datatheorem
Prevent AppSec Data Breaches

API SECURE

Hack | Extract | Detect | Protect

PRODUCT OVERVIEW

Data Theorem's API Security product is designed to:

1. Inventory all your APIs
2. Hack your APIs
3. Remediate security issues within the CI pipeline

The analyzer engine continuously discovers vulnerabilities in multi-cloud/on-premise environments and provides critical alerts/remediation solutions in real time.

PLATFORM FEATURES

✓ Inventory all applications and APIs
Real-time Alerts on Shadow APIs
Hack all RESTful APIs, Web Apps (SPA), and Serverless Apps

✓ Detects configuration and implementation flaws

✓ Provides secure code via Jira, Jenkins, etc.

✓ Instant compliance reporting

✓ Dynamic run-time security review across all 5 pillars of security:
- Authentication
- Authorization
- Encryption
- Availability
- Auditing

BENEFITS

- Continuous inventory of RESTful APIs, Serverless, and Single Page WebApps
- Systematically hack all attack points using common hacker techniques
- Identify the most critical vulnerabilities across all of your native and third-party APIs
- Instantly get alerts on new, changed, and exposed APIs via Slack/Teams
- Uncover shadow APIs leaking customer data
- Reveal your entire black box / grey box API attack surface
- Auto-remediate issues before a data breach occurs
- Save time & money by reducing the burden on IT, development, and operations staff
- Compliance reports are available within minutes for PCI, GDPR, CCPA, HIPAA, FTC, OWASP, MITRE, NIST, and more
- Find and fix security issues in CI pipelines, preventing them migrating into production

DATA SHEET

SECURITY FOR ALL

A common frustration for distributed teams is that many security tools are limited in function and only allow one user to have insights into vulnerability management and control over resolving them. For API security, application and infrastructure teams will need to address issues simultaneously. Our automated security tools are solving this to allow custom access for different, designated roles.

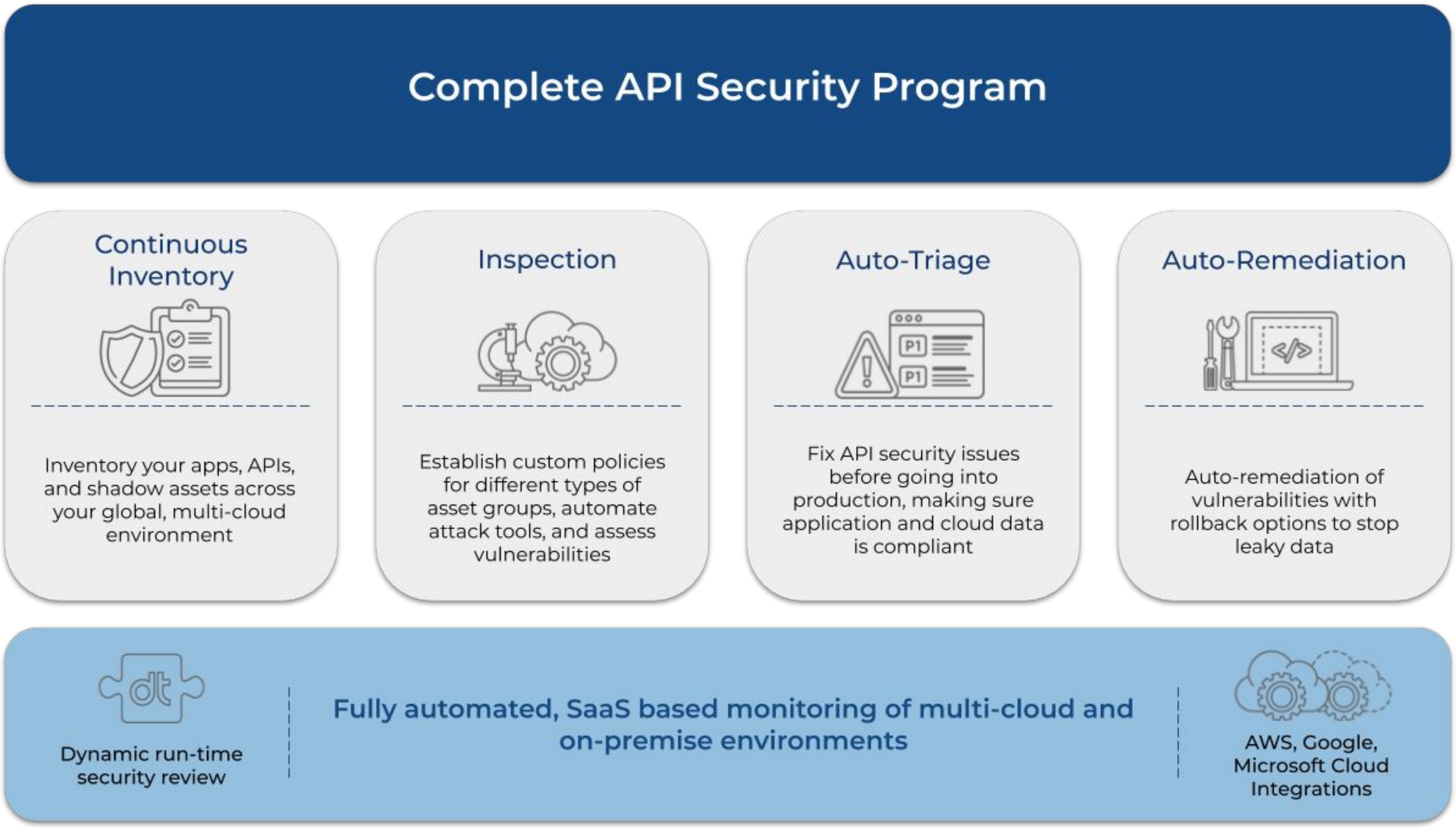
For example:

Infrastructure engineer: Has access to all results, can invite new users to the portal, access compliance reporting, and can close any issue at any time.

Security: Has access to zero apps by default, but must be given access to all security monitoring. The security user can close issues at any time and access reporting 24/7, but has no other access beyond closing issues one-by-one.

Developer: Has access to apps by default, but cannot close issues. The developer account allows viewing of secure code and remediation summaries.

> "With Data Theorem, we have continuous security testing in place for all of our apps in the app stores with security discovery and inspection across our modern APIs."
>
> Head of Security, Evernote



Complete API Security Program

Continuous Inventory

Inventory your apps, APIs, and shadow assets across your global, multi-cloud environment

Inspection

Establish custom policies for different types of asset groups, automate attack tools, and assess vulnerabilities

Auto-Triage

Fix API security issues before going into production, making sure application and cloud data is compliant

Auto-Remediation

Auto-remediation of vulnerabilities with rollback options to stop leaky data

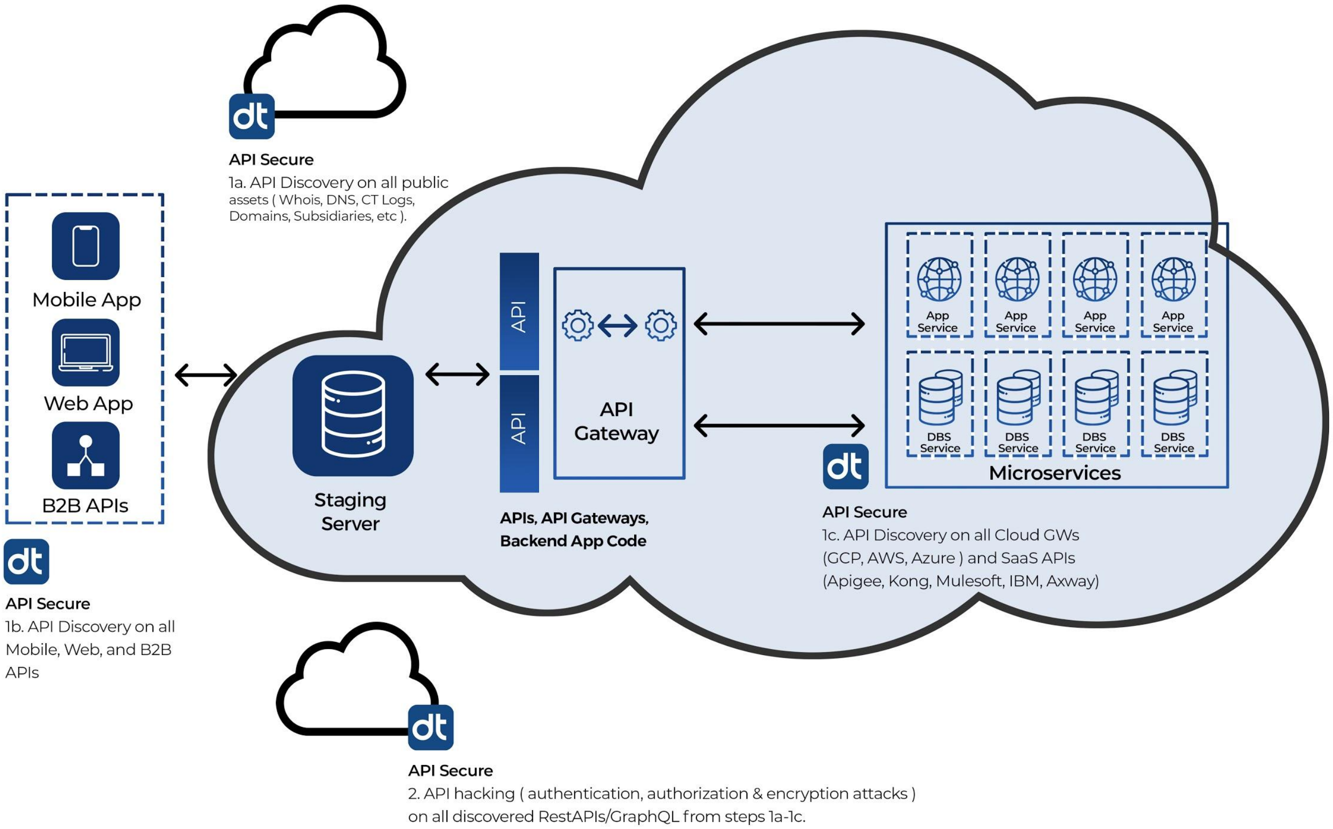
Dynamic run-time security review

Fully automated, SaaS based monitoring of multi-cloud and on-premise environments

AWS, Google, Microsoft Cloud Integrations

API SECURITY AUTOMATION

“Many API breaches have one thing in common: the breached organization didn't know about their unsecured API until it was too late.” ***Gartner advises that companies*** “adopt a continuous approach to API Security”. Data Theorem specializes in proactive security and goes beyond securing the perimeter to inventory, continuously monitor, and remediate shadow APIs, leaky data, and resolve storage configurations. The result is a program that is designed to secure your data at every level.



API Secure
1a. API Discovery on all public assets (Whois, DNS, CT Logs, Domains, Subsidiaries, etc).

API Secure
1b. API Discovery on all Mobile, Web, and B2B APIs

APIs, API Gateways, Backend App Code

API Secure
1c. API Discovery on all Cloud GWs (GCP, AWS, Azure) and SaaS APIs (Apigee, Kong, Mulesoft, IBM, Axway)

API Secure
2. API hacking (authentication, authorization & encryption attacks) on all discovered RestAPIs/GraphQL from steps 1a-1c.

datatheorem

Data Theorem is a leading provider of modern application security. Its core mission is to analyze and secure any modern 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