Alinto

White Paper

Email: the weak link in Office 365?

Summary

Introduction

Digital transformation is more than ever at the heart of companies' concerns. Each organisation is rolling out dematerialisation projects, process redesign, digital workplace, collaborative spaces, etc. In most companies, this involves **the deployment of Office 365, now called Microsoft 365**.

But technology remains a formidable playground for cybercriminals. Among the different forms of attacks, there are **ransomware, spam or phishing emails...** These are serious threats for companies, which can have serious consequences on their business.

Very often, these attacks come from fraudulent emails. And Outlook, from the Office 365 suite, is not spared. What solutions - Microsoft or others - are available for better security? How can you protect your email? Is it possible to be accompanied by a partner? We answer all these questions in our white paper.

Microsoft 365 adoption in companies: the state of play

Microsoft 365 is a suite massively chosen by companies for its numerous applications, its practicality and also the place it occupies on the market. However, after months of use, many organisations realise that these tools are little or poorly used. **The ROI is therefore not necessarily there**. In this article, we have decided to give you some figures and a report on the real adoption of Office 365 and the reasons for failure.

Office 365 adoption: the numbers

Microsoft's suite was launched in its current subscription-based form almost ten years ago. It brings together a number of applications that meet the daily and business needs of companies: the historical tools (Word, Excel, PowerPoint, etc.), and new web services (OneDrive, Yammer, etc.). In 2019, the Office 365 suite had **155 million active users**. It was renamed Microsoft 365 in early 2020.

According to a Forrester report, deploying Office 365 can generate a 162% ROI in three years. Provided that the suite is used properly. The Microsoft 365 Report study reports that **88% of IT decision-makers have fully deployed Microsoft 365 in their company**. According to an article in the JDN, 80% of CAC40 companies are equipped with it. The main reason for this choice is the flexibility of the offer to respond to the complexity of organisations.

However, the figures should be treated with caution. The Microsoft report indicates that most companies have not yet adopted the software suite in all its functionalities, particularly with regard to security. So when is a tool considered adopted? Is it just being connected to Microsoft? If so, 100% of users are using it, because they are connected to email. But effective adoption is more complex: it is when the transformation it brings about is real and concrete, with new collaborative modes for example.

Using Office 365: the most popular applications

In terms of usage, it is clear that despite the integration of Office in the cloud, **users are sticking to old practices**: creating documents locally, sharing files by email... Logically, users should do without email, at least to exchange or share documents internally. OneDrive allows you to generate secure sharing links. So they don't really take advantage of the suite's strengths.

In detail, the most used applications in the third quarter of 2019 are :

- Outlook / Exchange: **59 %**
- Equipos: **41 %**
- Skype Business: **23 %**

Vemos que a las aplicaciones verdaderamente colaborativas les cuesta despegar. Esto se debe a que muchos usuarios desconocen a qué aplicaciones tienen acceso (el 47% según el Informe de Microsoft 365), así como las ventajas que aportan.

Office 365 ROI: why is it stuck?

In reality, **the adoption of the Office 365 suite is not as obvious as the user companies would have us believe**.

Here are some figures that prove it:

- **34%** of users are reluctant to change
- **47%** do not know which applications they have access to
- **29%** lack time for training

Companies need to constantly monitor their teams' usage in order to support them in the right direction. And that's where the problem lies. Deploying guides to explain how to do things is not enough, you have to create scenarios, show and convince people of the benefits of the collaborative suite. It's about **starting a real internal transformation process**, and few companies do this. They consider that if users connect to their email and a few applications from time to time, it is a successful deployment. However, the ROI is not up to their expectations! And for good reason, the price of licences has increased by 10% in 2019!

For better adoption of Office 365, here are some tips:

- Putting the suite at the heart of the company's digital transformation
- Involve management by setting targets
- Management must also be a user of the solutions to set an example

While the adoption of Microsoft 365 is a quantitative reality, its "qualitative" adoption by corporate users is not yet optimal. Although the suite has all the qualities required for secure collaborative work on paper, it comes up against the obstacles put forward by users, which can **slow down the digital transformation process of organisations**.

Office 365: what does it change for email?

Email is a central tool for a company. If it breaks down, the whole business takes a hit! And if it doesn't have a BCP (Business Continuity Plan), it's quite a handicap.

In 2018, 56% of businesses were using the Office 365 suite (now Microsoft 365). In order to receive emails, these companies have to go through the Exchange server, which provides access to emails, calendar and documents stored on the servers. For reasons of simplicity, many organisations therefore choose to equip themselves with the publisher's end-to-end services. Often at the expense of security. This is what we will analyse in this article.

What are the email features of Office 365?

Outlook is the most widely used business email service. And for good reason, it has several key features:

1. Access **additional services**: calendar, task and note management, etc.
2. Create **custom signatures**
3. Checking **multiple mailboxes** simultaneously
4. Facilitating **collaborative work**
5. Send an email **from Word**
6. **Seamless integration** with other Microsoft office software
7. Improving **email security**
8. Accessing messaging in a **mobile situation**
9. Organising **folders and files**

However, there are still holes in the system, especially in the area of inbound and outbound email security. Microsoft's protection packages are not free, and many companies do not take up the option. As a result, many email systems have little or no security and are left in the hands of hackers, or at least vulnerable. The danger is accentuated with the massive and rapid introduction of teleworking: without a strict framework and **security software** (anti-spam, anti-phishing) for messaging, a company's entire activity is threatened by a simple email.

What are the alternatives to Office 365?

CIOs would like to reduce their dependence on Microsoft. However, replacing a link in the chain such as Exchange could make users' daily lives more fragile. And such a change is not easy.

Firstly, because Microsoft operates in a vacuum: all applications are interdependent and alternatives are not always easily interoperable. Companies therefore often take the "**Outlook, Exchange and Active Directory**" package to work, without looking for other solutions.

On the other hand, changes in tools generate constraints for users. Organisations therefore do not want to disrupt their habits.

However, there are alternatives to better protect email. It is possible to keep Outlook, for example, but to **choose another sending server than Exchange**. This is totally transparent for users, but allows for better email security and not being totally dependent on Microsoft.

Outlook email is very convenient, fully compatible with all Microsoft applications, thus enhancing collaboration. However, it is entirely possible to use external providers to integrate Office functionality and make it interoperable.

Office 365 deployment: how to ensure email security?

Ransomware attacks are on the increase and affect everyone, even small businesses. **These malicious programs are most often introduced through an e-mail**. Therefore, you should not take the aspect of securing your professional e-mail system lightly. In addition to making your employees aware of basic actions (not opening emails with strange objects or attachments, changing passwords regularly and not using the same one everywhere, etc.), other solutions must be put in place to **guarantee your IT security**.

In this article, we take a look at the current state of Exchange email security and give you our advice on how to protect your email.

Securing Exchange messaging: what figures and what issues?

Most ransomware attacks are opportunistic and take advantage of low levels of digital maturity in organisations. Since 2018, attacks have intensified and are increasingly coupled with other malware such as cryptovirus or other Trojan horses. This makes it easy for hackers to encrypt company data, as well as private data, and demand a ransom for access to your own data.

The damage to companies often goes far beyond the loss of a few data:

- stop of production
- fall in turnover associated with
- legal risks (e.g. with the RGPD)
- damage to reputation
- loss of confidence
- The gendarmerie also notes cases of suicides of employees following scams against the president.

In the guide “Attacks by ransomware, all concerned” published by the government, several companies testify:

- In November 2019, the **Rouen University Hospital** could no longer access a business application. The IT department then found that the workstations and servers had been encrypted. It was ransomware.
- In October 2019, the **M6 group** was subject to a ransomware attack, cutting off access to the internet, which is essential for radio broadcasts in particular.
- In April 2019, **Fleury Michon had** to cut off all employee internet access following a ransomware attack. Business came to a complete halt for three days and was degraded for a fortnight.

The starting point for these attacks is often an e-mail. However, the issue of securing e-mail, but also the entire IT infrastructure, is still not taken seriously enough. And the figures from a survey conducted by SoftwareONE prove it:

- **44% of respondents do not use Microsoft Intune** (mobile device and application management);
- **37% do not use Microsoft Azure Advanced Threat Protection** (advanced threat identification, detection and investigation);
- **36% do not use Microsoft Azure Information Protection** (document protection).

There is still progress to be made in countering threats and anticipating attacks.

Email protection: our three tips

To reduce the risks and protect your business, there are several actions you can take. However, if we were to give you our top tips, we choose the following three.

1 Raising awareness among your employees

Malware attacks often originate from emails received by an employee. It is therefore essential to **remind employees of good practices and to instil reflexes in their use of email**: do not open suspicious objects or attachments or those from unknown recipients, report any problems to the IT department, etc. This is not an absolute defence, but a necessary step in reducing the risk of attacks.

2 Securing your IS

Of course, it is essential to secure your information system. This involves managing access rights to applications, partitioning the IS to limit the risk of propagation to all workstations, keeping the various applications up to date, as this improves their security, and regularly backing up your data.

3 Opting for email protection solutions

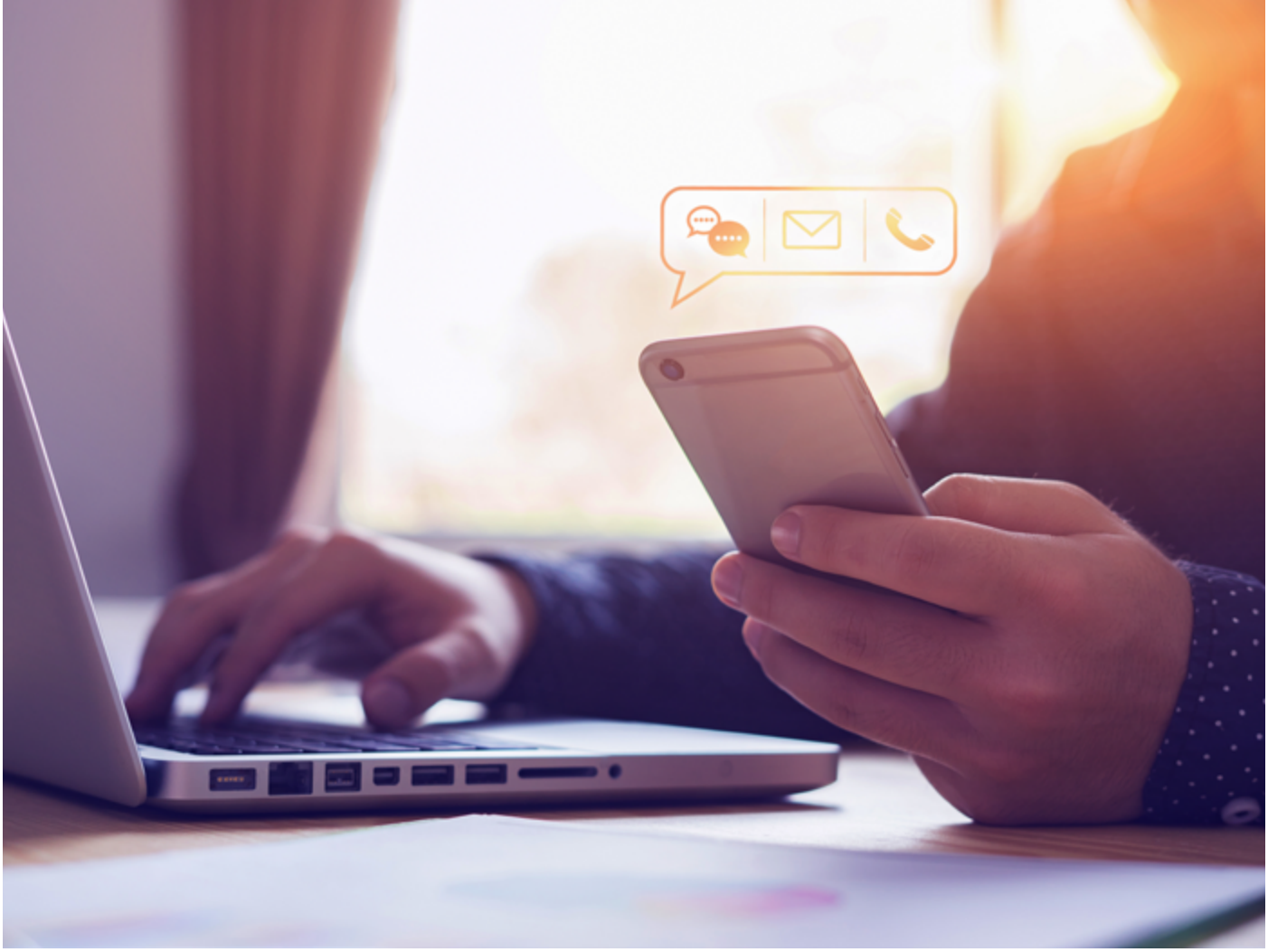
Finally, for maximum security of your emails, it is important to equip workstations with anti-spam and anti-virus software. **These tools identify and block malicious emails, prevent compromise and avoid encryption of your data**. However, they are not sufficient on their own. For optimal protection, it is important to keep them updated, to make sure that no malicious applications are installed on servers, workstations, etc.

Email filtering: why choose an additional solution?

In connection with our last tip, even if Microsoft offers email security solutions, equipping yourself with external solutions is a plus considered indispensable by the ANSSI (French National Agency for Information Systems Security). First of all, the figures prove that **companies do not always choose the security options available with Microsoft or do not use them**. This already creates a loophole.

Secondly, software specialising in the maintenance of messaging systems is the result of continuous R&D efforts devoted to these aspects and offers advanced solutions. This also helps to overcome the limitations of dependence on Microsoft, which is not necessarily infallible in this respect.

At Alinto, we offer products that adapt to all email systems. Beyond the anti-spam protection of incoming emails, we also take into account outgoing emails, offering a Business Continuity Plan (BCP), quarantine or archiving functions. Everything you need to improve your business email security. Do you have any questions? Don't hesitate to contact us!



Email management: going beyond email

Email management is strategic for a company. And it goes beyond sending and receiving emails. Email is a common entry point for cyber attacks. Securing it therefore requires the deployment of anti-spam software, the implementation of a Business Continuity Plan (BCP), but also secure hosting. This is the subject we will address in this new article.

#1 - Antispam and antivirus

To improve email filtering, it is essential to use an anti-spam and anti-virus solution. These tools give the email a score that allows it to be considered as acceptable or as spam, or even to be rejected. The evaluation criteria can be configured by the administrators and adapted to each user. Some examples: image/text weight, subject, sender, content, etc. But also more technical criteria.

Security rules can evolve according to the needs and specificities of each company. This is the advantage of choosing a suite of **adaptable and easy-to-use email protection services** like Alinto Protect. This filtering also allows you to protect the reputation of your domain name and to avoid being blacklisted by recipients.

#2 - PCA

When the messaging service is no longer accessible, the entire activity of a company is impacted. Having a BCP (Business Continuity Plan) is therefore essential. It allows you to **guarantee access to emails thanks to a backup webmail**. However, not all email protection software offers this. However, with the increase in cyber attacks, this functionality is essential.

An article in the newspaper Le Monde reports that following a cyber attack, the foreign employees of Bouygues Construction found themselves out of work due to a lack of access to their professional emails. This is the kind of situation that the Alinto Protect secure email relay allows to avoid thanks to a PCA insured and monitored 24/24. Users have access to their emails, even in the event of a breakdown, and this avoids **too great** an **impact on the business**.

#3 - Quarantine

Some emails are sometimes considered as spam even though the user considers it acceptable and wants to receive it. It is therefore essential to have a solution that allows you to **keep control over the various emails** that pass through the mail server.

This is what the quarantine service allows. Users receive a summary of quarantined emails and can choose to receive them or not. The frequency of sending the report is **customisable by the administrator**.

With Alinto Protect, quarantined emails are kept for 30 days, allowing users to keep control of their mailbox.

#4 - Archiving

To go beyond simple email management, some companies wish to benefit from an email archiving system, often to meet **regulatory obligations**. These features also compensate for server incidents or data loss... Storage is also optimised, reducing the volume of email directly on the server, sometimes making it inefficient.

The Alinto archiving service keeps an unmodifiable copy of all messages for the set period. Again, the administrator can set and modify the rules per domain and/or users.

#5 - Accommodation

The location of hosting is also a sensitive issue for companies. And this problem has been reinforced since the implementation of the RGPD (General Data Protection Regulation). With the web giants, it is difficult to know where data is hosted. By using a secure relay service such as Alinto's, companies have the possibility to choose their hosting, in France or in Europe.

Alinto services are hosted on private clouds, in data centres in France, Switzerland, Germany or Spain. Customers can also choose to host their data themselves. Y**ear-round 24/7 support and maintenance is available**.

For a more efficient maintenance of the professional messaging, it is recommended to equip oneself with a software that presents the functionalities listed in this article. Alinto offers this through a transverse and agile solution. To know more about it, it is here!

Microsoft 365 support: why choose Alinto?

In order to prevent the deployment of the Office 365 suite from failing and to ensure that security is placed at the centre of your use, especially with regard to your email, you have decided to call on a partner.

However, it is difficult to find one's way through the plethora of offers and providers available. In this article, we give you five criteria to guide you in your choice.

#1 - Opting for proximity

Microsoft is a major software company, which equips **80% of the CAC40 companies**. This indicator says a lot about the power of the company, but also about the number of employees and the turnover. If you are an SME or ETI, and you need specific support, turn to a human-sized partner, like Alinto.

Thus, you benefit from personalised support and follow-up by a team that knows your problems and will be able to **guide you in your deployment**.

#2 - Choosing security expertise

However, using a human-sized partner does not mean neglecting its **security expertise**. This is a major issue for companies, especially with the advent of teleworking and the digitalisation of companies.

With Alinto, you trust a partner who has been an expert in email security for 20 years. The group covers all the problems related to email and invests year after year in R&D to anticipate the trends in security and the fight against hackers.

#3 - Focus on responsiveness

In connection with proximity, calling on a partner of human size guarantees you more reactivity on the part of the support teams, to respond to your needs quickly. This is not always the case with larger partners, who sometimes charge for level 2 support, with the first level only managed by a scripted call centre.

At Alinto, you have immediate access to specialists and we are committed to providing a **24/7 supervised service to ensure your business is always secure**. In addition, we offer a Business Continuity Plan (BCP) in case of unavailability of your email service. All this in a powerful service package, at no extra cost.

#4 - Trusting objectivity

To deploy Office 365, why not simply trust Microsoft? This is often the first idea that comes to mind. However, choosing an external partner allows you to obtain **objective support, totally focused on your needs and not on commercial objectives**.

At Alinto, we know all the major email services and our protection solution is adapted to each of them. So we have no interest in recommending one over another. We base ourselves on your needs and specificities, to **propose you the best solution**.

#5 - Choosing accommodation in France

If you want to host your data in Europe, or even in France, but do not want to take care of it yourself, you can entrust your partner with the hosting. Make sure that **your data is sovereign** because it is precious, read the fine print!

Our Alinto services are located in France, Switzerland, Germany and Spain. We continuously upgrade our infrastructure to provide **maximum resilience and security**. We are committed to guaranteeing a sovereign service offering very high availability.

You now have all the cards in hand to choose your partner and to be supported in the implementation of your secure messaging and Office 365 suite. Why don't we talk about it?

Conclusion

Email has no reason to be the weakest link in Office 365, provided it is well protected. And that's why dedicated solutions exist: both through user behaviour, but also by using the right security software.

About Alinto

Founded in 2000, Alinto is a company specialised in the email business: email service in SaaS mode, anti-spam, email server... through several products:

- **Alinto Protect**: the secure email relay that immunises against Internet risks by ensuring permanent access to emails.
- **Alinto Gateway**: The SMTP mail relay allows servers or applications to send emails to guarantee a so-called “clean” traffic.

Present in France, Switzerland and Spain, Alinto has more than 30 employees and provides a quality service to more than three million users. More than 15 million emails are sent every day thanks to its email services.

The Alinto group brings together several entities since 2016 to position itself as a major player in electronic messaging. It is composed of the following companies:

- **Cleanmail**: Swiss company specialising in cloud-based antispam filtering since 2002
- **SerenaMail**: Spanish specialist in e-mail security (spam filtering).
- **Alinto**: secure messaging services.

This allows the group to consolidate its market position and expand its international development.

Lyon (siège)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Paris
31 rue de Reuilly
75012 Paris
+33 141 58 15 33

Madrid
Calle Aniceto Marinas, 48
28008 Madrid
+34 91 005 29 64

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com