SOLUTION BRIEF

datatheorem

AI Security

Defending Apps & APIs from AI-Augmented Attacks

Attackers now use artificial intelligence to discover exploits faster, generate evasion techniques at scale, and automate account takeover and fraud campaigns. Data Theorem addresses both sides of the equation: AI security capabilities woven across Code SAST Secure, API Secure, Mobile Secure, and Mobile Protect give security and engineering teams continuous, automated defense: from runtime threat blocking to AI-generated code auditing and intelligent auto-remediation.

The AI Attack Surface Is Expanding: Your Defense Must Too

AI-enabled attackers validate exploits at machine speed, LLM-generated code introduces vulnerabilities traditional tools miss, and overlay malware with AI-orchestrated jailbreaking bypass signature-based defenses. Supply chain blind spots leave AI-written dependencies unvetted in production.

The Expanding AI Threat Surface

AI-Augmented Cyberattacks

Attackers use AI to validate exploits at machine speed, automate credential stuffing, and scale account takeover and fraud campaigns beyond human capacity.

AI-Generated Code Risk

LLM-written code introduces vulnerabilities that traditional static tools miss, including insecure patterns and hallucinated dependencies with no security history.

Runtime AI Threats

Overlay malware with AI-orchestrated jailbreaking, prompt injection, and memory scraping bypasses signature-based defenses and targets deployed apps at runtime.

Supply Chain Blind Spots

AI-written third-party dependencies enter production unvetted, carrying vulnerabilities and unknown licenses that expand your attack surface invisibly.

Four Capabilities Built for This Threat Landscape

Data Theorem addresses each vector above with integrated capabilities spanning exploit discovery, runtime defense, automated remediation, and supply chain integrity.

SOLUTION BRIEF

datatheorem

Defending Your AI Attack Surface

Discover exploits before attackers do, block AI-driven attacks at runtime, remediate automatically, and patch open source risk at machine speed.

AI-Powered Exploit Discovery

- Reverse engineers binaries and compiled apps without source code
- Dynamically tests apps and APIs with deep runtime analysis
- Pinpoints exploitable vulnerabilities, not just theoretical risks
- Generates real proof-of-concept payloads
- Chains attack primitives to simulate real-world breaches

Defend Against AI-Driven Attacks

MOBILE PROTECT

- AI-driven attack path mapping
- Prompt injection detection
- Memory scraping and data exfiltration defense

API SECURE

- Prompt injection and LLM abuse detection
- AI scraping defense
- Password spraying and login automation prevention

AI-Powered Auto Remediation

- Native MCP support for AI-enabled IDEs
- Finds security issues in SKILL.md files via AI Agent CLI
- APIs designed for LLM-driven remediation
- Context-aware fixes aligned to real exploitability

AI Code Patch

- Continuously scans your open source supply chain
- Identifies actively exploitable vulnerabilities
- Automatically generates and applies secure patches
- Reduces exposure from zero-day to near zero

How to Get Started

1

Assess Your AI Exposure

- Request a no-cost attack surface assessment at datatheorem.com/demo

2

Deploy Platform Coverage

- Enable the AI AppSec Agent for automated triage and remediation

3

Automate & Scale

- Activate LLM-backed auto-remediation via MCP in AI-native IDEs

datatheorem

Data Theorem's Analyzer Engine continuously analyzes APIs, mobile, and cloud applications for security flaws and data privacy gaps. The platform has detected more than 1 billion eavesdropping incidents and currently secures more than 8,000 enterprise applications worldwide.

Learn More

www.datatheorem.com

info@datatheorem.com

Schedule a Demo →

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