# Overview of SOC 2 Policies and Data Theorem Product Coverage

## Third Party Assessments: SOC 2

### 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.

### SOC2

The Service Organization Controls (SOC 2) is based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). SOC2 aims to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy, and this is how the "trust service principles" are defined. SOC 2 is not a certification but an external auditor's evaluation. While there is no checklist or defined control set for SOC 2, there is criteria for which adequate controls must be designed. The criteria is tested independent of an attack surface, so all checks against the Trust Service Principles could apply for Mobile, Web, API, and Cloud type applications and/or assets.

### How it is done

In SOC 2 CC4.1, COSO Principle 16 states that "The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." Further, the Criteria goes on to state in its "Points to Focus on": "Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments." Penetration testing would be one acceptable method of proving adherence to Trust Services Principles.

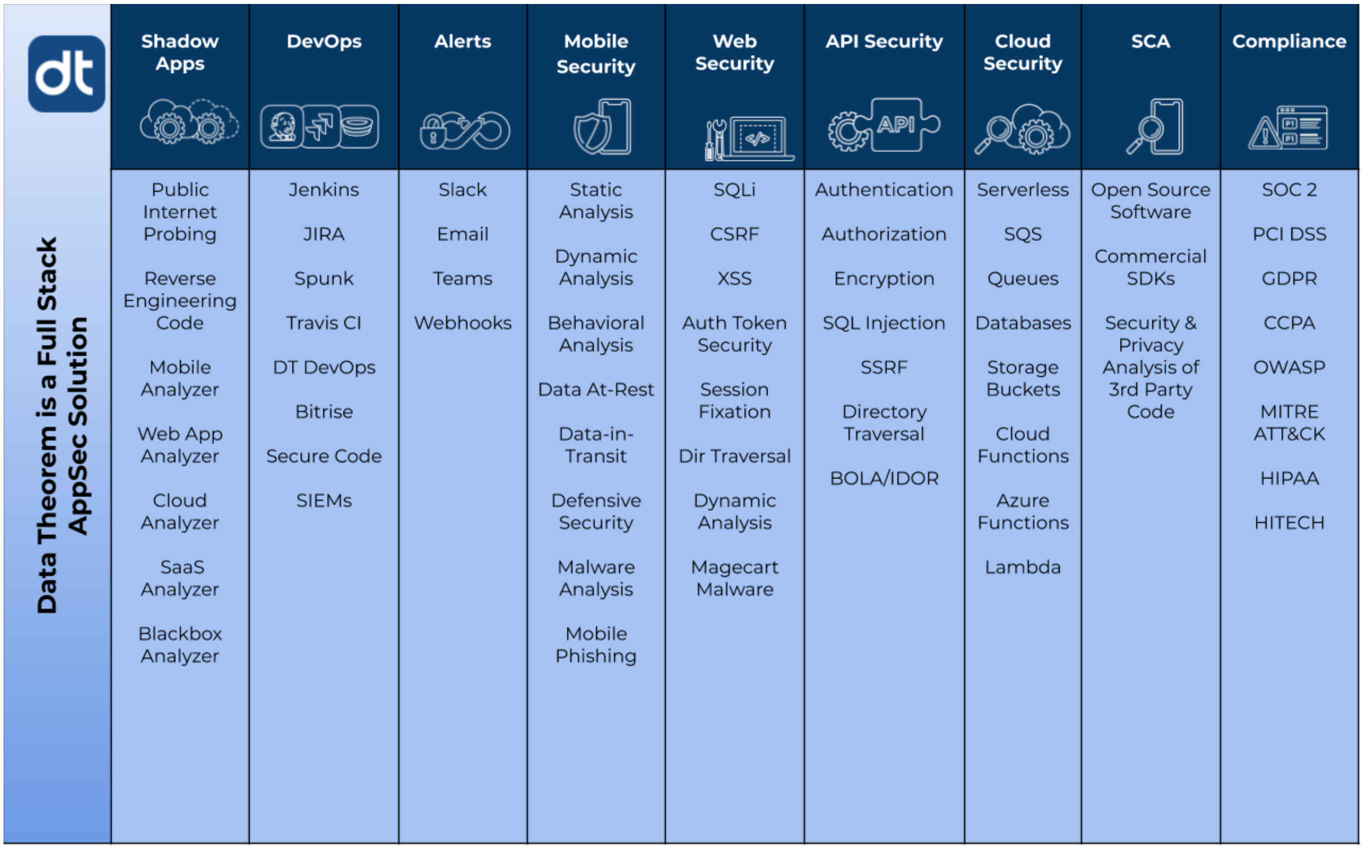
With regards to vulnerability scanning and according to CC7.1, "To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities." Additionally in the points of focus it is stated that the entity should "conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis." This means that a penetration test requirement is recommended on a periodic basis. Data Theorem provides both penetration test checks as well as vulnerability scanning checks. Refer to below table for a specific breakdown of the required checks that Data Theorem supports:

| SOC 2 Trust Service Principles | AICPA definition | Data Theorem Defensive and Offensive Product Suite: Features/Capabilities |
|---|---|---|
| **Security** | Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives. | Protection for data at rest and data in transit. Analysis of all attack surfaces includes but not limited to encryption, authentication, TLS/SLS, HTTPS, and more. |
| **Availability** | Information and systems are available for operation and use to meet the entity's objectives. | Disaster Recovery, performance monitoring, incident handling (DevOps). Automating security scanning as part of the cycle, including pre-production testing, production testing, automated ticket creation into bug trackers, automated triage, and real-time alerts. |
| **Processing Integrity** | System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. | |
| **Confidentiality** | Information designated as confidential is protected to meet the entity's objectives. | Protection of Leaky Data and PII. Hacker Toolkits (Keys to the Kingdom, Hack & Extract). Alert and Remediation options: flagging of any leaky data or PII whether in your own code or third party code |
| **Privacy** | Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives. | Compliance with privacy policies and regulations (GAPP). Verify compliance with SOC2 along with any other privacy policies or regulations such as GDPR. |

## 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.

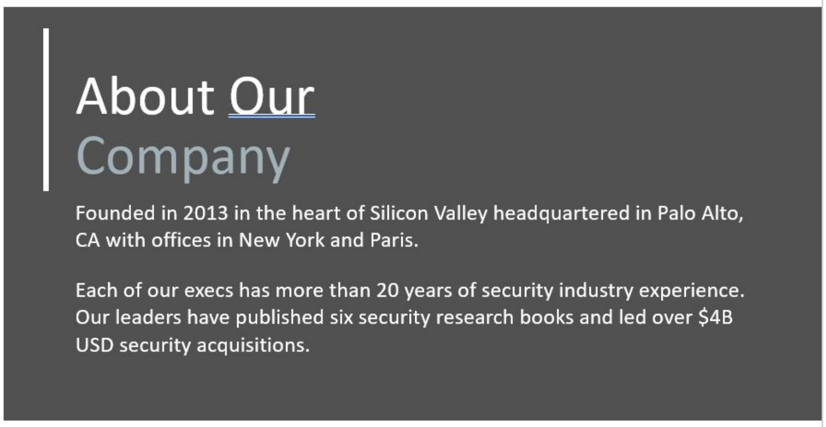
Reference: TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy- Includes March 2020 Updates, AICPA 2020.



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