GOOGLE WORKSPACE CLIENT-SIDE ENCRYPTION

Remote and hybrid work have driven digital transformation, boosting collaboration and Google Workspace adoption. IT departments must support this shift while keeping sensitive data compliant and secure. Google recommends external key management to maintain full control over data privacy and sovereignty.

90%

accelerated deployment,
reducing delivery from months to days

Content Encryption

Encrypts content before it leaves the user's browser.

Key Control

Only you hold the decryption keys.

Data Shielding

Shields sensitive data even from Google servers.

User Experience

Seamless browser-based experience.

Data protection and sovereignty at your fingertips

Choosing CryptoHub affords customers a winning formula to boost their organizational performance and gain a competitive advantage. The unified cryptographic platform combines HSM-backed encryption, PKI, and key management on a single device, eliminating the need for multiple vendors or fragmented solutions.

Futurex's Google Workspace Client-Side Encryption (CSE) provides a seamless and powerful solution for securing sensitive data across Gmail, Meet, Drive, Docs, and more. With browser-based deployment and rapid setup, administrators can implement CSE across their organization in under a day.

Customer challenges

- Data sovereignty
- SaaS adoption
- Zero-trust security
- Key management
- User segmentation
- Post-quantum readiness

Winning With CryptoHub

- Unmatched scalability
- Flexible delivery
- Industry-leading security
- Cost savings
- Operational efficiency
- Comprehensive integration
- Manage a dispersed workforce
- Unified platform

Gmail encryption support

CryptoHub enhances Gmail security by providing external management of 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.

This approach gives organizations complete control over email encryption, ensuring privacy, compliance, and security without disrupting user productivity.

Cloud deployments

Alternatively, you can choose to take the cloud route and leverage our global network of VirtuCrypt data centers that offer seamless, low-latency HSM services worldwide and support hybrid, on-premises, and cloud deployments for maximum flexibility and business continuity.

Google Workspace

How It Works

In minutes, CryptoHub's wizard creates a Google key ring, then configures users and keys in just a few clicks.

1. Log into the Google Workspace Admin Console.
2. Add Futurex as your external key service (KACLS).
3. Configure encryption policies for Gmail, Meet, Drive, Docs, Sheets, and Slides.
4. Users can start encrypting their data immediately - no additional software or plugins required.

Start your 30-day trial today

PCI HSM

TOP INNOVATOR ABIresearch #1 in Payment HSM Innovation FUTUREX

PCI P2PE

PCI PIN

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

PCI DSS

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