Qanapi Key Management Services for Google Workspace Client-Side Encryption

Thank you for downloading this Qanapi solution brief. Carahsoft is the master government aggregator for Qanapi Cybersecurity solutions.

To learn how to take the next step toward acquiring Cybersecurity solutions, please check out the following resources and information:

For additional resources:
carah.io/qanapi-resources

For upcoming events:
carah.io/qanapi-events

For additional Qanapi solutions:
carah.io/qanapi-solutions

For additional Cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
Qanapi@carahsoft.com
571-591-6210

To purchase, check out the contract vehicles available for procurement:
carah.io/qanapi-contracts

Qanapi's Key Management Service for Google Workspace Client-Side Encryption

Take full control over your organization's data. Teams leveraging Google client-side encryption to lock their data before it reaches the cloud can use Qanapi's Key Management Service (KMS) to control encryption keys and unlock the data—enhancing privacy, security, and compliance.

Strengthen Security

Control encryption keys to separate them from data, adding an extra layer of security.

Simplify Compliance

Create, manage, and control encryption keys to fulfill compliance requirements.

Mitigate Risks

Own your encryption keys to fully control your data – minimizing security exposure.

Qanapi KMS Features

- **Encryption Key Management**

  Manage your organization's encryption keys for control over data encryption and decryption.

- **Key Control & Rotation**

  Create, manage, rotate, and retire encryption keys to enhance security.

- **Google Workspace Integration**

  Encrypt Google Workspace apps while maintaining productivity and boosting security.

- **Identity Authentication**

  Leverage Google Identity or any OpenID Connect IdP to restrict access to authorized personnel.

- **Audit Logging and Monitoring**

  Gain full visibility into who is accessing your data, for what purpose, and when.

- **Data Residency Controls**

  Ensure U.S. data sovereignty by storing encryption keys within the continental U.S.

- **Role-Based Access Controls**

  Utilize your Google Workspace permissions to set policies on who can access which data and when.

- **Multi-Tenancy and Cloud Flexibility**

  Operate within multi-tenant or private cloud environments on Google Cloud.