Fortanix®

Solution Brief

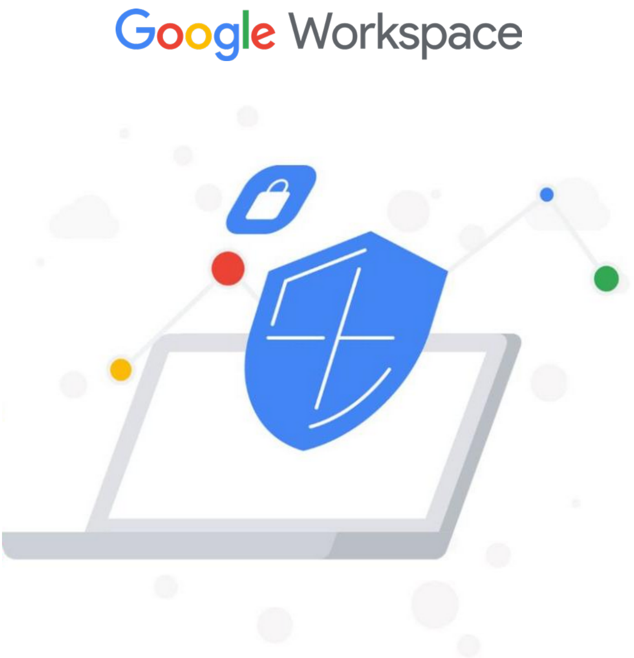
Fortanix for Google Workspace

Retain possession and control over your encryption keys with Fortanix while leveraging the processing capabilities and power of Google Workspace. Fortanix Data Security Manager SaaS (DSM SaaS) integrates with Google Workspace Client-side encryption (CSE) to address all your data sovereignty and compliance requirements.

Challenge

Google Workspace has been the productivity suite of choice for small businesses and Fortune 500 corporations alike. Needless to say, it safely harbours petabytes of sensitive or regulated data belonging to these organizations.

While Google runs atop the latest cryptographic standards, many organizations seek greater security and control over their cloud encryption keys. Especially the ones which operate in highly regulated industries — like defence, aerospace, or government. Housing the authentication keys separate from the storage system makes the data indecipherable to the CSP. At the same time, users can continue to leverage their collaborative services, access content on numerous devices, and share encrypted files externally.



Solution

With Fortanix Data Security Manager SaaS (DSM SaaS), customers can bring a FIPS 140-2 Level 3 certified External Key Management Service for Google Workspace. Fortanix DSM SaaS integrates directly into Google Workspace Client-Side Encryption (CSE) capability for external key management. CSE allows customers to protect their data in Google Cloud — separating data from the key. The database encryption keys are managed outside of Goggle Workspace in the customer's Fortanix DSM SaaS account. What users end up getting is:

Complete control over encryption keys:

For leveraging Google CSE users need to need to set up their encryption key access service with an external key manager that abides to CSE requirement.

No access to plain-text content:

For leveraging Google CSE users need to need to set up their encryption key access service with an external key manager that abides to CSE requirement.

Minimized impact on user experience:

For leveraging Google CSE users need to need to set up their encryption key access service with an external key manager that abides to CSE requirement.

Using Client-side encryption is optional for eligible Google Workspace customers, who can deploy CSE to their entire organization or a select set of users within their organization.

Joint Value Proposition

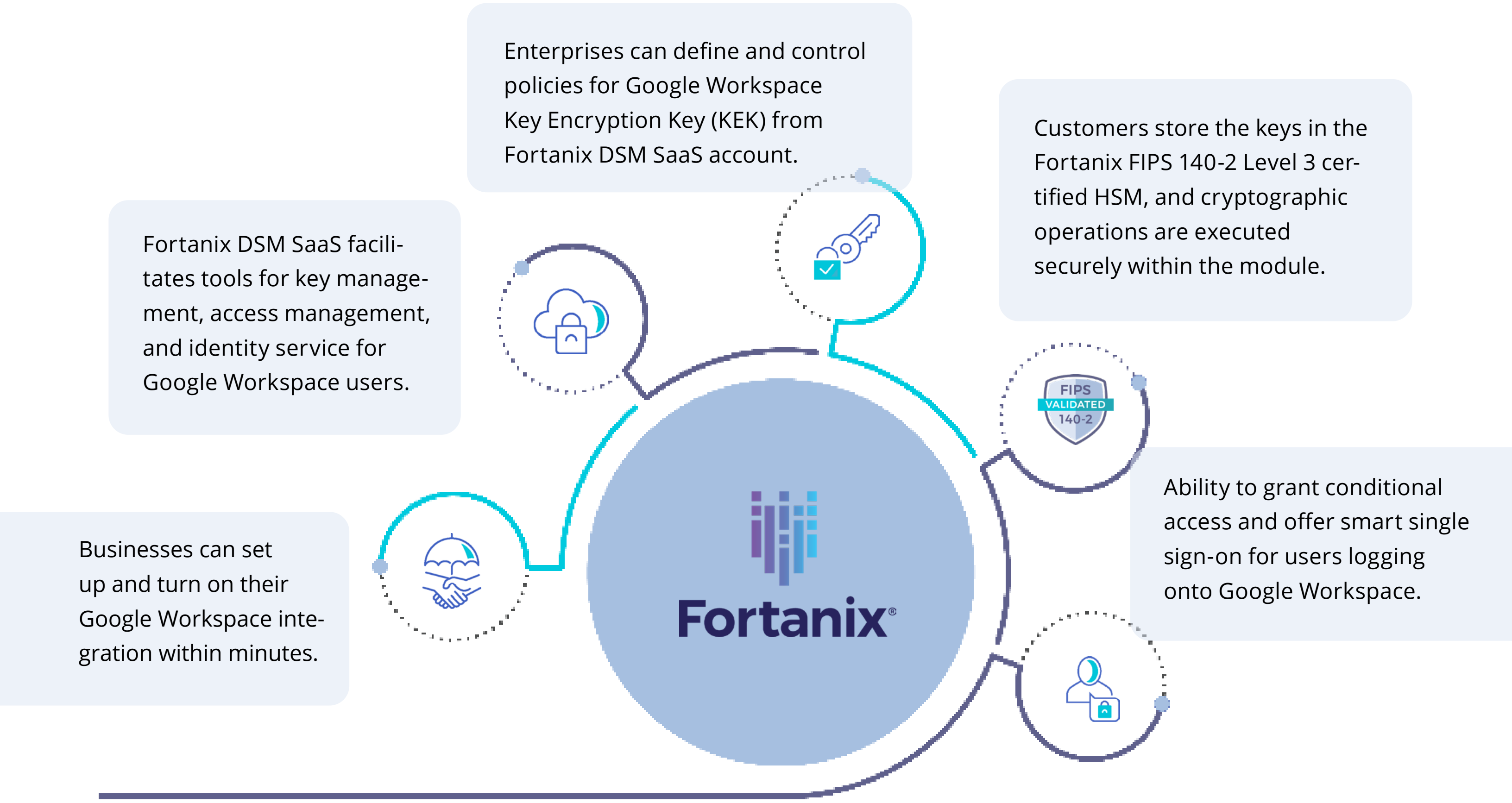
Google Workspace Client-side encryption aims at bolstering data confidentiality while touching upon a varied range of data sovereignty and compliance requirements. This is in addition to the industry-leading cryptographic standard that Google uses to encrypt all data at rest and in transit between facilities.

Fortanix Data Security Manager integrates with Google Workspace External CSE to replicate the same level of security for the keys as in an on-premises environment while moving their data to the cloud. Not only is the data undecipherable to Google, but the encryption keys are also never stored in GCP. The user has complete control over the authorization of Google Workplace data and keys.

Users also get to define and control policies for Google Workspace Key Encryption Key (KEK) from Fortanix DSM SaaS account. Upon receiving the file, the corresponding data encryption key is decrypted using customer-provided keys only after authenticating the user with customer-controlled authentication.

Fortanix DSM SaaS provides FIPS 140-2 Level 3 hardware-based protection, with complete separation between users and regions as needed. It also offers centralized management with audit logging, enterprise-level access controls, multisite and hybrid cloud support, built-in encryption, key management, tokenization, and support for various interfaces, including REST APIs, PKCS11, CNG JCE, and KMIP.

Core Integration Features



Enterprises can define and control policies for Google Workspace Key Encryption Key (KEK) from Fortanix DSM SaaS account.

Customers store the keys in the Fortanix FIPS 140-2 Level 3 certified HSM, and cryptographic operations are executed securely within the module.

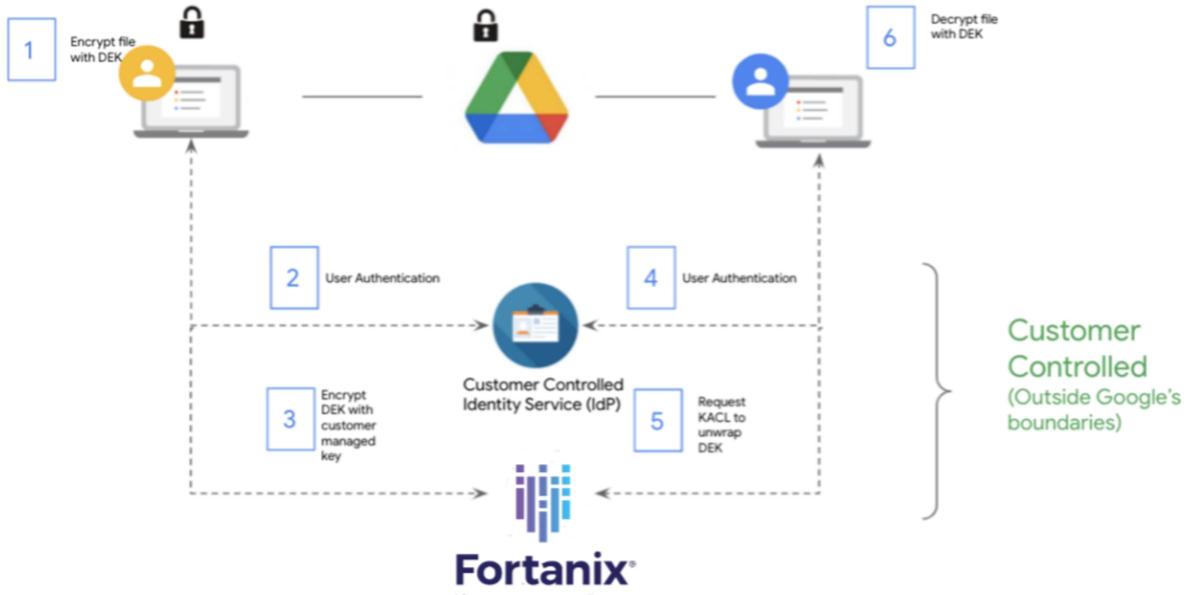
Ability to grant conditional access and offer smart single sign-on for users logging onto Google Workspace.

Businesses can set up and turn on their Google Workspace integration within minutes.

Fortanix DSM SaaS facilitates tools for key management, access management, and identity service for Google Workspace users.

How Does Google Client-Side Encryption Work?

Google Workspace CSE works for browsers and mobile apps by encrypting and decrypting content on the end user's devices. The Google Workspace client calls into Fortanix DSM SaaS that the customer has configured and deployed, and the client performs cryptographic operations to seal and unseal Google Workspace content.


1
Encrypt file with DEK
6
Decrypt file with DEK
2
User Authentication
4
User Authentication
Customer Controlled Identity Service (IdP)
3
Encrypt DEK with customer managed key
5
Request KACL to unwrap DEK
Fortanix
Customer Controlled
(Outside Google's boundaries)

Google Workspace CSE uses envelope encryption to protect data and it relies on web browsers for performing client-side operations. First, a data encryption key (DEK) is generated in a Google Workspace client, and it's used to encrypt the data symmetrically. Then the DEK is handed over to Fortanix DSM SaaS to be encrypted symmetrically using a Key Encryption Key (KEK). The encrypted content and the encrypted DEK are then sent to Google infrastructure for storage.

Business Benefits

Centralized Management

A SaaS modeled key management service that lets you manage, store, use, rotate and destroy all the symmetric and asymmetric cryptographic keys for your Google Workplace projects.

Speedy Setup

Get integrated, up and running in minutes.

Key provenance

Control the location and distribution of your Google Workspace keys.

Unmatched Scalability

Collaborate and scale globally over Google Workspace with zero worries of keys storage location and management. Keys are never cached on Google cloud and access can be revoked anytime.

Superior Control

Eliminate risks of key compromise in shared infrastructure with complete key confidentiality even from governments.

About Fortanix

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks. For more information, see **www.fortanix.com**

About Google Cloud

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade cloud solutions that leverage Google's cutting-edge technology to help companies operate more efficiently and adapt to changing needs, giving customers a foundation for the future. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to solve their most critical business problems.

Google Cloud