Effortless digital communications security in Gmail

Empower your people to work securely within Gmail with unparalleled encryption, contextual machine-learning (ML) powered business rules, and secure file transfer.

Zivver prevents data loss and supports compliance with GDPR, CCPA, LGPD and more.

Seamless integration with the Google environment

Gmail alone doesn't offer enough to secure your sensitive data. Zivver integrates with Gmail to make achieving robust communications security simple - no change to existing workflows or processes.

01. Contextual ML powered error correction

ML powered business rules classify content and alert users to potential errors in Gmail before emails are sent, such as incorrect recipients added by autocomplete, wrong attachment for a specific recipient, the presence of sensitive data and more, as messages are composed.

02. Unparalleled encryption

Gmail supports secure email transport via STARTTLS, a very basic security measure that relies on your recipient's server settings to deliver a message securely. To create a secure connection, both the sender and recipient must use TLS. When a secure connection can't be created, Gmail delivers messages over non-secure connections - or not at all.

Zivver applies the highest industry standards to secure the connection between sender and recipient and prevent message interception. Our semantic-aware, tailored encryption analyses the sensitivity of email content and detects the recipient's security levels. Where these are insufficient for the required security level, Zivver routes the email via our own server to enforce secure sending.

03. Multi-factor authentication

Ensure only authenticated recipients access sensitive data with multi-factor authentication technology, inbuilt into Gmail. Zivver tailors the required authentication level based on recipient type and their security settings, and stores these to your organisation address book so recipient details only need to be entered once.

04. Zero keys, zero access

Unlike Gmail, Zivver operates a strict zero-knowledge policy. Messages are asymmetrically encrypted, and we don't store customer keys or any derivatives to be able to decrypt them. Only encrypted data is stored to disk meaning it is impossible for Zivver to view the content of messages sent with our service. This means nobody but the sender and recipient can access, decrypt and read message content.

05. Recall you can rely on

Recall messages and set expiration periods to control recipient access, even after sending. If the message is recalled before the recipient has opened it, Zivver can guarantee that any possible data leak has been contained.

These organisations already secure their email data

Zivver was recently identified as one of five representative vendors in the ‘Email Data Protection Specialists’ category in Gartner’s ‘2020 Market Guide for Email Security’.

Intelligent, effortless compliance

Our dashboard and audit logs provide a handy overview of email activity, so you can act swiftly if an incident occurs.

Easy for both sender and recipient

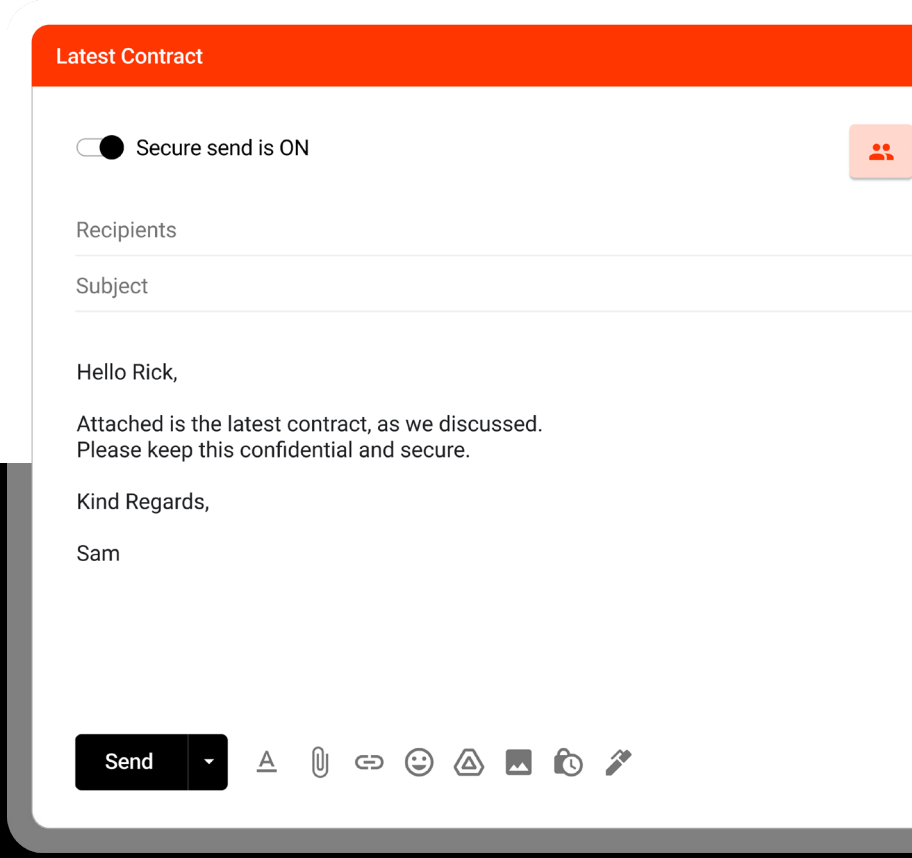
With single sign-on, employees are immediately logged into Zivver when they log in at their workstation, keeping the familiarity of Gmail at work, at home or on the go. Plus, there’s no need for recipients to create an account or download software to open a secure email sent by Zivver - we keep things simple for everyone.

Easy for admins

Our finely tuned out-of-the box business rules simplify data classification instantly, and the solution is deployed with minimal maintenance. Zivver’s proactive notifications make the solution one which employees want to use, embedding an organization-wide security lifestyle.

Download the Zivver for Gmail

Available in the Chrome Web Store



Zivver
5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300
contact@zivver.com

www.zivver.com

linkedin.com/company/zivver facebook.com/zivver @zivver_en