ZIVVER brings ‘triple safe’ outbound email security to UK market, to minimise data leaks due to human error

Submitted by: Bratton PR (Middlesex)
Wednesday, 16 October 2019

LONDON and AMSTERDAM – 16 October 2019 – ZIVVER (https://www.zivver.eu), a Dutch-founded data protection platform, announced today that it is making its unique outbound email and file transfer security solution available to the UK market for the first time. ZIVVER helps organisations to prevent data leaks, improve compliance and save costs from ineffective communication via fax, snail mail and courier, by securing outgoing emails and file transfers throughout the whole communications process, i.e. before, during and after sending. ZIVVER calls this ‘triple safe’ technology.

Research shows that employees spend an average of two and a half hours per day (https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-social-economy) working on emails. Its ease of use and flexibility contribute to its popularity. Email is, however, risky as well. The ICO’s Data security incident trends (https://ico.org.uk/action-weve-taken/data-security-incident-trends/) for Q4 2018 reported 79% of all data leaks were non-cyber related/due to human error by employees and in 41% of all known causes, the data leak was caused by sending information to the wrong person. The same report showed 11% of data security incidents were due to unauthorised access, mostly because of a lack of two-factor authentication (2FA). Only 6% of incidents were due to phishing.

Rick Goud, CEO & Co-founder of ZIVVER, said, “When working as a healthcare strategy consultant, everywhere I looked I saw sensitive data - such as patient data, price agreements, market performance and contracts - being processed, and people making use of solutions where security and feasibility were unclear. This is why we developed ZIVVER - a solution that is both technically strong and super user-friendly. After all, if people cannot use your technology, it does not work!”

Having gained 2,500 organisations as customers in the last two years - including 25% of all Dutch hospitals and local governments – and raised $12m in funding, ZIVVER is now bringing its proven data loss prevention (DLP) and compliancy enhancing technology to the UK as it expands across Europe.

Goud said, “The UK is a very interesting market for ZIVVER - its innovative tech culture mirroring that of the Netherlands, with growing volumes of sensitive information being sent digitally. This similarity makes our triple safe technology a perfect fit, helping organisations here to more easily and affordably stop data leaks happening through human error and unauthorised access. Our integrations allow workers to use their normal email environment, such as Outlook and Gmail, and the strong encryption and two-factor authentication we apply - across all outbound email and file transfer content – minimises security risks still further. Finally we give organisations, who hold the legal responsibility to prevent, identify and limit the impact of data leaks, the controls and reporting tools needed to be in control of their digital communication via email and file transfer.”

ZIVVER’s UK team comprises Chris Brown, VP Global Sales (ex-Digital Shadows, Solera Networks); Richard Fridge, UK Sales Manager (ex-BlueFort Security); Darren Parker, Channel Manager EMEA (ex-Illusive Networks and ForeScout) and Melanie Dawes, UK Marketing Manager (ex-CloudCall and Winshuttle). ZIVVER works exclusively through local security resellers in the UK and is currently formalising partnerships

with several VARs, as well as a value added distributor. It will unveil its channel program for the UK shortly.

The risks of sending emails and file transfers – and how ZIVVER solves them:
There are three different phases to consider when sending emails and transferring files; before, during and after. ZIVVER's solution is unique in its ability to mitigate the risks attached to all three, i.e. the entire communications process, while retaining email's user-friendliness. Here's how:

Before sending
• RISK: Human error, e.g. a worker sending information via email to the wrong person.
• SOLUTION: ZIVVER's technology helps to eliminate human errors by alerting users before they send an email about possible errors. E.g. that an email contains sensitive information (e.g. 'Your attachment X contains social security numbers, are you sure you want to share this?'), is addressed to an unusual recipient (e.g. 'You've never shared medical information with John Doe before, are you sure this is the correct recipient?') or is sent to a large number of recipients whose contact details will be exposed (e.g. 'You are sending this email to 50 recipients; maybe you want to use BCC for this?'). This feedback to users both raises their awareness and also reduces the likelihood of misaddressed emails, unintended sharing of sensitive information and sending sensitive information insecurely.

During sending
• RISK: Unauthorised access to sensitive data.
• SOLUTION: ZIVVER applies strong encryption and strong authentication (e.g. via a SMS text message or TOTP-code) across all email content (ZIVVER's key management policy ensures it never holds the data owner's keys, nor can it give access to third-parties, yielding better data access restraints than Google and Microsoft, for example).

After sending
• RISK: Identify and limit the impact of a potential data leak, e.g. damage to an organisation's brand and reputation, finances (including a possible GDPR fine) and customer churn.
• SOLUTION: ZIVVER provides real-time logging allowing organisations to identify real-time risks and potential data leaks. It limits the impact of data leaks by allowing senders to retract messages and then also show if the message and attachments were accessed, and by whom (audit logs). When retracting a message, ZIVVER guarantees that access by all recipients is no longer possible. Via this logging capability, users and organisations are able to assess the impact of a (potential) data leak, which is what GDPR and similar legislation requires.

Due to its three-in-one capability, ZIVVER is the most cost-effective outbound email security and file transfer solution available to UK organisations. From single users to 10,000+ employees, ZIVVER has product and pricing bundles to suit all sizes and sectors - from local government and healthcare, to accountants and legal firms – with ease of use and implementation proven factors in its success.

About ZIVVER
Co-founded in the Netherlands in 2015 by Rick Goud, Vincent van Donselaar and Alwin Schoemaker, ZIVVER provides outbound email and file transfer security to help public and private sector organisations prevent data leaks, improve compliance and save costs from ineffective communication via fax, snail mail

and courier. It is the only vendor in the market to offer a complete outbound email and file transfer security solution, tackling all three phases (before/during/after). In the last two years ZIVVER has secured 2,500 organisations as customers - including 20% of the Dutch healthcare market and 30%+ of local government - and has grown to 90 employees. In 2018, ZIVVER raised $12 million in funding in a transaction led by SaaS specialist Dawn Capital with participation from DN Capital and existing investor henQ Capital Partners.

For more information visit https://www.zivver.eu/ and follow us on Twitter (https://twitter.com/ZIVVER_EN) (@ZIVVER_EN) and LinkedIn (https://www.linkedin.com/company/zivver)

UK media contact:
Sally Bratton
Bratton PR
sally.bratton@brattonpr.com
+44(0)7930 301601