

Platform One SBIR Pitch Day Focus Areas

Q1 2025

Cloud Management Platforms

The Challenge: Regulated Multi-Tenancy

If there's a defining feature of the so-called cloud era, it is multi-tenancy at scale, achieved by an absolute commitment to self-service. On any of the major cloud providers, an individual or small business can create an account and deploy software with worldwide reach without ever communicating with a human being at the provider. It takes nothing but a credit card and a little bit elbow grease to get started. This low barrier to entry has enabled the creation of a virtually uncountable number of apps and services being created, stirring the pot of innovation and leading to an explosion of new products.

Within highly-regulated environments, there's significantly more friction even in what seem like similar environments. Compliance and regulatory concerns necessitate that applications and their owners comply with a number of controls, and that compliance must either be demonstrated (to a human via a questionnaire or ideally to a machine via automated analysis or testing) or enforced through "guardrails." All of this slows down the onboarding and change process.

Additionally, in a Defense context there are statutory requirements around how money appropriated by Congress is tracked and spent, so there is both a dearth of "free" tiers (a defining feature of many SaaS offerings) and a significant challenge in cost prediction and attribution.

Potential Solutions P1 Would Like to Explore

Platform One would be interested in learning more about commercial solutions to:

- Efficiently onboard customers into regulated environments, such as automated workflows to replace or augment traditional ticket-based IT Service Management systems, or similar;
- Rapidly generate or assess CI/CD pipelines and/or application configurations, reducing or eliminating the need for human touch on pipeline creation while allowing for the enforcement of security controls (e.g. requiring that unit tests pass with a certain level of code coverage, enforcement of linting standards, etc.)
- Attribute, track, predict, constrain, and report costs for cloud-based services such as databases and storage; in particular technologies or techniques that allow for services to swap between solutions of similar cost without intervention from the platform team.

Vulnerability Discovery & Management

The Challenge: Software Scale

Various executive orders, DoD Directives, and NIST publications continue to expand requirements around "software supply chains", including for open-source software. The sheer scale of the open-source ecosystem and the deep reliance on layered dependencies make this a difficult problem.

In recent years, the average time to exploitation of a published vulnerability has shrunk drastically. An accompanying increase in the use of "zero day" (previously unpublished) vulnerabilities shrinks the response time to effectively zero. At the same time, supply-chain attacks such as those against the XZ

compression library contra-indicate the consumption of new versions without any analysis of their safety and security.

Potential Solutions P1 Would Like to Explore

Platform One would be interested in learning more about commercial solutions to:

- Identify all of the software components used in a package, binary, image, or similar;
- Identify the chain of tools used to generate a released component, including but not limited to build automation tools (e.g. GNU Autotools, CMake), compilers, transpilers, linkers, packers, minifiers, and the like;
- Categorize changes to software source code or release artifacts such that human review can be reserved for the most consequential or riskiest changes;
- Apply sound techniques to assess the applicability of a CVE or a justification to a particular piece of software (reachability analysis, semantic search of documentation, etc.)

Artificial Intelligence Observability & Metrics

The Challenge: An Influx of AI Models and Tools

With the amount of “buzz” (and valuation!) around AI tools, every team and product seems to be incorporating Artificial Intelligence and Machine Learning today. Determining which of these tools are actually providing a real return on investment and which ones are just shiny objects requires some sort of measurement framework. Today, there is little to no standardization around measuring the effectiveness of most machine learning tools. In the same way that we’ve wrangled cloud into observability frameworks, we need to expose AI and ML metrics to the proper stakeholders.

Potential Solutions P1 Would Like to Explore

Platform One is interested in novel ways of conducting AI and ML observability. At this time, P1 is not specifically looking for ways to deploy models or ways to integrate LLMs with existing tools and processes – these areas have seen a glut of entrants, compared to the observability question.