# FUTUREX

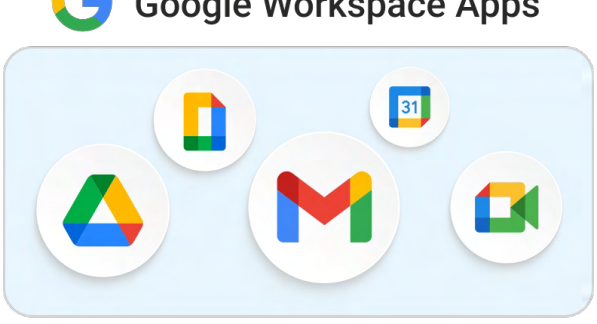
## *Google* Client-side Encryption

## The Growth Of Collaborative Work Environments

As remote and hybrid work drive digital transformation, the adoption of Google Workspace is rapidly increasing with projected annual growth rates as high as 18.5% by 2032. Organizations now prioritize security and compliance, seeking scalable, integrated productivity tools. Google Workspace Client-Side Encryption (CSE) addresses these needs by empowering enterprises and SMEs to protect sensitive data and meet regulatory requirements in an evolving digital landscape.

### *Google Workspace*

Google Workspace is a cloud-based suite that includes Gmail, Drive, Docs, Meet, and more. It is designed for seamless collaboration and communication. It offers business-grade security, custom email, real-time access from any device, scalability, robust storage, compliance, and AI-powered features to support organizations of all sizes.




## Why Do Google Workspaces Need Client-Side Encryption?

Organizations need an additional layer of security to keep sensitive business data private and secure. Google recommends using an external key management partner like Futurex for customer-controlled encryption keys. CSE encrypts data on the user's device, ensuring only the organization can decrypt it, supporting compliance and secure cloud collaboration across all industries.

## Google's Best Practices For Security Using Client-Side Encryption

These eight principles collectively ensure organizations retain complete control over their data privacy while leveraging Google Workspace's collaborative power.

- *Data privacy and control:* Encrypt data in the browser; Google never sees unencrypted content.
- *Customer-managed encryption keys:* Use external KACLS; maintain separation of duties.
- *Seamless user experience:* Minimal workflow disruption; supports collaboration.

- ***Strong access controls:*** JWT-based authentication and authorization; identity provider integration.
- ***Availability and resilience:*** Ensure KACLS and IdP uptime and backup to avoid data loss.
- ***Regulatory compliance:*** Meet privacy, compliance, and sovereignty requirements.
- ***Abuse prevention:*** Implement client-side threat scanning; enhance Workspace security settings.
- ***Key lifecycle management:*** Regular key rotation; use HSMs for cryptographic material protection.

## The Data Encryption Path

**1 Content Encryption**
Encrypts content before it leaves the user's browser.

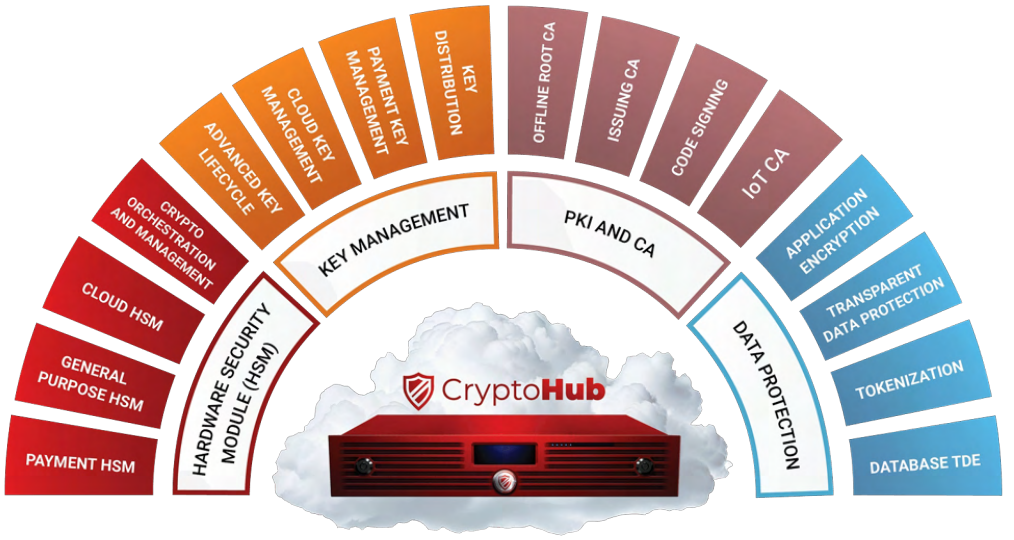
**2 Key Control**
Only you hold the decryption keys.

**3 Data Shielding**
Shields sensitive data even from Google servers.

**4 User Experience**
Seamless browser-based experience.

## How Does Futurex Support CSE Requirements?

Futurex delivers security excellence built over decades of developing customer-centric cryptographic solutions. The CryptoHub platform provides comprehensive, crypto-agile capabilities. This firmware-first unified cryptographic platform operates from a single device and deeply integrates with Google Workspace. It exceeds Google's best practice principles, making it the ideal choice for CSE and Gmail.

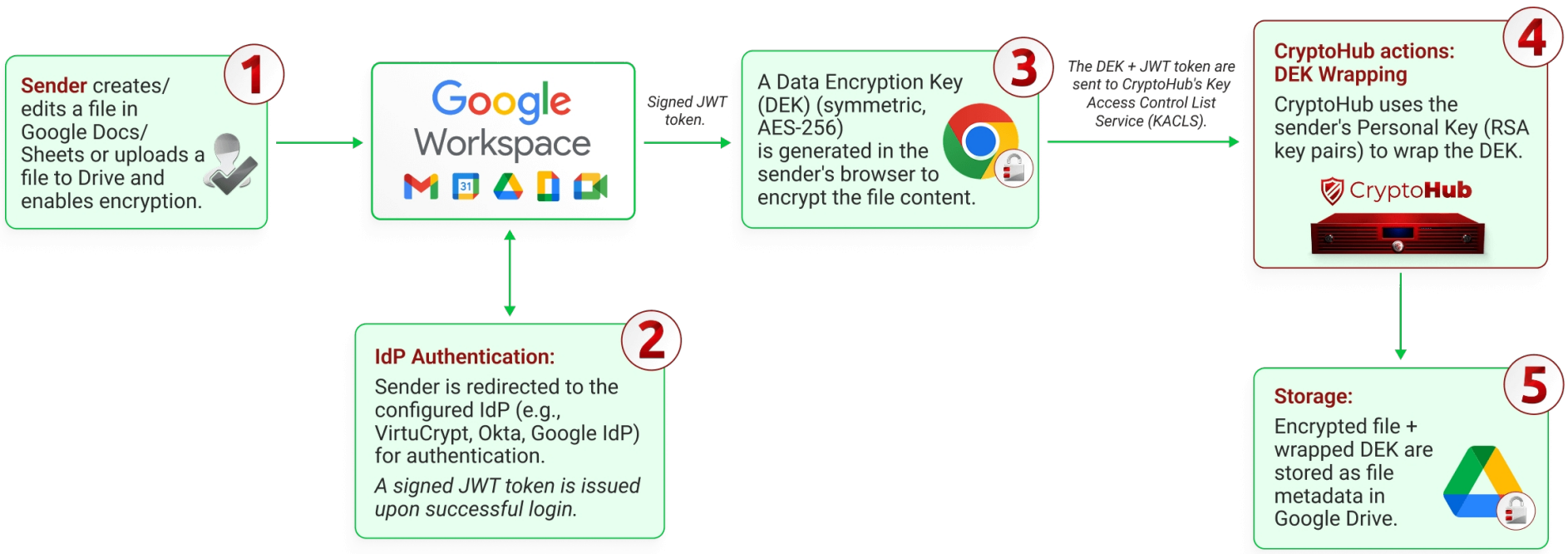



> **In an era marked by persistent data breaches and cyber threats, CryptoHub emerges as a beacon of security.**
>
> *—The World Financial Review.*

## CryptoHub In Action - How It Works

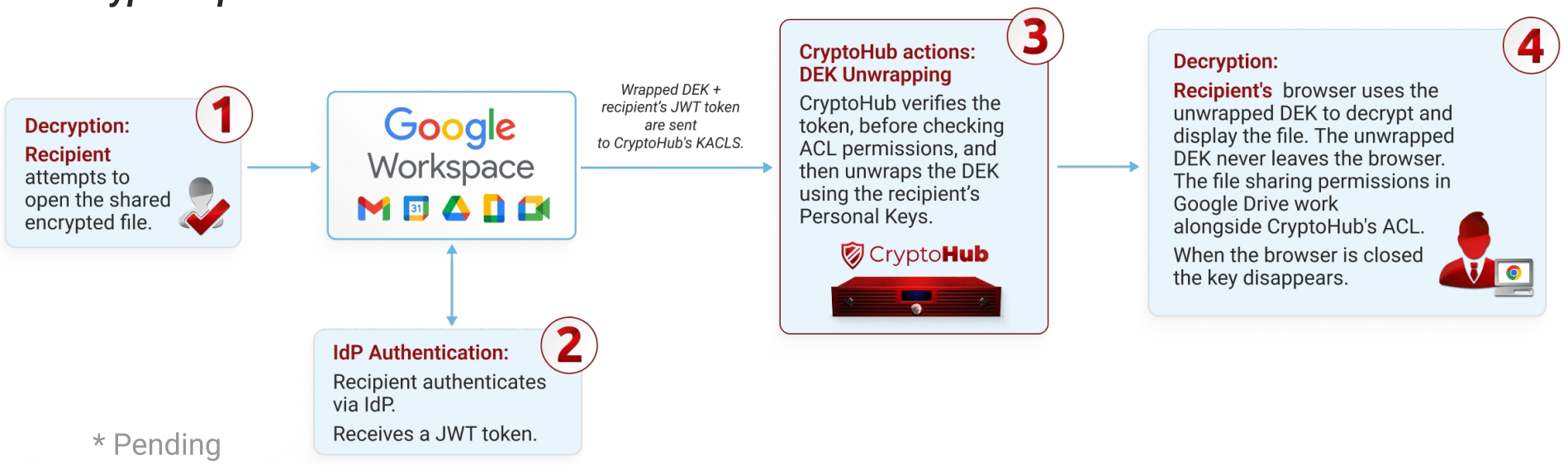
CryptoHub delivers the external key management, access controls, validated security, and operational efficiency required to fully align with Google's CSE security best practices, empowering organizations to protect sensitive data in collaborative environments.

## *Encryption process*




- ***Exclusive data control:*** CryptoHub enables organizations to manage and control their encryption keys externally, ensuring Google cannot access or decrypt sensitive data. All encryption and decryption occur in the user's browser, placing full data sovereignty in the hands of the enterprise.
- ***Validated hardware security:*** CryptoHub leverages FIPS 140-3 Level 3* and PCI PTS HSM v3 validated hardware, delivering robust, enterprise-grade protection for cryptographic keys and operations.
- ***Seamless integration and scalability:*** The platform integrates directly with Google Workspace CSE, supporting all use cases, including S/MIME for Gmail, while providing flexible deployment options (on-premises, cloud, or hybrid) to meet organizational needs and regional data residency requirements.
- ***Identity and access management:*** CryptoHub supports integration with leading identity providers (Google, Okta, VirtuCrypt), enforcing strict authentication and authorization for key access, which aligns with Google's recommendations.
- ***Operational simplicity and compliance:*** By centralizing cryptographic operations, key management, and policy enforcement, CryptoHub streamlines setup and ongoing administration, helping organizations maintain compliance with regulatory and data sovereignty mandates.
- ***High availability and disaster recovery:*** With multiple data centers and cloud options, CryptoHub ensures high availability, secure backup, and business continuity for key management infrastructure.

## *Decryption process*




* Pending

> **This innovative all-in-one hardware security module (HSM) and encryption key management solution is poised to redefine the standards of data protection.**
>
> *— Jordan French, Founder and Executive Editor, Grit Daily Group via Financial Tech Times.*

## Handling Gmail Encryption

| | Google E2EE | Futurex |
|---|---|---|
| **Key control** | Google Admin | External HSM + full lifecycle mgmt |
| **Compliance** | GDPR/HIPAA basics | FIPS 140-3*, audit trails |
| **Key storage** | Google Cloud | On-premises/VirtuCrypt |
| **Logging** | Limited | Hardware-enforced logs |
| **Deployment** | Native only | Native + Hybrid + Cloud-first |

Gmail's native E2EE improves security but does not eliminate all risks of unauthorized access or data exposure, especially when communicating outside the Google ecosystem or when key management is not strictly user-controlled.

Futurex's CryptoHub enhances Gmail security by externalizing S/MIME certificates and encryption keys, ensuring only authorized users can decrypt emails. The seamless process preserves Gmail's native experience while supporting regulatory compliance and robust key lifecycle management.

### *Gmail encryption process overview*

- ***Key generation and management:*** Admins use CryptoHub to create and manage S/MIME certificates and encryption keys for Gmail users.
- ***Certificate upload:*** Public certificates and wrapped private keys are uploaded to Gmail via the Gmail API.
- ***Client-Side encryption:*** Emails are encrypted in the user's browser before reaching Google's servers, so Google never sees plain-text content.
- ***Access control:*** Only authorized users can decrypt emails, validated by CryptoHub and Google's Key Access Control List Service.
- ***Ongoing key management:*** CryptoHub handles key rotation, revocation, compliance auditing, and supports aliases.

*Streamlined and secure email encryption with native PKI for Gmail*

**No 3rd-party CAs**

Eliminates reliance on external certificate authorities for security.

**Key rotation built-in**

Ensures regular updates of encryption keys for enhanced security.

**Rapid deployment**

Allows quick implementation of the system within a day.

Futurex's CryptoHub enables client-side encryption for Gmail by managing S/MIME certificates and encryption keys externally.

Email content is encrypted in the user's browser before being sent to Google, ensuring Google never accesses plain-text data.

CryptoHub integrates with Gmail APIs to upload users' public certificates and wrapped private keys, supports aliases, and enforces key access policies.

This setup preserves Gmail's native experience while giving organizations complete control over encryption keys and email security.

## Reduce Deployment Time By Over 90%

Transform weeks of integration into days and accelerate time to compliance. Futurex CryptoHub enables Google CSE setup in minutes, following a simple process to configure users and keys, create a key ring in Google, and start managing keys. Typically, it requires 10–12 clicks to set up Google CSE in Futurex CryptoHub. Log in, select the Google Workspace CSE service, deploy, configure roles and policies, enter the service account information, confirm the deployment, then register the external key service and identity provider in the Google Admin Console.

## Principal Advantages Of CSE

CryptoHub's architecture and operational model are well-suited for MSPs and enterprises seeking scalable, efficient, and future-proof client-side encryption solutions.

| Enterprise benefits | MSP suitability |
|---|---|
| **Exclusive data control:** Organizations retain sole control over encryption keys, ensuring only authorized users can decrypt sensitive information, even Google cannot access the data. | **Converged architecture:** CryptoHub unifies HSM, key management, and cryptography in a single platform with consistent features across all deployment models, unlike other vendors who separate these functions. |
| **Enhanced privacy and security:** CSE adds an extra layer of protection, making data indecipherable to third parties, reducing risks, insider threats, or government requests. | **Service parity:** All security algorithms, certifications, and applications are available in hardware and cloud offerings, allowing seamless migration and hybrid deployments. |

| Enterprise benefits | MSP suitability |
| --- | --- |
| **Regulatory compliance:** CSE helps organizations meet stringent regulatory and data sovereignty requirements, supporting compliance in sectors like healthcare, finance, and government. | **Operational simplicity:** Centralized, multi-tenant management and monitoring reduce complexity for MSPs and large organizations. |
| **Seamless collaboration:** Enterprises maintain the ability to collaborate in real time without compromising security or user experience. | **Innovation and flexibility:** CryptoHub's distributed processing and API-first design enable rapid adaptation to new use cases, including IoT and advanced tokenization. |
| **Peace of mind:** Knowing sensitive data remains private and protected builds trust with clients and stakeholders. | |

## Strategic Partner

With over 40 years in encryption, Futurex builds on a reputation for stability and innovation. Tier-1 banks, fintech firms, and global enterprises trust its proven track record of delivering large-scale, high-assurance encryption and key management. Futurex leads in quantum readiness as the only PQC-supporting HSM validated by PCI SSC.

Futurex's unified firmware powers all its cryptographic devices, ensuring seamless interoperability, fast security updates, and quick integration of new features. This design reduces complexity and lets customers adapt swiftly to changing compliance requirements.

VirtuCrypt data centers worldwide provide low-latency HSM services, enabling hybrid, on-premises, and cloud deployments for maximum flexibility and business continuity.

Over 15,000 organizations rely on Futurex for enterprise-grade data security through hardware security modules, key management servers, and cloud HSM solutions.

TRY CSE FREE FOR 30 DAYS

* Pending

FUTUREX

FUTUREX.COM

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents and delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

864 Old Boerne Road,
Bulverde, Texas 78163