This article is the first part of a three-part series that discusses how you can use Google Cloud products to help secure common data workloads:

- Part 1 (this article): Help secure data workloads in Google Cloud. Introduces the series and summarizes use cases for securing data workloads.
- Part 2: Help secure data workloads: Google Cloud products (/solutions/secure-data-workloads-gcp-products). Start here if you are unfamiliar with products that support security in Google Cloud.
- Part 3: Help secure data workloads: Google Cloud use cases (/solutions/secure-data-workloads-use-cases). Dive into a discussion of components and settings in the context of use cases.

This series is designed to help you learn how to interact with Google Cloud APIs, such as BigQuery and Cloud Storage, in a secure way.

When you secure your data workloads, the challenge is to grant enough access so that authorized entities can perform the appropriate tasks, but not so much that unauthorized entities get access to restricted data.

In Google Cloud, you can manage data security at different levels:

- **Service access.** Grant an entity access to the services storing the data.
- **Data access.** Grant an entity permission to interact with specific data. Data access can include the following:
    - Granting an individual identity read-only access to a single object (that is, granular access).
    - Preventing the listing of a group of objects outside of an authorized perimeter.
    - Applying rules similarly for humans and applications.

- **Data transit.** Encrypt, allow, or deny data flows between two entities, networks, or organizations.

Part 2 of this series discusses the following services:

- **Storage and databases**: Cloud Storage as an object store and BigQuery as a columnar database for structured data.
- **Compute**: BigQuery as an analytics tool and Dataproc as a data processor.
- **Networking**: Virtual Private Cloud, firewalls, and other features of the Google Cloud software defined network that help security at the network level.
- **Security**: Cloud Identity and Access Management (Cloud IAM) and Access Controls, which provide authentication and authorization features.

For more information about services in Google Cloud, see the Google Cloud Services (/docs/overview/cloud-platform-services) section in the platform overview. For more information about GCP products related to security, visit Security products and capabilities (/security/products/).

This solution focuses on key data workloads, but they rely on technologies common to Google Cloud services, and so can be reproduced for other security workloads:

- Cloud Storage and BigQuery are services accessible through an API. Other similar services (/vpc-service-controls/docs/supported-products) can follow the same concepts to protect their access.
- Dataproc is based on Google Compute Engine. Other products based on Compute Engine, such as Dataflow, support the same networking features, including Virtual Private Cloud and firewalls.

Part 3 of this series, Help secure data workloads: use cases (/solutions/secure-data-workloads-use-cases), uses the following terminology and concepts when addressing a use case:

- **Altostrat**. A fictional company that owns some data and wants to make it available to employees, partners, and customers in a secure way.
- **Admin**. An Altostrat employee who has sufficient rights to perform the required tasks. *Admin* and *Altrostrat's admin* represent the same person.
- **Identities**. Users or apps of Altostrat or of Altostrat's customers or partners.
- **Apps**. Entities that might need access to data, but that aren't individual users. For example, Dataproc or custom code running on Compute Engine are both considered entities.
- **Google Cloud APIs**. Google Cloud services that are API-based and supported by VPC (/vpc-service-controls/docs/supported-products) and Private Google Access (/vpc/docs/private-access-options#pga-supported). This series focuses on BigQuery and Cloud Storage as examples of Google Cloud APIs.

Part 3 explains implementation for the following use cases:

- Prevent access by non-domain identities (/solutions/secure-data-workloads-use-cases#prevent_access_by_non-domain_identities): How to manage which domains can be part of an organization and its projects.
- Limit access to data for specific identities (/solutions/secure-data-workloads-use-cases#limit_access_for_specific_identities): How to manage identities' general access to data located in Google Cloud data stores.
- Limit reads within BigQuery for specific identities (/solutions/secure-data-workloads-use-cases#limit_reads_within_bigquery_for_specific_identities): How to narrow down data access for BigQuery data, limiting access at the record level.
- Mitigate data exfiltration for apps (/solutions/secure-data-workloads-use-cases#mitigate_data_exfiltration_for_apps): How to allow only specific clients to access data and limit where they can export it to.
- Mitigate data exfiltration for users (/solutions/secure-data-workloads-use-cases#mitigate_data_exfiltration_for_people): How to prevent humans with access to the data from exporting it to unapproved locations, potentially outside of the organization.

- Manage access to Google Cloud services (/solutions/secure-data-workloads-use-cases#managed_access_to_gcp_apis): How to manage access based on the internet access of the client.
- Gateway for hybrid environment (/solutions/secure-data-workloads-use-cases#gateway-for-hybrid): How to use a gateway project to manage access to data in other projects in a centralized way.
- Manage access through Dataproc (/solutions/secure-data-workloads-use-cases#manage_access_through_cloud_dataproc): How to delegate data access for a group of identities through compute resources represented by a single identity.
- Proxy access (/solutions/secure-data-workloads-use-cases#proxy_access): How to provide a custom user interface to replace existing Google Cloud-provided user interfaces available in the Cloud Console.

Continue to the next parts of this series:

- Part 2: Help secure data workloads: Google Cloud products (/solutions/secure-data-workloads-gcp-products).
- Part 3: Help secure data workloads: Google Cloud use cases (/solutions/secure-data-workloads-use-cases).