Google is letting businesses try out client-side encryption for Gmail

Google has launched a beta of its client-side encryption for Gmail, letting businesses apply to test out the feature meant to make “sensitive data” and attachments unreadable even to Google. The company announced the beta, which Workspace administrators can sign up for until January 20th, in a blog post on Friday.

Once the feature is enabled and set up for a workspace’s users, they’ll have an additional option when using the web version of Gmail. Clicking on a padlock will let them choose to turn on additional encryption for the message, though they will have to give up some features to do so, including the ability to use emoji, a signature, and Smart Compose. Google says client-side encryption will be added to its Gmail app for Android and iOS “in an upcoming release.”



a:hover]:text-gray-63 text-gray-63 dark:[&>a:hover]:text-gray-bd dark:text-gray-bd dark:[&>a]:text-gray-bd [&>a]:shadow-underline-gray-63 [&>a:hover]:shadow-underline-black dark:[&>a]:shadow-underline-gray dark:[&>a:hover]:shadow-underline-gray”>Gif: Google

While the ability for users to encrypt messages will be managed by their administrators (which, in most cases, will be the companies they work for), the feature isn’t limited to just intra-office communications. You’ll be able to send encrypted emails “outside of your domain,” according to a Google help document, and even to people who use other email clients or providers, such as ones from Microsoft or Apple, according to Google spokesperson Ross Richendrfer. This is because “CSE for Gmail is built on S/MIME, an existing

standard for email," Richendrfer told *The Verge* in an email.

Google has been working on adding more encryption to Gmail for a long time. In 2014, there were reports that it was working on end-to-end encryption for the service, though it's worth noting that client-side encryption isn't exactly the same thing. While using either means that "encryption and decryption also always occur on the source and destination devices," Google's client-side implementation gives administrators control over the keys and lets them "monitor users' encrypted files," according to a help document from the company explaining the difference between the two forms of encryptions.

Right now, the Gmail beta is limited to Google Workspace Enterprise Plus, Education Plus, and Education Standard customers, according to Google's blog post. That means you can't try it out if you're on a personal account or using a lower-tier enterprise, business, education, or G Suite account.

With that said, given that the system currently relies on administrators using an API to upload certificates and encryption keys generated by an external management service, it's probably best that it's mostly being limited to companies with IT departments at this point. If you'd be willing to go through that sort of hassle, though, you can always use PGP within Gmail (or, more realistically, sign up for a Proton Mail account, which has).

https://www.theverge.com/2022/12/16/23513243/google-gmail-client-side-encryption-beta-enterprise