datatheorem
Prevent AppSec Data Breaches

AI Security

https://datatheorem.ai

AI OVERVIEW

Data Theorem's AI Security platform delivers an AI-native AppSec stack that integrates runtime defense, AI-driven exploit detection, and automated remediation across the SDLC. It blocks AI-augmented attacks using behavioral analysis, leverages DAST and AI models to discover and validate exploits, and provides LLM-backed APIs for consistent remediation output. With MCP support for AI agents and a developer-focused CLI for CI/CD integration, it embeds security directly into workflows.

An AI AppSec agent acts as a virtual FTE, continuously triaging and fixing issues, while supply chain controls ensure the integrity and security of third-party and AI-generated code.

AI Security

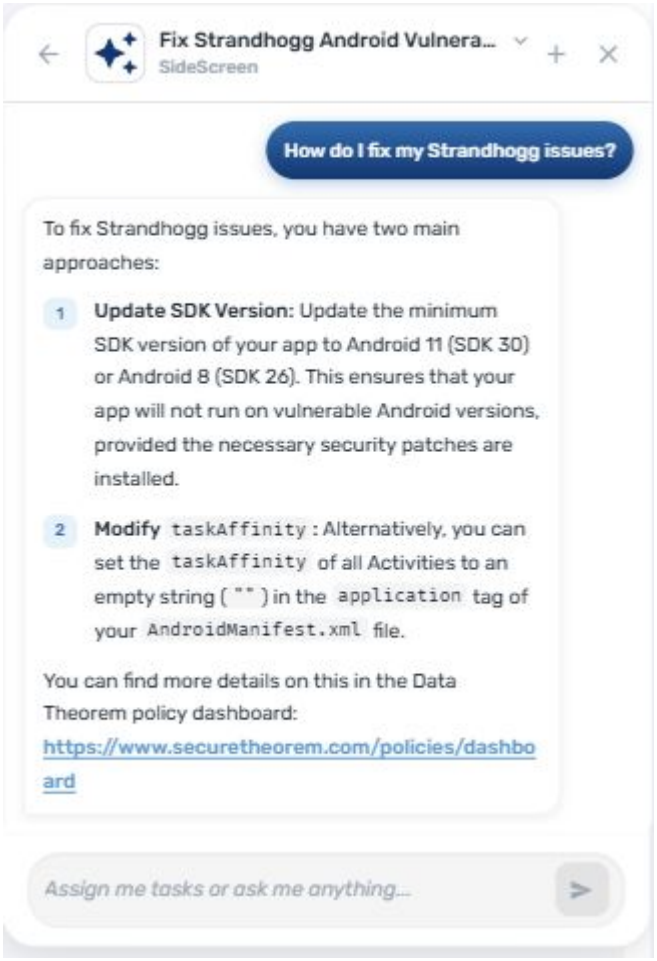
- Products/Features:
  - AI Runtime Defense
    - Block AI-Augmented Cyberattacks
  - AI Auto-Remediation
    - MCP for AI IDEs
    - CLI for Developers (Skills.md)
    - APIs for LLMs
  - AI-Enabled Exploit Discovery
    - DAST-Enabled Exploits
  - AI AppSec Agent
    - FTE for AppSec
  - AI Supply Chain
    - AI Code from 3rd Parties

Defend Apps & APIs from: AI-Augmented Cyberattacks

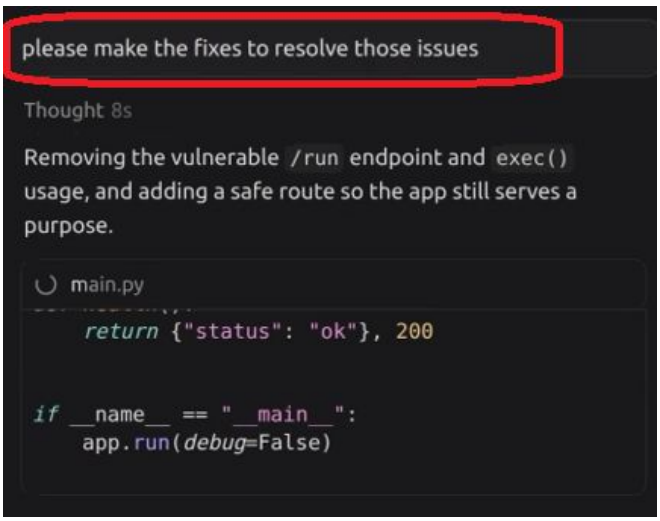
DATA SHEET

AI Security <Screenshots>

AppSec AI Agent



AI Auto-Remediation



AI in 3rd Party Code

datatheorem

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