

GFI White Paper

Email security – Cloud vs. On-premise solutions

Choosing whether to put your email security in the cloud or host it on premise is a major decision. Hopefully this white paper will help.

Contents

What's the difference.....	3
Cost – Top of most people's list.....	3
Feature set.....	3
Implementation time.....	3
Technical knowledge.....	4
Security.....	4
Continuity.....	4
Cloud vs. on-premise solutions applied to email security.....	5
Bottom line.....	5

What's the difference

GFI Software™ has been providing email security in the form of GFI MailEssentials and GFI MailSecurity for years and these products are among our best-selling security solutions. Recently we have added GFI MailEssentials Complete Online, a hosted solution. This gives customers the choice of running our award-winning email security solutions on premise or as a hosted, online solution.

To help you choose which solution best meets your needs, let's break down the individual benefits to make the alternatives clearer. In the end, the decision will most likely depend on the criteria that are most important in your situation.

Cost – Top of most people's list

On-premise solution – Means buying the software licenses up front and having to find or purchase the hardware needed to run it, unless you choose to load the software onto an existing server that has available bandwidth. So the initial outlay is likely to be high. There will be an annual maintenance cost, typically between 20% and 40% per year of the original license cost. Additionally, there will be ongoing costs associated with maintaining the on-premise solution, including eventual replacement of the hardware, and any necessary management of the solution itself.

Cloud – Annual licensing and no requirement for in-house hardware make the startup costs lower. GFI maintains the cloud-based infrastructure and software at a fixed annual cost, allowing companies better budgetary planning. Annual costs for cloud-based solutions tend to be higher than software maintenance agreement (SMA) costs so the long-term cost of cloud-based email security may be higher.

Decision – The cloud solution typically will have lower initial costs but may cost as much or more over the long term, dependent on the cost of maintaining the on-premise solution over the long term.

Feature set

On-premise solution – Running the on-premise version on your existing MS Exchange server will allow you to filter internal emails, along with inbound and outbound emails. The GFI MailEssentials software also includes a list manager.

Cloud – The hosted service filters inbound and outbound email, but not internal messages within an organization. The hosted service includes several key features not possible with an on-premise product, including built-in email continuity and an available integrated archive solution.

Decision – This will depend on the organization's choice of the most important functions for its email security solution. In cases where the filtering of internal mail, management capabilities, and integrated continuity and archive services are all important, the organization may want to consider a hybrid of both solutions.

Implementation time

On-premise solution – Acquiring and setting up the hardware and any infrastructure, then obtaining and installing the software, can take time, especially if there is lead time to procure new servers at the best price. Then there is the time required by your IT resource to install and configure the solution. If your MS Exchange server has available bandwidth you might install the software on that server, saving the time of sourcing and installing new hardware.

Cloud – Usually takes minutes once the decision is made.

Decision – This will depend on the company's need for the solution. If getting it in place ASAP is a priority then the cloud becomes an obvious choice. If there is less urgency then this decision point can be given a low priority.

Technical knowledge

On-premise solution – Internal technical staff or an outsourced IT provider needs sufficient knowledge to set up the hardware, install and configure the software. They will also be required to manage software updates and ongoing configuration changes.

Cloud – Far less technical knowledge is needed to implement GFI MailEssentials Complete Online, though it pays to have some awareness of the solution to get the most from its use. The cloud-based solution acts as a gateway, allowing it to work with any email server. You will need to modify your MX records, though for smaller organizations this is just a quick chat with your ISP.

Decision – If the availability of people with relevant technical skills is short or comes at a premium price, the ease of implementing a cloud-based solution with little or no ongoing maintenance requirements may be appealing.

Security

On-premise solution – Within the bounds of your own network, you have control of the levels of security and access your data is protected by. You know where it is stored and who has access to it, or at least, you should. Where customers want local control of security when storing or transmitting personal or sensitive information by email, an on-premise solution could be the better option.

Cloud – You are relying on a third party's systems to provide your data with adequate protection. They may have datacenters in different countries so you need to understand where your data will be stored and what protection it will have. The GFI datacenters work on a vastly different scale compared to the average company, and use layers of defense that would not be feasible for a small to medium-size business to implement, so the level of security may actually be stronger than your company is able to implement with an on-premise offering. Also note that the GFI MailEssentials Complete Online service does not store any emails for longer than the duration of the quarantine, unless the customer opts to use the archive service.

Decision – This is heavily dependent on the level of control that you would like to have when transmitting emails with sensitive data. In making this decision, you need to consider that, without the use of specialized software, all messages are sent in plain text across the Internet – meaning that email is an inherently insecure protocol. That said, some organizations are very sensitive as to how and where those messages are processed, and may or may not be comfortable with quarantined or queued messages being stored in the cloud until those messages are either released or deleted.

Continuity

On-premise solution – if you have a hardware or software failure then your on-premise applications may be down until you can resolve the issue. Power outages, natural disasters, viruses or malware, or other problems can potentially have a large impact on the productivity of your organization. These risks can in part be mitigated by implementing failover solutions but these will significantly increase the organization's infrastructure costs. In most cases, emails are queued at the sending mail server, which means that no emails are normally lost, but employees will not be able to access their emails until the organization's mail server is online and capable of receiving emails again.

Cloud – GFI MailEssentials Complete is hosted on multiple servers in more than one datacenter so the chances of them all failing at the same time are vanishingly small (and GFI offers a 100% uptime service level agreement). Once your email security is in the cloud, it can be accessed from anywhere, which should make your disaster recovery planning much simpler. Should your mail server be offline, emails are stored in GFI MailEssentials Complete Online and users can view and reply to messages through the web mail interface - providing your organization with email continuity.

Decision – Even when your email server is down, a cloud-based solution with email continuity will allow your staff to continue to send and receive email. Given the extent to which companies rely on email communications, the ability to have continued access to email regardless of the state of an organization's on-premise hardware and software is often an important factor in choosing an email security solution. It is also worth noting that most competing vendors either do not provide continuity, or charge significantly more for it – whereas continuity is included in the price with GFI's online solution.

Cloud vs. on-premise solutions applied to email security

Cloud hosted	On-premise
Advantages	Advantages
Enabled in minutes with minimal technical knowledge required	Greater control of the security around the solution and of stored messages
Spam, phishing and malware never reach your network	Ability to filter internal emails
No software licensing costs	Granular control over filtering methodology (e.g. selective enabling of blacklists)
No new infrastructure requirements	
No on-going maintenance – solution is kept updated and maintained automatically	Native Exchange integration (e.g., spam can be stored in the Exchange Junk Mail folder)
Load on email server is significantly reduced	Ability to license only the anti-spam or antivirus portion independently
Email continuity – you can continue sending and receiving email, even if your email server is down	Choice of antivirus software of up to five leading AV engines
You save on bandwidth, since spam and malware are blocked in the cloud	
Unique combination of zero-hour, virtualization-based, and traditional signature-based antivirus engines	
Disadvantages	Disadvantages
Potentially sensitive emails pass through GFI servers	Initial cost of software and hardware
Potentially higher long-term costs	Much longer set up time

Bottom line

There are many advantages to cloud-based solutions, especially for small or medium-sized organizations where IT resources are limited. Cloud-based solutions are faster and less expensive to implement, and the simple annual fee makes budgeting easier. On-premise software may work out to be less expensive in the long term, depending on the level of maintenance costs required for the on-premise hardware and software.

GFI has a long history of providing high-quality, cost-effective email security solutions. Both the on-premise and hosted versions of the GFI MailEssentials product line benefit from GFI's expertise and ongoing research and development in this area of security. While many competing vendors are abandoning their traditional software products in favor of cloud-based solutions, GFI believes that there are balanced arguments for both deployment models – the local control and security possible with an on-premise solution, versus the reduced management and added functionality allowed by the cloud. As a result, GFI's development strategy is to support and enhance both deployment options to provide companies with real choice for the long term.

Answer yes or no to the questions in the table below if you need more help deciding between an online or on-premise solution for your email security.

Decision questions	Yes/no
Is a lower startup cost important?	
Does the solution need to be implemented ASAP?	
Are your in-house technical skills lacking, overworked or non-existent?	
Is it ok that your email is filtered through our secure, remote servers?	
Would it be valuable for your employees to have continued access to email even if your email server is down?	
Do you have an interest in an integrated email security and email archive solution?	
Would you prefer a "set it and forget it" solution over a product that allows administrators to make various changes to the filtering methodology?	

If most of your answers are YES, then a hosted solution might better suit your needs.

If most of your answers are NO, then you should take a closer look at the on-premise solution.

If you have an even split, then you probably need professional help; contact one of our security resellers: They will be able to provide more help in making the right decision for your company.

[Show me GFI's on-premise email security solution](#)

[Show me GFI's online email security solution](#)

[I need help – Find a partner](#)

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit <http://www.gfi.com/contactus>



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.