DATA SHEET

datatheorem

API Secure

Discover, harden, test, and protect every API across mobile, web, and cloud.

01 OVERVIEW

API Secure is Data Theorem's full-lifecycle API security platform. It continuously inventories every REST, GraphQL, gRPC, SOAP, and serverless API, hardens posture across multi-cloud, attacks them with hacker-style tests, and defends against prompt injection, LLM abuse, and AI-augmented attacks at runtime via API Protect.

Discover, harden, test, and protect every API.

From discovery through runtime, API Secure covers the full API security lifecycle. Inventory, health, testing, and active protection in one platform.

02 CAPABILITIES

Platform capabilities

Continuous API discovery

Inventories every REST, GraphQL, gRPC, SOAP, and serverless API across multi-cloud. Surfaces shadow APIs in real time with Slack and Teams alerts.

API health and posture

Detects misconfigurations, weak encryption, and exposure across API gateways and serverless. Maps to the 5 pillars: authn, authz, encryption, availability, auditing.

Hacker-style API testing

Attacks discovered APIs with the same techniques real adversaries use. Black-box and grey-box coverage. Maps to the OWASP API Top 10.

Runtime API protection

API Protect monitors live API traffic via ALB logs and network taps. Blocks SSRF, SQLi, XSS, and OWASP API Top 10 attacks in production.

CI/CD remediation

Routes prioritized fixes and secure code samples into Jira, Jenkins, and the CI pipeline. Catches issues before they migrate into production.

Compliance reports on demand

Audit-ready reports for PCI DSS, GDPR, CCPA, HIPAA, OWASP, MITRE, and NIST. Generated in minutes, not weeks.

DATA SHEET

datatheorem

API SURFACE TESTED	REST · GraphQL · gRPC · SOAP | Serverless · SPA · B2B
COMPLIANCE REPORTS	PCI DSS · GDPR · CCPA · HIPAA · OWASP API Top 10 · MITRE · NIST · FTC

03 OUTCOMES

Key benefits

Find shadow APIs before attackers do

Continuous discovery across multi-cloud and on-premise surfaces shadow, zombie, and exposed APIs the moment they appear, with real-time alerts to Slack or Teams.

Hack before adversaries do

Hacker-style runtime testing reveals the entire black-box and grey-box attack surface and identifies the most critical vulnerabilities across native and third-party APIs.

Block attacks live in production

API Protect monitors live API traffic via ALB logs and network taps to stop SSRF, SQL injection, XSS, and OWASP API Top 10 attacks. No code changes required.

Audit-ready in minutes

On-demand compliance reports for PCI DSS, GDPR, CCPA, HIPAA, OWASP, MITRE, and NIST. Cut audit prep from weeks to minutes.

04 PILLARS

The 4 pillars of API Secure

1

Discovery & Inventory

Continuous, hacker-style discovery of every API across mobile, web, B2B, serverless, and cloud gateways.

2

API Health

Posture management across the 5 security pillars: authentication, authorization, encryption, availability, auditing.

3

Security Testing

SAST in CI plus DAST against discovered APIs. Real exploit techniques, not synthetic checks.

4

API Protect

Live API traffic monitoring via ALB logs and network taps (vTaps). No agents or code changes required.

05 AI / LLM

AI security for APIs, woven through

Prompt injection & LLM abuse

Detects malicious prompts and LLM-abuse attempts at the API layer, before they reach the model or backing data.

AI-augmented attack defense

Blocks AI-driven scraping, password spraying, account takeover, and login automation tuned to LLM-orchestrated traffic.

OWASP LLM Top 10 & MITRE ATLAS

Findings mapped to the OWASP LLM Top 10 and MITRE ATLAS frameworks for AI and LLM security audits.

ABOUT DATA THEOREM

Data Theorem provides full-stack application security across mobile, API, code, and cloud, with AI/LLM coverage woven through. Continuous, automated, hacker-style discovery and dynamic runtime analysis surface what matters and route fixes to the teams that own them. Our customers cover over 2.8 billion users and include 7 of the top 10 largest banks.

GET STARTED

www.datatheorem.com
info@datatheorem.com

Schedule a Demo →