Alinto

Cas d'usage

Etablissement de santé

• SÉCURITÉ DE L'EMAIL • RANSOMWARE • SECTEUR PUBLIC



Pourquoi les établissements de santé doivent-ils absolument contrôler leurs messageries professionnelles ?

Le filtrage des emails de **milliers de boîtes aux lettres** électroniques

Un **déploiement totalement transparent** pour les utilisateurs

La mise à disposition de **reportings** pour les Directions

Les organisations publiques et les établissements de santé plus particulièrement, sont une cible privilégiée des cyberhackers depuis quelques années. En effet, les attaques se sont multipliées, avec des conséquences non négligeables sur l'activité des établissements publics et parfois générant des frais très importants. À titre d'exemple, en 2021, **733 incidents de sécurité**, dont environ une centaine d'attaques informatiques, ont été répertoriés dans 582 hôpitaux en France*.

Beaucoup de ces attaques ont pour origine des emails frauduleux. Le contrôle spécifique et renforcé des emails est donc indispensable pour diminuer les risques et assurer la sécurité du SI de ces structures publiques. C'est d'autant plus important que les établissements de santé hébergent et exploitent des données personnelles très sensibles. Au-delà du fonctionnement des hôpitaux, c'est aussi la **confidentialité de ces informations** qui est en jeu.

C'est pourquoi la gestion stricte des messageries professionnelles est indispensable. Retours sur les enjeux.

*source : Cyberattaque à l'hôpital de Corbeil-Essonnes : « Nous n'avons plus accès à nos bases de données » – TF1 info

Le contrôle des flux des emails : un prérequis pour les établissements de santé

Les hôpitaux manipulent de nombreuses données dites sensibles, à commencer par des données de santé. Le service de messagerie est donc géré sur site “on-premise” : les établissements préfèrent en général ne pas utiliser d’hébergement cloud, ni recourir à des fournisseurs de type GAFAM. Le partage des données sensibles est souvent scrupuleusement encadré : les établissements de santé exercent un **contrôle total et renforcé des messageries des collaborateurs**. Et les solutions mises en place doivent être régulièrement challengées.

Même si les hôpitaux sont équipés depuis longtemps de logiciels de protection de la messagerie, ils sondent le marché et mettent en concurrence les différents éditeurs tous les quatre ans.

Les deux objectifs principaux sont **la lutte contre les spams pour diminuer les emails inutiles, et la protection contre les malwares** qui sont de plus en plus contenus dans les emails. Les cyberhackers sont en effet de plus en plus inventifs, les solutions de protection doivent pouvoir anticiper ces nouveaux modes d’attaques pour protéger les données de hôpitaux.

Protection renforcée et reporting sur mesure

Lors d'un changement de solution, les Directions techniques souhaitent bénéficier de logiciels au moins aussi efficaces que ceux déjà en place.

Le prix et les fonctionnalités sont aussi des critères de sélection. Et parfois, elles ont besoin d'aller plus loin avec des options comme la possibilité de disposer de **données chiffrées et de reportings pour les analyses**. S'il est possible de bénéficier de reportings sur-mesure en temps et en heure, c'est un vrai plus.

Des spams sous contrôle et une mise en quarantaine facilitée

Avant tout, il faut que **le déploiement soit totalement transparent pour les utilisateurs** et que le niveau de performance ne baisse pas.

En utilisant Alinto, les utilisateurs confirment qu’ils reçoivent moins de spams qu’avant, prouvant l'efficacité du service. De plus, ils apprécient grandement la mise en quarantaine de certains emails, qui filtrent la réception ou non de certains messages, pour ne passer à côté d’aucune information importante. Cela est gérable en un clic, alors que la procédure peut être plus complexe avec d'autres solutions.

À propos d’Alinto

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 :

- Le relais de messagerie sécurisé qui immunise des risques d’Internet en assurant un accès permanent aux emails.
- Le Gateway SMTP permet à des serveurs ou des applications d’envoyer des emails pour garantir un trafic dit « propre ».
- La solution de messagerie indépendante haut de gamme : partage d’agendas, calendriers et des dossiers des collaborateurs.

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.

Un support performant apprécié par l’équipe IT

Cleanmail simplifie également la tâche des équipes IT et l’assistance qu’elles fournissent en interne aux utilisateurs.

Les établissements de santé apprécient particulièrement la **souplesse de la solution**, qui facilite le support apporté aux utilisateurs. Quand ils rencontrent un problème, les hotlines internes peut configurer en quelques clics des listes blanches ou noires, peut consulter les logs pour voir si l’email est arrivé ou non. **Cela est pertinent et plus efficace**. Et c’est un vrai confort pour les personnes du service IT.

Pour la formation, deux heures suffisent pour que les équipes IT s’approprient l’outil.

La collaboration avec les équipes d’Alinto est appréciée par les acteurs de la santé. Elles sont réactives et agiles, tiennent les délais et répondent aux enjeux de la santé. De plus, Alinto est un acteur français, ce qui est un facteur important pour le secteur public. Le support est en France, c’est **un critère différenciant**.

Objectifs

- renforcer **la sécurité** des messageries professionnelles
- s’adapter aux évolutions des **cyberattaques**
- disposer de **reportings** pour la direction

Bénéfices

- une **protection efficace** contre les spams et les malwares
- un service de **mise en quarantaine** ergonomique
- un support **interne réactif et de qualité pour les utilisateurs**
- un webmail de secours