The benefits of integrating GFI MailEssentials with Microsoft Exchange Server

Current challenges

Consensus says that Exchange's built-in malware engine does not provide enough protection, enabling malware to potentially make it through to users' Inboxes. This is obviously a huge security risk for companies, especially in a time where ransomware is becoming an increasingly common form of attack.

Traditional Windows antivirus programs don't replace email-based antimalware solutions because Windows antivirus programs that run on Windows servers can't usually detect viruses, malware, and spam that are distributed only through email. There are a few exceptions, as some solutions use transport agents to intercept emails on the Exchange servers themselves and analyse them. However, it is not uncommon for these to cause problems, especially when it is time to upgrade Exchange.

In terms of anti-spam, Exchange does provide good protection. It uses transport agents to provide anti-spam protection such as connection filtering, sender/recipient filtering, content filtering, and more. However, the built-in agents that are available in Exchange 2016 and 2019 are relatively unchanged from Exchange 2010. This means that the level of protection offered by on-premises Exchange is miles away from Exchange Online Protection (EOP).

With Microsoft's strategy of "cloud first", companies need to subscribe to EOP in order to get the latest features and the greatest level of protection. Microsoft promotes the cloud service as secure, reliable and easy to deploy and manage. At the same time, organisations benefit from the well-known cloud advantages including increased flexibility, reduced costs and hardware requirements. All in all, EOP is a good fit for many companies.

The problem is that there are many organisations that prefer an on-premises security solution for Exchange. This could be due to objections to using cloud in general, or because of regulatory or legal requirements that prevent them from using such solutions. Organisations with on-prem Exchange often prefer an on-prem security solution. It allows them to stay in full control of corporate data and knowledge. Third-party security solutions are usually more customisable as well. The ability to tweak different security settings to meet an organisation's particular needs can be a big reason to choose third-party security software for Exchange.

GFI Mail Essentials helps organisations address all of these challenges.

Choosing GFI MailEssentials

1 Easy to install

GFI MailEssentials can be deployed on its own server(s), or it can be installed directly in the same server(s) as Exchange. Independently of the chosen method, it should be installed and configured in a way that makes it the email gateway for the organisation, both for inbound and outbound emails.

Installing MailEssentials on a mail gateway/relay server is commonly used for larger organisations, or those that wish to keep MailEssentials and Exchange (or any other mail server being used) separate for any reason, like patching, high availability, and so on. This way, spam and viruses are filtered before these emails are received on the mail server, thus reducing unnecessary email traffic. It also provides additional fault tolerance: if the mail server is down, organisations can still receive email since these are queued on the MailEssentials server(s).

Installing MailEssentials directly on Microsoft Exchange server is the easiest method and it does not require any additional configuration. This makes it extremely easy to set up and get up and running.

2 Easy to use

Thanks to a modern and fresh interface, GFI MailEssentials is easier than ever to use. Administrators will of course need to be familiar with anti-malware and anti-spam terms and technologies, but as long as they are, they will not have problems finding out where each feature is, how to configure it, and how to troubleshoot it should the need arise.
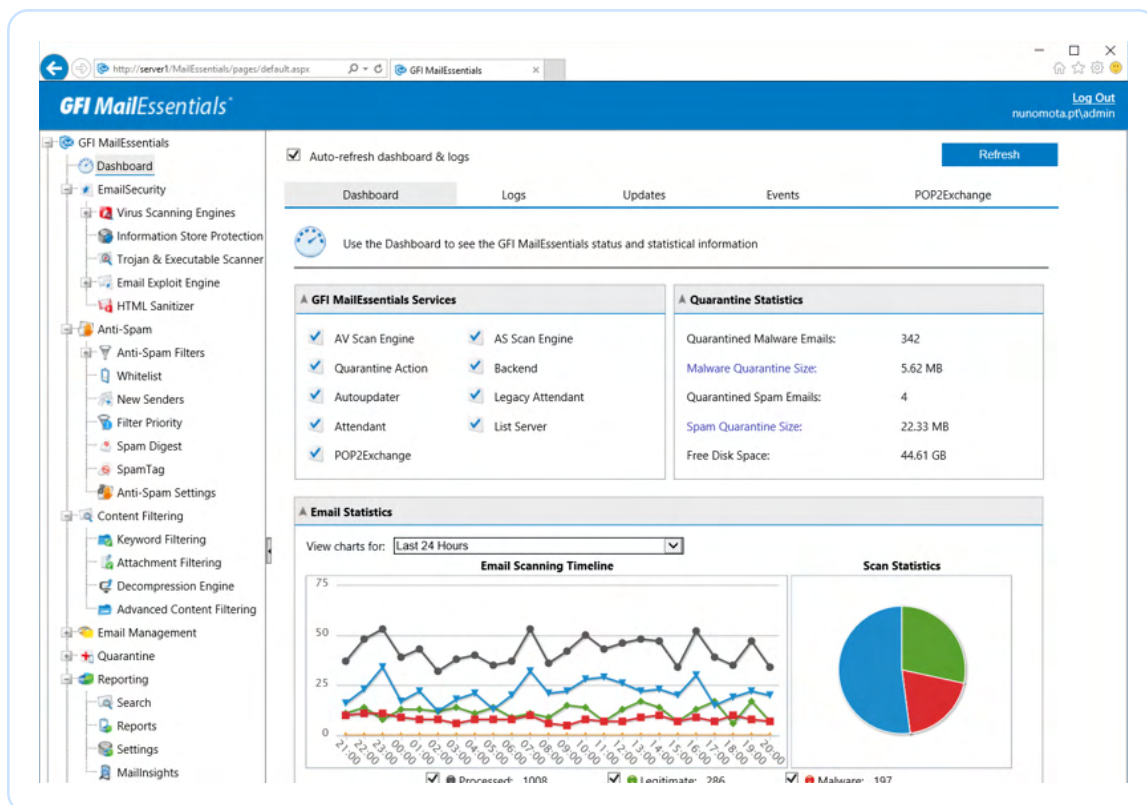
Everything is grouped per technology or feature and properly labelled, making the interface navigation simple and intuitive.

③ Completely on-premises

As already mentioned, many organisations prefer an on-premises security solution for their messaging environment. This is typically due to regulatory or legal requirements they must adhere to. No matter the reason, GFI MailEssentials is the perfect solution to address this issue since it is fully on-premises. Having such a powerful and complete solution fully on-premises without having to route emails through cloud solutions hosted by 3rd-party companies, is a big win for many companies. It guarantees that organisations retain full control over the solution and its upgrades, as well as the data itself.

④ Multiple anti-malware scanning engines

GFI MailEssentials provides multi-scanning techniques in order to achieve "Zero-Hour" malware protection, drastically reducing the time required to obtain the latest virus definitions against the latest threats. Organisations gain maximum protection for their email environment via three engines' heuristic and polymorphic malware detection methods, enabling them to take advantage of the strengths of each engine. The three anti-malware scanning engines are: Avira, BitDefender, and Sophos. Antivirus engine vendors have different response times to new viruses and malware, so this capability ensures MailEssentials can always detect new threats in the shortest possible time.

This also provides more control for the sysadmin over the malware scanning process (after all, different admins and organisations have their own preferences and requirements), and significantly lowers the business security risk.

5   Powerful anti-spam
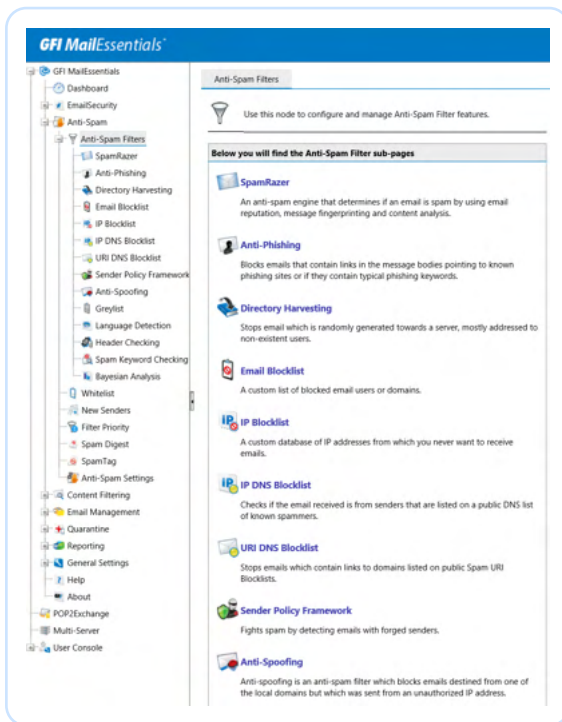
Another major feature of MailEssentials is its powerful anti-spam capability. This VBSpam-certified solution uses multiple anti-spam filters that combine SpamRazer technology, greylisting, IP reputation filtering, Bayesian filtering, and other advanced technologies to provide a spam capture rate of more than 99% and minimal false-positives, ensuring the safe delivery of important emails. The Bayesian Analysis, for example, is an anti-spam adaptive technique based on artificial intelligence algorithms, designed to withstand the widest range of spamming techniques available today. Organisations will have everything they could expect from a solid anti-spam solution, with 14 anti-spam technologies at their disposal.

6   Suitable for large environments

GFI MailEssentials provides a feature called multi-server, which makes it suitable for large and dispersed environments. Two common issues when managing a large messaging environment are:

- Ensuring that all servers are configured identically. When deploying multiple servers, how do you ensure they are all configured the way they should be? For example, a typical solution is to use a script to reduce the possibility of human error. But even then, how do you guarantee they remain identical going forward?

- Troubleshooting. How many times have you had to search the logs on individual servers, one by one, hoping to find what you were looking for?

The multi-server feature is designed to help with these issues. It enables communication between different GFI MailEssentials servers so that configuration data can be shared across them all. This is great for organisations with multiple email gateways and email servers, where managing individual servers can be a tedious task without a unified console, not to mention being prone to errors and misconfiguration. Once multi-server is configured, this problem is solved and day-to-day configuration tasks can be done using a single unified console.

Synchronised data include the attachment, keyword and advanced filtering rules, and black/white lists. Quarantined emails from different GFI MailEssentials scanning servers are stored in a central server of your choice. This gives you a central quarantine to maintain for your entire organisation.

GFI MailEssentials logs all email flow activity to a central reporting database so you can consolidate all your email flow reports and easily detect any mail flow trends or issues. These unified settings are highly customisable, giving you total flexibility in how you deploy GFI MailEssentials on your network.

Conclusion

Cloud solutions like Exchange Online Protection are great for many organisations. However, they are not suitable for everyone. Some organisations cannot use cloud services due to regulatory or legal requirements. Some simply prefer to keep everything on-premises as much as possible; others might just not be able to afford it.

GFI MailEssentials is on-premises email protection software that will meet the anti-spam and antimalware requirements for most, if not all, organisations. It is simple to configure and manage, yet extremely powerful and effective.

Get your free GFI MailEssentials trial