Vragen, antwoorden en communicatie tussen Follow The Money en Zivver

Inhoudsopgave

Mail van Follow The Money met initiële vragen – vrijdag 29 augustus 2025

Beste Rick,

Bij deze onze vragen over en rond de overname. Zou je de ontvangst kunnen bevestigen?

1 - hoe is Zivver met Kiteworks in contact gekomen?

2- wat is/zijn de reden(en) geweest om met Kiteworks in zee te gaan?

3 - is Zivver bekend met het gegeven dat in het management van Kiteworks Israëliërs zitten die eerder in Unit 8200, de afluisterdienst van het Israëlische leger hebben gewerkt? Zo ja, sinds wanneer is Zivver hiermee bekend?

4 -is Zivver bekend met het feit dat Unit 8200 o.a. is gespecialiseerd in de ontsleuteling van informatie? Zo ja, wat betekent dit voor de samenwerking met Kiteworks?

5 -zo nee, hoe reageert Zivver op deze informatie?

6 - zo ja, wat was dan toch de reden om voor Kiteworks te kiezen?

7 -kan Zivver garanderen dat vertrouwelijke info die via Zivver wordt verstuurd, niet in Israël of de VS belandt? Zo ja, hoe?

8 - klopt het dat Zivver niet werkt met end-to-end encryptie, maar dat binnengekomen berichten worden ontsleuteld op servers van Zivver waarna het leesbare bericht aan de ontvanger wordt getoond? Zo niet, hoe verloopt het proces van versleuteling en ontsleuteling?

9- klopt het dat Zivvers systemen dan kortstondig die berichten in leesbare vorm kunnen verwerken? Zo niet, welke maatregelen treft Zivver om dit te voorkomen?

10- kan Zivver aangeven in hoeverre Zivver en haar systemen worden geïntegreerd binnen (de systemen van) Kiteworks?

11 -Kan Zivver aangeven welke personen? van Kiteworks direct bij de overname betrokken waren?

Is het mogelijk om deze vragen uiterlijk maandag 1 september om 18:00 te beantwoorden?

Met vriendelijke groet (mede namens mijn college Sebastiaan Brommersma)

Reactie op mail met antwoorden op vragen – Maandag 1 september 2025

Beste Siem en Sebastiaan,

Nogmaals dank voor het delen van jullie vragen met ons. In de bijlage vinden jullie onze uitgebreide antwoorden. We hebben geprobeerd deze zo volledig en transparant mogelijk te beantwoorden.

Aan de manier waarop sommige vragen geformuleerd zijn, lijkt het erop dat enkele van de geraadpleegde bronnen informatie hebben verstrekt die onvolledig of misleidend was, of waar onvoldoende technische diepgang in zat. Onderwerpen als encryptiemodellen, e-mailbeveiliging, compliance-vereisten en de verschillen in hoe leveranciers zoals Microsoft, Google en anderen data verwerken en beveiligen, zijn zeer technisch en vragen om de juiste context. Helaas worden deze onderwerpen vaak te simplistisch of onjuist uitgelegd. Soms onbedoeld, soms vanuit commerciële motieven.

Mocht er behoefte zijn aan verdere context of verduidelijking, dan help ik daar uiteraard graag bij. Dit zijn belangrijke vraagstukken: veel organisaties gebruiken vandaag de dag nog steeds oplossingen die hun gevoelige informatie onvoldoende beschermen, vaak volledig toegankelijk voor Amerikaanse autoriteiten onder de CLOUD Act en daardoor ook kwetsbaarder voor onderschepping of aanvallen door hackers. Bij gebruik van Microsoft365 en GSuite, zonder een oplossing als Zivver, zijn eigenlijk alle mails kwetsbaar voor onderschepping en opvraging.

Omdat wij onze antwoorden hebben afgestemd met onze internationale collega's sturen we deze in het Engels mee, ervan uitgaande dat dit voor jullie geen probleem is.

Ik zie jullie reactie graag tegemoet.

Met vriendelijke groet,

Rick Goud

Answers to questions Follow the Money on the Acquisition of Zivver

(translated from Dutch)

1 – How did Zivver get in contact with Kiteworks?

ANSWER:

As is the case with many successful, high-growth, VC-backed companies, Zivver has been approached by numerous organizations over the past years that expressed interest in acquiring us for our team and technology. One of those companies was Kiteworks, who reached out to us for the first time in late 2020. Kiteworks' team reached out to Zivver's former VP of Engineering through a mutual friend. The VP of Engineering then made the introduction with Zivver's CEO. Since then, we have stayed in touch with them (as well as with other parties), because we were extremely impressed by their vision, performance, technology, and team.

---

2 – What was/were the reason(s) for entering into a partnership with Kiteworks?

ANSWER:

Zivver has built a unique position in Europe as the only company (to our knowledge) that can fully protect organizations from the impact of the U.S. CLOUD Act when using Microsoft or Google technology. By applying asymmetric encryption where Zivver itself has no access to the decryption keys (customers/users hold the keys needed to decrypt the data), we ensure that:

- Zivver is unattractive to hackers,
- insider threats are neutralized, and
- governmental data requests cannot be complied with, simply because the keys do not exist in our possession.

This stands in stark contrast to Microsoft 365, Google and most to all other (secure) email vendors, where providers have access to all emails and attachments by keeping decryption keys in their possession, leaving organizations highly exposed to CLOUD Act risks and potential data breaches. Moreover, Zivver is the only vendor in Europe capable of ensuring that emails are stored in encrypted form even within Microsoft and Google clouds; a capability no other vendor offers.

Over the past year, however, we increasingly received two new types of customer requests:

1. **Broader coverage beyond email and file transfer:** Customers asked if we could extend our zero-access encryption and Data Leak Prevention (DLP) capabilities to other use cases, such as secure file collaboration (as an alternative to SharePoint, OneDrive, Google Drive, etc.), secure digital forms/questionnaires, and in the interaction with AI/LLM's (think ChatGPT) where data sensitivity and CLOUD Act exposure are equally high.
2. **Deployment flexibility:** Customers wanted the ability to use our technology not only in the public cloud, but also On-Premise or in Private Cloud environments, to further mitigate any risks of U.S. hyperscalers (Azure, AWS, Google).

To address these needs, we evaluated three strategic options:

1. Build the required technology ourselves; discarded as it would take too long.
2. Acquire companies with the right technology; we explored this path, but found no solutions in Europe or beyond that were secure, mature, compelling, or affordable enough.
3. Partner with or join a complementary company; this proved the best route.

Kiteworks stood out as a potential strategic partner. Since we first met them, they had significantly expanded their product with secure file collaboration and other capabilities, successfully acquired five additional companies in the UK and EU to strengthen their portfolio, and secured over USD 450 million in growth investment from some of the world's leading private equity firms, while keeping the firm's leadership and employees as the largest shareholders. Just as importantly, they share our culture and mission: protecting sensitive data at the highest possible standard. Like Zivver,

Kiteworks holds ISO 27001 and SOC 2 Type II certifications, but in addition they have achieved FedRAMP High-ready authorization (something very few companies worldwide can claim) and are one of the rare vendors able to help organizations achieve CMMC Level 2 certification. Kiteworks already serves the world's most demanding customers, including many governments, IP-heavy industries, banks, law firms, and insurers, with on-premise, private cloud, and even air-gapped deployments.

In short, Kiteworks ticked every box: they enable us to deliver what our customers are asking for but couldn't find elsewhere, while also allowing us to scale Zivver's technology globally much faster than we could have achieved on our own. It is important to note that Kiteworks was not even the highest bidder. We deliberately chose Kiteworks. Not for financial reasons, but because they were the best fit for our customers in terms of security, vision, capabilities, and long-term alignment.

---

3 – Is Zivver aware that Kiteworks' management includes Israelis who previously worked in Unit 8200, the interception service of the Israeli army? If so, since when has Zivver been aware of this?

ANSWER:

As part of the due diligence process leading up to the acquisition, Zivver conducted a thorough review of Kiteworks' leadership team, including the backgrounds of key executives such as CEO Jonathan Yaron, Chief Product Officer Yaron Galant and Chief Business Officer Amit Toren. This review confirmed their prior service in Israel's Unit 8200, which is a matter of public record (see https://www.kiteworks.com/company/press-releases/kiteworks-adds-strategic-and-innovative-depth-to-its-executive-leadership-team-with-four-strategic-hires/ and https://www.calcalistech.com/ctechnews/article/hyqfxfc5c). Zivver has been aware of this since the early stages of contact in 2020. It's important to note that mandatory military service is required for Israeli citizens, and Unit 8200 is an elite signals intelligence and cyber unit that attracts top talent in technology and cybersecurity. This experience reflects the high caliber of leadership at Kiteworks, contributing to our expertise in building secure, innovative data protection solutions, with the goal to use their and others' experience to build the most secure data exchange solution in the world. All three executives completed their service decades ago, and have since, as many other Unit 8200 alumni, become American citizens and built successful careers in the U.S. enterprise software industry, residing and operating in the San Francisco Bay Area. Each of them has not been under the command of Unit 8200 for many years now.

Kiteworks was founded in Singapore (not Israel), is an American company, and has no office or legal entity in Israel. Its executives and employees are selected for their deep experience and proven expertise, just as any leading company seeks to attract the best talent in its field. 60% of all Kiteworks' employees are employed in the EU. The vast majority all R&D takes in place in the European development hubs (Amsterdam, Regensburg, Sofia, Zurich, and Timișoara), and in Singapore. Less than 3% of the company are Israeli and employee origins across Kiteworks represent more than 30 countries.

---

4 – Is Zivver aware that Unit 8200, among other things, specializes in the decryption of information? If so, what does this mean for the cooperation with Kiteworks?

ANSWER:

Yes. Far from being a concern, this background enhances our cooperation with Kiteworks by bringing world-class knowledge in threat detection, data protection and preventing unauthorized access to data to the table. Unit 8200 alumni are renowned for founding and leading successful tech companies globally, including Check Point Software Technologies, Palo Alto Networks, and Wiz (acquired by Google); all software used by most governments, banks etc nationally and globally. Last year, The Wall Street Journal published an article describing the contribution of the Unit alumni to the world's cybersecurity, with the following headline: "**Silicon Valley's Hot Talent Pipeline Is an Israeli Army Unit; Unit 8200 has become an incubator for cybersecurity startups defending the world's biggest companies against hackers**" (see https://www.wsj.com/tech/silicon-valleys-hot-talent-pipeline-is-an-israeli-army-unit-e8368b4d). Further, there are over 450–500 cybersecurity companies in Israel's ecosystem, a significant portion (20–30% based on trends) founded by Israelis relocated HQ abroad, mainly to the US for market access, funding, and talent. Among ~30 global cybersecurity unicorns, a large percentage are Israeli-founded. So being Israeli led in cybersecurity instills confidence for us, not uncertainty. For Kiteworks and now Zivver, this translates to stronger product development in secure data exchange having a team with some of the best technologists and cyber specialists in the world.

---

5 – If not, how does Zivver respond to this information?

---

6 – If so, what was still the reason for choosing Kiteworks?

ANSWER:

Zivver chose to join forces with Kiteworks because of the strong strategic alignment in delivering uncompromising data privacy, security, and innovation, which far outweighs any outdated perceptions of past affiliations. This partnership enables us to expand our security offerings exponentially, combining Zivver's AI-enabled secure email solution with Kiteworks' comprehensive Private Data Network (PDN) for email protection, file sharing, managed file transfer, and more, all under a zero-trust architecture. For European organizations, this means a credible alternative to hyperscalers, with full control over data storage, customer-held encryption keys, and no black boxes, ensuring zero-access security regardless of channels. The executives' elite backgrounds, including service in Unit 8200 early in their career, actually underscore Kiteworks' expertise in cybersecurity, contributing to a platform that prioritizes threat prevention and compliance over any speculative concerns. Ultimately, this acquisition reflects our shared commitment to making secure, sovereign data exchange accessible and robust for global customers.

---

7 – Can Zivver guarantee that confidential information sent via Zivver will not end up in Israel or the US? If so, how?

ANSWER:

Yes, confidential information sent via our platform will not end up in Israel or the U.S. Zivver remains fully EU-hosted, locally managed, and protected by zero-access encryption. No emails or files sent or received via Zivver are transferred outside the EU. Our zero-access encryption (meaning only senders and intended recipients hold the keys to decrypt messages) ensures that confidential information shared or received via our platform cannot be accessed by Zivver, Kiteworks, or any third party. Zivver can even ensure that Microsoft and Google cannot access sensitive emails and files shared from Outlook or Gmail. This is unlike all other "Secure Email" vendors currently active in the Netherlands, who cannot prevent access to data by Microsoft and Google. Also, most of these "Secure Email" vendors, similar to Microsoft and Google, keep decryption keys in their possession, making them attractive to hackers, vulnerable to insider threats, and subjective to governmental subpoenas.

Our solution is independently tested by third parties at least once a year. We hold stringent certifications including ISO 27001 and SOC 2 Type II, maintain our own dedicated security team, and welcome customer-led security reviews, penetration tests, or even code reviews when needed. Our security model is built on trust, which is why we are fully transparent about our architecture, processes, and certifications, continually striving for the highest standards.

Important to note: Many of our central government, health care, insurance and banking customers repeated their DPIAs and security reviews after the acquisition, and all concluded that the risk profile has not materially changed and Zivver is still the best solution for secure email and secure file transfer, taking security, compliance and usability into account. Of the few dozen of larger organizations that repeated their DPIAs and security reviews after the acquisition, every one of them with expiring contracts explicitly renewed their contract and none of them terminated the contract.

---

8 – Is it correct that Zivver does not use end-to-end encryption, but that incoming messages are decrypted on Zivver's servers after which the readable message is displayed to the recipient? If not, how does the encryption and decryption process work?

ANSWER:

Zivver uses **zero-access encryption,** which ensures we **cannot decrypt or access customer data.** Unlike Microsoft, Google and many to most (secure) email providers, Zivver never stores the keys needed to decrypt sensitive emails and files (private keys) and thus cannot access the content of customer communications. True end-to-end encryption (E2EE) is unworkable for email, because it requires both sender and recipient to use the same tool (as with WhatsApp or Signal), which is

simply an unrealistic requirement for the billions of people who use email daily across different providers. Therefore, E2EE is currently not in use for email encryption on any meaningful scale by organizations in the Netherlands, Belgium, UK, and other countries in Europe or, to our knowledge, the rest of the world. Also, most organizations don't want E2EE, as that would mean data is only readable on sender/recipient devices. Organizations would then lose valuable functionalities like advanced DLP (Data Leak Prevention) capabilities, functionalities for forensic investigations, etc which are required under GDPR, NIS2, ISO 27001, and other laws.

There is some adoption of E2EE email protocols PGP and S-MIME, mostly in fixed communication relationships between select departments of enterprise organizations and government agencies that work with very sensitive information (e.g. SECEM-2 for the European Commission). Kiteworks acquired Swiss email encryption provider Totemo several years ago. Their PGP and S-MIME solutions have been added to Kiteworks' Email Protection Gateway (EPG) and as such will become available to Zivver customers in due time.

Our zero-access model has been reviewed by many independent experts, and is officially approved and trusted by governments, banks, and large insurers. These organizations consider Zivver's approach far superior to the encryption used by Microsoft, Google, and most other vendors that EU organizations rely on today for sharing sensitive data. Microsoft, Google, and most (secure) email vendors encrypt messages on their servers where the ciphertext and the decryption keys co-exist. This is like putting a strong lock on your front door but leaving the key under the doormat. Such designs are inherently (more) vulnerable to insider threats, government access requests, or hacking. Zivver's model avoids all of this.

For a detailed overview, see our blog on zero-access encryption (https://www.zivver.com/blog/the-benefits-of-zero-access-encryption-for-email-security) and the attached white paper, but below a summary:

Zivver's model: Zero-access encryption

Instead of E2EE, Zivver applies **zero-access encryption**, which is very close in terms of confidentiality but actually works for open, interoperable email and supports compliance.

- **Asymmetric keys (RSA-2048):** Zivver generates a public/private key pair for every user.
- **Public key:** stored for encryption.
- **Private key:** never stored. Instead, Zivver creates a key-derivation function (PBKDF2) using a user-specific secret from the customer's Identity Provider (IdP) such as Azure AD, ADFS, or Okta.
- **Result:** Only if the IdP later provides that secret again (after strong authentication) can the private key be reconstructed temporarily in memory for decryption.

Encryption process (sending a message)

- When User A sends a message to Users B and C, the message body and each attachment are encrypted separately with the public keys of all participants.

- Encryption is performed as a streaming process in RAM.
- Once encryption is complete, the memory used is immediately overwritten.

Decryption process (receiving a message)

- When User B opens the email in Outlook with the Zivver add-in:
  - Zivver checks with the IdP: who is the user, was strong authentication used (e.g. with MFA), and is she authorized to access the mailbox?
  - If valid, the IdP passes the user-specific secret via SAML.
  - Zivver uses this secret with the KDF to reconstruct the private key in memory only.
  - The ciphertext is decrypted and displayed to the user.
- Again, all of this happens only in RAM; nothing is written to disk, and memory is wiped immediately afterward.

---

9 – Is it correct that Zivver's systems can then temporarily process those messages in readable form? If not, what measures does Zivver take to prevent this?

ANSWER:

As described above, end to end encryption for email is not feasible/workable for any organization that wants to use it for their broad email communication and Zivver's zero-access encryption model has been extensively reviewed by experts and broadly approved and has been qualified by customer as superior to all other potential solutions. Zivver's zero-access encryption model ensures that during encryption and decryption plaintext is kept ephemerally in RAM and decryption, where RAM is wiped immediately after use, and cannot be accessed by Zivver, Kiteworks, or anyone else. It is inherent to the process of encryption (transforming readable data into encrypted data) and decryption (transforming decrypted data into readable data), that the technology that handles this process handles data in readable form. That is unavoidable and holds true for all email encryption solution in broad use today. The question that should be put central, and that customers have, is how to ensure that the software/system that handles the encryption and decryption process, does this in a secure way without any vulnerabilities or backdoors.

What makes that experts state our solution gives this assurance is:

- We use proven RSA 2048 asymmetric encryption. Pending the availability of post-quantum encryption for production system, this is still best-practice
- During encryption and decryption plaintext is kept ephemerally in RAM, where RAM is wiped immediately after use, and cannot be accessed by Zivver, Kiteworks, or anyone else.
- We hold the highest security certifications, including ISO 27001 and SOC 2 Type II.
- We use only EU-based data centres that meet the strictest security standards.
- Our systems (with availability of code) are independently tested by external experts every year.

- Customers are invited to run their own penetration tests or even conduct direct code reviews, which some large customers/government actually do/have done.

This transparency is why our architecture is trusted and officially approved by governments, hospitals, banks, and insurers as more secure than the encryption approaches of Microsoft, Google, and most other "secure email" vendors. As said, many of our larger central government, health care, insurance and banking customers repeated their DPIAs and security reviews after the acquisition, and all concluded that the risk profile had not increased and Zivver is still the best solution for secure email and secure file transfer, taking security, compliance and usability into account. Of the few dozen of larger organizations that repeated their DPIAs and security reviews after the acquisition, every one of them with expiring contracts explicitly renewed their contract and none of them terminated the contract.

The only way to reduce reliance on trust in a vendor even further is to run a certified secure solution on-premises rather than in the cloud. In that setup, organizations can monitor and verify themselves that no data ever leaves their servers. This is exactly what Kiteworks offers with its Private Data Network (PDN).

---

10 – Can Zivver indicate to what extent Zivver and its systems are being integrated into (the systems of) Kiteworks?

ANSWER:

Zivver continues to serve its customers as it always has. The service remains unchanged for existing customers, with the same hosting in the EU, the same compliance to GDPR, the same security architecture and certifications, and the same contractual agreements, the seem local management. Nothing changes for customers in how they use Zivver today.

What will change over time is that Zivver and Kiteworks are working together to make Zivver's unique email DLP and zero-access encryption capabilities available inside Kiteworks' Private Data Network (PDN). The PDN is a unified platform that secures email, file sharing, managed file transfer (MFT), and other forms of private data exchange.

This means that in the future, Zivver customers who wish to migrate and/or expand will be able to:

- Deploy the PDN on-premises, in a private cloud, or in an EU-based public cloud, while keeping Zivver's key email security functionalities.
- Combine Zivver's secure email with additional sovereign solutions such as file collaboration, secure web forms, and managed file transfer.
- Manage all of this through **a single policy framework and unified audit trail**, giving organizations stronger compliance, better visibility, and simplified governance.

In short, the integration with Kiteworks gives customers more control, higher security, stronger data sovereignty, broader use cases, and more flexible deployment options, without changing how Zivver works for them today.

---

11 – Can Zivver indicate which persons from Kiteworks were directly involved in the acquisition?

ANSWER:

The acquisition process was led by Kiteworks' executive team, with key involvement from Chief Business Officer Amit Toren, who oversaw strategic alignment and negotiations, and Ian Griffith, Director of Corporate Development. As CEO and Chairman, Jonathan Yaron provided overall leadership and approval for the deal. Other supporting roles included members of the product, legal, and finance teams, though specific names beyond the executive level are not publicly detailed. From Zivver's side, CEO Wouter Klinkhamer, Chief Innovation Officer Rick Goud, COO and General Counsel Reinout Bautz, Legal Director Jochem Hummelen and CISO Nadine Hoogerwerf were central to the discussions, ensuring a shared vision for data privacy and security. In the process, Zivver's leadership team met all Kiteworks' C-level leaders, most to all of Kiteworks' senior management and many managers and individual contributors. Similarly, Kiteworks' leadership team met Zivver's managers as well as various important employees.

Mail met aanvullende vragen FTM over beveiliging – 9 september 2025

Beste Rick,

Dank nog voor het toesturen van de uitgebreide antwoorden. We hebben naar aanleiding hiervan nog een aantal vervolgvragen, die we graag aan je voorleggen.

1. In jullie antwoord onder 7 garanderen Zivver en Kiteworks dat vertrouwelijke informatie niet in handen van Israël en/of de VS eindigt, onder meer omdat de data wordt beschermd door wat jullie zero-access encryption noemen.

Inmiddels hebben wij geconstateerd dat de informatie die verschillende Zivver-gebruikers via de webapplicatie versturen (berichten, en bijlagen) in platte tekst, leesbaar naar de servers van Zivver worden verzonden.

Hiervan was onder meer sprake bij berichten die zakelijke Zivver-gebruikers naar individuen zonder Zivver-account stuurden en bij verkeer tussen twee zakelijke Zivver-gebruikers.

Wij constateerden dit ook bij het account van een Nederlandse overheid.

Hoe verhouden deze constateringen zich tot de stelling dat vertrouwelijke informatie door middel van zero-acces encryption wordt beschermd?

Kan Zivver garanderen dat deze informatie niet in handen komt van de VS en/of Israël? Zo ja, hoe kan zij dit waarmaken?

In welke gevallen cq in welke situaties of bij welke producten is er wel en in welke is er geen sprake van zero-access encryptie?

2. Op jullie website staat dat Zivver voor alle type aangeboden pakketten (starter, professional, ultimate, zie link) asymmetrische zero knowledge encryptie bevatten.

Hoe verhoudt dit zich tot de situatie waarbij er geen client side encryptie plaatsvindt?

Bij welke diensten, producten, gevallen vindt er server side encryptie plaats en hoe is het sleutelbeheer in die gevallen geregeld?

3. In het antwoord onder 7 staat voorts dat vertrouwelijke informatie die via Zivver wordt verzonden in de EU wordt opgeslagen en dat Zivver verzekert dat Microsoft en Google niet bij gevoelige data kunnen.

Inmiddels constateerden wij dat Zivver voor haar werkzaamheden gebruikmaakt maakt van Cloudfront (Amazon) voor de verwerking van vertrouwelijke berichten. Ook in platte tekst.

Garandeert Zivver dat deze berichten niet in handen kunnen komen van de VS en/of Israel? Zo ja, hoe kan zij dit waarmaken?

4. Zivver maakt blijkens de website gebruik van foutpreventie software die onder meer in staat is om fouten en gevoelige gegevens in berichten te detecteren. Zivver maakt daarbij gebruik van machine learning.

Zivver maakt ook (blijkt wederom uit de website) gebruik van AI-tools die e-mails inhoudelijk scannen op mogelijke bedreigingen.

Wordt bij deze acties de inhoud van berichten verwerkt, en, zo ja, waar (op wiens servers) vindt de verwerking plaats?

Indien dit op servers van meerdere partijen gebeurt, dan graag een toelichting.

Aangezien onze planning is om einde deze week te publiceren, zouden wij jullie reactie graag uiterlijk donderdagochtend 11 september om 12:00 uur ontvangen. We vertrouwen erop dat dit geen probleem is en zien uit naar jullie nadere bericht.

Is het wederom mogelijk de ontvangst van deze mail te bevestigen?

Met vriendelijke groet, (mede namens mijn collega Sebastiaan Brommersma)

Reactie Zivver op aanvullende vragen FTM – 11 september 2025

Beste Siem en Sebastiaan,

Dank voor jullie vervolgvragen en voor de tijd en diepgang die jullie in dit onderzoek hebben gestoken. Wij waarderen de grondigheid en de gelegenheid om toe te lichten hoe Zivver werkt, ook ten opzichte van oplossingen die nu door de meeste organisaties worden gebruikt voor het delen van zeer gevoelige informatie.

Zoals uit de antwoorden zal blijken, raken veel van de aangehaalde punten aan de fundamentele werking van het internet zelf en de standaarden die vrijwel elke digitale toepassing vandaag de dag ondersteunen, van bankapps tot overheidsdiensten/-portalen. Dit is niet uniek voor Zivver, maar weerspiegelt wereldwijd erkende best practices die door overheden en standaardisatieorganisaties zijn goedgekeurd. Wanneer de werking van deze standaarden, best practices en de expliciete aanbevelingen van het NCSC en Europese instanties ter discussie zou worden gesteld, gaat het niet om een specifiek punt van kritiek op Zivver, maar om een fundamentele twijfel aan de digitale infrastructuur waarop de hele wereld vertrouwt, met alle gevolgen van dien. Tot op heden is er echter geen enkele reden of aanleiding om daaraan te twijfelen, en mocht dat onverhoopt toch aan de orde zijn, dan kunnen wij dit, zoals uit de antwoorden blijkt, eenvoudig mitigeren.

Wat Zivver veiliger maakt dan andere (e-mail)oplossingen die worden gebruikt, is dat wij aanvullende controles toevoegen bovenop deze wereldwijde standaarden: zero-access encryptie at rest, technologie voor foutpreventie, sleutelbeheer onder regie van de klant, jaarlijkse onafhankelijke pentests, hosting uitsluitend binnen de EU, en zelfs de mogelijkheid voor klanten om hun eigen security- en code-reviews uit te voeren. Dit gaat veel verder dan wat de meeste applicaties of e-mailoplossingen bieden.

Het enige mogelijke aandachtspunt dat men zou kunnen aanvoeren, is het theoretische vertrouwen in publieke cloudproviders die binnen de EER zijn gevestigd, zoals Azure en AWS – namelijk dat zij niet op grote schaal alle data van gebruikers real-time aftappen en doorsturen naar overheden. (Data opvragen onder de Cloud Act is niet mogelijk, omdat noch AWS/Azure noch wij over de decryptiesleutels beschikken). Een dergelijk scenario waarbij alle data real-time zou worden afgetapt, is echter niet realistisch: als dit zou gebeuren, zou dit onmiddellijk leiden tot een wereldwijd conflict en ontwrichting van het gehele digitale ecosysteem, met alle gevolgen van dien. Juist voor organisaties die zich desondanks zorgen maken over dit punt, zijn wij de samenwerking met Kiteworks aangegaan. Samen kunnen wij klanten nu de mogelijkheid bieden de volledige oplossing volledig on-premises, in een private cloud of zelfs in air-gapped omgevingen te draaien. Dit geeft organisaties volledige soevereiniteit en direct toezicht, waardoor zij zelf kunnen verifiëren dat er geen data hun infrastructuur verlaat. En zo gebruiken honderden zeer gevoelige (overheids-)organisaties in Europa en de rest van de wereld Kiteworks al vele jaren.

Wij vinden het belangrijk om te benadrukken dat de gestelde vervolgvragen niet verband houden met de samenwerking met Kiteworks. De antwoorden beschrijven de manier waarop Zivver sinds de oprichting opereert, waarmee alle audits en aanbestedingen zijn doorstaan en waarbij wij door

overheden, ziekenhuizen, verzekeraars en andere kritieke organisaties zijn geselecteerd als de veiligste keuze voor e-mailbeveiliging. De samenwerking met Kiteworks voegt simpelweg extra flexibiliteit in uitrol en maximale datasoevereiniteit toe.

Zie bijgaand de antwoorden op jullie vragen. Wij horen het graag als daar nog vragen of opmerkingen over zijn. Wij vertrouwen erop dat de publicatie feitelijk en in de juiste context plaatsvindt, en lezen desgewenst graag vooraf mee om eventuele onjuistheden te voorkomen.

Met vriendelijke groet,
Rick

Answers to follow-up questions Follow the Money on the Acquisition of Zivver

1. In your answer under 7, Zivver and Kiteworks guarantee that confidential information will not end up in the hands of Israel and/or the US, partly because the data is protected by what you call zero-access encryption.

In the meantime, we have found that the information various Zivver users send via the web application (messages and attachments) is transmitted in plain text, readable, to Zivver's servers.

This was the case, among other things, with messages that business Zivver users sent to individuals without a Zivver account and with traffic between two business Zivver users.

We also observed this with the account of a Dutch government body.

How do these findings relate to the claim that confidential information is protected through zero-access encryption?

Can Zivver guarantee that this information will not end up in the hands of the US and/or Israel? If so, how can it ensure this?

In which cases, situations, or products is there zero-access encryption, and in which cases is there not?

ANSWER:

Data sent via Zivver client applications is **never transmitted in plain text**. All communication is protected in transit with **TLS/HTTPS using only secure cipher suites:** the worldwide standard for securing sensitive data online, fully in line with the Dutch NCSC's recommendations (NCSC TLS Guidelines) and the guidelines from the European Committee (see here). This is the same method trusted by banks, governments, and hospitals and endorsed by all major cybersecurity authorities. If TLS/HTTPS were ever deemed insecure, the entire internet, global financial system, and digital infrastructure would be at risk and we would all have much bigger challenges than email to say the least.

Once received via HTTPS by Zivver servers, messages and attachments are immediately processed and secured with Zivver's **zero-access encryption** (as described in previous answers). This ensures that readable content never touches disk, is only handled ephemerally in memory, and is

inaccessible to Zivver, Kiteworks, or any third party. Furthermore, all messages and attachments received by Zivver are protected with storage encryption, in line with best practises in AWS, resulting in all customer messages and attachments being double-encrypted at rest.

Zivver undergoes annual expert penetration tests, uses only EU-based datacentres with the highest certifications, and even allows customers to run their own penetration tests or perform direct code reviews. In practice, our approach has never been challenged in any pen test or code review, because it is widely recognized as the best-practice for securing email on a large scale.

The only theoretical risk would be if **mass surveillance or data exfiltration across all EU datacentres of AWS and Azure** were to occur, where they exfiltrate all data from all virtual machines. If that happened, every bank, government, and hospital would be compromised, and society would face far bigger problems than email alone. However, to also mitigate this risk, Zivver uses the AWS Nitro virtualization system (see here), which is designed to assure that such a risk is not valid.

For organizations that nonetheless want to remove this residual risk, this is exactly why we partnered with Kiteworks. Kiteworks uniquely enables customers to run the entire solution **fully on-premises or in a private cloud**, where they can directly monitor and verify that no data ever leaves their servers.

Why no extra client-side encryption on top of HTTPS?

We can offer additional client-side encryption on top of HTTPS. However, while offered, this has never been actually requested by customers and has never been flagged in audits or penetration tests. There are three clear reasons why:

1. HTTPS/TLS with secure cypher suites is already trusted worldwide. If it were broken, the entire internet, not just email, would be compromised.

2. Most of our government and enterprise customers require deep packet inspection via their proxies and firewalls for malware scanning and compliance. Extra client-side encryption would make this impossible.

3. Performance issues. Encrypting large files fully on end-user devices would cause significant delays, especially in virtual desktop environments widely used in government and healthcare.

---

2. On your website it states that for all types of offered packages (starter, professional, ultimate, see link), Zivver uses asymmetric zero-knowledge encryption.

How does this relate to the situation in which no client-side encryption takes place?

For which services, products, or cases does server-side encryption occur, and how is key management arranged in those cases?

ANSWER:

For all Zivver packages (Starter, Professional, Ultimate), the same security model applies: data in transit is always protected with TLS/HTTPS with secure cypher suites, and once received, messages and attachments are secured with asymmetric zero-access encryption streaming in memory, allowing no-one to access the data. Security is never optional, it is always enabled by default.

Key management works the same across all services: public keys are stored for encryption, while private keys are never stored. This ensures that plaintext never touches disk and is never accessible to Zivver, Kiteworks, or third parties.

---

3. In the answer under 7, it further states that confidential information sent via Zivver is stored in the EU and that Zivver ensures Microsoft and Google cannot access sensitive data.

We have since observed that Zivver uses Cloudfront (Amazon) for its operations in the processing of confidential messages. Also in plain text.

Does Zivver guarantee that these messages cannot come into the hands of the US and/or Israel? If so, how can it ensure this?

ANSWER:

CloudFront is a globally used service from Amazon Web Services (AWS) and one of the market leaders for securing and accelerating internet traffic. It is widely relied upon by governments, banks, and hospitals to protect against DDoS attacks, optimize performance, and ensure reliable communication.

All data sent through CloudFront is protected with TLS/HTTPS, never transmitted in plain text. This is the same worldwide standard endorsed by the Dutch NCSC and all cybersecurity authorities.

If, hypothetically, CloudFront were subject to uncontrolled and unreported mass surveillance or data exfiltration, it would not only affect Zivver but every major government, bank, and critical infrastructure organization that depends on it. In such a scenario, society would face far bigger challenges than email alone.

If this theoretical risk were ever to become real, Zivver could add client-side encryption on top of HTTPS, but to date no regulator, auditor, or penetration test has ever flagged CloudFront as a security risk. That is why we, like the rest of the world, continue to use it as a trusted and secure part of our infrastructure unless proven or requested otherwise by customers.

---

4. Zivver, according to the website, uses error-prevention software that can, among other things, detect mistakes and sensitive data in messages. Zivver uses machine learning for this.

Zivver also (again according to the website) uses AI tools that scan emails for potential threats.

Does the content of messages get processed during these actions, and if so, where (on whose servers) does the processing take place?
If this takes place on servers of multiple parties, please provide clarification.

ANSWER:

Yes, if an organization's policy requires DLP (data loss prevention) functionalities like human error prevention or compliance checks then message content is processed briefly in memory to apply those checks. Nearly all organizations want these features as human error (e.g., sending to the wrong recipient, attaching the wrong file, or sharing sensitive data externally by mistake) is by far the leading cause of data leaks. Regulations such as GDPR, NIS2, and DORA specifically require organizations to put measures in place to prevent these kinds of incidents. DLP-tools that scan data, like virus scanners and firewalls, are pivotal to preventing data leaks and readable access to data is a must have for such features.

The way it works:

- When a message is sent, it is first transmitted securely to the Zivver platform via TLS/HTTPS.
- On the platform, the message content is scanned and classified in memory by our policy engine to check for potential errors or compliance violations.
- This also happens only ephemerally in RAM. The content is never stored on disk, never accessed by any human, and immediately after processing it is stream-encrypted with Zivver's zero-access encryption.
- From that point on, only the encrypted version exists.

All processing happens within Zivver's EU-based infrastructure, never on third-party servers. The checks are part of the same secure workflow as encryption and do not introduce any additional security risk. On the contrary: they are essential to help organizations meet compliance obligations and prevent the most common causes of data leaks.

3e mail van FTM met vragen – 11 september 2025

Geachte heer Goud, Beste Rick,

Dank voor onderstaande. Ik heb voor nu nog een korte opvolgende vraag.

Jullie schrijven in de antwoorden onder 2 dat alle Zivver packages hetzelfde security model gebruiken. Ik begrijp dit zo, dat dit model hetzelfde is voor alle mogelijke manieren waarop Zivver kan worden gebruikt (binnen de webapplicatie, de Outlook en de Gmail ad-ins en evt. andere opties). Kortom: voor alle Zivver diensten en producten.

Kunt u mij vandaag nog even laten weten of ik dit zo goed zie?

Met vriendelijke groet,

Sebastiaan Brommersma

Reactie op 3e mail FTM – 11 september 2025

Beste Sebastiaan,

Dank voor je vraag. Ik weet niet zeker wat je bedoelt en waar je heen wilt. Is het anders handig om even te bellen?

Voor de duidelijkheid: alle Zivver-pakketten (dus start/professional/ultimate) gebruiken hetzelfde sterke beveiligingsmodel obv zero-access encryptie en afgedwongen sterke transportencryptie obv best-practices, etc wat veel veiliger is dan dat van andere oplossingen die op dit moment door veel organisaties worden gebruikt.

De mogelijkheden in de verschillende gebruikte applicaties zijn echter wel anders door de aard van een webapplicatie. Zo zijn er in Outlook met Zivver-integratie, omdat dit een lokale applicatie is op Windows, meer aanvullende lokale veiligheidsinstellingen en controles beschikbaar. Zo kan lokaal bijvoorbeeld worden ingesteld dat bepaalde gevoelige informatie (zoals staatsgeheimen) nooit naar welke server dan ook mag worden gestuurd (niet naar Zivver, niet naar M365), iets wat met Outlook alleen (zonder Zivver) niet mogelijk is.

Dat is ook de reden waarom (vrijwel) al onze overheidsklanten, zorginstellingen en andere kritieke organisaties onze Outlook-integratie gebruiken en raden we dit alle organisaties ook aan.

Met vriendelijke groet,
Rick

4e mail van FTM met vragen – 11 september 2025

Ha Rick,

Dank voor je bericht. Heel behulpzaam.

De vraag is:

Biedt Zivver, in welke configuratie dan ook, de mogelijkheid om versleuteling van berichtinhoud (tekst, documenten, …) te laten plaatsvinden in de browser/computer/server van de klant alvorens deze over TLS naar Zivver wordt gecommuniceerd?

Dus: payload encryption *voorafgaand* aan transport-layer encryption?

Zo ja, welke?

Ik hoor graag van je. Als dat vanavond lukt zou dat heel fijn zijn!

Groet! Sebastiaan

Reactie op 4e mail FTM – 11 september 2025

Beste Sebastiaan,

Ja, zoals we (in het Engels) onderaan het antwoord op vraag 1 al hebben aangegeven, bieden we in gesprekken met klanten de optie om client-side encryptie (AES 256) als aanvulling op TLS toe te passen bij alle Zivver-applicaties. Tot nu toe is daar echter nog nooit concreet vraag of behoefte naar geweest, om de genoemde redenen:

1. HTTPS/TLS met moderne en sterke cipher suites is wereldwijd de standaard en wordt vertrouwd. Als dit zou worden doorbroken, zou niet alleen e-mail maar het hele internet onveilig zijn.
2. Overheden en grote organisaties vereisen deep packet inspection via proxies en firewalls voor malwarescanning en compliance. Extra client-side encryptie zou dit onmogelijk maken.
3. Performanceproblemen: het volledig lokaal versleutelen van grote bestanden zorgt voor aanzienlijke vertragingen, zeker in virtuele desktopomgevingen die juist veel gebruikt worden in overheid en zorg.

Client side encryptie als harde eis zou ook betekenen dat organisaties zouden moeten stoppen met mailen vanuit alle andere applicaties (zoals CRM-systemen, zaaksystemen, EPD's, enz.) die geen client-side encryptie ondersteunen; en dat betreft, zover bij ons bekend, alle dergelijke 'bronsystemen'. Daarmee zouden veel essentiële werkprocessen stil komen te liggen.

Zoals eerder aangegeven hebben veel grote (overheids)klanten na de overname opnieuw risico-analyses uitgevoerd en geen enkele aanvullende beveiliging op dit punt gevraagd. Uit die analyses blijkt telkens dat er op andere onderdelen veel grotere risico's spelen. Daarnaast geldt dat zolang organisaties in de praktijk nog gewoon werken met M365, Google en andere e-mailoplossingen (waarvan bekend is dat US overheid er gewoon bij kan), er binnen diezelfde organisaties veel grotere risico's bestaan dan het theoretische scenario van massale cloudafluistering. Om die reden zien klanten extra beveiliging op dit punt, en de nadelen die dit met zich meebrengt, niet als een verbetering. Hun prioriteit ligt bij veel grotere en tastbaardere risico's, waar nog veel meer winst te behalen valt.

Belangrijk om toe te voegen: Kiteworks biedt client side encryption aan via S/MIME- en PGP-opties. Die technologie gaan we nu combineren met Zivver, zodat we samen maximale flexibiliteit en keuze kunnen bieden aan klanten die dit wél belangrijk vinden.

Met vriendelijke groet,
Rick