Google Workspace adds anti-phishing, client-side data encryption

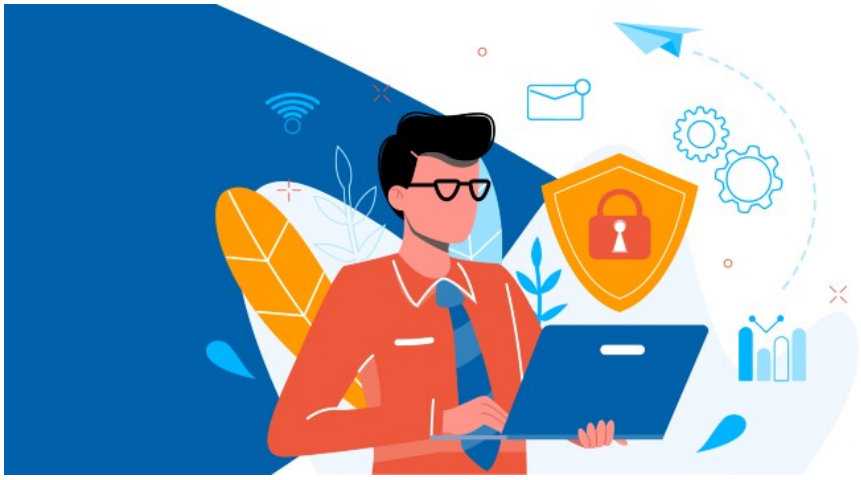
After allowing free use, Google also updated some security features for Google Workspace.

Google Workspace (formerly G Suite) has just updated its client-side encryption capabilities and added anti-phishing and malware protection on Google Drive. These new additions are part of Google's focus on data security.

Client-side encryption

Google says that Google Workspace uses the latest encryption standards to encrypt data stored or transferred between its facilities. The next big step is that Google Workspace users will have direct control over the encryption keys and identity services they choose to access those keys. This is the encryption option from the client side.

When client-side encryption is enabled, only you and your partners can access your encrypted Google Drive documents. When you want to share access, you'll have to share your encryption key.



This feature will be especially useful to organizations and individuals that often have to store sensitive or confidential data. Google is rolling out a beta version of this encryption feature to Workspace Enterprise Plus and Workspace Education Plus users.

Initially, this feature will support Google Drive, Docs, Sheets, and Slides. After that, it will also support other Google Workspace services like Gmail, Meet and Calendar. To enable client-side encryption, you will also need to select one of the key access service partners (e.g. Flowcrypt, Futurex, Thales or Virtu) for key management and access control.

You can also build or integrate your own encryption key service by relying on an API that Google will roll out later this year.

Anti-phishing and malware features

Google says all Google Workspace customers will benefit from Google Drive's built-in protections that block phishing and malware content. This new feature even has the ability to protect users from internal threats and also from user errors.

In an enterprise environment when these protections are enabled, all suspicious files on Google Drive will be automatically tagged with warnings. A tagged file is only visible to its owner and IT administrators.

As a result, files suspected of containing malicious code will not spread throughout the organization, significantly reducing the number of people affected by a malicious attack via Google Drive.