



CASCADe 2027 NON-CONFIDENTIAL SUMMARY »

AI Agent Vending Machine: Trustworthy AI Agent Builder for Novices and Experts

Overview

Universities, healthcare systems, enterprises, small and mid-sized businesses and other organizations increasingly want AI assistants to support departments, labs, courses, and clinics, but building one that is accurate, safe, and genuinely useful requires prompt engineering, evaluation design, and safety review skills that most staff and faculty do not have. Purple Studio solves this by letting anyone describe what they need an AI agent to do in plain language, then automatically generating a complete, reviewable agent — including guardrails, checked knowledge-source links, a recommended model with cost estimate, and proposed adversarial tests the builder can run to check that the agent behaves as intended.

Purple Studio is the agent that helps build agents, itself built by agents. Above all it is a player-coach: it teaches and guides the user while helping them build well-structured, tested and safe agents. Those agents are largely platform-agnostic and not proprietary by design; they run on nebulaONE or any similar platform.

- **Removes the technical expertise barrier:** Non-technical staff and faculty can build working AI agents without prompt-engineering or safety-review training.
- **Builds in trust rather than bolting it on:** Every Workshop agent is offered a safety review, its links are checked, and its builder can run cost-capped adversarial tests before release.
- **Scales institutional capability:** Because it runs on a platform already used by more than 100 universities and healthcare systems worldwide and works with other agent platforms too, the approach can extend well beyond UW.
- **Proven in use:** A CoMotion staff member drafted the first version of this profile with an agent they built in Purple Studio.

Description

Purple Studio is a software platform (modality: enterprise AI tooling / research tool for institutional AI governance) that converts a plain-language description of a desired AI assistant into a fully specified, reviewable agent definition — role, instructions, guardrails, checked knowledge-source links, a recommended underlying model with an associated cost estimate, and about a dozen proposed adversarial test scenarios. Every link Studio lists for an agent is checked before it is attached (HTTPS only, no private-network or look-alike addresses, and a live page), system prompts carry no links, and sensitive-data protections (redaction, authorization) are built into the generation process rather than added afterward.

COMOTION REFERENCE »
BDP 9341

INNOVATION MANAGER »
Laura Dorsey

SECTOR »
Agentic AI

LEAD INVESTIGATOR »
Jared Reimer, Lead AI Architect,
University of Washington
Information Technology (UWIT)

UNIVERSITY OF WASHINGTON
COMOTION »
1100 NE Campus Parkway, # 200
Seattle, WA 98195
Tel: (206) 543-3970
uwcomotion@uw.edu
comotion.uw.edu



A key technical differentiator is Purple Studio's "honesty contract": the Workshop is instructed never to claim that a tool ran, a check passed, or a score was produced without that turn's unpredictable run receipt, and testing measures how often it slips — directly addressing the hallucination and false-confidence failure modes that undermine trust in AI assistants. Each build promoted beyond the lab is regression-tested by Crucible, a separate UWIT test harness, on 17 pass/fail criteria scored by an LLM judge combined with deterministic detectors (the current production build passed 17 of 17 in a 501-turn staging round), then promoted through a four-environment pipeline before reaching production.

Purple Studio is available to everyone at UW, more than 100,000 students, faculty and staff, at purple.uw.edu, and is used every day; more than 1,300 agents have been built on Purple. Current users include UW departments, labs, courses, and clinics that want department-specific AI assistants but lack in-house prompt-engineering and AI safety expertise.

The platform is a Model Context Protocol (MCP) server in TypeScript (240 source files, about 73,000 lines) with 4,973 passing automated tests, 361 pages of documentation, 56 Architecture Decision Records, infrastructure defined as code and a gated four-environment promotion pipeline; it has reached 273 versioned releases since development began in April 2026. It runs today on Cloudforce's nebulaONE platform, used by more than 100 universities and healthcare systems worldwide, but it does not depend on nebulaONE: Purple Studio is platform-agnostic by design, works with competing platforms, and can be ported to other hosting environments.

Technology Readiness Level (TRL)

Purple Studio is assessed at TRL 9 — a fully developed product deployed and operating in its intended real-world application at UW, with successful deployment and ongoing use. The platform has been in continuous production use at UW since July 2026 and is now available to everyone at UW, more than 100,000 people, at purple.uw.edu. It has 273 versioned releases (v2.0.0 through v13.12.21), passes 4,973 automated tests, and every build promoted beyond the lab is regression-tested by Crucible on 17 criteria and promoted through a gated four-environment pipeline before reaching production. It runs live on Cloudforce's nebulaONE platform and has been presented at the Notre Dame Higher Ed AI Forum, the Microsoft Azure Customer Advisory Board, the Cloudforce nebulaONE Customer Advisory Board, numerous UW events, and to leading universities worldwide.

Value Proposition

- **Anyone can create an agent:** Non-technical staff and faculty can create working AI agents without needing prompt-engineering, evaluation, or safety-review expertise.
- **Reduces hallucination and false-claim risk:** The honesty contract and run receipts reduce the risk of the agent-building tool claiming actions, checks, or results that never happened, and testing measures how often it slips.
- **Built-in quality assurance:** Every build promoted beyond the lab is automatically scored by Crucible on 17 criteria and promoted through a gated four-environment pipeline before deployment, and builders can run cost-capped adversarial tests on their own agents.
- **Teaches as it builds:** Purple Studio is a player-coach: it teaches and guides while it helps build the agent, explaining its design choices and next steps and increasing the long-term AI literacy and judgment of its users.
- **Platform reach:** Running on nebulaONE, a platform used by more than 100 universities and healthcare systems worldwide, which Purple Studio makes far more useful (Cloudforce has expressed interest in

incorporating it), while also working with other platforms, provides an early market and path to adoption beyond UW.

Intellectual Property Position

Assessing patent landscape currently. Purple Studio is protected as original software, developed within a UW-owned Azure DevOps repository with a full version-controlled history (953 commits and 273 versioned releases, v2.0.0 through v13.12.21, as of October 14, 2026).

Market Opportunity

- Broader customer segments include other higher-education institutions, particularly the more than 100 universities and healthcare systems worldwide already using the Cloudforce nebulaONE platform (including the University of Oxford, UCLA, the University of Maryland and London Business School) on which Purple Studio runs.
- Organizations that want to embrace AI but lack prompt engineering and AI safety expertise.
- Organizations that care about AI agent safety and reliability.
- Key unmet needs addressed include preventing AI assistants from fabricating information, mishandling sensitive data, or overstating their own performance.
- Market size: Purple Studio serves any organization that builds AI agents: enterprises, small and mid-sized businesses, healthcare systems and public agencies, as well as higher education, where 5,819 institutions in the United States and other jurisdictions participate in federal student aid programs alone (NCES, 2023-24). The opportunity extends well beyond universities and the education market.
- Demand is already visible at UW: the number of agents active on Purple each month rose from 60 in April to 369 in September 2026, and more than 1,300 agents have been built.
- Competition comes from agent builders inside commercial AI products (for example custom GPTs in ChatGPT, Microsoft Copilot Studio, Google Gemini Gems and Claude Projects) and from in-house prompt engineering. Purple Studio's differentiators are its player-coach approach, run receipts, link validation, safety review, FERPA and medical-redirect defaults, regression-tested building, builder-run testing, and agents that are not locked to any one platform; any competitor could add similar features.
- Commercialization paths include incorporation into nebulaONE (Cloudforce has expressed interest), licensing to other agent platforms, a multi-tenant service for enterprises, businesses and institutions, or a spinout licensing the software from UW. Each needs multi-tenant isolation, configurable branding and compliance defaults, and a team beyond today's single maintainer.

References

University of Washington Information Technology. *Purple Studio*. <https://it.uw.edu/guides/artificial-intelligence/purple/>