

# Asset Compliance AI

An IT compliance platform

---

Gemini Ultra 1.0 Hackathon

Team Titan Warriors

# Team Titan Warriors

1. Dhruvin Koshiya
2. Colwin Fernandes
3. Shreyash Patel
4. Bhavya Soni
5. Neel Patel
6. Vance Cochrane

# Use-Case

**Internal IT Compliance and Chat Application to improve Asset Patch management and auditability.**

## Stack:

- Streamlit
- Langchain
- Google GenAI
- LLM: Gemini Pro 1.0

**Goal:** Build Asset Compliance Application with measurable time improvements for gathering audit information.

# Business Case

“The total addressable market (TAM) for IT compliance, specifically in the cybersecurity sector, is estimated to be between **\$1.5 trillion to \$2.0 trillion**. This represents a significant opportunity for cybersecurity technology and service providers, indicating a massive gap between the current market size of approximately \$150 billion and the potential market size. The under-penetration of cybersecurity solutions is one of the key factors contributing to this opportunity.” **McKinsey 2022**

“Gartner's analysis for 2024 emphasizes the significant influence of generative AI, increasing cybersecurity incidents, and the need for outcome-driven metrics in bridging communication gaps within organizations. They also highlight the growing importance of security behavior and culture programs, resilience-driven third-party cybersecurity risk management, continuous threat exposure management, and extending the role of Identity & Access Management to improve cybersecurity outcomes.” **Gartner 2024**

**So there is a definite play to be had in this market.**

McKinsey 2022: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers>

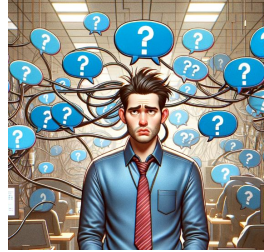
Gartner 2024: <https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024>

# Target Personas



## IT Compliance Teams

- What is my compliance level?
- What version of OS is at the latest patch level?
- Which of my assets is running application X?



## IT Support Teams

- Which machines do I have to patch?
- Which of my assets is running Windows?

# Existing Solutions and its limitations

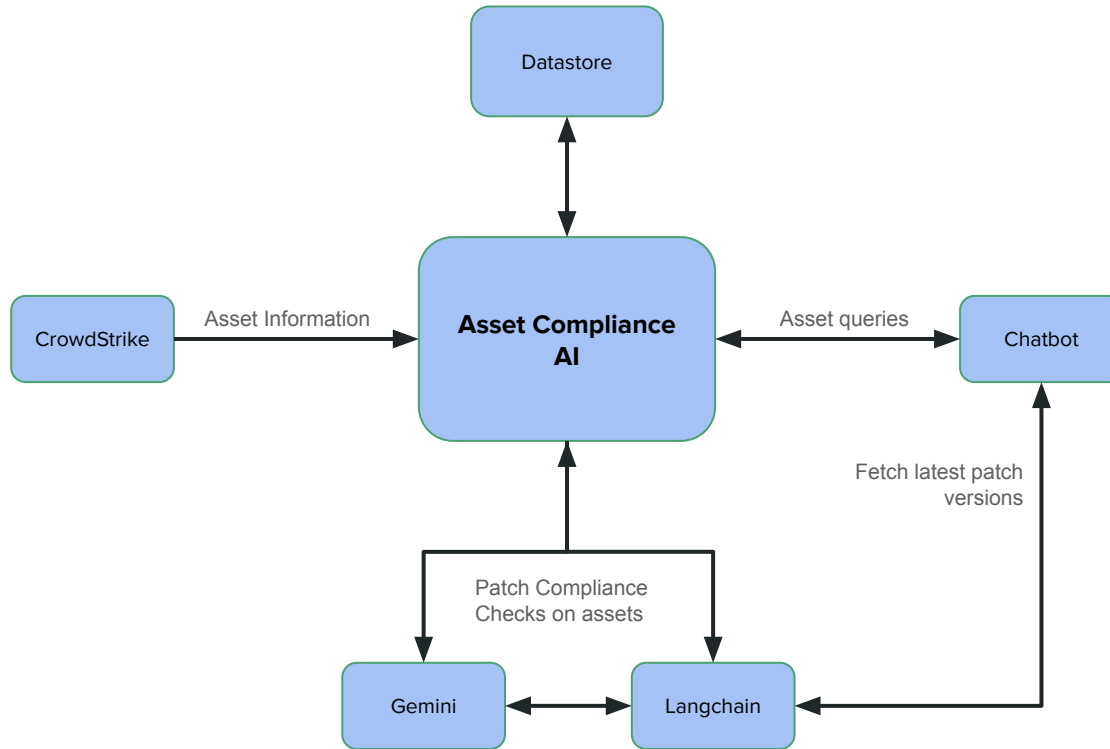
## Pain Points

- IT Compliance Teams spend too much time dealing with information gathering.
- The asset landscape at an organizational level is constantly in flux.
- Many organizations lack a comprehensive asset inventory.
- Audit's take up a lot of time on the part of the IT department.

## Existing Solutions

- Manual processes are used to gather the necessary information for compliance.
- Costly tools are put in place to mitigate issues related to compliance.

# System Architecture



# Demonstration

## Addressing the Pain Points

- Asset inventory
  - Show the current inventory up front.
- Patch levels
  - Highlight the existing inventory patch status for OS and applications.
- Quickly assess specific applications and hosts
  - Using the Compliance AI chatbot, get information about specific applications and hosts.



Thank you!