

AI Security

AI Governance | AppSec AI Agent

AI OVERVIEW

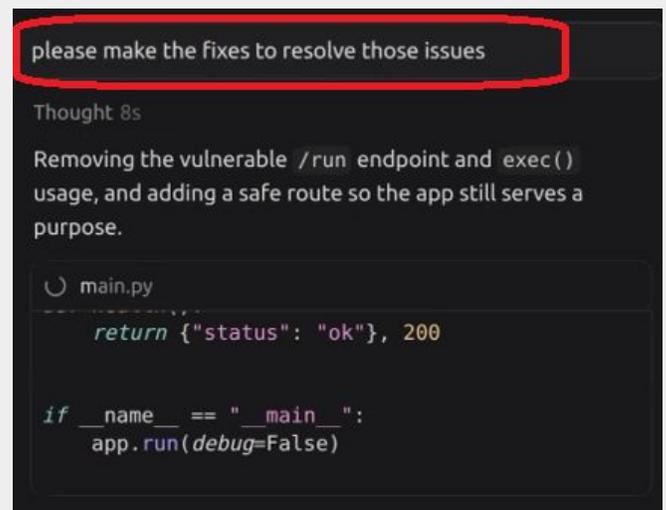
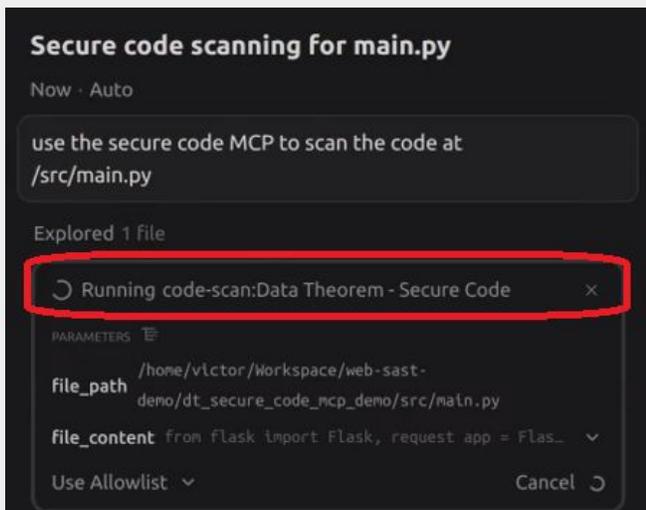
Data Theorem's AI Security platform includes a variety of product and features.

- MCP Server For AI Coding Assistants
 - Use prompts to scan code & implement secure code in PRs (via VSCode, Github Copilot, Claude, Cursor, etc.)
- AI Governance
 - Discover & Govern the use of AI in your business
- AppSec AI Agent
 - An intelligent security engineer who runs as an FTE
- GenAI Usage in your Supply Chain
 - Detects the use of GenAI tools in your supply chain (e.g., DeepSeek)
- AI Watermarking & More!

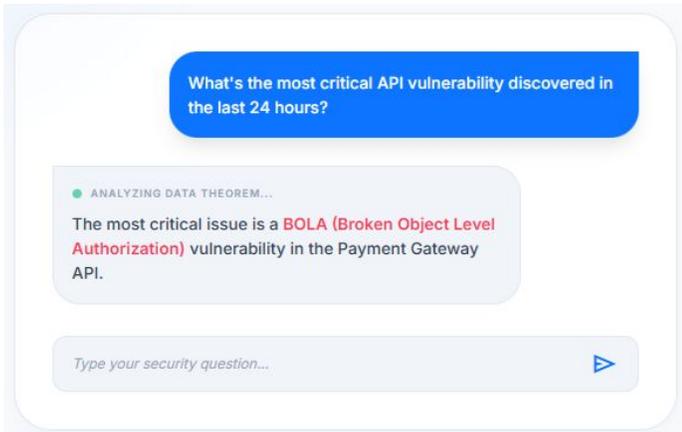
AI Security

- ✓ Products:
 - MCP for AI Coding Assistants
 - AI Governance
 - AppSec AI Agent
- ✓ Features within existing Products
 - Mobile, Code & API Secure
 - GenAI Usage in the Supply Chain
 - Source Code generated by GenAI
 - 3rd Party AI Servers scraping PII from your APIs
 - AI Watermarking

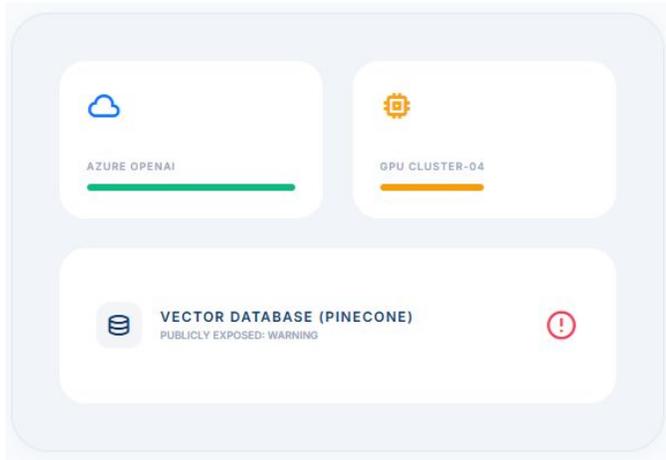
MCP Server for AI Coding Assistants



AI Security <Screenshots>



AppSec AI Agent



AI Governance (AI Usage in the Cloud)



GenAI in Code

Copyright © 2026 Data Theorem, Inc. All rights reserved.



Data Theorem is a leading provider of application security. Its core mission is to analyze and secure any application anytime, anywhere. The Data Theorem Analyzer Engine continuously analyzes APIs, Web, Mobile, and Cloud applications in search of security flaws and data privacy gaps. Data Theorem products help organizations prevent AppSec data breaches. The company has detected more than 1 billion application eavesdropping incidents and currently secures more than 8,000 modern applications for its Enterprise customers around the world.

LEARN MORE

Web: www.datatheorem.com
 Email: info@datatheorem.com
 Demo: www.datatheorem.com/demo

