
PORTFOLIO OVERVIEW

Ten solutions, one evidence architecture.

Read at a glance, this looks like ten products. Read at the architecture, it is one thing built ten times: every solution operates inside a declared boundary, records what it did, and emits signed evidence an assessor can verify without us. The products differ in what they govern. They do not differ in how they prove it.

Wagoner Enterprises, LLC. Founded May 2023. Bruce Wagoner, Chief Technology Officer. 202-794-3282. Washington, D.C. metro area.

10

Solutions across four capability families

TRL 5 to 6

Validated in a relevant environment; two solutions proven on live pursuits

One spine

Boundary, audit record, and signed evidence in every product

No lock-in

Open standards, portable data, written exit path

What every product shares.

This is the part that matters to an acquirer, an assessor, and a program office for the same reason: it is the reason a second product costs less to authorize than the first.

01

A declared boundary

Every product states where its data lives and what, if anything, crosses out. Disconnected operation is the default mode, not a special edition.

02

An immutable audit record

Every access, inference, and data flow is written in one record shape, hash chained. A write failure fails the operation it describes.

03

Signed, verifiable evidence

One Evidence Pack format across the portfolio: manifest, content hashes, attestation chain, offline verification. Structure published openly.

One deployment shape

Containerized, Kubernetes-deployable, configuration as code. The same artifacts move across tiers by changing the environment profile.

The practical consequence: a program that has assessed one Wagoner product has already assessed most of the next one. The control evidence, the audit model, and the deployment pattern are the same artifacts with different contents.

FAMILY 01

Classified AI Operations

Running and validating models where the network ends.

AirGap LLMOps

Governs the model lifecycle across an air gap. Releases are built and signed on the connected side, verified on receipt inside the enclave, then promoted through policy gates and watched for drift and tamper.

Open (<https://wagonerenterprise.com/solutions/airgap-llmops.html>)

Aegis

Governed AI assurance and adversarial validation: probes AI guardrails and agent permissions under non-destructive campaigns, emits detection content for purple teams, and packages results as signed, OSCAL-ready evidence a disconnected reviewer can verify.

Open (<https://wagoneenterprise.com/solutions/aegis.html>)

FAMILY 02

Authorization & Evidence Automation

Producing the artifacts an assessor asks for, continuously, as a byproduct of the work.

DevSecOps Evidence Builder

Turns a repository or container artifact into SBOMs, normalized findings, least-diff remediation, POA&M drafts, and a signed Evidence Pack.

Open (<https://wagoneenterprise.com/solutions/devsecops-evidence-builder.html>)

Vigil

Links controls to evidence, runs scheduled continuous monitoring with snapshots and trends, and generates schema-validated OSCAL SSP, SAR, and POA&M packages under an approval lifecycle.

Open (<https://wagoneenterprise.com/solutions/vigil.html>)

LLM Procurement Compliance Harness

Standardizes vendor transparency intake, memo-aligned evaluation, and risk review into one signed, portable Procurement Pack.

Open (<https://wagonerenterprise.com/solutions/m2604-procurement-harness.html>)

FAMILY 03

Data & Policy Automation

Turning written policy into enforced, auditable configuration.

ClassifyAI

Classifies documents using policy as code, routes every decision to human adjudication, and keeps a hash-chained record throughout. Inference runs inside the boundary; no data leaves it.

Open (<https://wagonerenterprise.com/solutions/classifyai.html>)

Palisade

Turns flow, identity, asset, and Kubernetes telemetry into ranked Zero Trust changes, compiled for four enforcement targets with a blast-radius estimate, a rollback artifact, and signed, offline-verifiable evidence.

Open (<https://wagonerenterprise.com/solutions/palisade.html>)

Mission Platforms

Whole platforms rather than single capabilities. Halo is bought by platform owners and security teams. PursuitIQ and Rostrum sit on either side of the same pursuit and are bought by a contractor or integrator rather than by a government program.

Halo Security Platform

Sits between an AI agent and what it is reaching for, decides whether to allow, sandbox, escalate, or deny, and records every decision in a tamper-evident ledger that produces OSCAL-ready evidence.

Open (<https://wagonerenterprise.com/solutions/halo-security-platform.html>)

PursuitIQ

Governed capture and proposal operations: opportunity discovery and win probability, solicitation parsing, compliance matrix, collaborative authoring with a governed AI copilot, readiness checks, and auditable export.

Open (<https://wagonerenterprise.com/solutions/pursuitiq.html>)

Rostrum

Rehearses a team against the evaluation panel they will face, joining the meeting they already use and scoring the session against the real evaluation criteria.

Open (<https://wagonerenterprise.com/solutions/rostrum.html>)

The four questions every reviewer asks.

Is it authorized?

No. No product holds an ATO, a FedRAMP authorization, or an Impact Level accreditation. Products are engineered to the discipline of a system on a path to authorization.

How mature is it?

TRL 5 or TRL 6 by solution. PursuitIQ and Rostrum are TRL 6, demonstrated in a relevant environment on live federal pursuits; the remaining solutions are TRL 5, validated end to end in a relevant laboratory environment. All are engineered to enterprise deployment standards. Production hardening and accreditation are scoped per program.

Where does our data go?

Nowhere. Not retained, not trained on, not accessed. A self-hosted in-boundary inference mode is available so no model call leaves the authorization boundary.

What if we want out?

Open standards, portable data, documented configuration, and a written exit path. Test the export during the pilot rather than taking the commitment on trust.