GFI White Paper

Email security: Hosted or on-premise?

Choosing the correct option(s)

GFI®

Contents

Introduction

Email is at the very core of how we communicate today, and nowhere is this more prevalent than in the workplace. With the broad availability and adoption of broadband, email has quickly risen to supplant both the phone and fax machine as the primary form of day-to-day and legally-binding business communication[1].

Among the reasons that email has evolved into a communications staple are its sheer speed and cost effectiveness. The shift away from leased lines to municipal broadband such as DSL has lowered the cost of email communication and increased its use, as flat rate connectivity for small and medium-sized businesses has significantly lowered the cost of internet access for all, compared with leased lines and WAN connections that charged by the megabyte. It has also made it easier for even the smallest of businesses to host their own mail server on the premises.

However, with Internet access and email use now so heavily interwoven into modern business practices, the security implications for businesses are bigger than ever. With so much communication taking place in a stored data form, companies have to pay extra careful attention to data protection and storage laws. This is in addition to any industry-specific guidelines on information management best practice that an organization needs to follow, as well as the duty of care an organization must uphold to the people who have supplied data in email form – such as customers, suppliers and staff – to ensure that inbound, outbound and stored email is kept safe and secure.

Companies also need to pay close attention to the problems created by spam and other unwanted and unsolicited email traffic. Despite many successful law enforcement crackdowns on notorious email spam senders, spam traffic continues to consume bandwidth and storage, with some 40 billion spam messages currently being dispatched daily[2].

Cybercriminals are increasingly turning their attentions to business users in order to perpetrate crimes such as data theft, not only against individuals, but also the organizations those individuals work for[3]. This means that company email has become the new battleground for email scammers, spammers, malware writers and other opportunistic criminals, as well as being a high-risk point of access in the company IT infrastructure for both malicious and unintended data destruction by current and former employees.

All this means it is paramount that your mail server or email service is paired with robust security solutions to mitigate security threats, such as malware and spam, out of end-users mailboxes.

Ensuring email remains safe, secure and reliable is essential. There are a number of different approaches that you can take to achieve it, whether you want to place the security resource on-site within the confines of the business network, or move security off-site completely – perhaps along with the rest of your email infrastructure – into the cloud.

Delivering security inside the organization

Hosting your own email server inside the business is still the most popular way of maintaining email services in the workplace. According to analyst group Gartner, despite alternative options such as externally hosted cloud-based email gaining popularity in some sectors, by 2013, 82% of businesses will still be using on-premise email hosting solutions, most commonly in the form of an on-site email server, either in the form of an integrated small business server package or as a standalone server solution, such as Microsoft Exchange.

Retaining email resources on-site brings with it management and maintenance overhead that need to be met by on-site IT staff, so it is essential that both the mail server and the security solution running alongside it are effective and relatively hassle-free. Email security solutions play a pivotal role in filtering spam and other unsolicited messages, ensuring viruses are intercepted and isolated before being delivered to users and ensuring that the mail server and data such as address books[4] are not compromised by malware in transit.

There are a number of benefits to retaining both the mail server and email security solution on-premise:

- **Complete control over all aspects of the solution** – On-premise deployment means you can choose exactly how, when and where the solution is deployed, as well as keeping full control over what hardware is used or reused to host the deployment.
- **Ring-fencing inside the corporate network** – By keeping the security solution and the mail server on the premises, both can be protected by existing edge defenses such as firewalls and DMZs, as well as being integrated into existing IT policy and management processes.
- **In-house staff can react to issues** – The IT department can retain full control over the solution, ensuring that issues and required changes can be actioned immediately; additionally IT skills and knowledge of the solution are retained and reused in-house.
- **Low long-term running costs** – The initial one-off cost of buying a mail server can be high, but is offset by minimal on-going costs, usually in the form of maintenance agreements. Purchasing and deploying an on-premise email security solution offers the same benefit in the form of a fixed one-off cost, with low on-going costs for maintenance and security updates.
- **Customization** – With an on-premise software security solution, you retain full control over settings and configuration, allowing the IT department to maintain a level of protection and lock-down that is appropriate to the organization, and to factor in configuration and access exceptions that might not be as easily achieved by an off-site or shared security solution.

Cloud email security

Deploying a software solution is not the only option for on-premise email security. With more organizations moving their email to the cloud, or simply wishing to keep their email security at arm's length where a third-party specialist can maintain and update the solution, the cloud-based email security service is growing in popularity.

Cloud-based email security works as a buffer between the mail server and the wider Internet. All inbound and outbound email is received at the security service before being passed to the mail server, whether that server is also in the same cloud, a different cloud, or even back on the premises. Doing this ensures that the content is virus-free and confirms with content policy before it is released for sending or for downloading to a client PC.

This buffer approach delivers a range of end user and IT department benefits:

- **Inbound and outbound virus scanning** – all email traffic passes through the cloud product, ensuring that malware is stripped from messages before they reach the client computer in either direction.
- **Spam filtering before the point of reception** – spam and blacklisted content can be intercepted and retained off-site before it ever reaches the mail server, let alone the client.
- **Centralized maintenance and updates** – email security in the cloud benefits from faster deployment of new definition files, system updates, refreshed blacklists and content filters. One update by a solution provider updates all cloud instances.
- **Ease of administration** – web based consoles make it easy to configure and alter security settings from any location, as well as monitor email traffic and the level of malware being intercepted.
- **Point of failover** – if the email server fails or has to be taken down for planned maintenance; mail can be queued in the cloud until the mail server is back online.

There are operational and acquisition benefits to the cloud approach, such as requiring no physical hardware to be purchased or maintained on site. There are no software licenses to buy, and capacity can be scaled up or down as the business requires. Paid-for licenses need no longer be exhausted or left unused due to a contraction in the number of users.

The up-front costs are low, with many vendors charging preferential rates to set up a cloud service, while monthly or yearly recurring charges are often on a par with the maintenance and security update costs of an on-premise solution. Cloud services can offer such an attractive price point by taking advantage of economies

of scale associated with shared datacenters and hardware running at full capacity, whilst using virtual images to separate customer instances to comply with data protection and compliance regulations.

Cloud services are also an attractive business model for start-ups. Small businesses with say, fewer than five employees may, initially, not want to invest in an email server and email security until it has established the business and starts to grow. With a cloud-based service, the organization focuses on running the business and leaves the email strategy to third-parties. This is also a cost-effective option as the organization may not be in a position to hire dedicated IT resources.

Cloud-based security is also suitable for those companies that are in a period of constant growth. In this situation, the business may opt to have the email server hosted on premise for security and compliance purposes however to avoid having to deal with licensing of an email security solution and maintenance, it chooses a cloud-based service that takes care of its email security needs.

Hybrid security models – bridging on-site with the cloud

The scenario described above is a perfect of example of the hybrid approach, bridging on-site with the cloud.

The hybrid model is interesting as it can retain a footing in both areas – cloud and on-premise software deployment. The hybrid model allows for a staged migration from conventional on-site email services to a fully cloud-based environment, or can allow an organization to retain on-site services that it is required to do so to comply with local laws, compliance regulations and industry best practice (for example, ensuring that a financial services client does not have its data stored out of the country of regulation or on shared infrastructure).

The hybrid approach also allows for a multi-layered approach to email security, building in additional resilience and failover by ensuring that the cloud is supported by on-premise in the event of an outage and vice versa. The hybrid approach can also allow organizations to implement multiple instances of the same technology type, such as multiple AV engines, separated by a security platform to avoid false-positives.

Some organizations, which already have on-premise email security solutions installed, may also deploy a cloud solution to cut down on unnecessary volumes of spam email reaching the server, particularly if the business does not have high bandwidth internet access. Using the cloud service, the volume of email is cleaned first in the cloud, and then the filtered email is cleaned again by the security solutions on-premise. This saves on bandwidth and gives the business another level of security.

Summary

There are many options available to ensure robust email security is maintained in the workplace. The emergence of business-ready cloud email services has broadened the market and the options and the ways of working that are open to business users, but it is important that an option is chosen because it best fits the organization, not because it is the popular format of the moment.

It is essential for each business to assess its own needs, preferred operating processes and the way that users currently use email resources. If implementing a security solution is going to change the way people currently work, it is important to ensure that the change will be beneficial for productivity and accuracy of work, and that it will be accepted by users rather than circumvented by the use of personal email accounts in the workplace.

You must ask some clear and probing questions of the business, as well as ensure that the IT department has the necessary capacity and skill set to implement and maintain your chosen solution. You should also think about your longer-term email plans. For example, you may be retaining your email server on site today, but want to move to the cloud in the future. In which case, a hybrid multi-layer security solution deployed now would provide you with the flexibility to gradually migrate to the cloud, while retaining on-premise control and on-premise functionality as needed to satisfy workflow, legacy applications and regulatory requirements as needed.

1. http://www.networkworld.com/community/node/18555
2. http://www.theregister.co.uk/2011/07/01/cybercrims_shift_focus/
*3. http://www.crn.com/news/security/229400887/epsilon-data-breach-paves-way-for-phishing-security-pros-warn.htm;jsessionid=EM0K75qYz3QxC283nNilYw**.ecappj03*
4. http://www.eweekeurope.co.uk/knowledge/blame-for-ipad-email-breach-lies-with-att-7699

GFI 2466 oct11

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

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

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

GFI®