Google adds client-side encryption to Gmail and Calendar. Should you care?

reader comments

20 with

Share this story

On Tuesday, Google made client-side encryption available to a limited set of Gmail and Calendar users in a move designed to give them more control over who sees sensitive communications and schedules.

Client-side encryption is a generic term for any sort of encryption that’s applied to data before it’s sent from a user device to a server. With server-side encryption, by contrast, the client device sends the data to a central server, which then uses keys in its possession to encrypt it while it’s stored. This is what Google does today. (To be clear, the data is sent encrypted through HTTPS, but it’s decrypted as soon as Google receives it.)

Google’s client-side encryption occupies a middle ground between the two. Data is encrypted on the client device before being sent (by HTTPS) to Google. The data can only be decrypted on an endpoint machine with the same key used by the sender. This provides an incremental benefit since the data will remain unreadable to any malicious Google insiders or hackers who manage to compromise Google servers.

Abbreviated as CSE, client-side encryption was already available for Google Drive, Docs, Slides, Sheets, and Meet for users of Google Workspace, which the company sells to businesses. Starting on Tuesday, Google is rolling it out to customers of Gmail and Calendar Workspace.

“Workspace already encrypts data at rest and in transit by using secure-by-design cryptographic libraries,” Ganesh Chilakapati, Google’s group product manager for Google Workspace, and Andy Wen, director of product management for Google Workspace security, wrote. “Client-side encryption takes this encryption capability to the next level by ensuring that customers have sole control over their encryption keys—and thus complete control over all access to their data.”

It’s probably an exaggeration to say Google’s CSE gives customers “sole control” of their encryption keys. That’s because CSE keys can be managed by a handful of external encryption key services that partner with Google. Technically, that means these providers will have at least some control over the keys. Google does give CSE users the option of setting up their own key service using a Google programming interface.

Advertisement

CSE is significantly different from PGP (Pretty Good Privacy) mail encryption that was popular with security-minded people a decade ago. That system offered true end-to-end encryption since the contents could only be decrypted with a key in the recipient’s possession. The difficulty of managing a different key for each party eventually proved too cumbersome, particularly at scale, so the use of PGP has largely vanished and been replaced with end-to-end encryption apps such as Signal.

Here’s an overview of the Workspace data CSE does and does not protect:

Service	Data that’s client-side encrypted	Data that’s *not* client-side encrypted
Google Drive	• Files created with Google Docs Editors (documents, spreadsheets, presentations) • Uploaded files, like PDFs and Microsoft Office files	• File title • File metadata, such as owner, creator, and last-modified time • Drive labels (also called Drive metadata) • Linked content that’s outside of Docs or Drive (for example, a YouTube video linked from a Google document) • User preferences, such as Docs header styles
Gmail	• Email body, including inline images • Attached files**Note:** Attaching client-side encrypted Drive files isn’t yet supported	• Email header, including subject, timestamps, and recipients lists
Google Calendar	• Event description • Attached Drive files (if CSE for Drive is turned on) • Meet audio and video streams (if CSE for Meet is turned on)	Any content other than the event description, attachments, and Meet data, such as: • Event title • Event starting and ending times • Attendees list • Booked rooms • Join by phone numbers • Link for Meet

Service	Data that's client-side encrypted	Data that's *not* client-side encrypted
Google Meet	• Audio streams • Video streams (including screen sharing)	• Any data other than audio and video streams

The middle ground CSE is intended to occupy is aimed at organizations with strict compliance requirements that are mandated by law or contractual obligations. CSE gives these customers more control over the data Google stores while at the same time making it easy for authorized users to decrypt for sharing and collaboration.

"Users can continue to collaborate across other essential apps in Google Workspace while IT and security teams can ensure that sensitive data stays compliant with regulations," Tuesday's post from Google stated. "As customers retain control over the encryption keys and the identity management service to access those keys, sensitive data is indecipherable to Google and other external entities."

Last year, Google published this video designed to show what the user experience is like.

[embedded content]
Solving for digital sovereignty with Google Workspace.
The blue circle with the shield in the following images indicates that the content in the documents, calendars, or video chats is protected by CSE:

Of course, CSE only works if the software hasn't been altered. In the event it's maliciously altered to store keys or copies of unencrypted data, all bets are off.

Overall, CSE provides an incremental improvement over the current protections available from Google. People and organizations with specific uses or requirements may find them useful, but the masses are unlikely to clamor for it anytime soon.

https://arstechnica.com/?p=1920868