Alinto

Livre blanc

Janvier 2021

# L'email : maillon faible d'Office 365 ?

# Sommaire

# Introduction

La transformation numérique est plus que jamais au cœur des préoccupations des entreprises. Chaque organisation déploie des chantiers de dématérialisation, de refonte des processus, de digital workplace, d'espaces collaboratifs… Dans une majorité d'entreprises, cela passe par un **déploiement de Office 365, désormais appelé Microsoft 365**.

Mais, la technologie reste un terrain de jeu formidable pour les cybercriminels. Parmi les différentes formes d'attaques, on recense les **ransomware, les emails spam ou phishing…** Ce sont des menaces sérieuses pour les entreprises, qui peuvent avoir des conséquences importantes sur leur activité.

Bien souvent, ces attaques proviennent d'emails frauduleux. Et la suite Office 365, n'est pas épargnée : Le mail est la porte d'entrée digitale de l'entreprise. Une vraie stratégie et des règles doivent alors être déployées. Quelles sont les solutions - Microsoft ou autres - disponibles pour une meilleure sécurité ? Comment protéger sa messagerie ? Est-il possible de se faire accompagner par un partenaire ? Nous répondons à toutes ces questions dans notre Livre Blanc.


# Adoption Office 365 dans les entreprises : état des lieux

Par Rodolphe Frering,
Directeur Marketing & Commercial

Microsoft 365 est une suite massivement choisie par les entreprises pour ses nombreuses applications, sa praticité et aussi la place qu'elle occupe sur le marché. Pourtant, après des mois d'utilisation, beaucoup d'organisations se rendent compte que ces outils sont peu ou mal utilisés. **Le ROI n'est donc pas forcément au rendez-vous**. Dans cet article, nous avons décidé de vous livrer des chiffres et un état des lieux sur l'adoption réelle d'Office 365 et les raisons des échecs.

# Adoption Office 365 : les chiffres

La suite de Microsoft a été lancée sous sa forme actuelle par abonnement il y a près de dix ans. Elle réunit de nombreuses applications répondant aux besoins quotidiens et métiers des entreprises : les outils historiques (Word, Excel, PowerPoint…), et de nouveaux services web (OneDrive, Yammer…). En 2019, la suite Office 365 comptait **155 millions d'utilisateurs actifs**. Elle a été renommée Microsoft 365 début 2020.

D'après un rapport Forrester, déployer Office 365 peut générer un ROI de 162 % en trois ans. À condition que la suite soit bien utilisée. L'étude Microsoft 365 Report rapporte que **88 % des décideurs IT ont entièrement déployé Microsoft 365 dans leur entreprise**. D'après un article du JDN, 80 % des entreprises du CAC40 en sont équipées. La principale raison de ce choix est la flexibilité de l'offre pour répondre à la complexité des organisations.

Cependant, les chiffres sont à prendre avec des pincettes. Le rapport Microsoft indique que la plupart des entreprises n'ont pas encore adopté la suite logicielle dans toutes ses fonctionnalités, en particulier en ce qui concerne la sécurité. Du coup, à quel moment considère-t-on qu'un outil est adopté ? Est-ce seulement être connecté à Microsoft ? Dans ce cas, 100 % des utilisateurs l'utilisent, car ils sont connectés aux emails. Mais l'adoption effective est plus complexe : c'est lorsque la transformation qu'elle induit est réelle et concrète, avec par exemple de nouveaux modes collaboratifs.

# Utilisation Office 365 : les applications les plus populaires

En termes d'usages, force est de constater que malgré l'intégration d'Office dans le cloud, **les utilisateurs s'en tiennent aux anciennes pratiques** : création de documents en local, partage des fichiers par email… En toute logique, les utilisateurs devraient se passer des emails, du moins pour échanger ou partager des documents en interne. OneDrive permet de générer des liens de partage sécurisés. Ils ne tirent donc pas vraiment parti des points forts de la suite.

Dans le détail, les applications
les plus utilisées au troisième trimestre 2019 sont :

- Outlook / Exchange : **59 %**
- Teams : **41 %**
- Skype Entreprise : **23 %**

On voit que les applications réellement collaboratives peinent à décoller. Ceci s'explique par le fait que nombre d'utilisateurs ne savent pas à quelles applications ils ont accès (47 % d'après le Microsoft 365 Report), ainsi que les bénéfices qu'elles apportent.

# ROI Office 365 : pourquoi ça coince ?

Dans la réalité, **l'adoption de la suite Office 365 n'est pas si évidente que les entreprises utilisatrices veulent bien nous le faire croire.**

Voici quelques chiffres qui le prouvent :

- **34 %** des utilisateurs sont réticents au changement
- **47 %** ne savent pas à quelles applications ils ont accès
- **29 %** manquent de temps pour se former

Les entreprises doivent surveiller en permanence les usages de leurs équipes afin de les accompagner dans le bon sens. Et c'est là que le bât blesse. Déployer des guides pour expliquer comment faire ne suffit pas, il faut créer des scénarios, montrer et convaincre des bénéfices de la suite collaborative. Il s'agit d'entamer une réelle démarche de transformation interne, et peu d'entreprises le font. Elles considèrent que si les utilisateurs se connectent à leur messagerie et à quelques applications de temps en temps, c'est un déploiement réussi. Cependant, le ROI n'est pas à la hauteur de leurs attentes ! Et pour cause, le prix des licences a augmenté de 10 % en 2019 !

Pour une meilleure adoption d'Office 365,
voici quelques pistes :

- Placer la suite au coeur de la transformation digitale de l'entreprise
- Impliquer les directions en fixant des objectifs
- La direction doit aussi être utilisatrice des solutions pour montrer l'exemple

Si l'adoption de Microsoft 365 est une réalité quantitative, son adoption "qualitative" par les utilisateurs des entreprises n'est pas encore optimale. Si la suite présente sur le papier toutes les qualités requises pour un travail collaboratif sécurisé, elle se heurte aux freins avancés par les utilisateurs, ce qui peut **ralentir la démarche de transformation digitale des organisations**.

# Office 365 : qu'est-ce que ça change pour l'email ?

Par Olivier Gilles,
Directeur des services

L'email est un outil central pour une entreprise. S'il tombe en panne, c'est toute l'activité qui en prend un coup ! Et si elle n'a pas de PCA (Plan de Continuité d'Activité), c'est un sacré handicap.

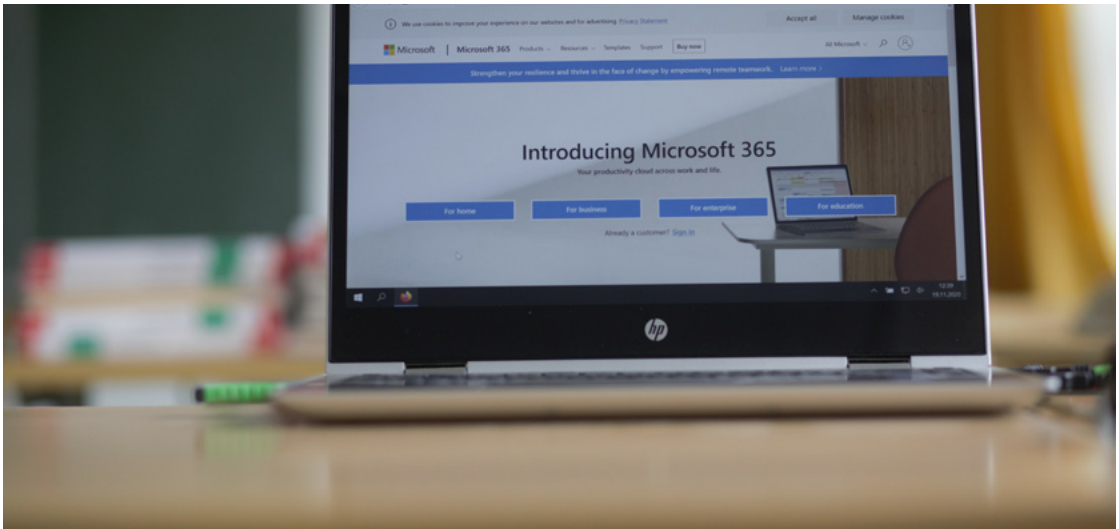
**En 2018, 56 % des entreprises utilisaient la suite Office 365 (aujourd'hui Microsoft 365)**. Pour recevoir leurs emails, ces entreprises sont embarquées dans un cloud qui permettra entre autre d'avoir un accès aux emails, aux calendriers et aux documents stockés sur les serveurs de Microsoft. Pour des raisons de simplicité, beaucoup d'organisations choisissent donc de s'équiper des services de l'éditeur de bout en bout. Souvent au détriment de la sécurité. C'est ce que nous allons analyser dans cet article.

# Quelles sont les fonctionnalités email d'Office 365 ?

Outlook est le service le plus utilisé en matière de messagerie professionnelle. Et pour cause, il présente plusieurs fonctionnalités clés :

1. Accéder à **des services additionnels** : calendrier, gestion des tâches et notes…
2. Créer des **signatures personnalisées**
3. Consulter **plusieurs boîtes de messagerie** simultanément
4. Faciliter le **travail collaboratif**
5. Envoyer un **email depuis Word**
6. Une **intégration parfaite** avec les autres logiciels bureautique de Microsoft
7. Améliorer la **sécurité des emails**
8. Accéder à la messagerie en **situation de mobilité**
9. Classer les **dossiers et fichiers**

Cependant, des trous dans la raquette persistent, surtout en matière de sécurité des emails entrants et sortants. Les offres de protection de Microsoft sont payantes, beaucoup d'entreprises ne prennent pas l'option. Nombre de messageries sont donc peu, voire pas sécurisées et sont livrées aux mains des hackers, ou tout du moins vulnérables. Le danger est accentué avec la mise en place massive et rapide du télétravail : sans cadre strict et **logiciel de sécurisation** (antispam, anti-phishing) des messageries, toute l'activité d'une entreprise est menacée par un simple email.



# Quelles sont les alternatives à Microsoft 365 ?

Les DSI voudraient réduire leur **dépendance à Microsoft**. Cependant, remplacer un maillon de la chaîne comme Exchange pourrait fragiliser le quotidien des utilisateurs. Et un tel changement n'est pas chose aisée.

D'une part, car Microsoft fonctionne en vase clos : toutes les applications sont interdépendantes et les alternatives ne sont pas toujours facilement interopérables. Les entreprises prennent donc souvent **le package "Outlook, Exchange et Active Directory"** pour fonctionner, sans rechercher d'autres solutions.

D'autre part, les changements d'outils génèrent des contraintes pour les utilisateurs. Les organisations ne souhaitent donc pas perturber leurs habitudes.

Cependant, des alternatives existent pour mieux protéger la messagerie. Il est possible de garder Outlook par exemple, mais de **choisir un autre serveur d'envoi que Exchange**. C'est totalement transparent pour les utilisateurs, mais permet d'avoir une meilleure sécurisation de la messagerie et de ne pas dépendre totalement de Microsoft.

La messagerie Outlook est très pratique, totalement compatible avec toutes les applications de Microsoft, renforçant ainsi la collaboration. Cependant, il est totalement possible de faire appel à des prestataires externes pour intégrer les fonctionnalités Office et les rendre interopérables.

# Déploiement Office 365 : comment garantir la sécurité de l'email ?

Par Philippe Martaille,
Responsable Avant-Vente

Les attaques par ransomware sont de plus en plus nombreuses et concernent tout le monde, même les petites entreprises. **Ces programmes malveillants s'introduisent le plus souvent par le biais d'un mail**. Il ne faut donc pas prendre à la légère l'aspect sécurisation de votre messagerie professionnelle. Au-delà de la sensibilisation de vos collaborateurs aux actions basiques (ne pas ouvrir des emails aux objets ou pièces jointes étranges, changer régulièrement de mot de passe et ne pas utiliser le même partout…), d'autres solutions doivent être mises en place pour **garantir votre sécurité informatique**.

Dans cet article, nous dressons un état des lieux de la sécurisation des messageries Exchange et vous livrons nos conseils pour bien protéger votre messagerie.

# Sécurisation des messageries Exchange : quels chiffres et quels enjeux ?

La plupart des attaques ransomware sont opportunistes et profitent d'un faible niveau de maturité numérique des organisations. Depuis 2018, les attaques s'intensifient et sont de plus en plus couplées à d'autres logiciels malveillants tels que les cryptovirus ou autres cheval de Troie. Les données des entreprises, et des particuliers également, sont donc facilement cryptable par les hackers, qui demandent alors une rançon pour pouvoir accéder à vos propres données.

Le préjudice pour les entreprises va souvent bien au-delà de la perte de quelques données :

- arrêt de la production
- chute du chiffre d'affaires associé
- risques juridiques (avec le RGPD par exemple)
- altération de la réputation
- perte de confiance
- La gendarmerie relève également des cas de suicides de collaborateurs suite à des arnaques au président.

Dans le guide "Attaques par rançongiciels, tous concernés" édité par le gouvernement, plusieurs entreprises témoignent :

- En novembre 2019, le **CHU de Rouen** ne pouvait plus accéder à une application métier. La DSI a constaté ensuite que les postes de travail et serveurs ont été chiffrés. C'était un ransomware.
- En octobre 2019, le **groupe M6** a fait l'objet d'une attaque au ransomware, coupant l'accès à internet, pourtant indispensable pour les émissions de radio notamment.
- En avril 2019, l'entreprise **Fleury Michon** a dû couper tous les accès internet des collaborateurs suite à une attaque au ransomware. L'activité s'est arrêtée complètement pendant trois jours et a été dégradée pendant deux semaines.

Le point de départ de ces attaques est souvent un mail. Pourtant, les questions de sécurisation des messageries, mais aussi de l'ensemble du parc IT, ne sont encore pas assez prises au sérieux. Et les chiffres issus d'un sondage mené par SoftwareONE le prouvent :

- 44 % des répondants n'utilisent pas Microsoft Intune (gestion des appareils et des applications mobiles) ;
- 37 % n'utilisent pas Microsoft Azure Advanced Threat Protection (identification, détection et enquête sur les menaces avancées) ;
- 36 % n'utilisent pas Microsoft Azure Information Protection (protection des documents).

Des progrès sont encore à faire pour contrer les menaces et anticiper les attaques.

## Protection des emails : nos trois conseils

Pour réduire les risques et protéger votre activité, plusieurs actions sont à mettre en place. Cependant, si nous devions vous livrer nos meilleurs conseils, nous choisissons les trois suivants.

## 1 Sensibiliser vos collaborateurs

Les attaques par des logiciels malveillants proviennent bien souvent des emails reçus par un collaborateur. Il est donc primordial de **rappeler les bonnes pratiques et faire naître des réflexes dans leur utilisation de l'email** : ne pas ouvrir les objets ou pièces jointes louches ou de destinataires inconnus, remonter les éventuels problèmes à la DSI… Ce n'est pas un rempart absolu, mais une étape nécessaire pour diminuer les risques d'attaques.

## 2 Sécuriser votre SI

Bien évidemment, il est primordial de sécuriser votre système d'information. Cela passe par la gestion des droits d'accès aux applications, le cloisonnement du SI pour pouvoir limiter le risque de propagation à tous les postes, de maintenir à jour les différentes applications, car cela permet d'améliorer leur sécurité, et de sauvegarder régulièrement vos données.

## 3 Opter pour des solutions de protection de la messagerie

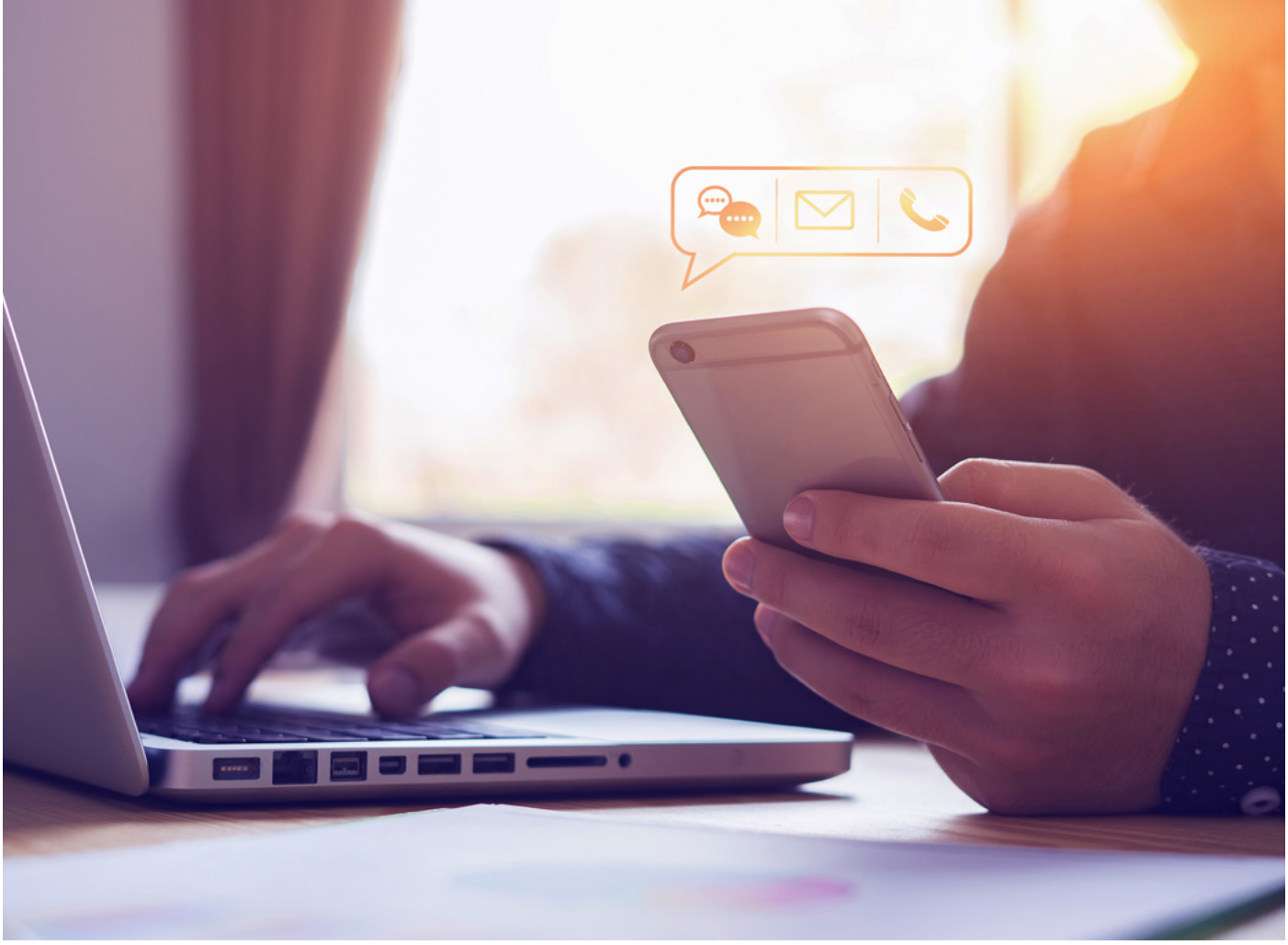
Enfin, pour une sécurité maximale de vos emails, il est important d'équiper les postes de travail de logiciels antispam et antivirus. **Ces outils identifient et bloquent les emails malveillants, empêchent une compromission et évitent le chiffrement de vos données**. Attention cependant, ils ne se suffisent pas à eux-mêmes. Pour une protection optimale, il est important de les mettre à jour, de s'assurer qu'aucune application pernicieuse n'est installée sur les serveurs, postes de travail...

# Filtrage des emails : pourquoi choisir une solution supplémentaire ?

En lien avec notre dernier conseil, même si Microsoft propose des solutions de sécurisation des emails, s'équiper de solutions externes est un plus considéré comme indispensable par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Tout d'abord, les chiffres prouvent que **les entreprises ne choisissent pas toujours les options de sécurité disponibles avec Microsoft ou ne les utilisent pas**. Cela crée déjà une faille.

Ensuite, les logiciels spécialisés dans la maintenance des messageries sont issus  d'efforts de R&D en continu consacrés à ces aspects et proposent des solutions avancées. Cela permet aussi de pallier les limites de la dépendance à Microsoft qui n'est pas forcément infaillible à ce sujet.

Chez Alinto, nous proposons des produits qui s'adaptent à toutes les messageries. Au-delà de la protection antispam des emails entrants, nous prenons également en compte les emails sortants, proposant un Plan de continuité d'Activité (PCA), une mise en quarantaine ou encore des fonctions d'archivage. Tout ce dont vous avez besoin pour améliorer la sécurité de votre messagerie professionnelle. Des questions ? N'hésitez pas à nous contacter !



# Gestion de la messagerie : aller plus loin que l'email

Par Olivier Gilles,
Directeur des services

La gestion de la messagerie est stratégique pour une entreprise. Et cela va plus loin que l'envoi et la réception d'emails. La messagerie constitue en effet une **porte d'entrée commune pour les cyberattaques**. La sécurisation de cette dernière passe donc par le déploiement de logiciels antispam, par la mise en place d'un Plan de Continuité d'Activité (PCA), mais aussi par un hébergement sécurisé. C'est le sujet que nous abordons dans ce nouvel article.

# **#1** - Antispam et antivirus

Pour améliorer le filtrage des emails, il est indispensable de s'équiper d'une **solution antispam et antivirus**. Ces outils attribuent à l'email une note qui permet de le considérer comme recevable ou comme spam, voire de le rejeter. Les critères d'évaluation sont paramétrables par les administrateurs et adaptables à chaque utilisateur. Quelques exemples : le poids image/texte, l'objet, l'expéditeur, le contenu, les langues... Mais aussi des critères plus techniques.

Les règles de sécurité peuvent évoluer au gré des besoins et spécificités de chaque entreprise. C'est là l'avantage de choisir une suite de **services de protection de messagerie adaptable et facile d'utilisation comme Alinto Protect**. Ce filtrage obtenu permet également de protéger la réputation de votre nom de domaine et de ne pas être blacklistés par les destinataires.

# **#2** - PCA

Lorsque le service de messagerie n'est plus accessible, c'est toute l'activité d'une entreprise qui est impactée. Disposer d'un PCA (Plan de Continuité d'Activité) est alors indispensable. Il permet de **garantir l'accès aux emails grâce à un webmail de secours**. Attention cependant, tous les logiciels de protection de la messagerie ne le proposent pas. Pourtant, avec la recrudescence des cyberattaques, cette fonctionnalité est indispensable.

Un article du journal Le Monde relate que suite à une cyberattaque, les employés étrangers de Bouygues construction se sont retrouvés au chômage technique, faute d'accès à leurs emails professionnels. C'est le genre de situation que le relais de messagerie sécurisé Alinto Protect permet d'éviter grâce à un PCA assuré et surveillé 24/24. Les utilisateurs ont alors accès à leurs emails, même en cas de panne, et cela évite un **impact trop important sur l'activité**.

# **#3** - Mise en quarantaine

Certains emails sont parfois considérés comme spam alors que l'utilisateur le considère acceptable et souhaite le recevoir. Il est donc indispensable de disposer d'une solution permettant de **garder le contrôle sur les différents emails** qui transitent sur le serveur de messagerie.

C'est ce que permet le service de quarantaine. Les utilisateurs reçoivent un récapitulatif des emails mis en quarantaine et peuvent choisir de les recevoir ou non. La fréquence d'envoi du rapport est **personnalisable par l'administrateur**.

Avec Alinto Protect, les emails mis en quarantaine sont conservés 30 jours, permettant ainsi aux utilisateurs de garder le contrôle sur leur boîte mail.

# #4 - Archivage

Pour aller plus loin que la simple gestion des emails, certaines entreprises souhaitent bénéficier d'un système d'archivage de leur messagerie, souvent pour répondre à des **obligations réglementaires**. Ces fonctionnalités pallient également à des incidents de serveurs ou des pertes de données… Le stockage est aussi optimisé réduisant le volume d'email directement sur le serveur, le rendant parfois contre performant.

Le service d'archivage d'Alinto garde une copie non modifiable de tous les messages pendant la période paramétrée. Là encore, l'administrateur peut fixer et modifier les règles par domaine et/ou utilisateurs.

# #5 - Hébergement

La localisation de l'hébergement est aussi une question sensible pour les entreprises. Et cette problématique est renforcée depuis la **mise en application du RGPD** (Règlement Général sur la Protection des Données). Difficile avec les géants du web de savoir où sont hébergées les données. En passant par un service de relais sécurisé comme celui d'Alinto, les entreprises ont la possibilité de choisir leur hébergement, en France ou en Europe.

Les services Alinto sont hébergés sur des clouds privés, dans des data center en France, en Suisse, en Allemagne ou en Espagne. Les clients peuvent également choisir d'héberger leurs données eux-mêmes. **Un support et une maintenance 24/7 toute l'année sont disponibles**.

Pour une maintenance plus efficace de la messagerie professionnelle, il est recommandé de s'équiper d'un logiciel qui présente les fonctionnalités listées dans cet article. Alinto propose cela à travers une solution transverse et agile. Pour en savoir plus, c'est par ici !

# Accompagnement Office 365 : pourquoi choisir Alinto ?

Rodolphe Frering,
Directeur Marketing & Commercial

Pour éviter que le déploiement de la suite Office 365 ne tienne pas ses promesses et que la sécurité soit placée au centre de votre utilisation, surtout au niveau de votre messagerie, vous avez décidé de faire appel à un partenaire.

Difficile cependant de s'y retrouver dans le florilège d'offres et de prestataires disponibles. Dans cet article, nous vous livrons cinq critères pour vous guider dans votre choix.

## **#1** - Opter pour la proximité

Microsoft est un éditeur important, qui équipe **80 % des sociétés CAC40**. Cet indicateur en dit long sur la puissance de l'entreprise, mais aussi sur le nombre d'employés et le turn-over. Si vous êtes une PME ou ETI, et que vous avez besoin d'un accompagnement spécifique, dirigez-vous vers un partenaire à taille humaine, comme Alinto.

Ainsi, vous bénéficiez d'un accompagnement et d'un suivi personnalisé, par une équipe qui connaît vos problématiques et saura **vous guider dans votre déploiement.**

## **#2** - Faire le choix de l'expertise en matière de sécurité

Cependant, faire appel à un partenaire à taille humaine ne veut pas dire qu'il faut négliger **son expertise en matière de sécurité**. C'est un enjeu majeur pour les entreprises, surtout avec l'avènement du télétravail et la digitalisation des entreprises.

Avec Alinto, vous faites confiance à un partenaire expert de la sécurité de la messagerie depuis 20 ans. Le groupe couvre l'ensemble des problématiques liées à l'email et investit année après année dans la R&D pour anticiper les tendances en matière de sécurité  et de lutte contre les hackers.

## **#3** - Privilégier la réactivité

En lien avec la proximité, faire appel à un partenaire à taille humaine vous garantit plus de **réactivité** de la part des équipes support, pour répondre à vos besoins rapidement. Ce n'est pas toujours le cas avec des partenaires de taille plus importante, qui vont parfois facturer un support de niveau 2, le 1er niveau n'étant géré que par un centre d'appel scénarisé..

Chez Alinto, vous accédez tout de suite à des spécialistes et nous avons à cœur de fournir un **service supervisé en 24/7 afin de garantir en permanence la sécurité de votre activité**. De plus, nous proposons un Plan de Continuité d'Activité (PCA) en cas d'indisponibilité de votre service de messagerie. Tout cela, dans un package de service performant, sans coûts supplémentaires.

## **#4** - Faire confiance à l'objectivité

Pour déployer Office 365, pourquoi ne pas simplement faire confiance à Microsoft ? C'est souvent la première idée qui coule de source. Cependant, choisir un partenaire externe vous permet d'obtenir un **accompagnement objectif, totalement focalisé sur vos besoins et non sur des objectifs commerciaux**.

Chez Alinto, nous connaissons tous les services de messagerie majeurs et notre solution de protection s'adapte à chacun d'entre eux. Nous n'avons donc pas d'intérêt à vous recommander untel plus qu'un autre. Nous nous basons sur vos besoins et spécificités, pour **vous proposer la meilleure solution**.

## **#5** - Choisir l'hébergement en France

Si vous souhaitez héberger vos données en Europe, voire même en France, mais que vous ne souhaitez pas vous en occuper vous-même, vous pouvez confier l'hébergement à votre partenaire. Assurez-vous de la **souveraineté de vos données** car elles sont précieuses, lisez les petites lignes !

Nos services Alinto sont situés en France, en Suisse, en Allemagne et en Espagne. Nous faisons évoluer continuellement nos infrastructures pour apporter un **maximum de résilience et de sécurité**. Nous avons à cœur de garantir un service souverain offrant une très haute disponibilité.

Vous avez maintenant toutes les cartes en main pour choisir votre partenaire et vous faire accompagner dans la mise en place de votre messagerie sécurisée et de la suite Office 365. Et si nous en discutions ?

# Conclusion

L'email n'a aucune raison d'être le maillon faible d'Office 365, à condition qu'il soit bien protégé. Et c'est pour cela que des solutions dédiées existent : à la fois à travers les comportements des utilisateurs, mais aussi en utilisant les bons logiciels de sécurisation.

# À propos

Fondée en 2000, Alinto est une entreprise spécialisée dans les métiers de l'email : service de messagerie en mode SaaS, anti-spam, serveur email... à travers plusieurs produits :

- **Alinto Protect :** le relais de messagerie sécurisé qui immunise des risques d'Internet en assurant un accès permanent aux emails.
- **Alinto Gateway :** le relais de messagerie SMTP permet à des serveurs ou des applications d'envoyer des emails pour garantir un trafic dit « propre ».

Présent en France, Suisse et Espagne, Alinto compte plus de 30 personnes et assure un service de qualité à plus de trois millions d'utilisateurs. Plus de 15 millions d'emails sont envoyés chaque jour grâce à ses services de messagerie.

Le groupe Alinto rassemble plusieurs entités depuis 2016 pour se placer comme acteur majeur de la messagerie électronique. Il est composé des entreprises suivantes :

- **Cleanmail :** entreprise suisse spécialiste du filtrage antispam dans le cloud depuis 2002
- **SerenaMail :** spécialiste espagnol de la sécurité du courrier électronique (filtrage antispam).
- **Alinto :** services sécurisés de messagerie.

Cela permet au groupe d'affirmer sa position sur le marché et d'étendre son développement international.

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