



The critical need to monitor email communication in healthcare



Email filtering of **23,000 email accounts**



Fully transparent deployment for users



Provision of **reports** to management

Public organisations and healthcare institution have become popular targets of cyberhackers in recent times. The frequency of attacks has multiplied, leading to significant consequences for the operations of public establishments and often resulting in substantial costs. For instance, in 2021, 582 hospitals in France recorded **733 security incidents**, including approximately a hundred computer attacks.

Many of these attacks originate from fraudulent emails. It is crucial to implement stringent email control measures to mitigate risk and ensure the safety of healthcare structures' information systems. This becomes even more critical due to the extensive storage and utilization of personal data by healthcare institutions. Beyond the seamless functioning of hospitals, it is also the **privacy of this information** that is at risk.

This highlights the importance of implementing strict management for professional email messaging. A review of the challenges.

Email flow control: a prerequisite for healthcare institutions

Hospitals handle a vast amount of sensitive data, including health information. As a result, the management of their messaging service is typically kept on-premises. These establishments generally prefer not to utilize cloud hosting or rely on providers such as GAFAM. The sharing of sensitive data is carefully regulated, with healthcare facilities maintaining **strict control of employees' e-mail accounts**. Furthermore, the implemented solutions must be continuously challenged.

While hospitals already employ email security software, they regularly assess the market and compare different vendors every four years.

The primary objectives of this initiative are to **combat spam and protect against the growing inclusion of malware** in email communications. As cybercriminals become more inventive, it is crucial for protection solutions to anticipate these evolving attack methods and safeguard hospital data.

Enhanced protection and customized reporting

During the implementation of a new solution, technical departments aim to ensure that the effectiveness of the existing solution is at least maintained or improved.

Price and functionality are also important factors in the selection process. Additionally, there may be a desire to go beyond the basics and opt for features like the availability of **quantified data and reports for analysis**. Having timely access to tailor-made reports is a significant advantage.

Effective spam control and user-friendly quarantine

One crucial aspect of deployment is ensuring **transparency for users** and maintaining the performance level.

With the implementation of Alinto solution, users have reported receiving fewer spam emails, confirming the efficacy of the service. Moreover, they greatly appreciate the convenient quarantine feature that filters certain messages to avoid missing important information. Managing the quarantine is as simple as a single click, whereas it can be more complex with alternative solutions.

Objectives

- Strengthen the **security** of professional messaging
- Adapt to evolving **cyberattacks**
- Have **reporting** capabilities for management

About Alinto

Founded in 2000, Alinto is a company specializing in Email services, which includes SaaS email messaging, anti-spam solutions, email servers, and various other products:

- A secure email relay that provides immunization against internet risks while ensuring uninterrupted access to emails.
- An SMTP Gateway that enables servers or applications to send emails, guaranteeing clean and reliable traffic.
- A high-end independent messaging solution that facilitates the sharing of calendars, schedules, and employees' folders.

With a presence in France, Switzerland, and Spain, Alinto has a team of over 30 employees. They provide quality services to more than three million users, with their messaging services handling over 15 million emails every day.

High-performing support appreciated by the IT team.

Cleanmail also streamlines the work of IT teams and enhances the support they provide to internal users.

Healthcare organizations especially value the **solution's flexibility**, which simplifies user support. When encountering an issue, internal hotlines can easily set up whitelists or blacklists with just a few clicks and check the logs to determine the status of emails. **This capability is relevant and significantly improves efficiency**, providing genuine comfort to the IT department staff.

A two-hour training session is sufficient for IT teams to become familiar with the tool.

Collaboration with Alinto's teams is appreciated by healthcare stakeholders. They showcase responsiveness and agility, meet deadlines, and address healthcare-related concerns. Furthermore, Alinto is a French actor, which is an important for the public sector. Support is based in France, which is a differentiating factor.

Benefits

- **Effective protection** against spams and malware
- User-friendly **quarantine service**
- **Responsive and high-quality internal support** for users
- Backup webmail