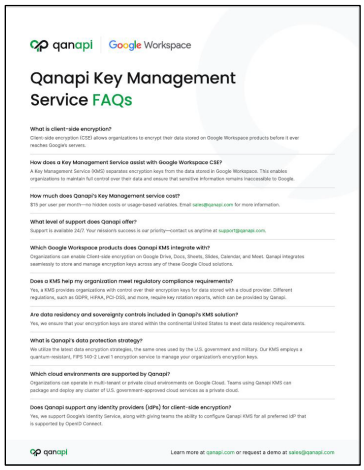
qanapi Google Workspace

Qanapi Key Management Service FAQs

What is client-side encryption?

Client-side encryption (CSE) allows organizations to encrypt their data stored on Google Workspace products before it ever reaches Google's servers.

How does a Key Management Service assist with Google Workspace CSE?

A Key Management Service (KMS) separates encryption keys from the data stored in Google Workspace. This enables organizations to maintain full control over their data and ensure that sensitive information remains inaccessible to Google.

How much does Qanapi's Key Management service cost?

$15 per user per month—no hidden costs or usage-based variables. Email sales@qanapi.com for more information.

What level of support does Qanapi offer?

Support is available 24/7. Your research success is our priority—contact us anytime at support@qanapi.com.

Which Google Workspace products does Qanapi KMS integrate with?

Organizations can enable Client-side encryption on Google Drive, Docs, Sheets, Slides, Calendar, and Meet. Qanapi integrates seamlessly to store and manage encryption keys across any of these Google Cloud solutions.

Does a KMS help my organization meet regulatory compliance requirements?

Yes, a KMS provides organizations with control over their encryption keys for data stored with a cloud provider. Different regulations, such as GDPR, HIPAA, PCI-DSS, and more, require key rotation reports, which can be provided by Qanapi.

Are data residency and sovereignty controls included in Qanapi's KMS solution?

Yes, we ensure that your encryption keys are stored within the continental United States to meet data residency requirements.

What is Qanapi's data protection strategy?

We utilize the latest data encryption strategies, the same ones used by the U.S. government and military. Our KMS employs a quantum-resistant, FIPS 140-2 Level 1 encryption service to manage your organization's encryption keys.

Which cloud environments are supported by Qanapi?

Organizations can operate in multi-tenant or private cloud environments on Google Cloud. Teams using Qanapi KMS can package and deploy any cluster of U.S. government-approved cloud services as a private cloud.

Does Qanapi support any identity providers (IdPs) for client-side encryption?

Yes, we support Google's Identity Service, along with giving teams the ability to configure Qanapi KMS for all preferred IdP that is supported by OpenID Connect.

qanapi Learn more at qanapi.com or request a demo at sales@qanapi.com

Qanapi Key Management Services

Thank you for downloading this Qanapi guide. 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 | Google Workspace

Qanapi Key Management Service FAQs

What is client-side encryption?

Client-side encryption (CSE) allows organizations to encrypt their data stored on Google Workspace products before it ever reaches Google's servers.

How does a Key Management Service assist with Google Workspace CSE?

A Key Management Service (KMS) separates encryption keys from the data stored in Google Workspace. This enables organizations to maintain full control over their data and ensure that sensitive information remains inaccessible to Google.

How much does Qanapi's Key Management service cost?

$15 per user per month—no hidden costs or usage-based variables. Email sales@qanapi.com for more information.

What level of support does Qanapi offer?

Support is available 24/7. Your mission's success is our priority—contact us anytime at support@qanapi.com.

Which Google Workspace products does Qanapi KMS integrate with?

Organizations can enable Client-side encryption on Google Drive, Docs, Sheets, Slides, Calendar, and Meet. Qanapi integrates seamlessly to store and manage encryption keys across any of these Google Cloud solutions.

Does a KMS help my organization meet regulatory compliance requirements?

Yes, a KMS provides organizations with control over their encryption keys for data stored with a cloud provider. Different regulations, such as GDPR, HIPAA, PCI-DSS, and more, require key rotation reports, which can be provided by Qanapi.

Are data residency and sovereignty controls included in Qanapi's KMS solution?

Yes, we ensure that your encryption keys are stored within the continental United States to meet data residency requirements.

What is Qanapi's data protection strategy?

We utilize the latest data encryption strategies, the same ones used by the U.S. government and military. Our KMS employs a quantum-resistant, FIPS 140-2 Level 1 encryption service to manage your organization's encryption keys.

Which cloud environments are supported by Qanapi?

Organizations can operate in multi-tenant or private cloud environments on Google Cloud. Teams using Qanapi KMS can package and deploy any cluster of U.S. government-approved cloud services as a private cloud.

Does Qanapi support any identity providers (IdPs) for client-side encryption?

Yes, we support Google's Identity Service, along with giving teams the ability to configure Qanapi KMS for all preferred IdP that is supported by OpenID Connect.