datatheorem
Prevent AppSec Data Breaches

WEB SECURE

Discover | Hack | Remediate

PRODUCT OVERVIEW

Full stack automated security testing that protects your modern web applications. Data Theorem's Web Secure product analyzes and protects single page applications (SPA), their embedded APIs, and underlying cloud resources. Customizable attack toolkits are designed to exploit vulnerabilities across the application stack. Take your security strategy one step further with approaches not offered by traditional web scanners.

PLATFORM FEATURES

- Modern programming language & framework support (JS, React Native)
- Dynamic/run-time analysis for SPAs, APIs, and domains
- Discovery and analysis of cloud application building blocks (queues, cloud storage, cloud databases)
- Customized hacking tools for potential data leakage: SQLi, XSS
- Delivers continuous fuzzing results for SPA associated APIs, a capability not covered by traditional web scanners

BENEFITS

- The Data Theorem **analyzer engine** cycles through discovery, hacking, and remediation steps in order to deliver an automated security approach.
- **Discover** API vulnerabilities in your project in a timely fashion and receive suggestions to **secure your code** or associated services. The discovery process works out-of-the-box and **inventories** your application landscape to reveal all building blocks across your application both in web and cloud without ever requiring any prerequisites or on-boarding from your team.
- **Inspection** runs automated hacking tools to exploit vulnerabilities and exercise potential attack vectors.
- **Remediation** helps you and your AppSec team manage the security lifecycle of internet-facing apps and APIs while you sleep, giving you peace of mind that your applications are ready for production. **Continuous** protection against vulnerabilities, automated and customized checks are delivered via alerts in your favorite team collaboration and/or DevOps platform.

DATA SHEET

DATA SHEET

What is a Modern Web App?

Traditional web 1.0 / 2.0 differs heavily with modern web capabilities. What used to be multiple page applications or MPAs that processed the majority of their data on remote servers has transformed into web apps that can handle rich user experience and high performance, similar to mobile applications. Today, Single Page Applications (SPAs) generate pages in real time, using Javascript frameworks, and oftentimes leveraging APIs hosted in the cloud in order to render the best-in-class experience seen by the user. This makes it difficult to uncover all pages, assets, and endpoints using traditional web crawler methodologies.

Data Theorem has developed a strategy for not just crawling the web indexes of your applications, but also emulating hacker personas with customized attack toolkits that span the four pillars of security: authentication, authorization, encryption, and availability.

"Web applications were involved in 43% of breaches...Hacking varieties, along with exploitation of a vulnerability...are associated in a major way with web applications...it is important to reassert that this trend of having web applications as the vector of these attacks is not going away. This is associated with the shift of valuable data to the cloud, including email accounts and business-related processes."

Verizon 2020 Data Breach Investigations Report

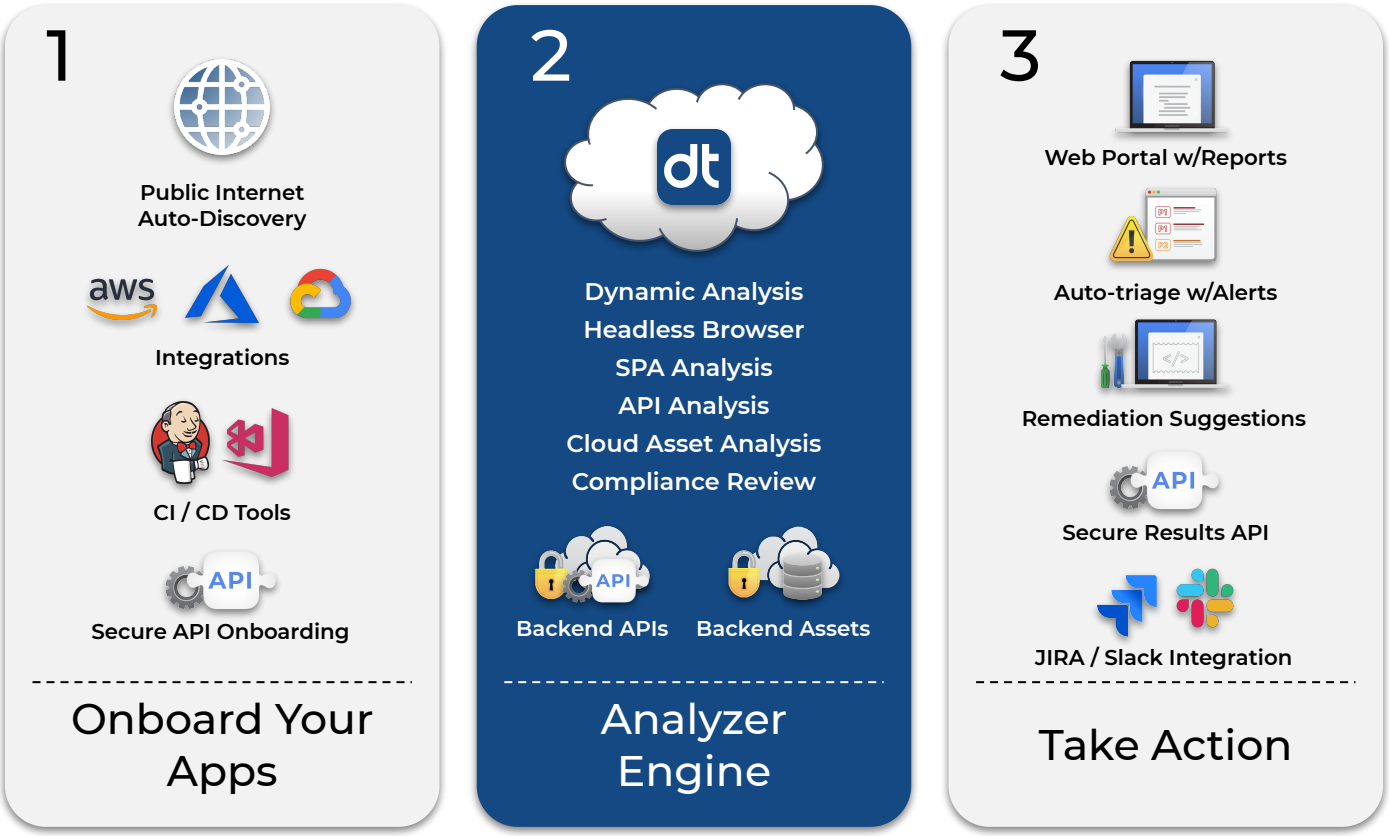
Single Page Web App
Dynamic page rewrite

APIs
RESTful / GraphQL

Cloud
CSPM / Serverless / Storage / Databases

HOW TO GET STARTED

Data Theorem's Web Secure provides a comprehensive discovery and inventory of all of your application assets. Our analyzer will automatically discover your SPAs on the Internet - no need to send us a list of SPAs to scan. Then, your team can configure and implement a custom policy across asset groups (i.e. groups of Apps and APIs). This will allow you to customize the severity of classes of issues as defined by your application or team. You can pick and choose which classes of issues to prioritized rather than adhere to a pre-defined security policy. Policy enforcement is done by the analyzer engine on a continuous basis. Not only does it search through SPAs found on the web, it also searches all backend APIs and underlying cloud resources. The analyzer engine results will differentiate between first-party and third-party APIs. Finally, take action with recommended remediation steps and/or auto-remediation policies to fix problems immediately.



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 scans APIs and mobile applications in search of security flaws and data privacy gaps. Data Theorem products help organizations build safer applications that maximize data security and brand protection. The company has detected more than 300 million application eavesdropping incidents and currently secures more than 4,000 modern applications for its Enterprise customers around the world.

LEARN MORE

Web: www.datatheorem.com
Email: info@datatheorem.com
Demo: www.datatheorem.com/demo