datatheorem
Prevent AppSec Data Breaches

CLOUD SECURE

Monitor | Hack | Protect

PRODUCT OVERVIEW

Data Theorem's Cloud Security product is CSPM + AppSec all-in-one:

1. Monitor your Cloud configs (CSPM), applications, microservices, serverless functions, key stores/keyvaults, Virtual Machines, Storage assets, Databases, etc.
2. Hack the Cloud on a daily basis in search of security vulnerabilities that can lead to data breaches
3. Protect the Cloud by preventing data breaches sourced from Cloud assets and configs.

Data Theorem's Cloud analyzer continuously discovers vulnerabilities in multi-cloud environments and provides mitigation solutions in real time.

PLATFORM FEATURES

- Monitor all Cloud configs, apps, and resources, including serverless apps, messaging queues, storage, databases, key vaults & key stores, etc..
- Support for multi-cloud environments (AWS, GCP/Azure)
- Data Theorem's Analyzer engine continuously correlates configuration, user activity, external and network traffic data.
- Custom alerts based on pre loaded priorities with secure code and auto-remediation
- Detects risky configurations, sensitive user activities, network intrusions, host vulnerabilities
- Instant compliance reporting

BENEFITS

- Continuous monitoring of multi-cloud environments, including backend application cloud building blocks
- Systematically hack all attack points using common hacker techniques
- Identify the most critical vulnerabilities across all of your cloud native apps & resources
- Instantly get alerts on new, changed, and exposed cloud data via Slack/Teams
- Uncover shadow Cloud apps leaking customer data
- Reveal your entire Cloud 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, SOC 2 and more
- Find and fix security issues in CI pipelines, preventing them migrating into production

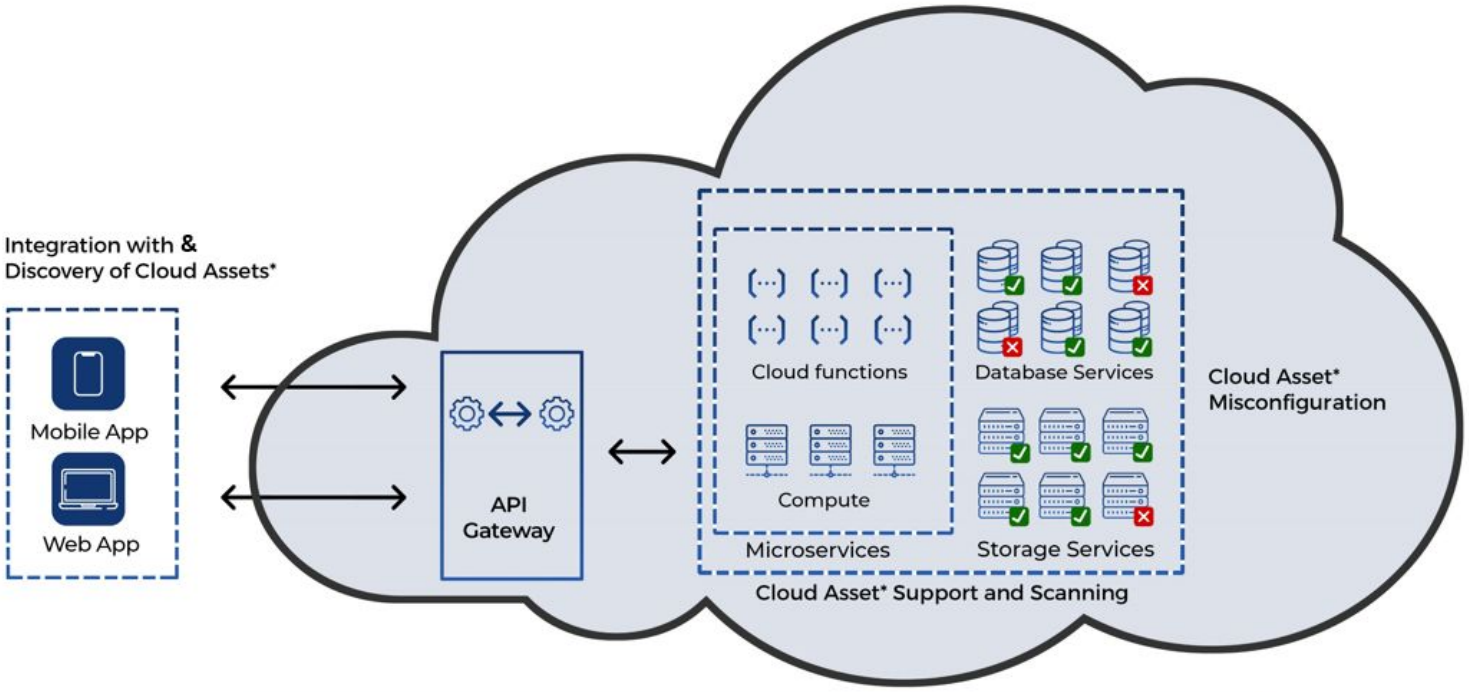
DATA SHEET

SECURITY FOR ALL

A common frustration for distributed teams is that many security tools are limited in function and only allow one group to have insights into vulnerability management and control over resolving them. For cloud security, application & infrastructure teams will need to address issues simultaneously using a full stack approach, from cloud infrastructure to cloud applications.

"Data Theorem's product...has a continuous discovery capability that identifies shadow [assets] by examining sources such as ... cloud-delivered APIs ... specifications (including Swagger/OpenAPI) ... in addition to enterprise API gateways (such as Google Apigee, MuleSoft and Kong)."

***Gartner Cool Vendors, Mark O'Neill, 18 May 2020**



*CSP Building Blocks:

1. Firewall Rules (AWS Security Groups, Azure Network Security Groups, GCP Firewall Rules)
2. Virtual Private Cloud
3. Storage (S3 Bucket, Blobs, Datastores
4. Functions (Lamba, Azure Functions, Google Cloud Functions
5. Containers (EKS, Kubernetes)

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

DATA SHEET