

Coalfire's Evaluation of Antigravity App & CLI

Dated: October 26, 2026

Summary: This document has been created to provide a high level perspective of Coalfire's independent evaluation of Antigravity App and Antigravity CLI.

Executive Summary

Coalfire Systems, Inc. ("Coalfire") was engaged by Google LLC ("Google") to perform an independent, third-party security assessment and penetration test of Google Antigravity App and Antigravity Command Line Interface (CLI). This evaluation was performed to determine the product's alignment with federal security requirements and provide both Google and its customers insights on the product's security posture.

Coalfire validated that Google's US Public Sector deployment instructions (scoped for FedRAMP High, DoD IL4/5, ITAR, and CJIS) allow the Antigravity App and Antigravity CLI to only communicate with a US-based cloud service API regional endpoint (aiplatform.us.rep.googleapis.com) targeting a project within an Assured Workloads regulated folder. This API endpoint is currently supported by corresponding Assured Workloads Data Boundaries.

Scope

Coalfire evaluated the Antigravity clients within a Coalfire-managed environment configured according to Google's US Public Sector deployment instructions. Testing included the following software packages and operating systems:

- Antigravity CLI, version 1.3.5, installed on Linux
- Antigravity CLI, version 1.3.4, installed on Windows
- Antigravity CLI, version 1.3.3, installed on MacOS
- Antigravity App (GUI), version 2.23.0, installed on Linux, Windows, and MacOS

Assessment Methodology

Coalfire uses a threat-informed methodology to discover vulnerabilities that criminals are most likely to exploit. The process relies on both manual and automated testing techniques. The methodology is compatible with security standards created by groups like the National Institute for Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP), and with common compliance frameworks like Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls (SOC) 2.

Assessment Results

During testing, Coalfire discovered zero (0) critical vulnerabilities, zero (0) high vulnerabilities, two (2) medium vulnerabilities, and one (1) low vulnerability. Google's process for evaluating and remediating identified vulnerabilities has been described within their FedRAMP assessment package.

Compliance Standards Considered

Customers are responsible for ensuring that Antigravity deployments are performed in alignment with their compliance requirements and framework specifications. The following framework considerations were made during Coalfire's evaluation of Antigravity:

- **Federal Risk and Authorization Management Program (FedRAMP):** Under the General Provider Responsibilities within FedRAMP's Minimum Assessment Scope, the FedRAMP PMO has noted within Identify Information Resources (MAS-CSO-IIR) that *"Software produced by cloud service providers that is delivered separately for installation on agency systems and not operated in a shared responsibility model (typically including agents, application clients, mobile applications, etc. that are not fully managed by the cloud service provider) is not a cloud computing product or service and is entirely outside the scope of FedRAMP under the FedRAMP Certification Act."* However, there are historical precedents within the FedRAMP Penetration Test Guidance, Version 3, that client side software has previously been considered within Attack Vector 6. This Attack Vector served as the basis for our Antigravity assessment.
- **DoD IL4/IL5:** As with FedRAMP, the Department of Defense Cloud Computing Security Requirements Guide does not provide prescriptive guidance for the evaluation and inclusion of a client application within a cloud service offering. To provide insights on the product's alignment with standard DoD requirements, our testing included penetration testing of the application and the verification that it is able to be configured to only communicate with endpoints deployed in Assured Workloads folders and the Gemini Enterprise Agent Platform (formerly Vertex AI), which is a cloud based product that was previously assessed at IL4/IL5.
- **ITAR:** Coalfire has verified that the in-scope Antigravity applications are installed locally on a customer's machine and can be configured to communicate with endpoints located in the United States. Specifically, the aiplatform.us.rep.googleapis.com endpoint.
- **CJIS:** Customers charged with implementing Criminal Justice Information Systems (CJIS) and/or protection of CJI data are provided a guide outlining shared responsibilities. https://services.google.com/fh/files/misc/cjis_implementation_guide.pdf Coalfire verified that the Antigravity App & CLI client applications are developed in alignment with Google's existing code development workflow, which has been tested as part of recurring FedRAMP assessments. Antigravity App & CLI are configurable upon being installed by the customer, and customers are responsible for reviewing, documenting, implementing, and recording configuration-controlled changes within their systems and applications.

About Coalfire

Coalfire is a leading 3PAO in the FedRAMP program, having performed extensive assessments for the world's leading cloud technologies. Our reputation has been built on the comprehensiveness of the assessments we provide to our clients and the overall thoroughness of our reviews on behalf of the US Federal Government. We stand behind all the work we perform and put forth unbiased deliverables outlining the findings from assessment activities.