VPC Service Controls

Define security perimeters for sensitive data in Google Cloud Platform services.

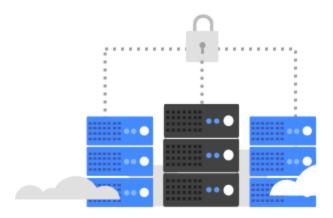**View documentation** (https://cloud.google.com/vpc-service-controls/docs/)

Try it free (https://console.cloud.google.com/freetrial/)

Establish virtual security perimeters for API-based services

VPC Service Controls allow users to define a security perimeter around Google Cloud Platform resources such as Cloud Storage buckets, Bigtable instances, and BigQuery datasets to constrain data within a VPC and help mitigate data exfiltration risks. With VPC Service Controls, enterprises can keep their sensitive data private as they take advantage of the fully managed storage and data processing capabilities of Google Cloud Platform.

Keep sensitive data private in a hybrid environment

Using VPC Service Controls and [Private Google Access](https://cloud.google.com/vpc/docs/private-access-options) (https://cloud.google.com/vpc/docs/private-access-options), enterprises can configure private communication between cloud resources from VPC networks that span cloud and on-premises hybrid deployments to keep sensitive data private. With a secure boundary in place, you can take advantage of fully managed Google Cloud Platform technologies like Cloud Storage, Bigtable, and BigQuery.

Mitigate data exfiltration risks

By enforcing a security perimeter around managed GCP services, organizations reduce the risk of data exfiltration. With VPC Service Controls, enterprises can help protect against data exposure due to misconfigured access controls, malicious users

copying data to unauthorized cloud resources, and attackers attempting to access sensitive data in GCP resources from the internet.

Enable context-aware access to GCP services

VPC Service Controls enables a <u>context-aware access</u> (https://cloud.google.com/context-aware-access/) approach of control for your cloud resources. Enterprises can create granular access control policies in GCP based on attributes like user identity and IP address. These policies help ensure the appropriate security controls are in place when granting access to cloud resources from the internet.

Centrally manage your security posture at scale

With VPC Service Controls, enterprise security teams can define fine-grained perimeter controls and enforce that security posture across numerous GCP services and projects. Users have the flexibility to create, update, and delete resources within service perimeters so they can easily scale their security controls.

Features

Define security perimeters for sensitive data in Google Cloud Platform services.

Audit logging

Maintain an ongoing log of access denials to spot potential malicious activity on GCP resources. Learn more about Stackdriver Logging (https://cloud.google.com/logging/).

Support for hybrid environments

Configure private communication to cloud resources from VPC networks that span cloud and on-premises hybrid deployments using Private Google Access (https://cloud.google.com/vpc/docs/private-access-options).

Context-aware access

Control access to GCP services from the internet based on context-aware access (https://cloud.google.com/context-aware-access/) attributes like IP address and a user's identity.

Perimeter security for managed GCP services

Configure service perimeters to control communications between virtual machines and managed GCP resources. Service perimeters allow free communication within the zone and block all service communication outside the perimeter.

Secure communication

Securely share data across service perimeters.

VPC Flow Logs

Flow logs capture information about the IP traffic going to and from network interfaces on Google Compute Engine. VPC flow logs help with network monitoring, forensics, real-time security analysis and expense optimization. GCP flow logs are updated every 5-seconds, providing near real-time visibility.

Pricing

There is no separate charge for using VPC Service Controls.

Get started

VPC Service Controls

View documentation (https://cloud.google.com/vpc-service-controls/docs/)

Try it free (https://console.cloud.google.com/freetrial/)