Overview of FedRAMP Policies and Data Theorem Product Coverage

Third Party Assessments: FedRAMP

What is It

Data Theorem helps your applications comply to third-party assessments when it comes to attestation for certain regulation standards. See below for what we support and what is required for penetration tests.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP third-party attestation is done by approved Third Party Assessor Organizations (3PAO). The testing includes both discovery and exploitation steps. Requirements for Web, API, and CSP testing requirements are bucketed together. CSPs must be identified as Iaas, PaaS, or SaaS. The sample workflows and test cases need to be provided by CSPs to determine the common use cases of the application functionality. For FedRAMP Mobile testing requirements, all platforms such as iOS or Android must be tested independently. See below for detailed information on each Attack Surface and the FedRAMP requirements.

	FedRAMP Pen Test Requirements		**Data Theorem**
Discovery	**Web/API (FedRAMP 5.2, Table 4)**	**Mobile (FedRAMP 5.3, Table 5)**	**Feature / Coverage in Mobile/Web/Api/Cloud Secure Products**
	Perform internet searches to identify any publicly available information on the target web application: Identify any publicly available documentation that can be leveraged to gain insight into potential attack vectors of the target web application. Determine if any publicly available vulnerability has been disclosed, which could potentially be leveraged to attack the target web application.	Perform internet searches to identify any publicly available information on the target web application: Identify any publicly available documentation that can be leveraged to gain insight into potential attack vectors of the target mobile application. Determine if any publicly available vulnerability has been disclosed, which could potentially be leveraged to attack the target mobile application.	Public Internet Discovery/Scanning: Find potential publicly available vulnerabilities or attack vectors
	Identify the target	Map all content and	Application Asset

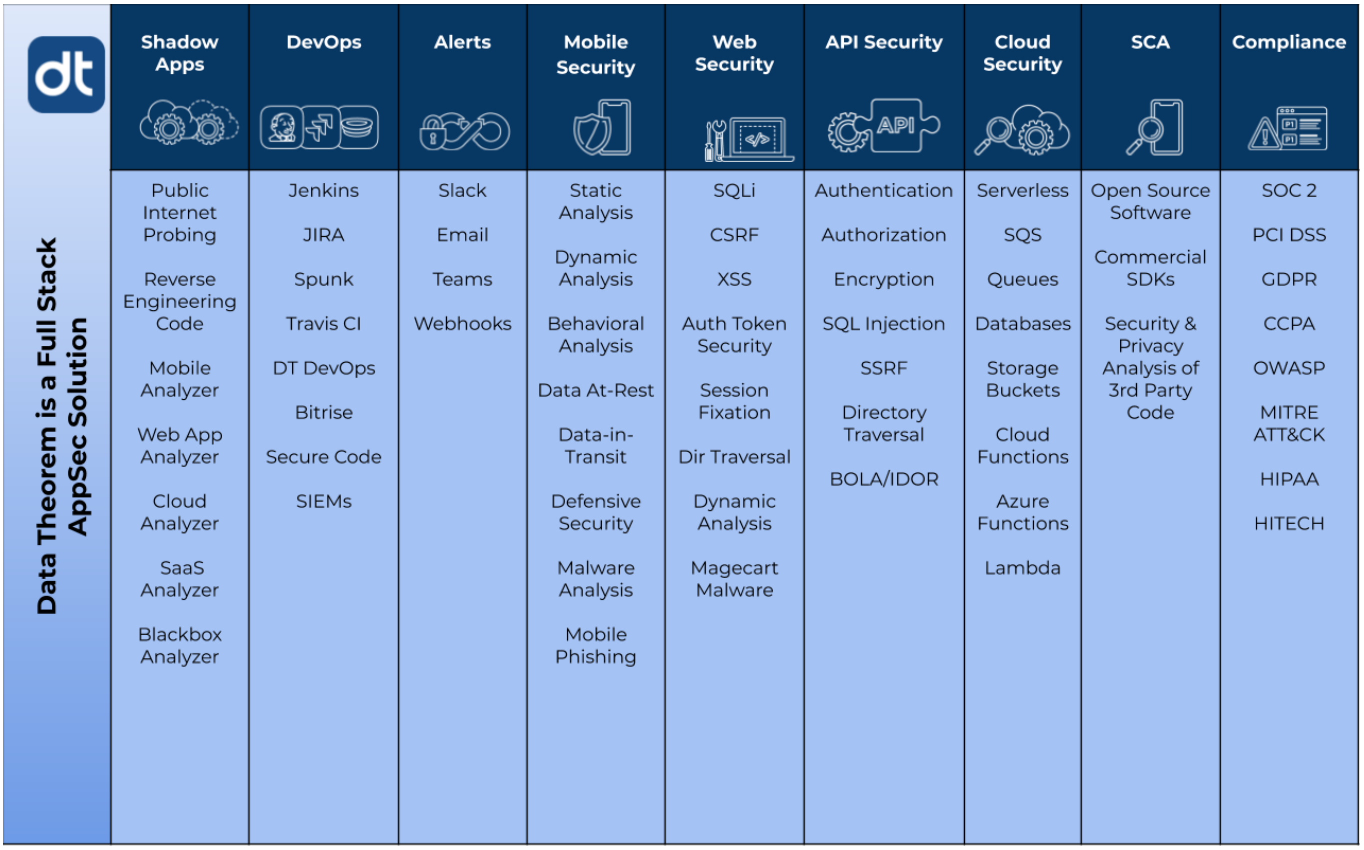
	application architecture: Identify all layers of the application including application servers, databases, middleware, and other technologies to determine communication flow and patterns within the application.	functionality: Navigate through the application to determine functionality and workflow.	Discovery: Map all content and functionality, navigate through the app to determine functionality and workflow
	Identify account roles and authorization bounds: Identify the roles associated with the cloud service and determine access limitations.	Identify all permission sets requested by the application: Inventory the permissions that the mobile application requests from the phone. Determine if there are any differences across mobile platforms.	Access: Authentication and Authorization checks including in Cloud Building Blocks
	Map all content and functionality: Create a sitemap detailing all levels of functionality within the web application. Please note: different account roles may have different access levels to functionality within the target web application.		User flow through app (dynamic scans)
	Identify all user-controlled input entry points: Map all areas of the application that take input from the user of the application.		User flow through app (dynamic scans)
	Perform web application server configuration checks: Perform web vulnerability scanning activity to determine if common web server configuration flaws are present that could lead to an access path.		Web Secure Configuration and Certification checks on web apps
Exploitation	**Web/API, FedRAMP 5.7.2 (Table 10)**	**Mobile, FedRAMP 5.7.2 (Table 10)**	**Data Theorem**
	Authentication and	Authorization: Identify	Dynamic Scans

	Session Management: Assess the application to determine how the target application creates and maintains a session state. Analyze account creation and management process.	issues related to role privilege enforcement across common customer roles in the cloud service. Attempt to bypass authorization restrictions.	
	Authorization: Identify issues related to role privilege enforcement across common customer roles in the cloud service. Attempt to bypass authorization restrictions.	Data Storage: Identify and inventory data being stored on the device. Determine if encryption is being utilized outside of platform level controls.	Encryption checks
	Application Logic: Attempt to circumvent controls to prevent bypass on intended logic patterns and application flows.	Information disclosure: iIdentify what information is being disclosed in log files and local cache stores	Hack & Extract, Keys to the Kingdom
	Input Validation: Perform injection attacks against all data inputs to determine if information or files can be inserted or extracted from the target application. Attempt to alter the backend.		SQLi and XSS hacking
Post-Exploitation	**Web/API, FedRAMP 5.8.1 (Table 15)**	**Mobile, FedRAMP 5.8.2**	**Data Theorem**
	Unauthorized Management Access: Use access to application to attempt to gain control of underlying infrastructure or management systems.	N/A: The test is focused on the test platform, and the device is out of scope.	Authorization checks
	Unauthorized Data Access: Attempt to demonstrate the potential to access additional data from sources outside the cloud service's intended scope.		Authorization checks

SUMMARY

Data Theorem supports the recommended criteria, and your organizations can operate at ease knowing that you will be ready for any third-party reviews.

Reference: FedRAMP Penetration Test Guidance, Version 1.0.1, July 2015.



Data Theorem is a Full Stack AppSec Solution

Shadow Apps	DevOps	Alerts	Mobile Security	Web Security	API Security	Cloud Security	SCA	Compliance
Public Internet Probing	Jenkins	Slack	Static Analysis	SQLi	Authentication	Serverless	Open Source Software	SOC 2
Reverse Engineering Code	JIRA	Email	Dynamic Analysis	CSRF	Authorization	SQS	Commercial SDKs	PCI DSS
Mobile Analyzer	Spunk	Teams	Behavioral Analysis	XSS	Encryption	Queues	Security & Privacy Analysis of 3rd Party Code	GDPR
Web App Analyzer	Travis CI	Webhooks	Data At-Rest	Auth Token Security	SQL Injection	Databases		CCPA
Cloud Analyzer	DT DevOps		Data-in-Transit	Session Fixation	SSRF	Storage Buckets		OWASP
SaaS Analyzer	Bitrise		Defensive Security	Dir Traversal	Directory Traversal	Cloud Functions		MITRE ATT&CK
Blackbox Analyzer	Secure Code		Malware Analysis	Dynamic Analysis	BOLA/IDOR	Azure Functions		HIPAA
	SIEMs		Mobile Phishing	Magecart Malware		Lambda		HITECH

About Data Theorem, Inc.

Data Theorem is a SaaS for modern application security. Our cloud-based technology analyzes APIs (RESTful), Mobile (iOS & Android), Web (Single-Page WebApps), and Cloud (Serverless & Storage) applications on a continuous basis in search of security flaws & data privacy gaps. By combining our extensive experience in information security/privacy with cloud-enabled scaling, we are able to provide customers a 365-day continuous security service for all layer-7 assets.

About Our Company

Founded in 2013 in the heart of Silicon Valley headquartered in Palo Alto, CA with offices in New York and Paris.

Each of our execs has more than 20 years of security industry experience. Our leaders have published six security research books and led over $4B USD security acquisitions.

For more information, please visit https://www.datatheorem.com.