zivver

Nine reasons why security leaders need to re-evaluate email security

Knowledge Article

In September 2020 Gartner released an update of its Market Guide for Email Security. The report begins by stating that “Dramatic increases in the volume and success of phishing attacks and migration to cloud email requires a re-evaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for the changing landscape”. Where traditionally the focus with email security was on protecting against phishing and malware attacks, it has become increasingly clear that this is no longer the biggest challenge. The new big challenge is email data protection.

This article will outline the why, what and how of the nine challenges organizations face to adequately protect data while still using ‘normal email’:

01. Prevent mistakes before sending emails and files
02. Prevent interception of email data
03. Prevent access by vendors and other third parties
04. Prevent unauthorized access after delivery
05. Limit and understand the impact of a mistake
06. Ease of use for employees
07. Ease of use for guest recipients
08. Easy to install, set-up and maintain
09. Have a positive business case

Why is email data protection your biggest challenge?

Email is still by far the most widely-used method for businesses to communicate. On average, employees spend roughly 2.6 hours dealing with 120 business emails per day. With an expected yearly growth of more than 4%, email will dominate how organizations communicate for at least the next decade. However, with new compliance and regulation requirements, an increasing number of data leaks and evolving cyber threats, a greater emphasis is now being put on email data protection.

Gartner analysts explain that: “Email was never designed to be a secure communication medium, and organizations continue to struggle to protect sensitive email content in transit and at rest. Email data protection products protect the confidentiality and integrity of email messages by enabling the transmission of sensitive information to intended recipients with the starkly reduced possibility of disclosure or alteration.”

So the combination of the vast and still growing popularity of email, alongside the fact that ‘traditional’ email was not built to mitigate the associated risks, makes email data protection one of the biggest challenges organizations are facing today.

2.6h

Average time employees spend on emails daily

4%

Expected yearly growth of email over the next decade

What are the challenges with email data protection?

To be able to improve email security, you first need to understand the challenges.

Email security can be separated in three main categories:

- Threat protection; help to mitigate phishing, spam and malware attacks
- Email data protection; help to protect from unauthorized access to data sent or received by e-mail
- Brand protection; help to ensure organization's email cannot be "spoofed"

Brand protection is mainly about implementing DMARC to avoid spoofing. As this is quite straight forward, this article focuses on explaining the difference between threat protection and email data protection.

The image below shows that email data protection involves various touchpoints at each stage of the communication's journey. This includes the process before, during and after sending an email, as well as upon receipt of an email (a reply for example). Email threat protection, however, strictly entails the process of receiving email. That's why email data protection is so much more difficult than threat protection.

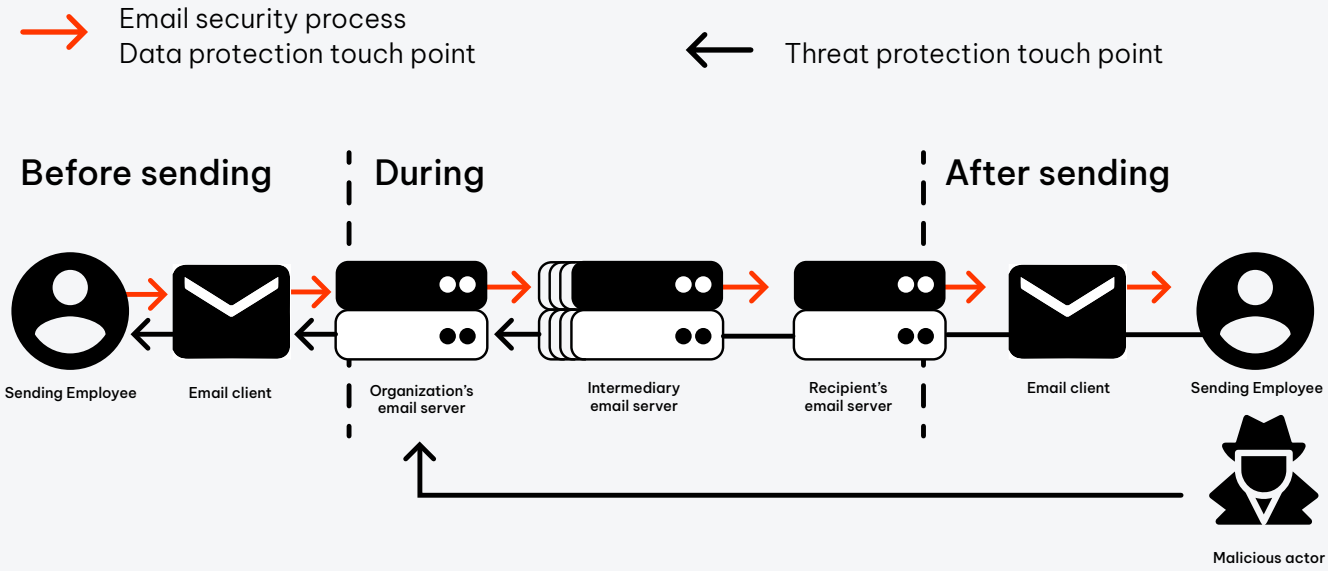

Figure 1: Schematic outline of the email process including security touchpoints

On the next page we describe the challenges with email data protection that organizations are looking to solve by using supplements or specialists that can enhance the security of Office 365, Gmail and other gateway based email systems in use by organizations.

01

Prevent mistakes before emails and files have been sent

Data leak reports across the world show that most data leaks are inadvertent mistakes made by employees, and usually stem from the following:

- Misaddressed emails: Sending information to the wrong person. Usually caused by the auto-complete feature of email clients where a previously addressed recipient was erroneously selected for another. This type of situation accounted for over 70% of reported data leaks in the United Kingdom in 2020.
- Failure to redact: Sending sensitive information that should have been omitted. Examples include 'forgotten' social security numbers in a separate worksheet of an Excel file, or a PowerPoint presentation containing patient names. This category of breach accounted for 5% of the known causes of data leaks reported to the ICO in the United Kingdom in 2020.
- Failed to use BCC: Putting recipients in To/CC and unintentionally exposing their identity. An example of this scenario is an NHS Trust who was emailing a newsletter to HIV patients, but exposed the entire distribution list by putting all recipients in CC instead of using BCC. This category represented 8% of the known causes of data leaks reported to the ICO in the United Kingdom in 2020.
- Failed to add proper message protection: Not protecting the information according to company policy. Some companies ask users to manually add a password to a PDF or ZIP file, for example, and text that password to the recipient. Some organizations have more user-friendly tools. Not properly adding the protection advised by the company can result in unauthorized access. The 'Unauthorized access' category accounted for 8% of the known causes of data leaks reported to the ICO in the United Kingdom in 2020.

Really improving email data security means helping your employees catch mistakes before they hit send. For this you need solutions that help people select the correct content, for the right recipient and with the appropriate security measures, every time. Some tools claim they 'prevent human error', but most are unfortunately not sophisticated enough and result in too many or too few alerts. This only addresses (partially) one of the errors above and such tools are not enabling for users, being either too invasive or too discreet.

02

Prevent interception of email data

Preventing interception of email data requires basically two things, 1) ensure email data is (properly) encrypted during transport (in transit) and 2) ensure encrypted data is transported to the intended destination (recipient's email server). This results in the following key challenges:

- Ensure data is properly encrypted: Secure email transport via STARTTLS is considered a very basic security measure. Surprisingly enough, in 2020, 12% of emails were still sent unencrypted. Even though enabling TLS nowadays should be one click away, this doesn't solve the problem, as there's a dependency on the recipient's server settings. Plus, STARTTLS is a so-called opportunistic protocol, meaning it tries to deliver an email encrypted, but if that's not possible it delivers the email unencrypted regardless. Although enforcing encryption is possible, this is not a solution as email has no fallback mechanism to deliver messages in that situation, meaning messages will not be delivered. This is naturally undesirable for most businesses. For this reason, adequate encryption of data remains a challenge.
- Ensure encrypted data is transported to the correct destination: Many organizations think that the aforementioned STARTTLS is the solution to effectively prevent interception of data. However, this only ensures encrypted transport, and not the actual delivery to the intended server. Various types of Man-in-the-Middle attacks can exploit the vulnerabilities of the transport of an email from point A to point B. This can result in an email being delivered to the server controlled by an attacker instead of the server of the intended recipient. This problem can only be solved by delivering emails using DNS-based Authentication of Named Entities (in short: DANE). Most big vendors, however, do not yet support DANE. Microsoft announced that they would support DANE by the end of 2021, Google has not made such an announcement yet.

To really improve your email data protection, you need to prevent the possibility of sensitive email data being intercepted. As encryption and ensuring correct delivery remains a challenge throughout the world, the current email solutions are not able to adequately prevent the possibility of sensitive email data being intercepted.

12%

emails still sent unencrypted in 2020

03

Prevent access by vendors and other third parties

Most organizations don't want third parties to be able to access their data. That is why they often ask vendors: 'Do you encrypt my data?'. The answer to that question is usually yes. This is actually not the right question to ask, as encryption is generally not the primary concern and many solutions will provide some form of encryption.

It is, however, essential to understand what happens with regards to key management -- who holds access to your organization's keys and thus to the data (as they will be able to decrypt the data)? The question to ask should therefore be: 'do you encrypt my data and can you ensure that only my organization and my recipients have the key to decrypt the data?' The ideal outcome is that only those that you want to have a specific key can have access to (part of) your data and no one else.

The answer to that question, however, is unfortunately almost always 'No', which makes the solutions provided by those vendors:

- Vulnerable to insider threats. We all understand the risk of that since the recent Twitter hack.
- Attractive to hackers. As there is often a single place where the keys to a lot of sensitive data is stored.
- Subjective to governmental data requests. As keys are available to the vendors, they can (and must in some countries) decrypt and share your data with governmental organizations upon request, without your involvement. With the recent invalidation of Privacy Shield, this should be of particular concern to many more companies.

Really improving your email data security requires preventing access by vendors and other third parties like hackers and governments. This means working with solutions that don't have access to your keys or the keys of the people you shared data with.

The most widely-used cloud email products, including Microsoft Office 365, Google, Mimecast, Egress, etc, all still retain access to your keys and data. There's a simple way to test this. If you have a solution with an account you've created, go through the 'Forgot password' flow. Can you still access your old messages and information after it's been reset? If so, how did the provider give you access to your old information while you misplaced your key? That is because the vendor, in this case, holds your keys.

04

Prevent unauthorized access after delivery

Two-factor authentication (2FA) is one of the most important measures to take when it comes to protecting your data. 2FA ensures that logging in with (usually weak) passwords is not sufficient to access information, because it requires something you have, like a mobile phone to get an additional code from either an authenticator app or SMS. 2FA is the only way to ensure that strictly the intended recipient can access the account and data. That's why it's needed for bank transactions, to access medical records, and even when Whatsapp is installed on a new device nowadays. With doctors sending sensitive medical information to a patient, or a lawyer discussing a sensitive lawsuit with a client, you also want to ensure that only the intended recipient can access the data, right? In these circumstances, you must actually ensure that's the case. Under the GDPR, organizations must be able to prevent unauthorized access. And 2FA is currently the only way to do so.

Therefore really improving your email data security entails being able to ensure authorized access to sensitive messages. This means protecting messages with 2FA, where the sender is able to determine if and with what second factor the recipient should authenticate themselves, before being able to access (sensitive) information. However, with most email systems you're not able to protect your messages with 2FA. Not Microsoft Office 365, not Mimecast, nor any other big vendors, except for Google that enables users to do so with its 'Confidential mode'. This, however, has limited functionality and suboptimal usability for the sender and recipient.

05

Limit and understand the impact of a mistake

Even with the most advanced Data Leak Prevention (DLP) systems, mistakes will happen occasionally. When they do occur, you naturally want to take all possible actions to mitigate their impact. When reporting a data leak to authorities you must even explicitly state which remedial actions you have taken to address the issue. For email, this would mean being able to revoke access to the relevant messages. In addition, you should be able to identify who already accessed each message and/or attachments to assess the potential impact of a mistake and who to reach out to. Finally, you need to be certain that after revoking access, anyone who didn't view the message yet is no longer be able to do so, as otherwise, the measure taken holds no value.

Really improving your email data security entails being able to limit the impact of an email mistake. This requires being able to effectively revoke messages and have visibility of the recipient's read status. These functionalities are not available with most email systems. With Outlook you can revoke a message, but you can't tell if it's successful or assess who may have already viewed the message, which defeats the purpose. With Office 365 OME only admins can retract messages via PowerShell, but only for recipients who did not receive their email in Outlook Desktop and Office 365, without actually knowing what the recipients are using. Therefore, this is not user-friendly and hardly effective. Most other solution companies don't offer this functionality either.

06

Ease of use for employees

Using a security solution should be as easy as possible for your employees. The GDPR even stipulates the need for data protection by design and default. If you make email data security (too) complex, (too) user-unfriendly, (too) workflow invasive, your employees won't use it and consequently the intended security of your data is compromised. Too often, solutions are bought that 'check the boxes' but don't solve any 'real world' problems, now that they are or will not be used by employees as they are too cumbersome or too invasive. It is naive, however, to think that a security solution will not impact users at all. Users will be required to take additional measures, like entering a mobile phone number to protect data with an SMS code. Users will be interrupted with in their workflow if they are about to make a possible mistake. The challenge for email security products is to make it as user-friendly as possible and let users understand they are helping them instead of bothering them.

This means that really improving your email data security requires solutions to be as user-friendly as possible, aiming to get as close to security by default as possible. With current solutions, this is however still not the case. Looking again at OME for example, the Microsoft website says: "To send an encrypted message from Outlook 2013 or 2016, or Outlook 2016 for Mac, select Options > Permissions, then select the protection option you need." This means that securing a message from Outlook is three clicks away, as it is in a sub-menu of a separate tab. Other vendors work with unannounced pop-ups that appear after hitting the send button to check for possible errors. Or they may ask senders to confirm the recipients and attachment. As the pop-ups are interfering with workflow (you thought you were ready when hitting the send button) users will often get frustrated. If messages are not sensitive and specific enough (why always ask for confirmation of recipients and attachments for an email you just sent moments ago?) users will also get annoyed and develop alert fatigue, resulting in zero effectiveness and total frustration.

07

Ease of use for guest recipients

When using email, often the goal is not only to provide information to the recipient, but generally to also interact with them. You hope or expect a response, or even to start a dialogue with them. Reading secure messages sent to recipients who are not using the same system and/or same standards as the sender, requires those recipients to retrieve the message from the same system used by the sender. This is often referred to as a message portal. That is really the only way to sufficiently protect messages, thus ensuring proper encryption and authentication, sent to these so-called guest recipients. To create the desired dialogue with these guests, their user experience in this portal environment is key. Such a portal should ensure that guest recipients can easily read and respond to the message, download any attachments, forward it, archive the communication, etc. If the solution does not offer this ease of use, recipients are less likely to read or respond to your message, and are inclined to ask your employees to send the information using 'normal email', which they will most likely do. This would subsequently result in your organization's security being compromised, as well as a failure to comply with the legal obligation to protect sensitive data adequately.

Really protecting your email data entails providing recipients with a convenient and positive user experience while maintaining security. This means that you should not force recipients to create an account, as it's an inconvenience for simply reading a message. This would also potentially result in low security, since recipients that are forced to create an account are likely to choose weak passwords so they can remember them. Recipients should, however, be able to create a (free) account. This is helpful when receiving numerous secure messages from multiple organizations per month, for example, so there's no need to authenticate yourself for each message. For that you want an account that allows you to easily read, reply, forward and even to initiate your own secure messages. However, most vendors either force recipients to create an account or don't offer the possibility to create one at all, resulting in a suboptimal recipient experience with the consequences outlined above.

08

Easy to install, set up and maintain

This one should be a no-brainer. You don't want to purchase additional hardware, upgrade your infrastructure, buy specific licenses or be forced upon migrations to Azure AD or Office 365 before being able to protect your email data. Just as you probably want to avoid spending months on a project to define your own domain model, data loss prevention and compliance rules, and configuring the system. This will result in faster implementation, higher adoption and thus quicker and better email data protection in your organization. Finally, keep maintenance low by syncing users from your Active Directory, integrate with your Single-Sign-On provider, leverage group policies for user settings and export log data to your SIEM system.

Therefore really protecting your email data as soon and comprehensively as possible means selecting an email data protection product that fits on top of your current infrastructure. Ideally one that blends in with your existing software and maintenance policies. It should provide as many out-of-the-box configurations, domain models and rules as possible to ensure you can be up and running in a few days instead of several months. Most vendors are not plug-and-play though, often require manual account provisioning, and can be complex to manage. For example, Office 365 customers increasingly report difficulties in configuring and maintaining the various, separate modules that are security and privacy-related (AIP, DLP, OME, Policy Tips).

09

Have a positive business case

Down the line, especially in these COVID-19 times, it's about justifying investment with a business case. Does the value that a solution adds or the savings generated outweigh the investment costs? This is better known as the return on investment (ROI). Still, a lot of solutions lack a clear value proposition or are perceived as expensive. Buying decisions can quickly fail at board level if the project team can't adequately underpin the positive business case of a solution, plus explain how the solution supports business goals. After hard work, long selection projects, much time and consequently money spent by the organization, the security risks unfortunately remain.

Thus really protecting your email data entails being able to present a positive business case to the board. This should clearly outline what the business requirements are and how the solution helps to meet those needs as part of the organizational strategy. How vendors help organizations to underpin and really demonstrate value differs greatly. As does the price. Many organizations see the E5 license that contains the Office 365 Advanced Threat Protection capabilities as very expensive. See and present email data protection as a value instead of a cost to your business.

Why do you need an email data protection specialist?

Very few, if any, of the aforementioned challenges with 'normal email' can be adequately tackled with existing email gateways that organizations have in place today. That's because most solutions in place focus on threat protection to keep out phishing, spam and malware, and not on email data protection. Although some solutions claim they do, organizations find that they provide only a small piece of the puzzle and usually in a non-user and/or non-recipient friendly way. Even for the big vendors like Office 365 and GSuite many organizations are referring to so-called Email Data Protection Specialists to address the issues we've outlined in this article.

Gartner named Zivver as one of five global representative Email Data Protection Specialist vendors. Zivver is the only vendor that provides features to address all nine challenges outlined here. Zivver enhances an organization's current email infrastructure by fitting on top of it. Use the service with existing email clients (Outlook, Gmail, OWA) to help employees make better decisions when handling sensitive data and avoid the most common types of data leaks by human error. This is further aided by strong encryption when data is in transit or at rest with zero-access guarantee. Additionally, the service provides out-of-the-box business rules and recipient authentication. All this makes installation, implementation and maintenance realistically achievable in a matter of hours or days, instead of months.

Finally, working with email data protection specialists can actually reduce costs. Products like Zivver are significantly cheaper than upgrading from Office 365 E3 to E5 licenses with better email data protection. What's more, having these products in place enables you to reduce costs of file transfer solutions and even cyber security insurance costs. The ROI usually lies between 2x-8x. And if you include reducing the use of letters, faxes and couriers the ROI is easily in the double digits. If all of the above is not enough to at least consider working with an email data protection specialist, what is?

Zivver
5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300
contact@zivver.com

www.zivver.com