Protect data in M365 with next generation email security

Zivver

Empower your people to work securely within Microsoft 365 with unparalleled encryption, contextual machine-learning (ML) powered business rules, and large file transfer.

Seamless integration with Outlook

Manage digital communications securely in the cloud, on-premise, and on any device, with ease.

How Zivver secures digital communications with Microsoft 365

01. Before sending

Alerting users to potential errors in real time, with contextual ML powered business rules

02. During sending

Protecting emails and files from unauthorized access with advanced encryption

03. After sending

Empowering instant recall of emails and attachments, access controls, and data logging

Contextual ML

Zivver uses ML powered business rules to classify content and identify errors in Microsoft 365, before emails are sent. Senders are alerted to potential mistakes, such as incorrect recipients added by autocomplete, wrong attachments for a specific recipient, and the presence of sensitive data.

One click or click free security

Securing digital communications should be effortless. With Zivver, you choose what level of security to apply and when.

Zero keys, zero access

Unlike M365, 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 communications. This means nobody but the sender and recipient can access and decrypt data.

Semantic-aware, tailored security levels

Contextual ML learns from user behaviour to provide real-time alerts to potential data leaks. Semantic-aware, Zivver notifies users to sensitive data and PII, incorrect recipients and more, based on the sensitivity of your content and detection of the recipient's settings.

Who we work with

NHS Digital

CYBER ESSENTIALS

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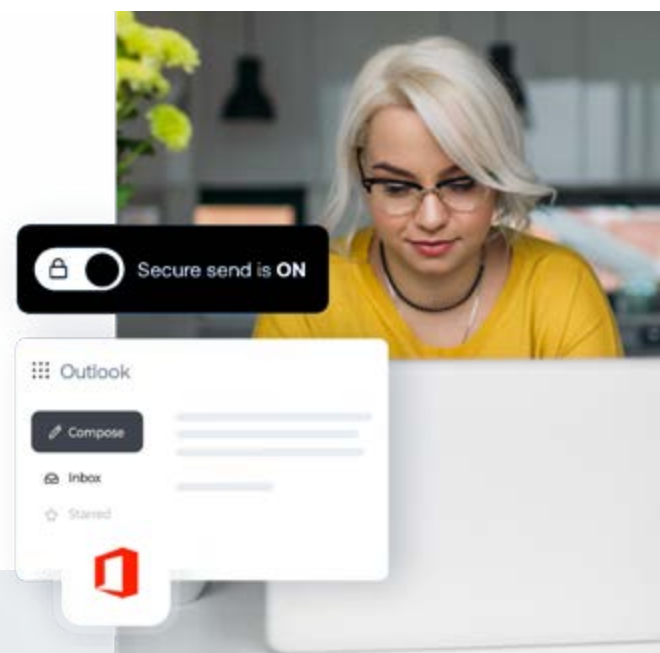
Zivver was recently identified as one of five representative vendors in the 'Email Data Protection Specialists' category in Gartner's '2020 Market Guide for Email Security'.

Recall you can rely on

A specific requirement of GDPR, Zivver enables users to restrict access to an email sent in error, immediately, at any time. If the message is withdrawn before the recipient has opened it, Zivver guarantees that any possible data leak has been contained. Unlike M365, Zivver's revoke function works for recipients with any email client, and users can set expiration periods to control recipient access, even after sending.

Registered post just got smart

Tracking and proving delivery of important, sensitive or time-critical communications is key for many of us. With Zivver your documents can be sent digitally with registered, verified proof of delivery.

Save on costs compared to standalone Office 365 E5 licenses

If you seek to de-risk your email interface, Microsoft's new E3 and E5 can be overkill, with organisation-wide changes to the way people work. Zivver, combined with an Office 365 E1 or E3 license, empowers secure work with minimal disruption, far more cost effectively than an E5 license.

Send any type of file up to 5TB from Outlook too

With Zivver, you can send any type of file up to 5TB from M365. Say goodbye to file transfer sites, say hello to efficiency.

Intelligent, effortless compliance

Our dashboard and audit logs provide a comprehensive 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 Microsoft 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.