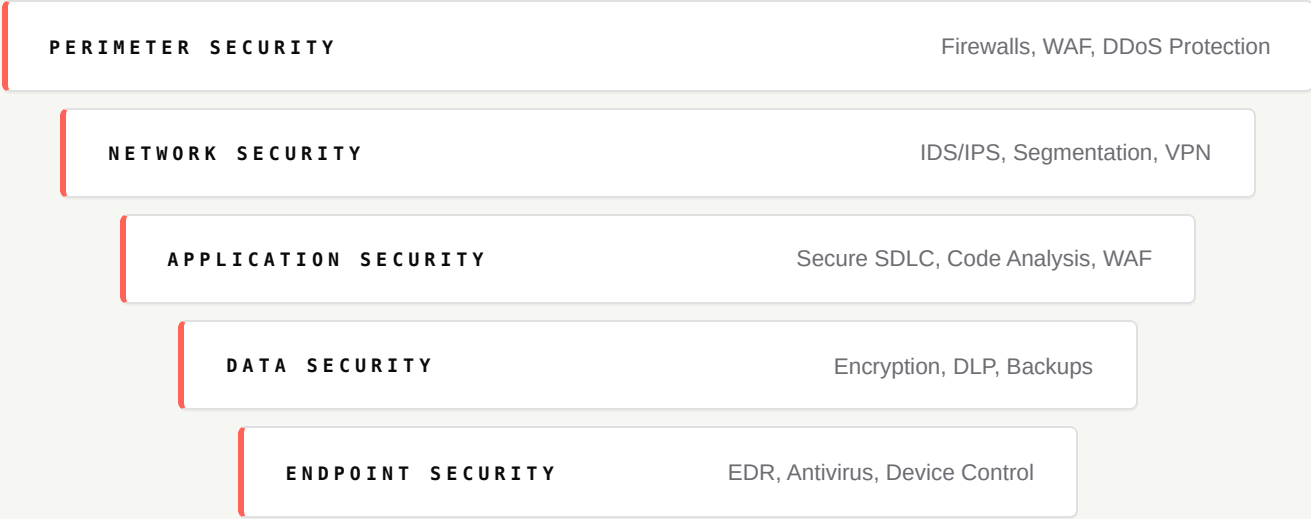
→ Manual Exploitation Audits

→ Compliance Readiness Checks

→ Perimeter Defense Hardening

→ Zero Trust Enforcement

SECURITY LAYERS

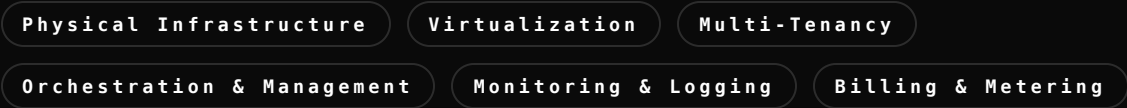


PILLAR DEEP-DIVE - 05

Cloud & DevOps

Continuous integration and delivery pipelines, container orchestration, infrastructure-as-code, and observability across hybrid and multi-cloud estates.

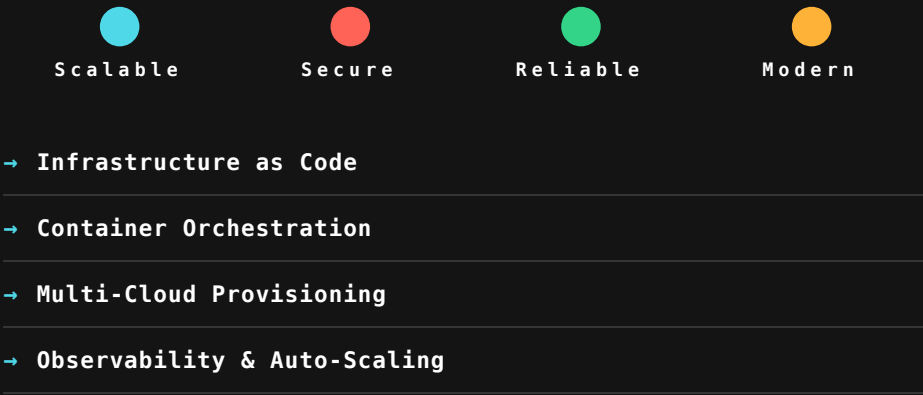
CLOUD ARCHITECTURE COMPONENTS



CORE CONCERNS

Perimeter security, DDoS protection, and public / private cloud isolation are enforced at every provisioning layer.

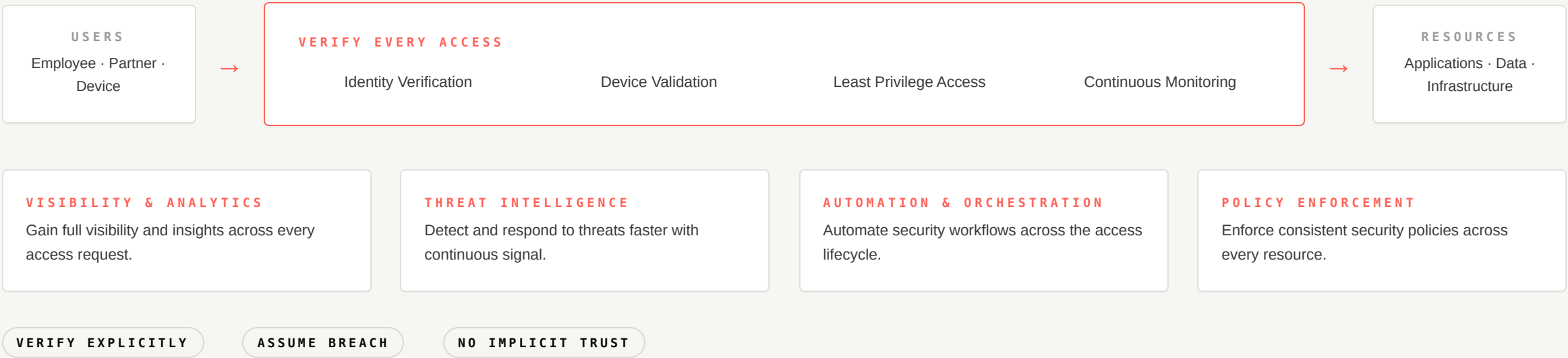
CLOUD BENEFITS



ENTERPRISE ARCHITECTURE

Zero Trust Architecture

Never trust, always verify. Every identity, device, and request is authenticated and authorized continuously — regardless of network origin.



OPERATING FRAMEWORK

Security Fundamentals

Every engagement is run against a continuous cycle rather than a one-time audit — the same loop our internal teams use to keep client environments defensible over time.



IDENTIFY & PROTECT

Map assets and exposure, then implement layered safeguards before they're needed.



DETECT & RESPOND

Continuous monitoring surfaces threats early; playbooks drive immediate, decisive action.



RECOVER

Restore operations and feed every incident back into people, process, and technology.

EXECUTION PIPELINE

Secure Software Development Lifecycle

Security review mechanisms are built into every lifecycle milestone, never appended after deployment.

01

Plan

Environment constraints and system scale rules before development.

02

Design

Secure architecture layouts, node schematics, sanitization plans.

03

Secure Build

Defensive logic patterns and static analysis configurations.

04

Secure Test

Automated scans combined with active manual VAPT exploitation.

05

Deploy

Isolated cloud instances guarded by fine-tuned perimeter rules.

06

Monitor

SIEM log tracking to intercept anomalies or drift immediately.

CI / CD BLUEPRINT

DevSecOps Delivery Pipeline

Every commit is built, scanned, tested, and deployed inside a single automated pipeline — with security gates enforced at each stage, not bolted on afterward.



Shift-Left by Default

Static and dependency scans run on every commit, so vulnerabilities surface in code review — not in production incident response.

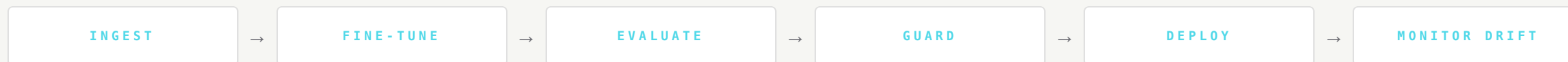
Human-Verified Gates

Automated tooling is paired with manual exploitation testing and a sign-off gate before anything reaches production traffic.

AI DEVELOPMENT LIFECYCLE

AI Development Lifecycle & RAG

From data ingestion to grounded inference — every AI system we ship is versioned, evaluated, and monitored like production infrastructure, not a research artifact.



→ LLM Fine-Tuning & Evaluation

→ Continuous Drift Monitoring

→ Guardrails & Policy Layers

→ Multi-Tool Agent Orchestration (MCP)

PLATFORM & TOOLING

Technology Ecosystem

A modern, scalable and reliable technology stack spanning cloud platforms, orchestration, CI/CD, data, and applied AI tooling.

CONTAINERS & ORCHESTRATION

Docker Kubernetes

INFRASTRUCTURE AS CODE

Terraform Ansible

CI/CD

GitHub Actions GitLab CI Jenkins

MONITORING & OBSERVABILITY

Prometheus Grafana

DATABASES

MySQL PostgreSQL Redis MongoDB

PROGRAMMING LANGUAGES

Python Node.js TypeScript Java Go
.NET

DEEP - DIVE

Docker & Kubernetes

Every workload we ship is containerized with Docker and orchestrated with Kubernetes — giving clients consistent environments from a developer's laptop to global production clusters, with self-healing, automated scaling, and zero-downtime rollouts built in.

BUILD

Application code is packaged with its dependencies into lightweight, portable container images.

→ Self-Healing Workloads

SHIP

Images are scanned, versioned, and pushed through the registry into staging and production.

→ Service Mesh & Ingress Control

→ ROLLING & BLUE-GREEN DEPLOYS

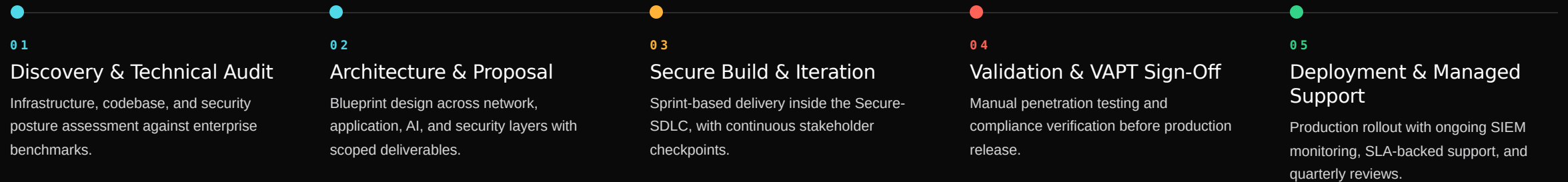
RUN

Kubernetes schedules, heals, and scales containers across nodes with no manual intervention.

→ Horizontal Pod Autoscaling

DELIVERY FRAMEWORK

Client Engagement Journey



SINGLE POINT OF CONTACT

Every engagement ships with a dedicated technical lead from discovery through go-live — the same engineer who designs the system stays accountable for defending it.

FORWARD ROADMAP

Innovation Roadmap

FY26

Foundation & Scale

Expand managed VAPT retainers, launch standardized Secure-SDLC tooling for mid-market enterprise clients, and formalize the AI Agent orchestration practice.

FY27

Platform & Automation

Ship an internal Zero Trust policy engine product, deepen multi-cloud disaster recovery offerings, and expand RAG-based enterprise knowledge systems.

FY28

Research & Frontier

Dedicated R&D track for autonomous security validation agents and continuous compliance automation across regulated industries.

Three years, one continuous lifecycle — every roadmap milestone builds on the same accountable practice, not a new vendor relationship.

GATEWAY HUB

Let's build the system you never have to worry about.

Agile AI is available for enterprise discovery calls, technical audits, and architecture consultations.

OFFICIAL DOMAIN

agileai.co.in

ENTERPRISE CONTACT

info@agileai.co.in

FOLLOW AGILE AI



INSTAGRAM



LINKEDIN



FACEBOOK



X



YOUTUBE