zivver

G-Cloud 15 Service Definition

Zivver – Secure Email Platform
Zivver Limited

Lot 2b Software as a Service (SaaS)

1. Introduction

Company Overview

Zivver is a privately held Dutch technology company founded in 2015 and headquartered in Amsterdam, operating under the legal entity Zivver B.V., with regional entities including Zivver Ltd in the United Kingdom. The company develops and provides secure-communication software encompassing outbound email security, secure eSignatures, and inbound email threat protection.

Zivver now supports over 11,000 organisations across sectors such as the NHS, Private Healthcare, Local and Central Government, Housing Associations, Education, Financial Services, Legal, Hospices and Charities. The company delivers its services via a cloud-based SaaS model and integrates with Microsoft Outlook (Desktop and Microsoft 365), Gmail, and mobile applications. Zivver has been recognised as a Representative Vendor in Gartner's Market Guide for Email Security in 2023, 2024, and 2025, is included in the CyberTech 100 list of leading global CyberTech companies, and has been recognised as a High Performer for both Email Encryption and Email Security in the G2 Summer Market Report.

Value Proposition

With organisations facing challenges brought on by rapid digital transformation, regulatory reforms, and hybrid working, the need for secure, efficient, and resilient communication is critical. Public sector and regulated organisations handle highly sensitive data, where a leak can result in heavy fines under UK GDPR, reputational damage, and operational disruption. Research by IBM shows that the global average cost of a data leak was over GBP 3.29 million in 2025.

The majority of data leaks occur while communicating sensitive information via email or portals. In addition to misaddressed messages, sharing incorrect files, or failing to follow policy, organisations face increasing threats from phishing, business email compromise, impersonation attacks, malware, and ransomware. Protecting employees and securing brand reputation are now equally important. Many existing tools for emailing or sharing sensitive information fall short: they offer limited human error prevention, lack zero-trust encryption, struggle to authenticate users effectively, and often do not integrate seamlessly with workflows.

Zivver addresses these challenges with a comprehensive platform of digital communication solutions:

- **Outbound Secure Email** delivers encrypted email communication and secure large-file transfer, strengthened by AI-driven human-error prevention to minimise data loss and ensure compliance. **T**he service can be optionally extended with **Secure eSignatures**, enabling secure document signing and

verification within existing organisational workflows.

- **Email Threat Protection** blocks phishing, prevents BEC scams, stops impersonation attacks, and eliminates malware and ransomware.

These solutions enable organisations in highly regulated sectors — including central and local government, financial services, healthcare, and legal — to communicate securely while enabling employees to work within familiar applications and workflows.

Examples of public sector customers include the UK's National Health Service (NHS), Oxford City Council, Manchester City Council, South Kesteven District Council, Calderdale Council, West Lindsey District Council, North Kestevan District Council, Hertsmere Borough Council, North Yorkshire Council, The British Library, the Dutch Judicial System (all courts, clerks, and lawyers), and the Dutch Ministry of Security and Justice and its subsidiaries.

What the Service Provides

Zivver is a Secure Email Platform offering Outbound Secure Email, Secure eSignatures, and Zivver Email Threat Protection. It integrates seamlessly with Outlook, Gmail, and mobile apps. Supported by dedicated administration and implementation teams, Zivver helps organisations prevent data leaks, improve employee security awareness, maintain regulatory compliance, and streamline secure messaging and document signing across existing workflows.

Zivver strengthens organisations' email ecosystems with a privacy and security layer across Microsoft Outlook (Desktop and Microsoft 365) and Gmail. Its Outbound Secure Email ensures encryption and compliance, Zivver Secure eSignatures enables secure, verified document signing, and Zivver Email Threat Protection delivers AI-driven inbound security that uses multilayer machine learning, behavioral analysis, NLP, and computer-vision to detect and stop advanced threats—including phishing, BEC, QR-based attacks, malware, ransomware, and malicious attachments—while adaptive AI continuously improves detection and automates triage.

Social Value

Social Value Declaration

At Zivver, we believe our impact goes beyond offering secure communication technology. We are deeply committed to generating real, measurable social value through the way we treat our people, develop their potential, and ensure equitable opportunity. We pledge to deliver meaningful value across fair working conditions, in-work progression, and equality of opportunity, all aligned to the PPN 002 Social Value Model.

Kickstart economic growth

To promote fair working conditions, we will extend our current engagement survey by Q2 2026 to include both employees and contractors, giving voice to the full team working under this contract. In Q1 2026, we will deploy an anonymous "speak up" tool within our HR system, allowing any member of our workforce to raise concerns about wellbeing, bullying, or harassment confidentially. We will monitor survey participation rates, the volume of speak-up reports, and our follow-up actions, embedding this feedback into our governance processes and reporting mechanisms to ensure continuous improvement. These steps align with the PPN 002 requirement to measure and monitor engagement, involve staff in decision-making, and act on issues identified.

Our commitment to in-work progression means supporting career development for everyone working on the contract. By Q2 2026, we will launch a department-focused Learning & Development policy that addresses both technical ("hard") and interpersonal ("soft") skills, which can also be used for training that leads to recognised qualifications by employees. We will offer mentoring, mock interviews, CV coaching, and careers guidance from our recruiters. Through these interventions, we aim to upskill our workforce, support personal and professional growth, and strengthen engagement and loyalty.

Break down barriers to opportunity

On equality of opportunity, we will conduct a comprehensive equal pay audit by Q4 2026, monitor and report on any gender and ethnicity pay gaps, and introduce transparent pay and reward processes. These steps reflect our commitment to address and correct inequalities, ensuring that every person in our workforce, regardless of background, receives fair compensation and a real chance to progress.

Zivver is committed to generating meaningful social value under this contract by enhancing fair work, promoting in-work progression, and advancing equality of opportunity. Our commitments are concrete, measurable, and will be embedded in

governance, reporting, and improvement processes. Through these actions, Zivver aims to create a more inclusive, fair, and empowering workplace, delivering not only contractual value but social value that speaks to our core mission.

Overview of the G-Cloud Service

Zivver provides a comprehensive platform of digital communication solutions:

- **Outbound Secure Email and Secure eSignatures** – Enables encrypted emails, large file transfers up to 5TB, zero-access encryption, AI-based human error prevention, secure electronic signing, authentication, and legal proof of delivery. Integrates with Outlook (desktop and web), Gmail, and mobile apps.

- **Email Threat Protection** – Detects and blocks phishing, business email compromise, impersonation attacks, malware, and ransomware.

Outbound Secure Email and Secure eSignatures are hosted on AWS public cloud with multi-factor authentication and zero-access encryption. Zivver Email Threat Protection is delivered via managed SaaS platforms.

Operational benefits include: reducing data leak risks, improving employee security awareness, enforcing organisational policies, strengthening protection against inbound email threats, and facilitating secure messaging and document signing within existing workflows.

Zivver Outbound Secure Email

Zivver is the effortless, smart, secure digital communications platform powering the next generation of secure digital communications.

Zivver is a secure digital communications platform with a core focus to provide a secure email and file transfer solution to organisations, helping them effectively communicate in a digital way, and enable their employees to continue working from their existing applications as much as possible. In working from within their existing email application, such as Outlook and Gmail, Zivver helps its customers save costs associated with ineffective communication methods such as message portals, letters, fax and file transfer applications, whilst preventing data leaks and complying with rules and regulations.

Zivver's solution provides secure email and large file transfer, certified email, human error prevention, data protection policy enforcement and secure electronic eSignatures. With these products, features and separately priced add-ons, Zivver uniquely helps organisations to prevent data leaks in the entire communication journey when sharing information before (human error prevention and policy enforcement), during (zero-access encryption in transit and at rest) and after

(authentication, access control, logging and reporting) sending and receiving of information.

Zivver's Outbound Email Security: Design Principles

Zivver's entire secure digital communications platform is built on three core principles. Applying these principles, we believe that we can empower your employees with the tools to reduce the risk of misdirected emails, prevent unauthorised access by unintended recipients, apply appropriate levels of security measures based on the content of emails and create a culture of security awareness.

Effortless

The platform is designed to minimise user effort and integrate seamlessly into existing workflows. Key characteristics include:

1. Email client, address and device agnostic
2. No recipient account needed
3. Instigate secure mode by default or in one click
4. Native SaaS – no hardware & remote updates
5. Embeds & integrates at the point of use (such as the Outlook email client)
6. Same UX and UI across the platform

Smart

The platform applies intelligent controls to support users and organisations in making secure communication decisions. Examples include:

1. Semantic-aware, tailored security levels
2. Machine learning powered business rules
3. Contextual, real-time user error correction
4. User-empowered controls
5. Active memory – replicates security measures per recipient
6. Data and protocol transformation

Secure

Security underpins all platform capabilities, with a focus on strong encryption, compliance, and control for both senders and recipients. Capabilities include:

1. Zero keys, zero access – unparalleled encryption
2. Sender to Recipient protection
3. Full compliance – GDPR, NTA, ISO27001, SOC2
4. Instantly revoke access – any message, any time
5. User-level authentication
6. Legal proof – legally prove sending

Zivver Outbound Email Security: Overview

Zivver is designed to make digital communication smart, effortless, and secure. This section outlines the functionalities and services provided by Zivver to customers and users. Zivver's offering consists of the following components:

Platform	Standard platform functionalities are essential to our products, providing secure and efficient communication for every customer. These standard platform functionalities are included in Zivver's Secure Email and File Transfer product package, ensuring a fully operational experience. In addition to these standard functionalities, we offer a selection of optional platform functionalities, available to all customers at no additional cost. These optional functionalities are designed to meet individual needs and preferences, allowing for a more tailored experience.
Products	Products are built on top of the Platform and support users in achieving a primary business requirement or use case. Platform and Products features and functionalities listed below are included in the Core Product offering price in the G-Cloud 15 Pricing Document.
Apps & Integrations	Customers and users use the Platform and Products through Zivver's suite of Apps and Integrations. This includes integrations for Outlook, Gmail, mail servers and third-party applications, as well as Zivver's web and mobile app. Only the Encryption Gateway and Data Loss Prevention (DLP) Gateway have an additional cost which can be found in the G-Cloud 15 Pricing Document.
Add-ons	Add-ons are optional functionality that work on top of our Products to provide enhanced and/or additional functionality for specific use cases. Some add-ons are available at no additional cost, while others require a paid subscription. Pricing information for paid add-ons is provided in the G-Cloud 15 Pricing Document.

NB: Minimum technical requirements may apply for certain functionalities. See Zivver Minimum Technical Requirements below for more information.

Platform

The Platform consists of core functionalities that are available in all Products. These core functionalities consist of standard functionalities which are always included as well as optional functionalities that customers can choose to use at no extra cost.

Standard Platform Functionalities	
Secure communication with anyone	Zivver enables you to communicate securely with any (one who has an) email address (including systems and/or shared mailboxes) regardless of whether they have a Zivver account or not.
Zero-knowledge encryption	Zivver encrypts all messages and files in such a way that the sender and recipient (organisations) are guaranteed to be the only ones who have access to the content. Zivver uses a technique called the Bring-Your-Own-Key principle which only allows the decryption of the content with the user key (sender or recipient).
Strong user authentication	Zivver requires users to be strongly authenticated to use the Platform. Zivver offers 2-factor authentication using a Hash-based One Time Passcode (HOTP) via SMS or using an Authenticator app. User authentication can also be delegated to the customer using a Single-Sign-On integration between Zivver and your ADFS or other SAML v2-compatible identity provider. If using SMS authentication for users, this will incur an additional charge. Details regarding SMS costs are available in the Zivver pricing document.
Strong recipient authentication	To ensure the intended recipient is the only one who can access a digital message, strong recipient authentication can be enforced. This can be achieved using Zivver-account verification, Hash-based One-Time Passcode (HOTP) via SMS or an agreed access code. As an optional fallback, organisations can also use an HOTP via email.

	If using SMS authentication for users, this will incur an additional charge. Details regarding SMS costs are available in the Zivver pricing document.
Manage authentication information of recipients	For efficient use of strong recipient authentication, using for example HOTP via SMS or an access code, it is essential that the recipient authentication data can be reused by users and their colleagues. To achieve this, Zivver enables admins to centrally manage or upload the recipient authentication information.
Organisational address book	The Zivver platform has the ability to store contact data like that of any other email client for repeat use, including name, email address, contact phone number, and access code. This address book can be accessed by all users within an organisation without compromising the privacy of the user in the address book.
Guest accounts	Guest recipients do not need a Zivver account to open secure Zivver messages. However, they are able to create a free personal (consumer) account. Having an account does not only make it easier for users to read their messages but also enables them to securely send messages and files themselves.
Read indicator	Zivver shows the user whether a message and/or any attachments have been opened (decrypted) or downloaded by a recipient.
Revoke access to sent messages	Zivver offers users the possibility to revoke access to sent messages. Access can be revoked only for recipients or for the recipients as well as the sender. If a message is revoked, Zivver guarantees that all recipients that have not yet opened (decrypted) the message, will not be able to do so.

	All events are logged for a complete audit trail.
User management	Zivver offers administrators the possibility to easily manage user accounts by, for example, creating, editing, and deleting accounts. This can be done manually in the Zivver web application, or automatically with, for example, the organisation's Active Directory, Excel lists, or a SCIM 2.0-compatible service. Zivver products can function without the user management tools, but then all user administration and password management needs to be done manually.
Insights	Zivver Insights provides a variety of frequently used dashboards and flexible data export capabilities to assess how well Zivver is protecting against email data leaks and determine where you can make continuous improvements.
Administrator & User Audit Trails	Zivver logs all administrator actions by default, including, but not limited to, creating, changing, and deleting accounts, changing settings, and switching functionalities on and off. By default, Zivver also logs user actions and their communication behaviour. In case of a possible data leak, this functionality is essential to investigate the incident. This information is available in the audit trail via the Zivver Web App and can be exported for further analysis.

Optional Platform Functionalities (No Additional Costs)	
Pre-notification emails	To help avoid secure emails being ignored or distrusted by first-time recipients, Zivver offers prenotification emails. When a recipient is about to receive their first secure Zivver message from an organisation, Zivver

	can send out a pre-notification email which explains what Zivver is, why it's being used, and that they can expect a secure message to arrive soon. Pre-notification emails can be sent from an organisation's own domain (using the optional 'send on behalf of your own domain' functionality) and fully branded in an organisation's own corporate identity (using the Custom Branding add-on).
Send on behalf of your own domain	With this functionality, Zivver can send secure messages on behalf of users and the domain of the organisation instead of noreply@zivver.com. This creates a more consistent brand image and better overall recipient experience.
Default message expiration policy	Zivver offers organisations the possibility to set a default expiration moment for messages, after which messages become unavailable for the recipients or everyone (meaning the sender as well). Organisations can set a default expiration moment (in hours, days, weeks) in accordance with their standard policy.
Email verification	Next to the strong methods of recipient verification mentioned above (Zivver-account, HOTP via SMS, access code) Zivver also offers the option to verify recipients using a Hash-based One-Time Passcode sent via email. Customers can choose whether or not to allow email verification of recipients. This option is more secure than sending a regular email, but less secure than other methods of recipient verification already mentioned (Zivver-account, HOTP via SMS, access code).
Transport Security Compliant delivery	Using Transport Security Compliant delivery, Zivver can also deliver secure messages directly to the inbox of the recipient using transport layer encryption (but without message encryption) if the recipient's mail server supports a minimum level of transport

	encryption and server authentication: ● TLS v1.2 and higher ● TLS v1.2 and higher combined with a valid PKIX certificate ● PKIX + DNSSEC ● DNSSEC + TLSA Organisations can choose whether or not to allow Transport Security Compliant delivery and what the minimum level of transport security and server authentication is.
Single Sign-On (SSO)	With Single-Sign-On (SSO), users can easily log in to Zivver using their credentials from Microsoft Azure, Google G Suite, Okta, and other identity providers.
Synctool	The Synctool allows administrators to automatically provision, deprovision and manage user accounts based on the organisation's own Active Directory.
Assisted Mail Submission (AMS)	AMS is an optional feature in the Zivver Outlook Windows Add-in and the Zivver Outlook Web Access Add-in. It ensures that emails which should be sent securely via Zivver first pass through Microsoft Exchange without message encryption. From Microsoft Exchange, the message is then relayed to Zivver for secure delivery to the recipient(s). This ensures compatibility with other optional Microsoft or third-party capabilities which rely on an unencrypted message. For example: ● Exchange or a third-party application adding a signature or disclaimer to outbound emails. ● Document Management System Add-ins which file an unencrypted copy of the message. ● Secure Email Gateways which process all outbound emails.

Custom Support Channels	By default, the support channel provided to guest recipients of a Zivver message will direct them to the Zivver support team. For organisations that can and want to handle support enquiries internally, Custom Support Channels allows the default contact info to be changed to a custom domain and phone number.
Inbound Direct Delivery (IDD)	With IDD, organisations can choose to receive incoming secure messages to their mail server with transport encryption but without message encryption. This can be relevant for organisations that need to be able to archive the contents of secure messages, or for organisations that require users to be able to read secure messages on any device and have strict internal security measures and access control in place. Replies to IDD messages will be automatically secured by Zivver. When using a Zivver client integration, IDD messages will still be recognized as secure Zivver messages, allowing the recipient to use Zivver as they would without IDD.
Trusted Device Authentication	In order to make it as easy as possible for a guest user to open a secure message, Zivver offers recipients the option to trust the device they open the initial message with for 30 days. This means they will be able to skip the normal verification step for that duration. After having trusted their device, a guest user receives an email to confirm a trusted device has been added.

Secure Email & File Transfer	
Send a secure email	Users are able to choose whether or not to send an email securely. Using one of Zivver's client integrations, this can be done by simply toggling Zivver on or off directly within the user's regular email client. Users can also send secure email using one or more of Zivver's mail server or system integrations and the Zivver web/mobile application.
Receive a secure email	Users are able to receive secure message notifications. Using one of Zivver's client integrations, messages can be automatically decrypted, showing the contents of the message. Secure messages are also accessible via the Zivver Web App and mobile app. To be able to read received secure messages on any device, Zivver offers Inbound Direct Delivery as a free add-on.
Send (large) files securely	Users are able to select (large) files or folders to be sent securely. Files and folders of up to 5TB can be transferred. Using one of Zivver's client integrations, this can be done directly from within a user's regular email client. Files can also be sent securely using the Zivver web or mobile app, or one of Zivver's mail server or system integrations.
Secure file download	If a secure message can be directly delivered to a recipient (using Inbound Direct Delivery or Transport Security Compliant verification) but one or more attachments are too large to be handled by the recipient's mail server, Zivver will automatically turn the attachment(s) into a secure download link. This allows the recipient to still access the attachment(s) without losing the benefit of a directly delivered secure message. In this case, the recipient will be verified with email verification.

Apps & Integrations

Zivver offers several different apps and integrations through which customers, administrators and users access Zivver functionality. Only the Encryption Gateway and Data Loss Prevention (DLP) Gateway have an additional cost which can be found in the G-Cloud 15 Pricing Document.

Zivver's apps and integrations can be broken down into three categories:

1. Apps: Zivver's own email clients

2. Mail client integrations: Integrations in users' email clients

3. System integrations: Integrations with customers' mail servers and third-party systems

Please note: Not every app or integration offers access to all functionalities described in this document in isolation. For example:

● Administrator functionalities are available in the Zivver Web App but not the mobile app.

● Functionality like revoking access to a message is only available through client integrations or the Zivver apps, not the mail server and system integrations.

● Large file transfer is available when using the Zivver apps or client integrations. When using mail server integrations and system integrations, the file size is usually limited by the sending system or mail server.

The Zivver apps (web and mobile) are always available to ensure that users always have access to all standard platform functionality.

Apps

Zivver's own secure email clients, available as a web app or native mobile apps, can be accessed from any modern device and included as part of the Core Product price shown in Zivver's G-Cloud 15 Pricing Document. They require users to navigate to the Zivver app to access Zivver functionality. Zivver offers the following apps:

● Web App (Available via https://app.zivver.com)

● Mobile app (Available for iOS and Android)

Client integrations

Client integrations are included as part of the Core product price shown in Zivver's G-Cloud 15 Pricing Document and are integrated directly into the email client of the user, ensuring the user can access Zivver functionality without leaving their email client. For example, users can toggle secure sending on/off, get real-time warnings of sensitive content, and enter recipient verification details such as a phone number before sending a secure message.

Zivver offers the following client integrations:

- Outlook Windows Add-in (Available as a COM Add-in)

- Outlook Web Access Add-in (Available as an M365 Add-in)
- The New Outlook Add-in (Available as an M365 Add-in)
- Gmail Chrome Extension (Available in Chromium-based browsers)

System integrations

Zivver's system integrations are separately priced add-ons from the core product offering, pricing can be found in Zivver's G-Cloud 15 Pricing Document. These system integrations consist of the Encryption Gateway and the Data Loss Prevention (DLP) Gateway, which embed Zivver's secure communication capabilities directly into manual and automated email flows behind the scenes. This allows customers and users to benefit from Zivver without a visible integration in their email client. Customers can decide themselves which emails should be sent securely, let their employees decide, or use Zivver's classification algorithms to decide. Each integration is outlined below:

● Encryption Gateway: Send secure Zivver messages or enforce a minimum level of transport security with a Zivver message as the fallback option. No sender interaction is required after a message is sent. Encryption Gateway can be integrated with mail servers and third-party systems and is available as an add-on.

● Data Loss Prevention (DLP) Gateway: Smart protection against data loss in outbound email flows without a client integration. Zivver scans outgoing emails for sensitive information and automatically sends messages securely if found. If required, DLP Gateway can interact with users after a message is sent. For example, to ask the sender for missing recipient verification details. DLP Gateway integrates with mail servers and with third-party systems (depending on the use case), and is available as an add-on.

Encryption Gateway and DLP Gateway can be integrated with mail servers and third-party applications. Encryption Gateway can be used for manual as well as automated workflows, while DLP Gateway is only recommended for manual workflows as interaction with the sender may be required.

System integrations are based on the Simple Mail Transfer Protocol (SMTP), ensuring compatibility with almost any system that is able to send emails. Using custom email headers, customers have fine-grained control over preferred delivery and recipient verification methods.

Cross-compatibility of apps & integrations

Multiple apps and integrations complement each other and can be used in parallel within a single organisation and even by a single user. For example, an organisation may use:

● Encryption Gateway to apply a minimum level of transport security to all outgoing emails.

● DLP Gateway to ensure that emails sent from mobile devices (or other devices without a Zivver integration) are automatically secured based on Zivver's classification algorithms.

● The Zivver (web or mobile) app to interact with DLP Gateway or send large files from mobile devices.

● A client integration on users' primary workstation for real-time suggestions while composing emails and access to Zivver functionality directly from their regular email client.

Zivver Secure eSignatures

Zivver Secure eSignatures is tightly integrated with **Zivver Outbound Email Security**, forming part of the same secure communication workflow. While Outbound Email Security ensures that emails and large file transfers are encrypted, authenticated, and protected from human errors, Secure eSignatures allows the documents being sent through these secure channels to be digitally signed and verified. Together, they enable organisations to securely send sensitive documents, ensure compliance, and provide legal proof of both delivery and signature—all while keeping users within their existing email applications and workflows.

Prepare a document for signature	Users are able to prepare a document for signature without leaving their email client. They can upload a .doc or a .pdf document and place fields anywhere in the document. Supported fields include a signature field, a date stamp field, and a custom text field.
Securely send out a document for signature	In order to send out the document for signature, users will have to turn Zivver on and securely send the email. Users can specify which recipients will need to sign the document and who simply needs to receive it. When sending the email and related documents, users have access to the standard platform functionalities (such as recipient authentication, revoke access, etc).
Signing a document	To sign a document sent via Zivver, recipients can proceed with or without a Zivver account. Without a Zivver Account: Upon receiving a signature request via email, they can initiate the signing process through a guided tour or navigate directly to the specific fields in the document that require their signature. If they

	prefer not to sign, declining the request is an option available to them. With a Zivver Account: For those who have a Zivver account, the process is streamlined within their email client, allowing for a direct and seamless signing experience. Regardless of the method chosen, all users have the ability to easily view the list of co-signatories, their signing status (whether pending or completed), receive notifications once all signatures are collected and download the original document for their records.
Document overview	A user can access an overview of all documents from within their email client. Here a user can see all documents that they sent out for signature, have signed themselves or for which they received a request to sign. Finally, a user can download any signed document and its corresponding audit report straight from the overview.
Audit report	Once all signatories have signed a document, all recipients (signatories and reviewers) will be able to download a corresponding audit report. The audit report contains information such as (but not limited to) the name of the document, the creator of the document, the signers, the status of the signature process and validation, the certificate holder, and timestamps of each step in the signing process.

Zivver Email Threat Protection

Zivver Email Threat Protection is a cloud-based service that safeguards organisations from malicious inbound emails, including phishing, business email compromise (BEC), impersonation attacks, malware, and ransomware. Delivered via a managed SaaS platform, it integrates with **Google Workspace** and **Microsoft**

email environments, analysing messages in transit before they reach users' inboxes.

Adaptive detection that drives Efficacy	Continuously detects and responds to new email threats with tailored detection logic that evolves at the speed of attackers, leveraging community-driven rules and AI/NLP-based analysis.
Full context and control	Provides total visibility into email threat detection, scoring, and verdicts. Policies can be customised to fit your environment, giving organisations control over security decisions.
AI-Powered Attack Score Verdicts	Uses Natural Language Processing (NLP) and Natural Language Understanding (NLU) to assess message semantics, context, and intent, forming a quantitative Attack Score Verdict.
Efficiency through automated mitigation	Reduces false positives and MTTR with automated email triage, backtesting, quarantining, and user report investigation, lowering manual intervention.
Community-driven rules	Leverages threat intelligence shared across a broad network of organisations for faster response to emerging attacks.
Whitebox logic and flexibility	Security rules are fully transparent and configurable, allowing adaptation to specific organisational requirements.
Reporting and analytics	Provides insights into detected threats, mitigation outcomes, and user behaviour to support governance and compliance.

Associated Services

Add-ons

Aside from the features that are part of Zivver's core product (Zivver Secure Email and File Transfer), we offer a number of additional capabilities that can be added on top of these products should an organisation have a need for them. This modularity ensures that organisations only pay for the features that they actually need and use. Zivver always works in tandem with organisations to determine their exact requirements and suggest relevant solutions based on those. Pricing for these add-ons is listed in our pricing document.

Add-on	
Error Prevention Rules	Human errors, such as sending an email to an incorrect recipient or inadvertently sharing sensitive information, are by far the largest cause of data leaks. Zivver offers organisations the possibility to activate business rules as an auxiliary tool to help their employees make the right choices and prevent errors when sending information. The organisation doesn't have to devise these business rules themselves; Zivver has developed best-practice business rules based on years of experience in numerous different sectors. Subsequently, organisations can choose what rules they want to use. There are various types of business rules: • Inform employees about sensitive information in their email and/or attachment. Examples are recognizing medical information, social security numbers, or credit card data; • Help employees in choosing the right security measures. For example, medical information has to be sent with two-factor authentication via an SMS code;

	● Warn employees about irregular recipients. For example, warn the employee that 'financial information was not sent to John.doe@email.com' before, that they are emailing a recipient with an email address similar to another potential and more likely recipient, or warn that the attachment contains an email address with a different domain name than the recipients'; ● Prevent employees from accidentally or deliberately exfiltrating data to their personal email address by recognizing likely personal email addresses; ● Prevent accidentally exposing recipients to each other by suggesting the use of BCC when there are an unusual number of recipients in the To/CC fields.
Encryption Gateway	Using Encryption Gateway, customers can send secure Zivver messages or enforce a minimum level of transport security with a Zivver message as the fallback option. Enforcing transport security on outgoing emails helps organisations comply with data protection regulations and modern security standards. Additionally, Encryption Gateway offers organisations and users the option to deliberately send emails as secure Zivver messages where required. In any case, it is up to the customer and/or user to decide which emails need to be sent via the Zivver Encryption Gateway.
Data Loss Prevention (DLP) Gateway	DLP Gateway allows organisations to route outgoing emails via the Zivver Platform and use Zivver's Error Prevention Rules to determine if a message needs to be sent securely or

	can be delivered directly to the recipient. Users simply use their normal email client, on their normal device, following their normal email workflow. Users also have the option to deliberately send an email securely. If the required recipient verification details are not present and fallback to email verification is not permitted, Zivver can send a notification to the sender asking them to provide the missing verification details using one of Zivver's apps. DLP Gateway can also prevent specific types of information from leaving the organisation. DLP Gateway can be integrated with mail servers and third-party applications, and can be used for manual as well as automated workflows.
Conversation Starter	Zivver's main functionalities are focused on communication that is initiated by your employees. In order to allow others to securely send information to your organisation on their own initiative, Zivver offers the option to create conversation starters. Zivver offers two types of conversation starters: • **Personal conversation starter:** This allows senders to securely send a message to a predefined recipient in your organisation. • **Open conversation starter:** This allows senders to determine to which email address within your organisation they want to send a secure message. Every conversation starter comes with a unique link so it can be included on a customer's website or email signatures.

Proof of Delivery	Proof of Delivery provides users with legally valid proof of delivery reports for every Zivver message they send, as well as proof of receipt reports for every Zivver message they receive. Reports contain timestamps of when messages were sent, received and opened, and also provide authentication information of the sender and recipient. The report can be accessed from within the Outlook Windows Add-in or the Zivver Web App.
Custom Branding	The guest portal is the environment in which users without a Zivver account can read and reply to messages from your organisation. This environment has a Zivver look and feel by default. However, Zivver offers customers custom guest branding, meaning that the guest portal displays the branding of the customer.
Advanced Administrative Toolkit	The Advanced Administrative Toolkit enhances control, efficiency, and security through three key capabilities: • **Organisational Units** Organisational units allow administrators to create subsets of the organisation that users can be assigned to. Each unit can have its own branding and notification settings, enabling tailored configuration where needed. In most deployments, Zivver organisational units are mapped to existing structures within an Active Directory environment. • **Role-Based Access Control** Role-based access control enables granular permission

management for Zivver administrators. For example, security officers can be restricted to viewing reports and security settings, while IT helpdesk staff may be permitted to modify user-level settings only. This division of responsibilities supports operational efficiency without compromising security.

Contact Sync
Contact Sync provides real-time synchronisation of contact information—such as phone numbers and access codes—from any external system via a REST API. This ensures users always have access to the most accurate recipient verification details, maximising security while minimising workflow interruption.

Maintenance

Cloud-hosted components of Zivver receive automatic updates, security patches, and performance improvements at no extra cost. On-premise components (e.g. some gateway installations) require customer administrators to download and install updates, while updates themselves are provided as part of the service.

Professional Services

Implementation, onboarding, configuration, and training are optional services priced separately. These services include guidance for administrators, user onboarding, policy configuration, and awareness training.

Storage and retention

Messages and attachments are retained until the sender revokes them or both sender and recipient have deleted them. Audit logs are retained for six years, in line with international standards. Support data is stored for two years after resolution. Backups are managed via AWS daily snapshots, retained for 30 days to allow point-in-time recovery. Retention periods are standard and not configurable; extended storage or archiving beyond these defaults would require discussion with Zivver.

2. Data Protection

Information Assurance

- Zivver is certified to ISO/IEC 27001:2022 and ISO/IEC 27017:2015 with all company activities included in the scope and in the statement of applicability (thus far exceeding only having certification for the data storage)
- Zivver services are hosted in our AWS Virtual Private Cloud across multiple ISO 27001 and SOC II certified data centres within the European Economic Area.
- Zivver is Cyber Essentials Plus certified
- Zivver has a CSA STAR Level 1 certification
- Zivver General Counsel is CIPP/E certified
- Zivver is SOC 2 compliant and can share a SOC 2 Type 2 report upon request.
- A security review and pentest is performed every 6 months by an external CHECK approved provider.
- Zivver holds a 'Privacy Verified' certification
- Zivver complies to the GDPR and annually engages legal experts to perform a privacy and compliance audit, checking Zivver for privacy by default, privacy by design, data minimization and other GDPR principles
- Zivver's standard terms provide full coverage of all terms that need to be documented between data processors and data controllers under GDPR
- Specific to healthcare:
    - Zivver complies to the DCB0129 standard and our Clinical Risk Management Plan, Hazard Log and Clinical Safety Case Report can be provided on request
    - Zivver provides assurances of practising good data security by complying to the NHS DSP Toolkit by exceeding standards. Review our record on the NHS DSP Toolkit website
    - Zivver is certified to NEN7510:2024, the Dutch norm for information security for healthcare, a more specific and stringent version of ISO27001.

Data Back-Up and Restoration

Zivver uses the reliable AWS backup services for all its backups. Zivver has a point in time recovery for 30 days, which means we can recover our data to any point in time in the last 30 days. Additionally, daily snapshots are made which are stored in our primary locations and copies of these snapshots are also made and are stored in alternative locations. The retention period of these snapshots is also 30 days. This mitigates the risk of unintended data loss and allows us to comply with an organisation's stringent recovery time and recovery point objectives. All data in backups are encrypted.

The backup strategy and the recovery procedures are reviewed annually by the security team. Additionally, Zivver annually tests the recovery procedures. The outcome is discussed with the management team.

The customers of Zivver all benefit from the above backup schema. There are no customizations possible. Yet, it is possible to periodically download customer data (Zivver messages) from Zivver via an explicit TLS SFTP connection to implement a separate backup solution. Optionally, admins can enable features to also save unencrypted copies of sent/received Zivver messages to Outlook for archiving and indexing purposes.

Business continuity statement/plan

At Zivver we work continuously to guarantee the availability of user data. A business continuity plan is in place to guarantee its services remain operational in case of a disaster. All our user data is securely stored in our Virtual Private Cloud, which is spread across multiple ISO27001 and SOC II certified data centres. The main application is hosted using AWS ECS to provide a highly available and scalable architecture.

The key business area of this continuity plan is the Zivver web application. The critical functions include application servers, database servers, SMTP servers, and other backend components, all of which work together to ensure seamless operation. Application servers handle user requests and rely on database servers for data storage and retrieval. SMTP servers manage email delivery that depends on application and backend services. Other backend components provide supporting services such as authentication, logging, and integrations with external systems, forming an interconnected infrastructure that underpins the web application.

All critical functions are set up redundantly in three availability zones to ensure high levels of resilience, meaning if, in the unlikely event, one availability zone becomes unavailable, we can instantly switch to the other zone and ensure continuity. All data is stored in the master database and a replica. These master and replica databases are also located in multiple different AWS availability zones. In case of an outage failover will happen automatically and the service remains available as normal, meeting our SLA of 99.8% uptime.

In addition to the fully redundant setup, Zivver has a crisis management plan to oversee the roles and responsibilities, communications and general logistics of a crisis. The business continuity plan and the crisis plan are tested at least annually. The outcome is discussed with the management team.

A more detailed plan can be provided to the buyer on request.

Privacy by Design

The General Counsel (CIPP/E certified) is accountable for Zivver's adherence to the GDPR. The General Counsel with the Information Security Officer and external legal advisory firm, specialised in privacy law are constantly making sure Zivver complies to the GDPR and adheres to the privacy by design principle.

For the Zivver product and services this means they are developed with the privacy by design principle in mind from the beginning. To facilitate this the product team uses privacy and security checklists for user stories and actively involves the Information Security Officer with new product/service initiatives. If required a Data Protection Impact Assessment is done to identify and assess the privacy risks. Based on this assessment protective measures will be implemented.

A key principle that Zivver always adheres to during product development is that neither Zivver nor its sub-processors should be able to access the content of the message sent via the Zivver product. Therefore, messages at rest are encrypted with best practice encryption and can only be decrypted by a sender or recipient of this message.

By using a public-key cryptosystem in combination with other technologies, Zivver works according to the "Zero Knowledge" principle. All keys are stored encrypted in our database and when data is retrieved it's done completely "in-memory" so that passwords, keys, attachments and contents of Zivver messages are never stored or available "at rest".

By storing data at rest in this way, it means all sensitive information shared via the Zivver service is fully encrypted without Zivver having access to the decryption keys. This strict Zero-Knowledge security by design approach ensures that only sender and recipients can access the contents of Zivver messages and not third parties. It is demonstrably not possible for Zivver to view the content of messages or access them because Zivver does not store a key or derivative in order to be able to decrypt messages.

When Zivver contracts a new vendor a privacy check is part of the review process to determine if the vendor complies to Zivver high privacy demands and the GDPR.

Additionally, Zivver contracted legal expert firm ICTRecht to be their external data protection officer (DPO). ICTRecht stands in very high regard on the topic of GDPR compliance. They are extremely well positioned to monitor and challenge Zivver's actions, handle data privacy related complaints of customers (if any), as well as provide overall advice for further improvement of Zivver's ISMS and data protection measures.

Annually Zivver engages legal experts to perform a privacy and compliance audit, checking Zivver for privacy by default, privacy by design, data minimization and other GDPR principles. Zivver holds a 'privacy verified' quality mark.

3. Using the service

Ordering and Invoicing

Order Processing

In the first instance please direct all inquiries and requests to publicsector@zivver.com at which point a team member at Zivver will respond within 24 Hrs on next steps, be this answering an enquiry for more information or to processing an order.

Please add following information to the email:

- The organisation name.
- Contact name with email address and telephone number.
- The nature of the enquiry e.g. require further information/placement of order.

Invoicing

- For the Services and all other activities in connection with the Agreement, the Client will pay Zivver what is stated in the Call off contract. All amounts are quoted in GBP, and exclude VAT. Zivver will absorb the 0.75% CCS framework levy in its pricing.

- The annual core product and add-on costs of the service will be invoiced upon the commencement of the Agreement and subsequently on an annual basis. Unless otherwise agreed upon, the variable SMS and data credits costs will be invoiced on a quarterly basis in arrears based on subsequent costing. Implementation of the Services will be invoiced upon completion of the implementation. Additional eSignature bundles will be invoiced in the month after they have been purchased. The invoices will have a payment term of 30 days, for which the Client accepts possible electronic invoicing.

- If payment is not made in time, the Client is obliged to pay, in addition to the amount owed and the interest due under the Late Payments of Commercial (Debts) Interest Act, all the judicial and extrajudicial collection costs, including the costs of lawyers, bailiffs and debt collection agencies.

In the event that the Client is declared bankrupt, applies for or is granted suspension of payments, the Client's activities are ceased or its business is wound up, all amounts owed to Zivver are immediately due and payable.

Availability of Trial Service

Zivver offers opportunities for potential customers to evaluate the platform prior to subscription.

Free guest accounts are available for Zivver Outbound Secure Email, enabling users to send and receive encrypted emails and large files directly through the Zivver

Web App. Organisations can easily explore these capabilities by creating a free trial account at: https://app.zivver.com/signup

In addition, a free Proof of Value (PoV) is available for Zivver Email Threat Protection, allowing organisations to evaluate detection effectiveness, remediation capabilities, and policy behaviour within their own environment before committing to full deployment.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

To support customers with the installation, configuration, policy creation and user onboarding, Zivver provides professional services implementation support, which are purchased at an hourly rate and we collaborate closely with each customer to assess the number of implementation hours required. Please refer to the Pricing Document for these rates. Supporting implementation is one of the USPs of Zivver that clients value most. Zivver has various playbooks to help organisations effectively implement Zivver, which includes various ways to onboard users depending on the needs and wishes of the organisation concerned.
Our implementation and overall customer support is valued greatly by our customers, shown by our NPS score of >40, our contract renewal rate of >95% and our positive reviews on Gartner.

On-Boarding

Continuous Support

Zivver offers continuous support to ensure organizations can effectively utilize the platform:

- **Knowledge Base**: A comprehensive resource center offers FAQs, video tutorials, and step-by-step guides to assist users in navigating the platform.
- **Dedicated Support Portal**: Users can submit tickets and receive personalized assistance from technical experts, ensuring timely resolution of issues.
- **Automated Email Security Administration**: The platform automates user account management throughout the employee lifecycle, from onboarding to offboarding, ensuring consistent application of security policies and compliance with regulations such as GDPR and HIPAA.

Off-boarding

Zivver provides a structured process for organisations wishing to discontinue use of the platform. The Exit Strategy Manual guides administrators through securely exporting all organisation data, revoking access, removing integrations such as

Single Sign-On and SMTP connections, and decommissioning backend services. Administrators may extract email encryption and file transfer data when required by downloading unencrypted copies of Zivver messages as .eml files. Additionally, an optional feature allows administrators to enable users to save unencrypted copies of sent, received, or opened Zivver messages to Outlook for archiving and indexing purposes.

Customers can export all data themselves—unencrypted—via an explicit TLS SFTP connection for up to 60 days after the contract ends, allowing organisations to use their preferred SFTP tool to download messages and files at intervals that suit them. No further data will be shared with the Zivver platform once offboarding is initiated, and all policies and notifications presented in the front-end will be cancelled.

Throughout the contract, each customer is supported by a dedicated Customer Success Manager (CSM) who conducts regular check-ins. As the contract approaches its end date, the CSM will discuss renewal options. If a customer chooses not to renew, Zivver will, upon request, either securely destroy or supply all remaining information held within the Zivver service. The exit process ensures that encryption keys and associated data are permanently removed, while audit logs and system metadata are retained in accordance with regulatory requirements, ensuring both data protection and operational continuity.

Service Migration

Zivver supports service migration by assisting customers in transitioning from their existing secure email or email security solutions to the Zivver platform. Migration activities depend on the services selected—Zivver Outbound Secure Email and Email Threat Protection as core offerings, with Secure eSignatures available as an optional add-on to Outbound. Secure eSignatures is a paid add-on, and pricing details are provided in the G-Cloud 15 Pricing Document. Migration may include configuring mail flow, enabling required integrations, preparing user groups, and aligning existing security and compliance controls with Zivver's policies. Where applicable, customers may export or retain configuration data from previous systems before switching. Zivver aims to ensure that migration is completed with minimal disruption to users and without impact on standard email functionality.

Scope

The Zivver platform provides secure digital communication services consisting of Zivver Outbound Secure Email, the optional Secure eSignatures add-on, and Zivver Email Threat Protection. The scope includes provisioning and configuration of the selected components in the customer's cloud email environment (such as Microsoft 365 or Google Workspace), as well as optional relay-based integration with third-party systems or email servers using Zivver's Encryption Gateway and DLP Gateway. This allows outbound messages from applications or mail servers to be routed through Zivver for encryption, policy enforcement, and secure delivery. The

service covers outbound email security, secure message delivery and file sharing, optional electronic signing workflows, and inbound email threat detection and remediation. The service does not extend to management of the customer's underlying email infrastructure, networks, endpoint devices, or third-party systems beyond supported relay and application integrations, nor does it include bespoke development or customisation outside standard platform capabilities.

Training

Zivver provides comprehensive training resources to ensure effective use of the platform:

- **eLearning Platform**: The platform offers structured learning modules, interactive content, and assessments to support users in developing proficiency in secure messaging and adhering to best practices.

- **QuickStart Guide**: A comprehensive guide assists administrators in configuring and setting up the platform, ensuring a smooth deployment process.

- **Demo Videos and Webinars**: Supplementary resources offer practical guidance for daily operations, helping users maximize the platform's capabilities.

Implementation Plan

Zivver's implementation process is based on our best practices with clients and provides tailored advice during the process. We have developed a playbook for this process which will be the blueprint of implementing the service. A detailed/customised implementation plan can be provided to the buyer on request. The engagement is conducted remotely, but the kick-off and (user) training activities can take place onsite if required. Our onsite and remote professional services consume the implementation hours without any differentiation in charges, providing flexibility and straightforwardness in our support structure.

Implementation Plan - Zivver Outbound Secure Email and Zivver Secure eSignatures

This section describes the onboarding and implementation approach for Zivver Outbound Secure Email and Zivver Secure eSignatures, delivered as part of the Zivver Secure Email Platform.

The steps of our implementation process are described below. Estimates have been provided to give organisations a general idea of how long an implementation process could take. Please note that each implementation process depends on the specific situation and complexities of an individual organisation and therefore

timelines may differ from the estimations provided below. During the intake meeting, specific timelines will be set together with the customer.

1. **Discovery Phase** - estimated duration: 4 - 8 hours

   During the discovery phase the project governance structure, scope and planning are defined. The project starts with an intake and your dedicated project manager will discuss the high-level implementation approach.

   Next, a kick-off will be planned and all relevant stakeholders will be invited to participate. During the kick-off, the detailed planning, scope, objectives, milestones and overall management of the project will be discussed. In addition, there will be room for a demonstration of the solution, to ensure all stakeholders are aligned with the to be implemented product.

2. **Design Phase**- estimated duration: 4 - 8 hours

   During the design phase the use-cases, functional requirements and technical requirements are being discussed. A design session will be organised with the relevant stakeholders and the output from the design phase will be used as input for the build phase.

3. **Build Phase**- estimated duration: 1 - 2 days

   The Zivver solution will be configured aligned to your technical requirements, including account provisioning and Single Sign-On (SSO) (if applicable). After successful configuration, your team will have the capability to conduct end-to-end tests, validating if secure messages can be sent and received.

   In addition, your administrators and champion users will be equipped with the necessary knowledge and skills to effectively support other users in your organisation.

4. **Validation Phase** - estimated duration: 4 - 8 hours

   During the validation phase the configured solution will be tested via User Acceptance Scripts that are based on the use-cases and requirements. In addition, your users will be onboarded to ensure they have access to the Zivver platform and can adequately test the new solution.

   Furthermore, our team will support the creation of guidance & onboarding materials such as communication templates, onboarding videos, FAQ scripts and Go-live documentation.

5. **Deployment Phase** - estimated duration: 2+ days

   Our team will provide support to ensure that all employees are successfully on boarded with Zivver accounts, ready to start sending/receiving secure messages. We will also support the successful launch of Zivver in the organisation and, if required, provider hypercare support during the initial days following the go-live, ensuring a smooth transition.

6. **Active Phase** - estimated duration: 1 - 2 hours

   Together with your Zivver project manager the project is evaluated and handed over to the operations. From this point on your point of contact within Zivver will be your dedicated Customer Success Manager.

A detailed implementation plan can be provided to the buyer on request.

Implementation Plan – Zivver Email Threat Protection (ETP)

This section describes the onboarding and implementation approach for Zivver Email Threat Protection (ETP), delivered as part of the Zivver Secure Email Platform.

Objectives and Scope

The implementation ensures the secure, reliable, and compliant activation of Zivver Email Threat Protection within the customer's Microsoft 365 or Google Workspace environment.

Scope includes:

- Tenant integration of ETP;
- Configuration of detection rules, automations, and threat-response workflows;
- Activation of Single Sign-On (SSO) and SCIM where applicable;
- Optional configuration of user-reported message workflows via an Abuse Mailbox and Autonomous Security Analyst (ASA);
- Operational handover and training of administrative staff.

The implementation covers inbound email threat detection and integrates seamlessly with other Zivver services (Outbound and eSignatures) where applicable.

Implementation Phases

Phase 1 – Discovery and design: Initial assessment - estimated duration: 1 - 2 hours

Activities

- Conduct a kickoff session to confirm scope, objectives, timelines, and roles;
- Identify any required global exclusions, gather administrator details (email addresses and roles), and ensure a global administrator is available. Determine required roles, retention periods, authentication settings, and message-access needs. Confirm how many mailboxes must be activated and the total number of mailboxes.

- Validate that technical prerequisites defined in the Zivver ETP SLA are met (e.g., Microsoft 365 or Google Workspace source, compatible browsers, SSO/SCIM readiness).

Phase 2 – Build: Tenant connection and base setup - estimated duration: 1 - 2 hours

Activities

- Provision the customer tenant within the Zivver Email Threat Protection cloud environment;
- Set up detection rules and integrations;

Phase 3 – Build: Security configuration and automations - estimated duration: 2 - 4 hours

Activities

Enable recommended automations to reduce administrative workload and improve threat response. Typical defaults include:

- Provide access to the ETP administrative console for designated customer administrators;
- Enable Autonomous Detection Engineer — the AI-powered detection module that automatically analyzes evolving threats, generates and validates detection rules, and adapts protection to your environment;
- Enable Autonomous Security Analyst (ASA) to automate analysis and triage of user-reported messages, provide explainable feedback, and reduce false-positive workload;
- Enable Email Bomb Protection;
- Automatic quarantine of messages flagged with a malicious score;
- Automatic routing of spam to junk/spam;
- Optional workflows for user-reported messages:
    - Quarantine based on user reports;
    - Herd immunity (auto-action when ≥5 users report the same message);
    - Automatic acknowledgement and classification feedback to reporting users.

<u>Single Sign-On (SSO)</u>

- Configure SAML-based SSO for administrator and analyst access;
- Best practice: enforce SSO as the only authentication method once validated.

<u>Abuse Mailbox and ASA</u>

- Set up an Abuse Mailbox (user mailbox, shared mailbox, or distribution list) for employee reporting of suspicious messages;

- Enable Autonomous Security Analyst (ASA) to automate analysis and triage of user-reported messages, provide explainable feedback, and reduce false-positive workload.

Notification and Alerting

- Configure administrator notifications using Microsoft 365 High Volume Email (HVE), where available;
- Define recipients and thresholds for alerting.

(Immutable) Audit Logging

- Optional: Enable mailbox auditing to track ETP/Sublime actions within Microsoft 365;
- Optional: configure export of Message Events or Audit Logs to AWS S3 or a SIEM.

Phase 4 – Validate: Testing and acceptance - estimated duration: 2 - 4 hours

Activities

- Conduct a testing period;
- Validate:
    - Threat detection effectiveness
    - False positives and false negatives
    - Behaviour of Automations, ASA workflows, and quarantine actions
    - Logging, auditing, and alerting accuracy

- Confirm that incident and escalation procedures align with the SLA (P0–P3 categories and response targets);
- Apply tuning of rules, exceptions, and policies.

Phase 5 – Deployment: Rollout to production

Activities

- Brief internal service desk teams and communicate guidance to end-users on reporting behaviour and ETP indicators;
- Perform enhanced monitoring during the initial production weeks.

Phase 6 – Active: Handover and continuous improvement

Activities

- Formal handover to the customer's IT/security operations teams;
  Schedule periodic operational and security reviews (e.g., monthly or quarterly) to assess:

    - Detection trends;

- Automation and ASA performance;
- Updates and enhancements delivered by Zivver and the Threat Intelligence Expert desk at Zivver.

Service Management

Business hours

Zivver business hours: Monday to Friday.

● United Kingdom 07:30 – 16:30 GMT

This is excluding public holidays in the Netherlands as support staff are not scheduled, however we exclusively monitor for P0 issues adhering to the SLA response time. Zivver commits to provide support in English. Any other languages will be provided on a best effort basis.

Service Constraints

Zivver operates its service within a defined set of constraints relating to availability, maintenance, functional modifications, configuration and support. The Zivver platform is designed for high availability, and the availability commitments applicable to the service are detailed separately under Service Levels in this document.

Zivver is entitled to take its systems, or parts thereof, temporarily out of service for maintenance, modification, or improvement purposes. Zivver endeavours to perform such activities outside office hours where possible. In cases where customer impact is expected, Zivver notifies customers in advance through established communication channels, including the admin newsletter and email notifications. Zivver is not liable for compensation for any damage or loss resulting from systems being taken out of service for maintenance.

Zivver may also introduce modifications to its systems from time to time to improve functionality or resolve errors. Where a modification results in a significant change to functionality, Zivver will promptly inform the customer. Modifications applicable to multiple customers cannot be excluded for individual customers. Zivver is not liable for any damage or loss resulting from such changes. If a modification has substantial adverse consequences for the customer, the customer may terminate the Call-Off Contract with 30 days' written notice in accordance with the G-Cloud 15 Call-Off Contract terms.

Customisation of the Zivver platform is intentionally limited. Customers may configure settings within the administrative interfaces; however, core functionality cannot be altered, and custom code or extensions cannot be introduced. This ensures platform security, stability, and maintainability.

Support is available during Zivver's published support hours. Requests submitted outside these hours, or via channels intended for end users, may not fall under the service commitments described in the Service Levels.

Service Levels

Service Category	Description	Service Level	Availability
Downtime	Availability of the Zivver service (back-end), measured as (365*24) minus (total duration of downtime per year), excluding scheduled maintenance which was previously communicated to the customer.	Uptime[1] 99.8%	24/7

Service Category	Description	Response Time[2]	Availability
P0 Incident	Incidents whereby the Zivver service is completely unavailable, affects all users and there are no workarounds possible. Both a response to a support ticket, and a notification sent via zivver.info count as a response in this case.	15 minutes	24/7
P1 Incident	Incidents whereby major functionality is impacted, or significant performance degradation is experienced. The issue is persistent and affects many users. No workaround is available. Notification of downtime on Zivver.info counts as a response in this case.	30 minutes	Zivver Business Hours
P2 Incident	Incidents whereby parts of the Zivver SaaS	4 hours	Zivver Business

	platform are not responsive, and working is difficult but still possible.		hours
P3 Incident	Questions or incidents whereby users experience a slight inconvenience but can continue working with Zivver secure email.	Best effort, Target: 8 Hours	Zivver Business hours

[1] Uptime is continuously monitored at https://www.Zivver.info. Historical uptime performance (last 12 months) can be found on: https://docs.zivver.com/sla

[2] Response time refers to the time span between receiving an incoming support request and the first contact made with the customer by the Zivver Support team or a notification on zivver.info.

Requesting Support

Enterprise customers should send the email to support@zivver.com clearly describing the issue at hand. P0 and P1 tickets can be submitted by the admin via support@zivver.com stating in the subject of the mail that it concerns a P0/P1 incident and contain all the following details:

- The desired scenario;
- The actual scenario;
- The frequency of occurrence;
- The number of users experiencing the issue;
- The impact of the issue on Zivver users.

Customers are requested to call as soon as possible within business hours after registering such incidents, to ensure the incident has been logged correctly & completely and to answer additional questions which may be required to resolve the incident as soon as possible.

Support requests logged via support@zivver.com are treated as end-user tickets and shall not be subject to the commitments stipulated in this service level agreement.

Escalation Route
Enterprise end-users are requested to report all incidents to the customer's internal helpdesk, which in turn can report these incidents to Zivver as described in the section 'Requesting Support' above. In the event of disagreement, Zivver support is obliged to involve the relevant Head of Customer Success. Subsequently, an executive director of Zivver will be involved in case of ongoing disagreement or by explicit request of the customer.

Service Level Constraints

In the following situations the service levels mentioned will not be applicable:

- In case the overall contract has not commenced, is invalid or is expired.
- In case the incident has not been logged through the correct channel.
- In case the customer did not comply in a timely manner with our release cycle requirements
- In case the customer did or does not comply with the Minimal Technical Requirements attached to the overall contract between the parties.
- In case of incidents due to force majeure.
- In case of a problem or malfunction as a result of actions by the customer or any of its end-users.
- If the customer is not available when Zivver reasonably requests assistance in determining or isolating the problem or the malfunction and in testing the solution.
- If licences for third party software, which are intended as a basis for the use of Zivver (such as Microsoft Outlook / Office 365) are not functioning properly, or are end-of-life according to Microsoft official lifecycle, or not available or not in a proper working condition.
- If the customer/end-user does not have an internet connection that is adequate (in terms of bandwidth and latency) and stable enough for the Zivver products to work properly.
- If third party platforms and/or applications are used by the Customer/end user and interact with the Zivver products, resulting in issues with the performance and/or functionality of Zivver products.
- In case of any malfunction due to incorrect or missing information provided by the customer to Zivver during the implementation process.

- In case the customer is not able to provide a test account that is representative for an account on the production environment of the customer in order to analyse and fix any issues; to the extent that Zivver cannot reproduce the issue on its own test environment

Irrespective of the applicability of any limitations described above, Zivver will always provide help on a best effort basis. However, in such an event the service levels and compensation included in the service level agreement will not be applicable.

Outage and Maintenance Management

Zivver is entitled to take its systems, or parts thereof, temporarily out of service for maintenance, modification, or improvement purposes. Zivver will endeavour to do so outside office hours as far as possible. Zivver will notify the customer accordingly in the admin newsletter as well as an initial notice email followed by a reminder email closer to the time. Zivver is never liable for compensation for damage or losses in connection with taking systems out of service for maintenance purposes.

Zivver is entitled to modify its systems, or parts thereof, from time to time in order to improve the functionality and to resolve errors. If a modification leads to a considerable change in the functionality, Zivver will promptly notify the Client. In the event of modifications that are relevant to multiple clients, it is not possible to leave out a specific modification only for the Client's benefit. Zivver is not liable to compensate for any damage or losses caused by such a modification. Should the aforesaid change in Zivver's functionality have substantial adverse consequences for the customer in its discretion, the Client is entitled to terminate the Call-Off Contract at any time by giving 30 days written notice as per the G-Cloud 15 Call-Off-Contract terms.

Type	Frequency	Support by Zivver	Customer Responsibility
Major release	When required	Zivver supports: • The most recent version of a major release. • The previous major release up to 12 months after the release of the most recent version.	The customer must have a version supported by Zivver in use.

Minor & Patch release	Scheduled & Ad-hoc	Zivver releases frequent minor releases with bug fixes and/or new functionality	The customer is advised to deploy the most recent minor version to ensure stable performance and have the latest functionality available.
Alpha & Beta release	Unlimited	For customers it is possible to have an Alpha & Beta-release of the plugin. Release of Alpha & Beta versions take place several times a year.	Participation in an Alpha & Beta release is always voluntary and is discussed with either your Customer Success Manager or Tech Support.

Financial Recompense Model for not Meeting Service Levels

Service	Description	Zivver Service Credit
Uptime	Uptime was >99,0%, but <99,8%	Customers receive a free 1- month extension of their Zivver contract
Uptime	Uptime was <99,0%	Customers receive a free 2- month extension of their Zivver contract
P0 Response Time	Response time was >30 minutes	Customers receive a free 1- month extension of their Zivver contract

To be eligible for a Zivver Service Credit as indicated above, the credit request must be received by Zivver on the e-mail address support@zivver.com, within three months after the occurrence of the alleged incident and must include:

- the words “Zivver Service Credit Request” in the subject line;
- the dates and times of the unavailability and/or P0/P1 incident that are relevant for the request;
- any other information that you may believe is of relevance, including Zivver ticket numbers (if any).

4. Provision of the service

Customer Responsibilities

The customer is responsible for ensuring that all minimal technical requirements are met, including supported operating systems, browsers, network connectivity, and client software, to guarantee compatibility and optimal performance. Customers must manage user roles, permissions, and access in accordance with organisational policies, and provide an identity provider that supports SAML 2.0 for SSO and SCIM for automated user provisioning where applicable. The customer is also responsible for applying any required configurations after updates or as instructed by Zivver, and for cooperating with Zivver during testing, validation, or troubleshooting activities. Failure to meet these responsibilities may affect the applicability of certain SLA guarantees, including uptime and incident response.

Technical Requirements and Client-Side Requirements

Each component of the Zivver platform has a number of technical requirements that the customer's infrastructure has to meet in order for (that component of) the platform to be able to function properly. This section describes the minimal technical requirements per component. Zivver cannot guarantee that the platform functions properly if requirements are not met.

In order to be able to provide the Services, the minimal product requirements set out below should be met at all times. Furthermore, Zivver reserves the right to further update and expand the 'Minimal Technical Requirements' according to market wide technological developments and new innovations.

Zivver follows the official support lifecycle schedule of Microsoft for its product portfolio. This update will be shared through admin newsletters or on our documentation portal.

Zivver for Outlook Windows

Product name	Zivver for Outlook Windows/Zivver Office plugin
Targeted platform	Microsoft Windows
	Minimal Requirements
System Requirements	a. Microsoft Windows 10 or higher b. Microsoft .NET Framework 4.8 or higher. c. Microsoft Outlook 2016 or higher d. Microsoft Edge WebView2.
Product Specific Requirements	a. HTTPS connection, port 443, TLS v1.2 or higher with https://*.zivver.com.

	b. Outlook in Cached Mode2 or Online Mode c. A Microsoft supported scenario when using different versions of Off

Zivver for Outlook Online and The New Outlook

Product name	Zivver for Outlook Online / Zivver for Outlook Web Access add-in
Targeted platform	Microsoft Outlook Web App (OWA) / Outlook on the web in a desktop browser / The New Outlook
	Minimal Requirements

System Requirements	a. Microsoft Exchange Online.
	b. In case used in OWA, one of the following modern browsers based on the latest General Available (GA)/Stable version of that browser:
	  a. Apple Safari (for iOS).
	  b. Google Chrome / Chromium (for Android/iOS).
	  c. Microsoft Edge based on Chromium.
	  d. Mozilla Firefox

Product Specific Requirements	a. The domain of the Zivver OWA add-in and that of the Zivver Webapp is included in the list of trusted sites in Internet Explorer. b. Only relevant for OWA: the browser settings allow third-party cookies and popups for specific domains. c. A centralised installation of the Zivver OWA add in requires an Azure/Exchange admin account with Global Admin.

Zivver WebApp

Product name	Zivver Webapp
Targeted platform	Desktop or mobile browser on any device.
	Minimal Requirements

System Requirements	1. One of the following modern browsers based on the latest General Available (GA)/Stable version of that browser: i. Apple Safari (for iOS). ii. Google Chrome / Chromium (for Android/iOS). iii. Microsoft Edge based on Chromium. iv. Mozilla Firefox.
Product Specific Requirements	n/a.

Zivver Mobile App

Product name	Zivver Mobile App
Targeted platform	Android / Apple iOS
Purpose	Securely send and receive messages directly from your Android or Apple mobile phone/tablet.
How to install	Google Play Store / Apple App Store
Current major version	n/a
	Minimal Requirements
System Requirements	a. The two most recent versions of: o Android o Apple iOS
Product Specific Requirements	a. HTTPS connection, port 443, TLS v1.2 or higher with https://*.zivver.com.

Zivver for Gmail

Product name	Zivver for Gmail/Zivver Chrome Extension
Targeted platform	Google Chrome OS laptop (Chromebook), desktop or laptop.

	Minimal Requirements
System Requirements	a. The stable version of Google Chrome.
Product Specific Requirements	a. One of the following Google Workspace licenses: Business Standard, Business Plus or Enterprise license. b. G Suite User Accounts are placed in one or multiple organisational Units. c. The primary email address of a User is the same as the user logon address. d. A Service Account can be created for the Chrome Extension.

Zivver SyncTool

Product name	Zivver SyncTool
Targeted platform	Microsoft Windows (Server)
	Minimal Requirements
System Requirements	a. Microsoft Windows 10 or higher. b. Microsoft .NET 4.8 or higher. c. Optional: Microsoft Windows Server 2012 (R2) with Extended Security Updates (ESU) or higher.
Product Specific Requirements	a. HTTPS connection, port 443, TLS v1.2 or higher with https://*.zivver.com. b. Modern Authentication (Certificate-Based Authentication) is used to connect to Exchange Online via Powershell. c. HTTP connection, port 80, can only be used for Exchange Online syncs. d. LDAP(S) connection, port 389 or 636 with Microsoft Active Directory.

	e. The synchronisation profiles are run manually or automatically when needed.

Single Sign-On Integrations

Product name	Zivver Single Sign-On Integrations
Targeted platform	n/a
	Minimal Requirements
System Requirements	a. The IdP uses Security Assertion Markup Language (SAML) v2.0.
Product Specific Requirements	a. The IdP's SAML 2.0 metadata XML file can be exported in plain text. b. The IdP sends a custom SAML attribute in the SAML assertion. Its value is based on an existing LDAP attribute. c. The user is identified by its email address in the communication between the IdP and the Service Provider (SP). d. The IdP authenticates the user and Zivver or the IdP will challenge the user for two-factor authentication (2FA).

Send on Behalf of your Domain

Product name	Send on behalf of your domain
Targeted platform	DNS Server
	Minimal Requirements
	These minimum requirements apply to every (custom) domain you want to allow Zivver to send on behalf of.

System Requirements	a. The ability to configure a CNAME record for zivverbounce. pointing to returnpath.zivver.com in your domain DNS settings b. The ability to configure a DKIM record (zivver._domainkey) in your domain DNS settings. c. Optional: the ability to configure a SPF record (include:_spf.zivver.com) in your domain DNS settings.
Product Specific Requirements	a. Zivver supports DMARC strict DKIM alignment. b. Zivver does not support DMARC strict SPF alignment, only DMARC relaxed SPF alignment is supported. c. Secure messages sent by Zivver on behalf of your domain will pass DMARC as long as the Zivver DKIM record is correctly configured.

Inbound Direct Delivery (IDD)

Product name	Zivver Inbound Direct Delivery (IDD)
Targeted platform	Email clients, mail servers or third-party applications that need to receive secure messages unencrypted.
	Minimal Requirements
System Requirements	The domain to which unencrypted Zivver messages are delivered: a. Has a valid certificate issued by a Certificate Authority. b. Supports TLS v1.2 or higher
Product Specific Requirements	a. IDD is enabled for all Zivver messages that are received on that domain. It is not possible to enable IDD only for a single Zivver account.

Zivver Plugin Assisted Mail Submission (PAMS)

Product name	Zivver Plugin Assisted Mail Submission (PAMS)
Targeted platform	Microsoft Exchange or a Secure Email Gateway (SEG).
	Minimal Requirements
System Requirements	a. Mail server / Secure Email Gateway (SEG) can submit emails to the following smart host: o Smart host: smtp.zivver.com. o Port: 25 or 587. o TLS: Yes, v1.2 or higher with STARTTLS. o Authentication with the Zivver SMTP Server is done by either: ▪ Messages submitted to the Zivver SMTP Server are from a claimed domain and pass SPF. ▪ By using a username and password generated in the Zivver admin portal. ○ Filter outbound messages on a custom mail header. ○ Zivver Office Plugin v6 (Zivver Outlook for Windows addin) or higher is installed in Microsoft Outlook.
Product Specific Requirements	a. There's an active Zivver account for the sending email address. b. The secure message is sent via the Zivver Office Plugin. c. Plugin Assisted Mail Submission (PAMS) functionality is enabled in the Zivver Office Plugin.

Zivver Encryption Gateway

Product name	Zivver Encryption Gateway (previously known as Mail Submission and Secure Relay).
Targeted platform	Third-party or in-house applications, Mail Servers and/or Mail Transfer Agents (MTAs), and Secure Email Gateways (SEGs).
	Minimal Requirements
System Requirements	a. The third-party application can create the following SMTP connection: o Outgoing server: smtp.zivver.com. o Port: 25 or 587. o TLS: Yes, v1.2 or higher with STARTTLS. o Authentication with the Zivver SMTP Server is done by either: ▪ Messages submitted to the Zivver SMTP Server are from a claimed domain and pass SPF. ▪ By using a username and password generated in the Zivver admin portal.
Product Specific Requirements	a. There's an active Zivver account for the sending ('From') email address. b. The Zivver account that's used to send the message from, is a member of the organisation for which the SMTP credentials are generated and/or of the organisation which claimed the account's domain. c. The domain from which emails are sent is claimed within Zivver. d. The maximum message size limit for Mail Submission is 400 MB. This means that the combined size of the submitted message plus any attachments should not exceed this limit. e. The maximum number of recipients is 50.

	f. If there are more than 25 recipients in the To and/or CC, they will be automatically added to the BCC.

Zivver DLP Gateway

Product name	Zivver DLP Gateway (previously known as Zivver Smart Relay)
Targeted platform	Mail Server / Mail Transfer Agent (MTA)
	Minimal Requirements

System Requirements	• SPF is implemented for the organisation's domain name(s) for outgoing emails.
	• The Mail Server / MTA can relay emails to the following smart host:
	  ○ Smart host:smtp.zivver.com.
	  ○ Port: 25 or 587.
	  ○ TLS: Yes, v1.2 or higher with STARTTLS.
	  ○ Authentication with the Zivver SMTP Server is done by either:
	  ■ Messages submitted to the Zivver SMTP Server are from a claimed domain and pass SPF.
	  ■ By using a username and password generated in the Zivver admin portal.

Product Specific Requirements	a. There's an active Zivver account for the sending ('From') email address. b. The Zivver account that's used to send the message from, is a member of the organisation for which the SMTP credentials are generated and/or of the organisation which claimed the account's domain. c. The domain from which emails are sent is claimed within Zivver. d. The maximum message size limit for Mail Submission is 400 MB. This means that the

	combined size of the submitted message plus any attachments should not exceed this limit. e. The maximum number of recipients is 50. f. If there are more than 25 recipients in the To and/or CC, they will be automatically added to the BCC.

Zivver Secure eSignatures

Product name	Zivver Secure eSignatures
Targeted platform	Microsoft Windows
	Minimal Requirements
System Requirements	See the Zivver for Outlook Windows requirements.
Product Specific Requirements	a. Zivver Office Plugin v6.2.0 or higher. b. Microsoft Edge WebView2. c. Supported file formats: .docx and .pdf. d. One of the following modern browsers based on the latest General Available (GA)/Stable version of that browser: ○ Apple Safari (for iOS). ○ Google Chrome / Chromium (for Android/iOS). ○ Microsoft Edge based on Chromium. d. Mozilla Firefox. e. Accounts that are added to Microsoft Outlook via MAPI are not yet supported.

Zivver Email Threat Protection

Product name	Zivver Email Threat Protection
Targeted platform	Desktop or mobile browser on any device.
	Minimal Requirements

System Requirements	2. One of the following modern browsers based on the latest General Available (GA)/Stable version of that browser: i. Apple Safari (for iOS). ii. Google Chrome / Chromium (for Android/iOS). iii. Microsoft Edge based on Chromium. iv. Mozilla Firefox.
Product Specific Requirements	n/a.

Development life cycle of the solution

Zivver uses an agile software development methodology to allow for flexibility to meet customer needs quickly. To guarantee the reliability of the product a clear development procedure is followed.

1. Product problems, needs or improvement are listed on the backlog and prioritised
2. Changes that need to be picked up are authorised
3. Changes are designed and planned
4. Changes are developed
5. Changes are reviewed by another developer
6. Changes are tested by QA (Quality and Assurance)
7. Changes are released to production

For the Zivver web application changes will instantly be available to all users. For the Zivver plugins, the user needs to install an update.

After-sales Account Management

Zivver employs a structured and proven account management approach for all its enterprise customers. Zivver's Customer Success team is dedicated to helping customers achieve their desired business results with Zivver. Their focus is to create a long-term partnership with the customers.

At the last stage of the initial commercial process, during contract negotiation, a Zivver Customer Success Manager (CSM) will be appointed. The Customer success Manager will be the single point of contact for the engagement after the contract is signed. The initial role of the CSM is to draft a ‘Customer Success Plan’ in close

cooperation with the customer. The CSM is accountable to organise all Zivver's activities and knowledge to help the customer to achieve the goals set out in the Customer Success Plan. Starting from initial implementation to life cycle support to obtaining business results and proactive knowledge sharing of recent security developments.

The CSM reports directly into the VP Customer Success and can draw on company resources to support the customer in order to meet the goals as defined in the Customer Success Plan. For the initial implementation, an implementation project leader will lead an implementation team under the accountability of the CSM. The size and composition of this team will depend on the situation of the individual customer. After the implementation, ongoing support will be delivered by Zivver's support organisation and under the accountability of the CSM. At agreed periods the CSM will take initiative to review together with the customer Zivver's performance and opportunities to improve which will be reflected back into the Customer Success Plan. In addition, Zivver organises customer events such as Know-How sessions during the year in order to keep customers updated on the latest security developments and best practices. The CSM will actively monitor Net Promoter Scores (NPS) and proactively engage with clients when scores indicate potential concerns. Finally, the CSM will oversee the contract renewal process as well as managing the offboarding process.

Termination Process

Each customer has their own dedicated Customer Success Manager (CSM). If the customer wishes to end their contract Zivver will, at the request of the customer and together with their CSM, destroy or supply all information that is still present in the Zivver service. The customer also has the functionality to export all data unencrypted themselves and have the ability to do this up to 60 days after the contract has ended. Zivver offers this download/export by means of an explicit TLS SFTP connection. This allows the organisation to use its own SFTP tool of choice to export the new messages and files at time intervals that suit them.

5. Our experience

Case Studies

Our service has been proven in real-world use by several prominent public-sector and healthcare organisations, including Preston City Council, Armagh City, Banbridge & Craigavon Borough Council, Royal Papworth Hospital NHS Foundation Trust, and The Wrekin Housing Group. Each implemented the service to overcome distinct data-security challenges and improve operational efficiency.

Preston City Council

Preston City Council found that its legacy email encryption system required external recipients to create and manage separate log-ins, which led to delayed

communication and low engagement. By working together with Zivver — including a three-month proof-of-concept during which the solution was tailored to the council's VDI environment and existing email-archiving setup — the council transitioned to a system where sensitive information (e.g., internal reports, partnership correspondence) could be sent securely and archived, without burdening recipients with extra login steps. This deployment included seamless integration into the council's Microsoft 365 email environment, an intuitive user interface where encryption is applied automatically when needed, and full staff testing and training to ensure usability.

As a result, the council experienced a significant reduction in email-related support queries, increased adoption of secure email by both staff and external partners, and faster turnaround times for sensitive communications. Recipient satisfaction improved notably due to the removal of portal logins, while staff confidence increased thanks to more reliable, policy-driven security workflows. Overall, the council strengthened its data-protection posture and improved operational efficiency in daily communication.

Armagh City, Banbridge & Craigavon Borough Council

Serving a large and diverse constituency, this council required a solution able to integrate tightly with its existing Microsoft 365 and Outlook infrastructure. Manual processes for sending large or sensitive documents were time-consuming, inconsistent, and created risk. Working with Zivver, the council carried out a full implementation that included integrating the Outlook add-in across the organisation, enabling compliant large-file transfer of up to 5 TB directly from Outlook, and configuring automated business rules to detect sensitive information, incorrect recipients, and other high-risk behaviours. Zivver also supported the council in replacing legacy file-sharing processes, mapping secure-send workflows to existing policies, and setting up real-time alerts and enforced secure delivery where required. These activities standardised secure communication, automated previously manual tasks, ensured consistent compliance with data-handling requirements, and significantly reduced the risk of mis-sent emails.

As a result, the council achieved faster and more consistent secure communication, with staff now using a unified workflow for both email and large-file transfers. The introduction of automated alerts and policy-driven controls led to a measurable decrease in misdirected emails and user mistakes, while secure-send adoption rose across departments without requiring additional training burden. External partners benefited from smoother, more reliable exchanges, and the council gained improved oversight of sensitive-data flows—enhancing compliance readiness and reducing operational risk.

Royal Papworth Hospital NHS Foundation Trust

As a specialist NHS hospital, Royal Papworth needed a secure two-way communication platform for staff, patients, and external collaborators. Their

previous system restricted inbound flows and imposed cumbersome authentication for recipients. By deploying our service, the hospital introduced a friction-free communication experience through seamless Outlook integration, enabling staff to send sensitive information and large files directly from their existing email client without relying on legacy file-transfer tools. External recipients — including patients — could reply securely via a one-time authentication link, eliminating the need to create accounts or manage portal logins. Real-time prompts supported users in preventing misaddressed emails or insecure sending, while built-in encryption, audit-trail visibility, and revocation ensured robust data protection. Together, these capabilities removed the manual steps, login barriers, and inconsistent workflows that previously slowed communication, resulting in faster, more user-friendly clinical, administrative, and research correspondence.

As a result, Royal Papworth saw a marked improvement in the speed and reliability of secure communication between staff, patients, and external partners. The removal of portal logins significantly enhanced patient accessibility and reduced support overhead, while automated safeguards improved staff confidence and reduced the likelihood of communication errors. Clinical and administrative teams reported smoother, more predictable workflows, and the organisation strengthened its ability to share sensitive health information in a compliant, user-friendly manner.

The Wrekin Housing Group

With tens of thousands of homes under management, The Wrekin Housing Group recognised that staff often sent sensitive tenant data without full awareness of the associated risks. Zivver replaced their legacy email-encryption solution with a seamless, one-click encryption system integrated into Outlook, including built-in two-factor authentication for external recipients. We configured automated business rules and contextual alerts to warn users when sensitive data or high-risk actions (such as wrong recipient or unsecured attachment) were detected. The rollout was supported with full implementation, configuration, onboarding and user training so secure emailing became the default. Post-deployment, the council gained real-time visibility into data-sharing behaviour via Zivver's reporting suite, enabling better compliance, improved data-loss prevention and strengthened audit readiness.

As a result, Wrekin Housing Group reduced the frequency of email-related security incidents, improved staff adherence to safe-sending practices, and eliminated the need for cumbersome legacy processes such as manual password-protected attachments. Both office-based and remote staff benefited from a more streamlined and consistent workflow, and the organisation gained greater assurance that sensitive tenant data was being handled securely. These improvements strengthened overall governance, supported regulatory compliance, and increased operational confidence across teams.

Clients

Contact Details

For any queries regarding this service or G-Cloud opportunities, buyers may contact the Zivver Public Sector team via: publicsector@zivver.com.