WHITEPAPER

Improve your **Office 365** security with **ZIVVER** to reduce data leaks, boost compliance and save on costs

Organizations are increasingly adopting cloud-based email systems. Gartner expects 70% of public and private companies to be using cloud email services by 2021[1]. When moving to the cloud, organizations are forced to (re)evaluate their privacy and security guarantees, data leak prevention (DLP) controls and measures to ensure compliance.

For large corporations and enterprises, Microsoft Office 365 is by far the most popular Cloud Office Solution, mostly because of its focus on security and threat protection capabilities. However, organizations that have high security or privacy demands are still reluctant towards migrating to Office 365. This is because specific encryption, authentication and DLP functionalities are lacking or are deemed insufficient. In addition, Office 365 customers increasingly report difficulties in configuring and maintaining the various, separate modules that are security and privacy related[2].

Most of the security and DLP functions Office 365 offers are only available in E5 license, which are considered costly. However, many organizations can generate a positive business case just by choosing the much cheaper E1 or E3 licenses, used in conjunction with ZIVVER. This is often considered a lower cost and more comprehensive email communication security solution.

Gartner

According to Gartner, organizations increasingly choose a so-called cloud email security supplement (CESS) to address gaps in the capabilities of either an incumbent secure email gateway, Office 365 and Google. We will outline why many organizations are opting to use ZIVVER as a CESS in combination with Office 365.

[1] Gartner 2019 Market Guide for Email Security https://www.gartner.com/document/3938516
[2] https://www.gartner.com/reviews/market/email-security/vendor/microsoft

More comprehensive and user-friendly DLP functionalities

DLP functionalities are required to make sure that sensitive data does not leave an organization via an incorrect method to the wrong individual. To understand what is specifically required of DLP functions, it is essential to look at causes of reported data leaks, as these incidents provide the best understanding of the risks that should be mitigated.

Looking at the causes of the about 14.000 data leaks reported to the ICO in 2019 for example, reveals the following:

Non-cyber related	74,4 %
⚠ Data sent to incorrect recipient	39,1 %
⚠ Wrong data sent to recipient	9,4 %
⚠ Use of To/CC instead of BCC	4,5 %
⚠ Loss/theft of information carrier	21,3 %

Cyber related	25,6 %
⚠ Unauthorized access	6,4 %
⚠ Phishing & Malware	17 %
⚠ Ransomware	2,1 %

From the causes above, the following should/can (partially) be addressed with DLP functionalities:

- **Preventing data sent to incorrect recipient:** These data leaks are often caused by sending an email to someone with a similar name and the auto-complete functionality kicking in. These data leaks can only be effectively prevented by tools that can detect unusual behavior and inform the sender about any anomalies before sending. For example, a tool that can detect when sending a particular type of information to a specific recipient is abnormal. This means that the tool must be able to auto-classify data that was sent in emails and files and relate that to different recipients in a so-called 'social graph'.
- **Preventing wrong data sent:** These data leaks are mostly caused by sending files that contained sensitive information the sender was unaware of that should not have been sent. Think for example of a case where someone adds patient social security numbers to an Excel file, while there are employee salaries still listed in Worksheet 2. These data leaks can only be effectively prevented with tools that can auto-detect sensitive information, also by scanning attachments, and inform the sender about this before sending.
- **Preventing use of To/CC instead of BCC:** These leaks are mostly caused by employees needing to share sensitive information with a large group of people independently, but do so by using email's To or CC field instead of BCC, thus exposing the identity of all recipients. A devastating 2019 example was when an NHS clinic sent out a newsletter email to its HIV patients but failed to use the BCC option[3]. Prevention requires tools that warn senders when sensitive information is about to be sent to numerous recipients, recommending to move those recipients to BCC.
- **Preventing unauthorized access:** One of the causes of these types of leaks is when employees/organizations "forget" to apply (proper) email protection in terms of encryption and authentication for a specific message. Proper email protection is, and will probably never be, done smoothly in cases where an email is being sent to a recipient that does not support the same (level) of protection. This results in a situation where most organizations tend to favor the recipient experience over security needs and let their employees decide when to protect an email. Sending the message securely often entails clicking on a button somewhere on a different tab in Outlook. Preventing these data leaks necessitates software to help employees select the proper security measures. This can be done via alerts or by automatically applying the company policy upon sharing sensitive content.

[3] *https://www.pressandjournal.co.uk/fp/news/highlands/1852746/probe-into-nhs-highland-hiv-data-breach-revealed/*

What DLP functions Office 365 has and lacks

Office 365 offers various separate products that can help organizations protect their information like Azure Information Protection (AIP), Data Loss Prevention Policies (DLP policies), Policy Tips and Office Message Encryption (OME). However, organizations have found these tools to have the following drawbacks:

⚠ **Unable to prevent misaddressed emails:** Microsoft's tools do not analyze relationships between the type of information being sent, the recipient or the sender's prior behavior patterns. This means they cannot detect unusual recipients, given the type of information being shared. Microsoft can only give warnings like "This email contains information of type X" or "You are about to share information outside of your organization", which is not sensitive and specific enough, leading to alert fatigue.

⚠ **Does not help to ensure the proper use of BCC:** Microsoft provides no functionality to help users identify and prevent these kinds of mistakes.

⚠ **Does not help users to apply the appropriate protection:** Microsoft's policy tips can only be used to notify the sender, not helping to (auto-)apply the appropriate security measures. To protect a message with OME in Outlook Desktop for example, the user always has to click a different button in a submenu of one of the tabs. OME can be configured to apply OME-encryption server side. This, however, is considered complicated, time consuming and limited in effectiveness due to rule limitations.

⚠ **Unable to retract messages and see read status:** With Microsoft it is not possible to effectively retract messages. Outlook provides this possibility, but gives no guarantees and does not work with other email clients. In addition, there is no possibility to see who read the message or accessed the attachments, meaning organizations cannot assess the impact of a data leak.

What DLP functions ZIVVER adds

ZIVVER provides a solution to all the things that are insufficient, complex or lacking in Office 365.

✓ **Detecting unusual recipients:** ZIVVER real-time classifies data when users compose a message, allowing to detect that sending a particular sort of information to a specific recipient is abnormal. This notifies users about this 'unusual behavior' before sending, while typing emails in clients like Outlook.

✓ **Suggest using BCC:** ZIVVER warns users when they are about to send information to numerous recipients in To or CC, prompting if necessary to move them to BCC.

✓ **Help users apply appropriate security measures:** data is classified in real time when composing a message, prompting users to select email encryption and the proper authentication settings (like applying 2FA-protection with SMS) as needed.

✓ **Retract messages and see read status:** ZIVVER enables users to retract messages at any time, while confirming recipients' status of accessing the message and attachments. If users retract a message and ZIVVER indicates it was not yet read, there is a guarantee that it did not result in a data leak. If someone did have access before the message was retracted, ZIVVER shows who it was and what they accessed, allowing the user and organization to understand the impact of a potential data leak.

Better encryption guaranteeing zero-access by third parties

Organizations dealing with very sensitive data want to protect their information as best they can. Usually encryption plays a vital role in this. Nowadays most cloud-based email solution providers, such as Microsoft, use encryption. With encryption, the biggest challenge lies not in applying it, because that has become easier and better. The real challenge actually lies in key management; who has access to the keys that can decrypt information?

As an organization, you want to ensure that only authorized persons can access the information.This includes the sender, recipients as well as possibly administrators from your organization, in the event of forensic investigations, for example. This by design excludes your service provider, as they would pose an additional risk, be a potential target for hackers and would be subject to governments/intelligence agencies' inquiries.

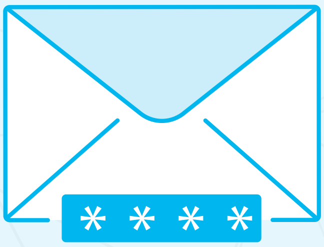
What encryption Microsoft offers

Office 365 by default stores messages and files encrypted. However, Microsoft always holds (a copy of) your keys in its possession/infrastructure, even when using Office Message Encryption and Bring Your Own Key (BYOK). On its FAQ-page Microsoft states:

> Does Office 365 Message Encryption and Bring Your Own Key with Azure Information Protection change Microsoft's approach to third-party data requests such as subpoenas?
>
> No. Office 365 Message Encryption and the option to provide and control your own encryption keys with Bring Your Own Key (BYOK) for Azure Information Protection was not designed to respond to law enforcement subpoenas.

What ZIVVER's encryption layer adds

ZIVVER uses best-in-class (asymmetric) encryption for the transport and storage of emails and files. Even ZIVVER cannot access your data that is stored on its platform as it does not have access to a users' keys to decrypt the information. Therefore your sensitive data is also kept safe from third parties. Confidential is truly confidential.



More privacy protection guarantees

Organizations in the EU have been required to comply with GDPR since May, 2018. This includes making sure they select suppliers that comply with GDPR and sign a GDPR-compliant agreement with processors of their privacy sensitive data.

What are the privacy concerns with Office 365?

After privacy concerns raised by various parties, Microsoft and Office 365 are currently under investigation by the European Data Protection Supervisor (EDPS). In anticipation of this, the Swedes recommended that public providers not use US-rooted web-based SaaS products such as email, and in some German states it is now illegal for schools to use Office 365.

How ZIVVER manages privacy

ZIVVER operates with stringent privacy controls. This varies from not being able to access sensitive information, only storing an organization's sensitive information in data centres in the EER, plus signing GDPR-compliant processor agreements with every customer. ZIVVER also enables its platform, including code and the company itself, to be inspected multiple times a year by independent legal/privacy experts, alongside technical experts at Deloitte. Having these privacy and security controls in place is unique and is one of the reasons why security-minded organizations such as the Dutch Court system use ZIVVER as their solution for secure email.

Better authentication of recipients

Email by nature lacks any form of user authentication. Strong authentication of users is, however, crucial in assuring that only authorized persons have access to sensitive information. That is why banks, healthcare organizations and 'even' WhatsApp nowadays use two-factor authentication, e.g. via an additional SMS-code, to verify a persons' identity.

What recipient authentication possibilities are offered by Office 365

Office 365 itself has no way to authenticate recipients outside of your organization. Using Office Message Encryption (OME), recipients can be authenticated by receiving an initial notification email with a link followed by a second email with a temporary access code. Using this does mitigate active and passive man-in-the-middle effects, both authenticate a user, as anyone having access to a mailbox can read that information. A more robust form of recipient authentication is lacking.

How ZIVVER adds two-factor authentication for recipients

ZIVVER provides out-of-the-box support for senders to authenticate their recipients with two-factor authentication (2FA), using SMS. ZIVVER will, in that case, automatically send an SMS code to the (mobile) phone number that the sender provided. In the event that the recipient was previously emailed by the organization, contact details are already available in Outlook or contact details were imported in ZIVVER by admins, e.g. from another system, the sender doesn't have to do anything. If no phone number is available for the recipients, ZIVVER provides fallbacks in the form of an organization-standard access code. This standard access code will be the code recipients need to enter for every message received from the organization, a sender-access code recipients will need to enter for every message from the specific sender. In addition, ZIVVER also provides the option of working with a verification email and delivering emails via the DANE email security protocol. This option will, however, provide no user authentication.

Easier to set-up and maintain

Organizations and resellers strive for optimal cost-effectiveness in the installation, configuration and maintenance of software solutions. This is fairly self-explanatory; everyone wants to save on costs.

Setting up and maintaining Office 365 security and privacy tools

As described, Office 365 has various tools that work separately but should be combined to attain the best possible security and privacy protection controls. Setting up AIP, DLP policies and OME has however been found to be complicated. On the one hand it is because of the complexity of the tools, otherwise organizations need to think of and create all rules, triggers and policies themselves. This can prove to be time consuming, complex and prone to error, usually also resulting in rules that do not align with the end-user behavior. Managing and improving settings are considered (too) cumbersome and time consuming.

How installing, configuring and maintaining ZIVVER works

ZIVVER was built with an understanding of existing tools and the infrastructure of organizations in mind. This resulted in it being easy to install and set up within hours, alongside a low effort to maintain, plus there is no need to buy additional software or hardware. Configuration is also easy. ZIVVER provides off-the-shelf business rules, developed, validated and maintained by ZIVVER, adapted to different markets and organization types. ZIVVER can synchronise users with the organization’s Active Directory and authenticate them via SAMLv2 compatible Single Sign On (SSO) providers like ADFS and OKTA. This all results in very low go-live and maintenance efforts.

More cost-effective

Costs are always important for organizations. It is, however, better to look at a business case as opposed to costs. This is due to the fact that securing an organization's emails often result in a very positive business case because it can, among more things:

- Reduce costs of data leaks, according to IBM[3], on average £4 million per breach
- Increase employee productivity
- Reduce costs of sending letters and using mail couriers
- Improve a company's reputation

Costs of Office 365 security and privacy tools

Being able to use the various security and privacy tools that Office 365 offers typically requires buying E5 licenses for all employees, which many organizations consider to be too expensive.

Business case for securing your communications with ZIVVER

The business case for ZIVVER is usually a positive one. One part is the various value drivers for secure email previously outlined; ZIVVER can help to significantly reduce data leaks, can be used to send digital letters in bulk from source systems, helps users to be productive and avoid the need to walk to fax machines or printers while also demonstrating to partners that the organization takes privacy and security seriously. In addition, as ZIVVER supports sending files up to 5.000GB as 'attachments', the costs of existing file transfer solutions, including USB sticks and DVDs, can be reduced too. Finally, many organizations generate a positive business case simply by, instead of opting for E5 licenses, choose E1 or E3 licenses and then use in conjunction with ZIVVER. For most organizations, this is a more cost-effective and comprehensive email communication security solution.

[4] *2019 Cost of a Data Breach Report. https://databreachcalculator.mybluemix.net/*

ZIVVER helps to prevent data leaks, improve compliance, and supports a positive business case when combining the service with Office 365. This is especially important for organizations priding themselves on safeguarding sensitive data. ZIVVER's data leak prevention controls are more comprehensive and found to be easier to use, set up and maintain. The encryption and authentication that ZIVVER provides guarantees zero-access to third parties in a way that other cloud solutions, including Office 365, cannot offer. This helps to simplify compliance with GDPR-like legislation on this topic. With an NPS score of 47 and a 4.8/5 on **Gartner Peer Review**, ZIVVER proudly provides safe communication to thousands of companies worldwide by adding a security and privacy layer on top of their existing email solutions such as Office 365.

Gartner

4.8 ★★★★★

☎ +44 (0) 203 285 6300
@ sales-uk@zivver.com
www.zivver.com

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