Did you miss the recent Google Cloud Security Talks event? Check out all of the great sessions on-demand (https://cloudonair.withgoogle.com/events/security-talks-march-2022)!

JUMP TO (#)

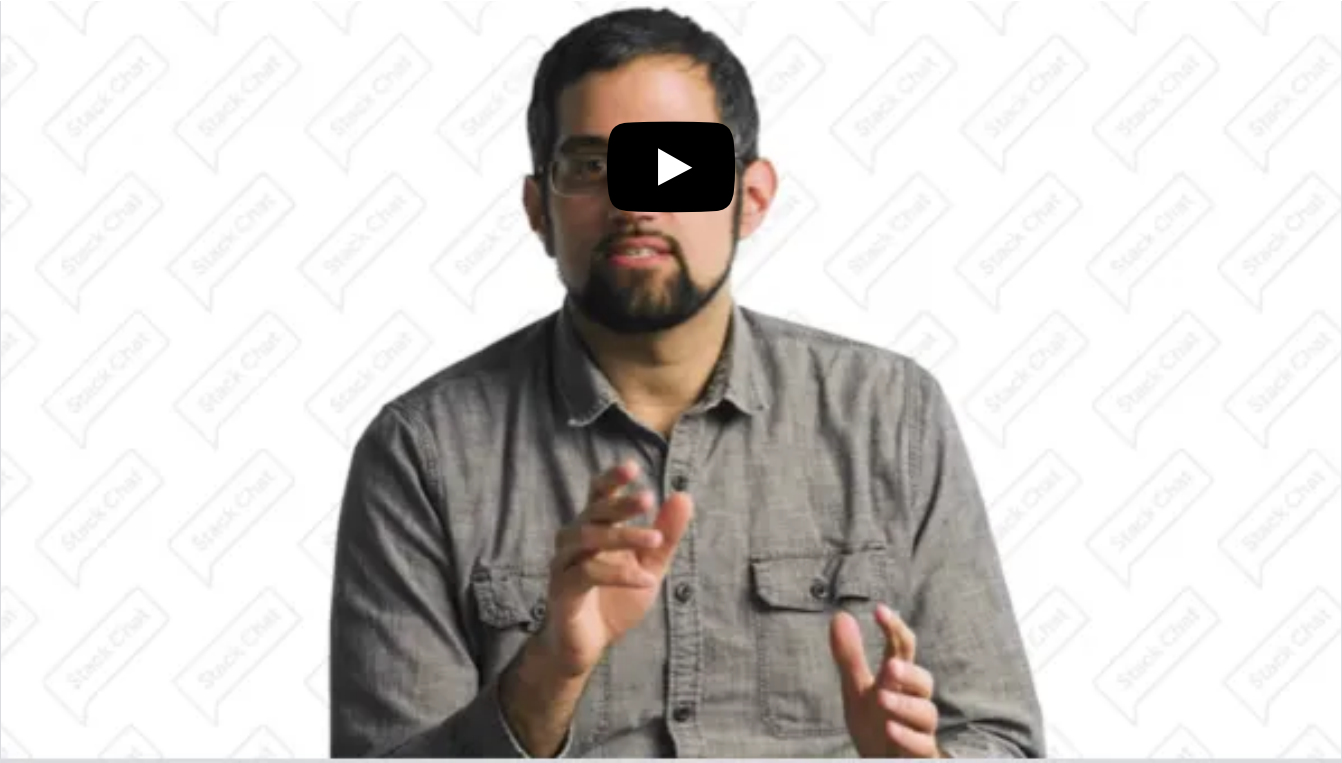
VPC Service Controls

Managed networking functionality for your Google Cloud resources.

New customers get $300 in free credits to spend on Google Cloud during the first 90 days. All customers get free usage (up to monthly limits) of select products, including BigQuery and Compute Engine.

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

- Mitigate exfiltration risks by isolating multi-tenant services
- Ensure sensitive data can only be accessed from authorized networks
- Restrict resource access to allowed IP addresses, identities, and trusted client devices (/context-aware-access)
- Control which Google Cloud services are accessible from a VPC (/vpc) network



(https://www.youtube.com/watch?v=Bu2uEX2nB9A&autoplay=1)

BENEFITS

Mitigate data exfiltration risks

Enforce a security perimeter with VPC Service Controls to isolate resources of multi-tenant Google Cloud services—reducing the risk of data exfiltration or data breach.

Keep data private inside the VPC

Configure private communication between cloud resources from VPC networks spanning cloud and on-premises hybrid deployments. Take advantage of fully managed tools like Cloud Storage (/storage), Bigtable (/bigtable), and BigQuery (/bigquery).

Deliver independent data access controls

VPC Service Controls delivers an extra layer of control with a defense-in-depth approach for multi-tenant services that helps protect service access from both insider

and outsider threats.

KEY FEATURES

Key features

Centrally manage multi-tenant service access at scale

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

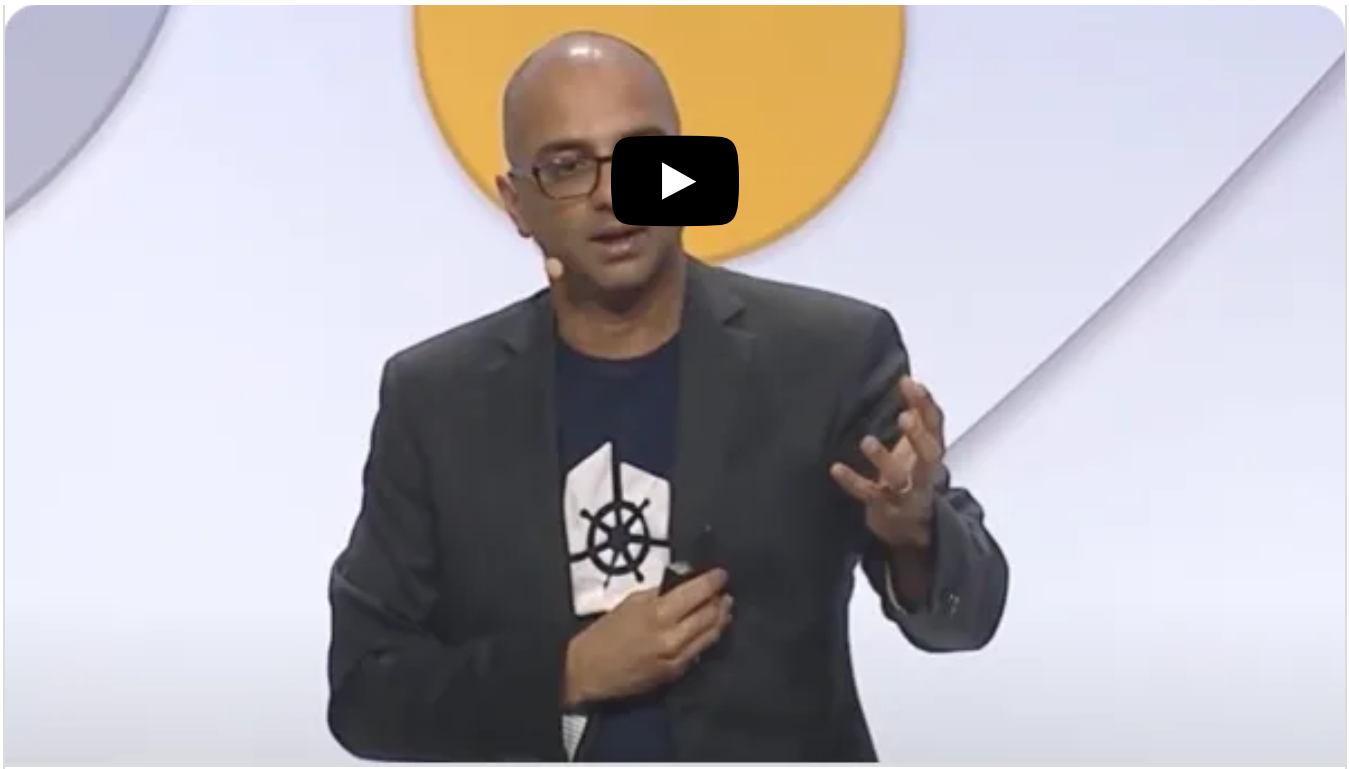
Securely access multi-tenant services

VPC Service Controls enables a context-aware access approach of control for your cloud resources. Enterprises can create granular access control policies in Google Cloud 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.

Establish virtual security perimeters for API-based services

Users can define a security perimeter around Google Cloud resources such as Cloud Storage buckets, Bigtable instances, and BigQuery datasets to constrain data within a VPC and control the flow of data. 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.

iew all features (#)



(https://www.youtube.com/watch?v=rGCU6Ajo0QE&autoplay=1)

WHAT'S NEW

What's new

Sign up (https://cloud.google.com/newsletter) for Google Cloud newsletters to receive product updates, event information, special offers, and more.

BLOG POST

Monitor VPC-SC violations with Data Studio

Read the blog (https://medium.com/google-cloud/create-a-data-studio-dashboard-to-monitor-vpc-sc-violations-on-your-google-cloud-organization-bf8f3bead691)

DOCUMENTATION

Documentation

BEST PRACTICE

Supported products and limitations

Explore a table of products and services that are supported by VPC Service Controls, as well as a list of known limitations with certain services and interfaces.

Learn more (/vpc-service-controls/docs/supported-products)

BEST PRACTICE

Service perimeter details and configuration

Learn all about service perimeters, including how they function, how to configure them, and the difference between enforced and dry run perimeters.

Learn more (/vpc-service-controls/docs/service-perimeters)

BEST PRACTICE

Creating a service perimeter

Find out how to create a service perimeter, including how to include projects and protect services.

Learn more (/vpc-service-controls/docs/create-service-perimeters)

BEST PRACTICE

Setting up private connectivity to Google APIs and services

See how to use VPC Service Controls to control access to Google APIs and services from hosts that use private IP addresses.

Learn more (/vpc-service-controls/docs/set-up-private-connectivity)

BEST PRACTICE

Setting up Container Registry for GKE private clusters

Learn how to configure DNS entries for using Container Registry with a Google Kubernetes Engine private cluster and VPC Service Controls.

Learn more (/vpc-service-controls/docs/set-up-gke)

BEST PRACTICE

Cloud IAM Roles for administering VPC Service Controls

Uncover the Cloud Identity and Access Management (Cloud IAM) roles required to configure VPC Service Controls.

Learn more (/vpc-service-controls/docs/access-control)

GOOGLE CLOUD BASICS

Concepts

Find an overview of VPC Service Controls along with a detailed guide covering everything from service perimeter configuration to audit logging.

Learn more (/vpc-service-controls/docs/concepts)

ARCHITECTURE

Transferring data from Amazon S3 to Cloud Storage

Learn how to harden data transfers from Amazon Simple Storage Service to Cloud Storage using Storage Transfer Service with a VPC Service Controls perimeter.

Learn more (/solutions/transferring-data-from-amazon-s3-to-cloud-storage-using-vpc-service-controls-and-storage-transfer-service)

ARCHITECTURE

Threat and data-theft prevention policies with VM-Series

Use a virtual machine to instill app-based policies that reduce your threat footprint by applying threat and data-theft prevention policies to your allowed traffic.

Learn more (/solutions/partners/threat-and-data-theft-prevention-policies-with-vm-series)

Not seeing what you're looking for?

View all product documentation (/vpc-service-controls/docs)

Explore more docs

Get a quick intro to using this product.

(/vpc-service-controls/docs/quickstart-service-perimeters)
Learn to complete specific tasks with this product.

(/vpc-service-controls/docs/how-to)
Browse walkthroughs of common uses and scenarios for this product.

(/docs/tutorials#VPC%20Service%20Controls)
View APIs, references, and other resources for this product.

Release notes

Read about the latest releases for VPC Service Controls

(/vpc-service-controls/docs/release-notes)

USE CASES

Use cases

USE CASE

Mitigate threats such as data exfiltration

VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses.

USE CASE

Isolate parts of the environment by trust level

VPC Service Controls delivers a method to segment the multi-tenant services environment and isolate services and data. It enables environment micro-segmentation based on service and identity. Service Controls enables clients to extend their networks to include multi-tenant Google Cloud services and control egress and ingress of data.

USE CASE

Secure access to multi-tenant services

VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private.

iew all technical guides (/tutorials#vpc%20service%20controls)

ALL FEATURES

All features

Coverage of services	VPC SC offers broad coverage of internet to service, service to service, VPC to service access controls.
Rich security logging	Maintain an ongoing log of access denials to spot potential malicious activity on Google Cloud resources. Flow logs capture information about the IP traffic going to and from network interfaces on Compute Engine. The logs provide near real-time visibility.
Support for hybrid environments	Configure private communication to cloud resources from VPC networks that span cloud and on-premises hybrid deployments using

	and on-premises hybrid deployments using Private Google Access.
Secure communication	Securely share data across service perimeters with full control over what resource can connect to others or to the outside.
Context-aware access	Control access to Google Cloud services from the internet based on context-aware access attributes like IP address and a user's identity.
Perimeter security for managed Google Cloud services	Configure service perimeters to control communications between virtual machines and managed Google Cloud resources. Service perimeters allow free communication within the zone and block all service communication outside the perimeter.

PRICING

Pricing

There is no separate charge for using VPC Service Controls.

Take the next step

Start building on Google Cloud with $300 in free credits and 20+ always free products.

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

Need help getting started?

Contact sales (https://cloud.google.com/contact/)

Work with a trusted partner

Find a partner (https://cloud.withgoogle.com/partners/)

Continue browsing

See all products (https://cloud.google.com/products/)