Google Cybersecurity Services

Advanced Data Security for Confident Collaboration in Google Cloud

If your organization needs additional layers of security in Google Workspace and Google Cloud, there are several options available to you. With Google- and third-party security solutions, you can strengthen data security, confidentiality, and compliance with regulations like ITAR, CMMC, GLBA, and CJIS.

Virtru: Data-Centric Security, Encryption, and Access Control

Virtru adds a layer of encryption and persistent control to data possessed internally and shared externally. It can be deployed as a client-side Chrome plugin, or as a server-side gateway that automatically protects sensitive data before it leaves your organization.

- Removes all third-party access to protected data
- Supports compliance requirements (CJIS, HIPAA, Pub1075, FERPA, PCI, and more)
- Allows the organization to maintain control of data shared outside of the Google ecosystem — including the ability to revoke shared information, restrict access to certain individuals, and change data access at any time
- Provides best-in-class user experience and easy, secure collaboration
- Supports Google Workspace and Google Cloud (GCP)

Google Client-Side-Encryption (CSE): Host Your Encryption Keys Separately from Your Cloud-Hosted Data

Google CSE allows organizations to encrypt their cloud-hosted data with keys stored separately, by the organization — so Google and other third parties cannot access your data. CSE supports Gmail, Drive, Calendar, and Meet.

- To use CSE, you need to select a third-party encryption key manager: Virtru, FlowCrypt, Fortanix, FutureX, Stormshield, or Thales.

BeyondCorp: Replace Your VPN

BeyondCorp is Google's implementation of the Zero Trust security model, enabling enterprises to control which people, and which devices, are permitted to access data that a customer's organization possesses internally. BeyondCorp enables staff to work from unsecured networks and connect to different apps with mobile device management (MDM), identity and access management (IAM), access proxies, and more.

- To extend BeyondCorp's Zero Trust protection to data shared externally, Virtru's data-centric security provides additional controls that follow data wherever it travels.

Chronicle: Security Analytics Platform

Know where your network and your data stand. Chronicle helps organizations detect, investigate, and respond to security threats — event logging and security information and event management (SIEM); networking traffic (firewalls, routers); endpoint data (mobile devices, computers), and cloud data (GCP, DDoS).

Mandiant: Incident Response and Threat Detection

Alerts customers to potential attacks and their source. Offers training and consulting for organizations seeking to fortify their resiliency.

Assured Controls: Access Management & Access Approvals

Strengthen security and data sovereignty by limiting data access to those with a true need to know. Enables Google customers to restrict data to certain Google staff based on location or technical requirements.

Cloud External Key Manager (CEKM): Third-Party Encryption Keys for Google Cloud, *Managed Outside Google Cloud*

Supports BigQuery, Lookr, Cloud Storage, and more.

- Key Providers include Virtru, Thales, Futurex, and Fortanix
- Managed by customer *outside of Google Cloud* (AWS, Azure, On-Prem)

Customer-Managed Encryption Keys (CMEK): Third-Party Encryption Keys for Google Cloud *Managed Inside Google Cloud*

Supports BigQuery, Lookr, Cloud Storage, and more.

- Key Providers include Virtru, Thales, Futurex, Fortanix.
- Managed by customer *within Google Cloud (GCP).*