VALLIGNUS

Vallignus Runtime Governance Capability Brief

Classification: Unclassified

Distribution: Technical Evaluation and Awareness

VALLIGNUS.COM

Overview

Vallignus provides deterministic runtime governance for autonomous AI systems.
It enforces execution boundaries at the moment authority is exercised, independent of model reasoning, intent alignment, or application logic.

The system is designed to address a growing control gap introduced by autonomous agents operating with persistent access to files, networks, credentials, and external tools.

The Problem

Modern AI agents are increasingly granted direct execution privileges in order to perform tasks autonomously.

These systems are capable of:

- Invoking tools
- Accessing file systems
- Initiating network requests
- Operating continuously without supervision

Current safeguards focus primarily on influencing model behavior through prompts, filters, or alignment techniques. These mechanisms do not enforce control at runtime.

As a result, agents often retain authority beyond intended scope, creating conditions for:

- Unauthorized network egress
- Privilege drift
- Infinite execution loops
- Unbounded retry behavior
- Limited accountability at decision time

This introduces operational and security risk in environments requiring strict execution control.

Vallignus Approach

Vallignus introduces an independent runtime governance layer positioned between autonomous agents and the systems they are authorized to access.

Rather than attempting to predict or influence agent behavior, Vallignus enforces deterministic constraints on execution itself.

Execution authority is evaluated at runtime for every attempted action.

If an action violates policy, execution is denied prior to system interaction.

Core Capabilities

- Execution level policy enforcement
- Deny by default execution posture
- Runtime interception of tool and network requests
- Deterministic allow or deny decisions
- Time bounded execution authority
- Structured audit records generated at enforcement time

These controls operate independently of model architecture, agent framework, or reasoning strategy.

What Vallignus Prevents

- Unauthorized external network communication
- Persistent privilege beyond intended task scope
- Uncontrolled retry and loop behavior
- Silent execution drift over long running sessions
- Post hoc only monitoring without prevention

Demonstrated Capability

A controlled enforcement demonstration was conducted in which an autonomous agent attempted an unauthorized external network request.

The request was intercepted at the execution boundary and denied prior to network transmission.

A structured audit record was generated synchronously at decision time.

Documentation of this enforcement event is available upon request.

Intended Use

Vallignus is designed for environments requiring enforceable execution control, including:

- Enterprise autonomous workflows
- Regulated infrastructure environments
- Security sensitive automation systems
- Long running or unattended agent deployments

Availability

Additional technical documentation and enforcement demonstration artifacts are available upon request.

Website: https://vallignus.com

Point of Contact

Name: Jacob Gadek
Title: Founder
Organization: Vallignus
Email: jg@vallignus.com
Website: https://vallignus.com