DATA SHEET

datatheorem

Cloud Secure

Cloud posture and hacker-style testing for the infrastructure behind your APIs and apps. Monitor, hack, and protect every cloud asset across AWS, Azure, and GCP.

01 OVERVIEW

Cloud Secure extends API Secure to the cloud infrastructure your APIs and apps run on. The Data Theorem Analyzer Engine inventories every config, app, microservice, serverless function, key vault, container, database, and storage asset across multi-cloud, attacks them with hacker-style techniques, and routes prioritized fixes upstream before a breach reaches your data.

Monitor, hack, and protect every cloud asset.

CSPM, hacker-style testing, and live alerts across AWS, Azure, and GCP.

02 CAPABILITIES

Platform capabilities

Multi-cloud asset coverage

Continuous inventory across AWS, Azure, and GCP. Configs, apps, microservices, serverless, key vaults, storage, databases, and VMs in one view.

CSPM and posture management

Detects risky configurations, exposed assets, weak encryption, and overprivileged identities. Ranked by severity and routed to the team that owns the fix.

Hacker-style cloud testing

Daily attacks on every cloud asset and exposed API surface. Real exploit techniques, not synthetic checks. Surfaces breach paths before adversaries do.

Continuous correlation engine

The Analyzer Engine ties config, user activity, network traffic, and external exposure into one signal. No more siloed alerts across CSPM and runtime tools.

Alerts and auto-remediation

Custom alerts on new, changed, and exposed cloud data through Slack and Microsoft Teams. Pre-built remediation paths route fixes upstream into CI before production.

Compliance reports on demand

Audit-ready reports for PCI DSS, GDPR, CCPA, HIPAA, SOC 2, OWASP, MITRE, and NIST. Generated in minutes, not weeks.

DATA SHEET

datatheorem

CLOUD PROVIDERS	AWS · Azure · GCP | Serverless · Containers · VMs · Storage · Key vaults
COMPLIANCE REPORTS	PCI DSS · GDPR · CCPA · HIPAA · SOC 2 · OWASP · MITRE · NIST

03 OUTCOMES

Key benefits

Reveal your full cloud attack surface

Continuous discovery surfaces shadow apps, exposed assets, and leaky configs across every region and account, with real-time alerts to Slack or Teams.

Hack before adversaries do

Daily hacker-style testing of cloud assets and APIs identifies the most critical breach paths across native and third-party services.

Auto-remediate before a breach

Prioritized fixes and secure code samples route into Jira and the CI pipeline. Catch and resolve issues before they migrate into production.

Audit-ready in minutes

On-demand compliance reports for PCI DSS, GDPR, CCPA, HIPAA, SOC 2, OWASP, MITRE, and NIST. Cut audit prep from weeks to minutes.

04 APPROACH

Monitor. Hack. Protect.

1 Monitor

Cloud posture across configs, apps, microservices, serverless, key vaults, storage, databases, and VMs in AWS, Azure, and GCP.

2 Hack

Daily hacker-style testing of every cloud asset and API. Common adversary techniques run against your live environment, not a synthetic copy.

3 Protect

Custom alerts and auto-remediation route fixes upstream before exposure becomes a breach. Findings ship into Slack, Teams, and CI.

#1 2025 CRITICAL CAPABILITIES FOR APPLICATION SECURITY TESTING

Gartner® ranks Data Theorem #1 in Cloud Native Apps.

Source: Gartner, Critical Capabilities for Application Security Testing, Mark Horvath, Jason Gross, Aaron Lord, Shailendra Upadhyay, 13 October 2025. Gartner is a registered trademark and service mark, and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Data Theorem.

PAIRS WITH

API Secure · Discovery, posture, hacker-style testing, and runtime protection for every API across mobile, web, and cloud. →

ABOUT DATA THEOREM

Data Theorem provides full-stack application security across mobile, API, code, and cloud, with AI/LLM coverage woven through. Continuous, hacker-style discovery and runtime analysis 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.

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

GET STARTED

www.datatheorem.com
info@datatheorem.com

Schedule a Demo →