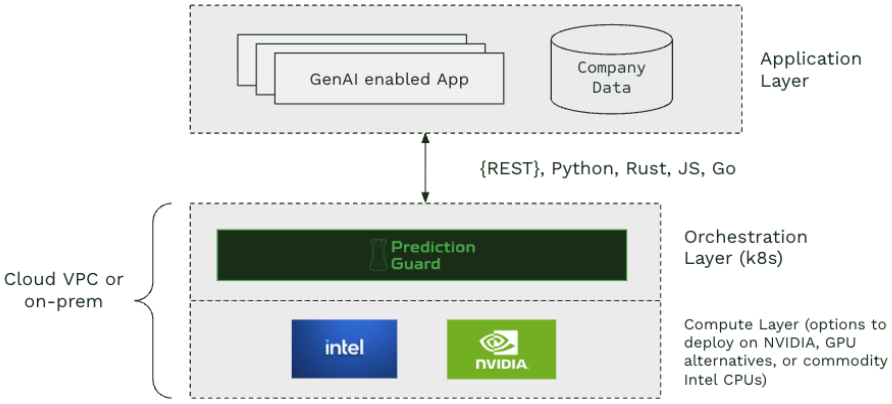
Quick Reference

Prediction Guard | AI Platform for Higher Ed

Self Hosted Prediction Guard Architecture



01. What is it?

A secure, on-prem AI platform that self-hosts AI model families, provides safeguards, and is developer friendly entirely within your campus environment—**no data ever leaves your network**

---

02. Core Benefits for Higher Ed

Feature	Description
Data Privacy & Compliance	No prompt data leaves the institution's infrastructure - ensuring student records, research data, and IP remain private and on-site.
Robust Security & Auditability	Real-time monitoring of model inputs/outputs for issues like PII, prompt injection, hallucinations, toxicity, etc. Track changes (API keys, model versions) to maintain full audit trails.
Deployment Flexibility	Supports on-premises, air-gapped, hybrid, or cloud VPC setups—ideal for secure campus environments. Supports GPUs, CPUs, and efficient hardware like GPU alternatives for performance scalability.
Model Optionality	Complete system hosting open-source models by task types, modality, and architectures—and you can even bring your own custom models.
Developer-Friendly Integration	Uses an OpenAI-compatible API—seamlessly works **in conjunction with existing tools** (LangChain, LlamaIndex, Vercel AI SDK, etc.) so you can build and deploy without relying on large 3rd-party AI platforms.

03. Ideal For...

- **Research computing teams** building AI-driven tools powered by student and grant-funded data.
- **Campus IT leaders** prioritizing compliance, privacy, and predictable costs.
- **Faculty and innovation units** who want the agility of generative AI *without* vendor lock-in or unexpected per-seat fees.

04. Value Highlights

- **Fixed-price deployment**—no per-user licensing costs.
- **Accelerates innovation** in AI-enabled teaching, research, and administration without adding headcount—or compromising security.
- **Own your AI stack**—retain full control over your data, model IP, and usage.

05. Next Steps

1. Let's set up a quick demo—see how your campus's existing tools can plug in via the API.
2. We'll discuss deployment options (on-prem vs hybrid), compliance needs, and budget.
3. You stay in control—secure, scalable AI without compromising data governance.

Third Party AI Platforms	On-Prem / On-Campus Platform
Data sent to 3rd-party provider (risk of data leakage)	All data stays inside campus network (no offsite transfer)
3rd-party controls infrastructure	Campus controls infrastructure
Consumption based API's	Fixed monthly cost, unlimited seats

Prediction Guard

GUARD YOUR DATA, UNLOCK AI VALUE

contact@predictionguard.com

Reach out for a demo: predictionguard.com/get-started