Adaptt

ADAPTT ASSURED AGENT PLATFORM (AAP)

Built to be authorized.

Adaptt is a cybersecurity-first company building the AAP: governed agents that build, test, and secure mission software, inside the customer boundary.

Adaptt

THE PLATFORM

Ratify is the first module of the Adaptt Assured Agent Platform (AAP).

Module	Stage	Scope	Status
Ratify	Authorize	Assessment, cited findings, package	Operating
Mend & Defend	Sustain	Remediation with explicit closure states; a defensive cyber lane	In development
Develop	Build	Attestation-gated pair programming	In development · Patent pending
Prove & Renew	Test · Refresh	Software assurance; bounded modernization	In development · Patent pending
Ratify	Monitor	Continuous lane: drift against the authorized baseline	Planned
Ship	Deploy	Moves the tested release into production, verified bit-identical, as a change for security impact analysis	Planned

Agents in the enclave: in a test on one disconnected workstation, Ratify ingested runtime records from the open-source NVIDIA OpenShell project as typed, control-mapped authorization evidence, each policy approval bound to a named person (October 2026).

Adaptt · adaptt.ai/platform · 2 · OpenShell result: v0.1.2 gateway log stream, one host, Docker driver, scripted test agent, synthetic data; measures how Adaptt makes OpenShell's enforcement record authorizable.

Adaptt

HOW THE PLATFORM WORKS IN DEVELOPMENT

Governed agents on one evidence fabric. Agents assemble and check the evidence; a named person decides.

Ratify · Authorize
Operating

Mend & Defend · Sustain
In development

Develop · Build
In development · Patent pending

Prove & Renew
In development · Patent pending

Ratify · Monitor
Planned

Ship · Deploy
Planned

THE SPINE EVERY MODULE RUNS ON · MEASURED OCTOBER 2026

Agents run in a sandbox

On one disconnected workstation, the open-source OpenShell sandbox enforced its declared policy: every policy-denied network, filesystem, privilege and process action stopped; every permitted one allowed; its records matched host observation.

One approval, one exact action, once

Each approval allowed one exact, rechecked action, once. A modified, stale, expired, replayed or revoked approval was refused, with a typed record naming the person who decided.

Hostile tasking contained

Every scored injected action that was followed or forced was contained and recorded: a restricted read, an outside URL or an out-of-workspace edit suspended the run; an audit-log edit was rejected at attestation.

The record answers for itself

From the evidence store alone, the six authorization questions were answered correctly for every incident, and each tampering was detected and named against the separate checkpoint.

Ratify turns the record into evidence

Ratify ingested the sandbox's runtime records as typed, control-mapped authorization evidence, each policy approval bound to a named person. The same cited package the authorizing official already reads.

Where it runs

Local models only, one workstation-class GPU, inside the customer boundary. The egress guard verifies zero external connections on every run. The operator, not the software, makes the decision.

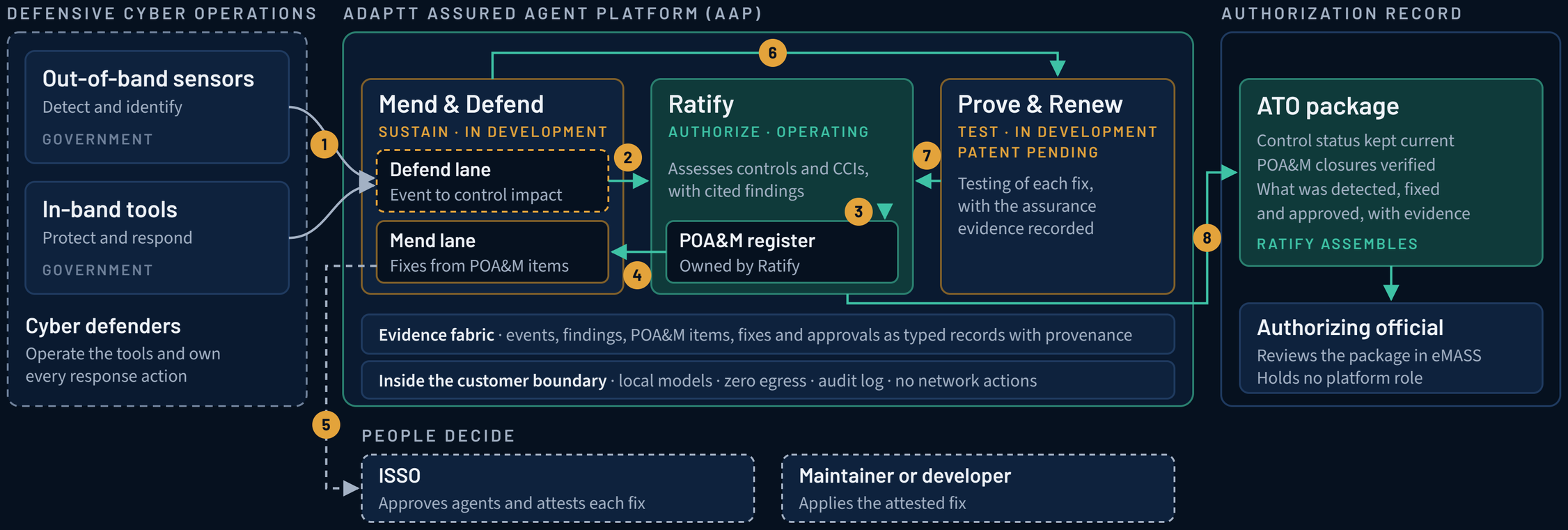
Spine results measured on one disconnected workstation (OpenShell 0.1.2, Docker driver, synthetic data), in automated tests and live runs with trace artifacts retained. Integrity detection covers edits by any party lacking both store-write and checkpoint-write authority.

Adaptt

HOW THE MODULES WORK TOGETHER · IN DEVELOPMENT

From detection to authorization evidence

The design carries what defenders detect and fix into the authorization record. Ratify operates today, and a named person decides every step.



1 Detect 2 Map to controls 3 Assess 4 Draft a fix from the POA&M 5 ISSO attests 6 Test the fix 7 Verify closure 8 Record in the package

Adaptt

THE PROBLEM

Systems need to change fast. The authorization process isn't built for speed.

Every control

An authority to operate (ATO) means checking the system against its full NIST SP 800-53 control baseline, one control at a time.

Every change

Each change to the system gets a security impact analysis (SIA) against that same control set before it goes live.

All by hand

Until now, the security team has done this work manually: hours of toil for every change.

> “The department must continue to identify and reform structural bottlenecks in the acquisition system such as the Authority to Operate (ATO) process, access to classified infrastructure, arduous accounting methods, and more.”
>
> Berkenstock, Gray & Manuel, “From Venture Capital to the Arsenal,” Hoover Institution, November 2026

Adaptt

RATIFY OPERATING

Cited, reviewer-ready findings against NIST SP 800-53 and 800-171.

1 · Assess

Point it at your policy corpus and control set. Every finding carries the document and section it came from.

2 · Review

Objective-level gaps, with drafted language for each. Ratify checks every citation against its source and flags any finding whose citation it cannot verify.

3 · Package

Ratify records every decision under the reviewer's name. The package is ready for your signature.

Change control

Ratify's change-control workflow starts each security impact analysis (SIA) from the change type, proposes each control's probability of impact for the ISSO to assess or confirm, and exports the approved SIA for review in eMASS.

POA&M tracking

Each deferral becomes a plan of action and milestones (POA&M) item with the reviewer's reason, criticality, and scheduled completion date, tracked from deferral to completion with exportable records.

Adaptt

HOW RATIFY WORKS OPERATING

Retrieval and a deterministic check around a small local model.

Policy corpus
System security plan, policies, procedures. Indexed on the node; nothing leaves it.

Control set
NIST SP 800-53 Rev 5 baseline with DISA CCIs, or NIST SP 800-171 Rev 2. Keys both lanes.

Scanner exports
ACAS (Nessus) and SCAP results as exported files.

Recorded change
A change the ISSO records and marks by type. The types select the starting controls.

›

1 · Retrieval
Keyword scoring plus a local vector index. The model is handed only what was retrieved.

2 · Local open-weight model
8B-class, served on the node. Drafts each finding, and the missing policy language, from the retrieved evidence only.

3 · Citation check, no model
Every citation is compared with the retrieved text: verified, partial, or unverified. Unsupported sentences are flagged, never credited.

System lane · CCI crosswalk, no model
Scanner finding to CCI to 800-53 control by fixed, revision-aware rules. No model in this lane.

Change lane · security impact analysis
Starts each SIA from the change type, proposes each control's probability of impact for the ISSO to assess or confirm, and exports the approved SIA for review in eMASS.

›

Cited findings and package
Per-control and per-CCI determinations, each with its document and section. Draft SSP language, POA&M register, tracked policy edits.

Documented against observed, per control: where the paperwork and the machines agree, disagree, or are silent.

A named person decides
Each finding is approved or deferred under the reviewer's name, with reason and timestamp. The operator, not the software, makes the decision.

Why the layers matter
In a pre-registered ablation on the same adjudicated set, the same model without retrieval scored 4 of 25 instead of 19. Without the citation check, citation correctness fell from 100 to 84 percent.

Where it runs
One workstation-class GPU, about 48 GB of memory, in one container. Disconnected; the egress guard verifies zero external connections on every run.

Adaptt

MEASURED, ON THE RECORD

Runs local, fast and accurate.

~12 min

all 110 NIST SP 800-171 controls on one workstation, on a partner organization's policy and procedure corpus

15 s

In internal testing, Ratify drafted a complete security impact analysis for review in a median of 15 seconds (10 representative changes, five repeats each, on one workstation graphics processing unit, with no network egress)

100%

citation correctness across 2,590 assessments over four corpora, five repeats each

99.39%

of control correlation identifier (CCI) references (3,910 of 3,934) in lab scanner results resolved to the governing 800-53 control by fixed rules

0

external network connections, verified on every run by the egress guard

Bounded internal benchmarks and adjudicated evaluation sets on one workstation-class node, with trace artifacts retained. Not adjudicated certification accuracy, assessor acceptance, or proof of operational implementation.

Adaptt

COMPANY

Built for programs that have to ship and stay authorized.

Founder Scott Worden has delivered solutions to Department of War challenges for more than two decades. Most recently he led the cybersecurity team at the U.S. Space Force Tools, Applications and Processing Lab to achieve ATO across multiple enclaves.

Adaptt started focusing on Super Intelligence (SI) solutions when it concluded that SI would transform the development to operations pipeline, and began building the Adaptt Assured Agent Platform.

- Veteran-Owned Small Business, SBA VetCert certified
- Cybersecurity Maturity Model Certification (CMMC) Level 2 (Self) 110/110, posted in SPRS
- Six provisional patent applications, assigned to Adaptt LLC
- Member, Linux Foundation and the Open Secure AI Alliance
- CAGE 12TS2 · Erie, Colorado

Adaptt

NEXT STEP

See Ratify run on your policies, inside your boundary.

adaptt.ai/ratify

scott@adaptt.ai

A live session runs on one workstation inside your boundary. The operator, not the software, makes the decision, and Ratify records every finding disposition as an audit event under the reviewer's name.