



WHITEPAPER

Why CIO's are jumping to the Cloud for email security

MailGuard Whitepaper, July 2010

WHY CIO'S ARE JUMPING TO THE CLOUD FOR EMAIL SECURITY

Email is an essential organisational tool, enabling internal and external communication. But as email traffic evolves into ever higher volumes, new threats and security risks become a major problem. Trojans, virus attacks, email and privacy violations, coupled with more sophisticated attacks from spammers are some of the growing problems faced by an organisation's IT department.

Your choice of email security system will play a vital role in reducing the level of threats entering your network.

This Email Security Whitepaper highlights the importance of implementing email security services to combat email-based threats, and compares the pro's and con's to both onsite and cloud solutions.

INBOUND EMAIL SECURITY:

Email is one of the most heavily utilised communication services within an organisation, growing at an annual rate of 20%. Simultaneously the volume of spam and other malware is also increasing, so the need to address email security is a high priority. Maintaining a healthy network not only means a secure working environment, it also allows users to operate efficiently without worrying about inadvertent release of threats into the system. Typically, email threats include:

- Eavesdropping
- Identity Theft
- Invasion of Privacy
- Message Modification
- False Messages
- Message Replay
- Unprotected Backups
- Repudiation (Sender denies that s/he sent it)
- Virus and Spam

OUTBOUND EMAIL SECURITY:

As well as concerns about inbound threats, an organisation must also consider the consequences of lax outbound security. A major concern is protection against employees sending out confidential information or data, whether deliberately or in error, and many organizations now exhibit heightened awareness to ensure that data breaches don't happen.

Forwarding malware and infecting clients, suppliers and business contacts can have serious repercussions for an organisation's brand, and considerable impact on revenue and profitability.

Stringent security around outbound email traffic is now as vital as inbound security.

IN- HOUSE MANAGEMENT VS HOSTED SECURITY: BENEFITS AND DISADVANTAGES

In-House Appliances

It is easy to underestimate the benefits of outsourcing to a hosted email security solution and continue to shoulder the burden of in-house email security. Managing network security is time consuming and expensive, and the true costs involved should be considered.

New forms of virus and malware are constantly being developed. Eliminating them means that your security must be updated to match. Continually upgrading to new software and hardware poses significant expense for security infrastructure, with training required to become familiar with new capabilities. To manage the explosions of spam and viruses traffic throughout their network, IT staff must constantly scramble to update or add servers and appliances to address the problem.

It is often assumed that in-house management is less expensive and of course, depending on the organisation, this may be the case. However even if less expensive, in-house management does not guarantee the most secure and reliable solution, and may face issues including:

- Email security is not an area of specific expertise for most IT staff
- Delay times downloading and testing patch leaving business exposed to new email threats
- Costly hardware and software updates, training and maintenance contracts
- Financial risk, legal liabilities and the potential for non-compliance with statutory and legal requirements
- Complex software and appliances having to be installed, configured and maintained, increasing the risk of system failure.

Hosted Solution

There is a growing trend towards adoption of a hosted service, compared to buying or licensing software and purchasing hardware appliances. The benefits of using third party services to manage infrastructure are now widely understood, as security becomes more complex and more difficult to manage in-house.

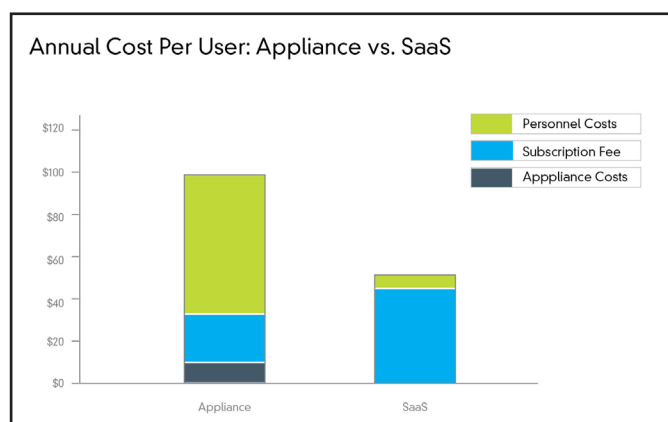
A growing number of SaaS providers offer enterprise grade solutions that exceed client expectations. IT staff are recognizing that one of the greatest benefits of outsourcing security is to make their lives significantly easier, while freeing up resources for other initiatives.

Organisations that have not yet explored SaaS services are leaving their business exposed to an increase in email and web threats, and often face difficulties in managing internal email archiving.

It's a critical decision whether to maintain email security in-house or through a third party. Choosing the best method for your organisation can give you a business advantage over competitors. So why should you adopt SaaS for email security?

AN INTEGRATED AND ADAPTABLE HOSTED SOLUTION OFFERS:

Lower costs. Hosted security services are generally significantly cheaper than on-premises security infrastructure. They provide support to end users, and eliminate most of the labour involved in managing security in-house. Over time, this benefit will increase as labour costs continue to rise.



Graph Source: Software-as-a-Service: A Comprehensive Look at the Total Cost of Ownership of Software & Information Industry Association (SIIA) 2006. Pros and Cons of SaaS Secure Web Gateway Solutions Gartner, 2007

Higher levels of protection. Hosted services provide up-to-the-minute technology designed to identify and eliminate threats and ensure that your email gateway is secure.

Free up internal resources. Outsourcing to a hosted security service means that the special needs of your business are dealt by specialist IT staff. The onus is now on your provider, and your network is their high priority, alleviating pressure on in-house IT staff. Their time is freed to proactively and effectively achieve organisational goals. Now there is no need to configure, monitor, maintain and manage software and email security.

Reduce network bandwidth. Third party security providers mean savings on bandwidth. Emails will be filtered, managed and maintained through the hosted service which frees up space on your network.

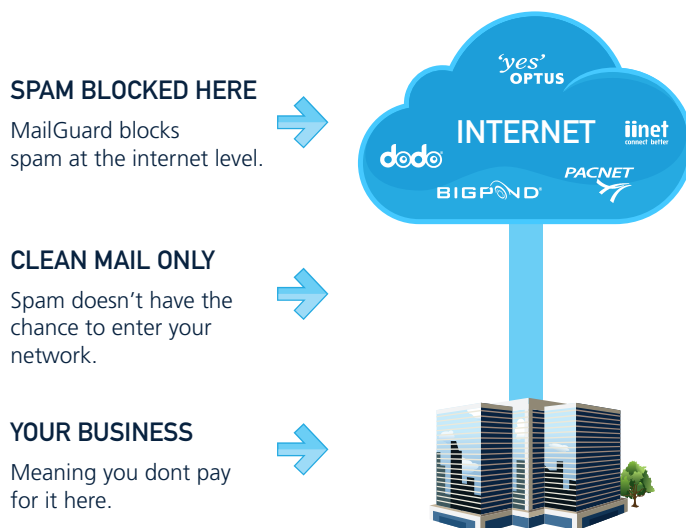
Optimised email capacity. As email traffic volumes continue to grow, mailbox size is spinning out of control, making management of the messaging environment even more difficult. Hosted providers can deploy traffic shaping and content filtering to assist in the elimination of unwanted and unsafe email, as well as offering archiving solutions, allowing significant increases in email capacity.

Increase future technology options. The impact of legacy systems on future technology and vendor decisions is minimized. You no longer have to manage complexities posed by sophisticated malware, spam and web-based threats, it's all done by your specialist provider.

ABOUT MAILGUARD EMAIL SECURITY

MailGuard is a fully-managed service that neutralises and manages threats before they enter your network. With multi-layered spam protection 'in the cloud' MailGuard successfully eliminates 99.97% of spam, constantly monitoring and combating new threats in real-time.

MailGuard proactively stops harmful viruses and spam from entering your network. It is a SaaS solution that sits 'in the cloud' reducing the impact on your network traffic. MailGuard filters all inbound and outbound email through multilayered protection systems located across our global data centres.



MailGuard is the most effective solution to protect your email gateway. It provides end-to-end security, delivering consistent protection against new and evolving spam and virus methods, whilst also protecting against data leakage and breaches of confidentiality.

Supported by comprehensive email usage reports, MailGuard protects against the unauthorised distribution of confidential or commercially sensitive information by providing a 360 degree view of your inbound and outbound email traffic.

MailGuard is a fully managed service that delivers peace of mind. Our dedicated team of security specialists and our systems are working 24 x 7 to stop email threats before they enter your network.

The benefits of MailGuard:

- Zero on-site footprint: No software or hardware. No licensing costs and no expensive integration costs as opposed to on-premises solutions, and no maintenance required from the end user.
- MailGuard's Triple Layer Anti-Virus protection is 'in the cloud', combating and eliminating threats before they can enter your network.
- Flexible customization of security preferences, rules, alerts and reports. MailGuard empowers you with knowledge and tools to manage your email security with confidence. • MailGuard's SaaS solutions can be deployed within hours, not days or weeks. Implementing MailGuard is a simple, quick process that allows you to increase your network protection with immediate effect.
- With MailGuard you only pay on a per-user, per-month basis, avoiding large upfront CAPEX. Deployment can be funded by OPEX budgets because it eliminates the hardware and software licensing and implementation costs associated with on-site solutions.

FURTHER INFORMATION

For more information, please visit www.mailguard.com.au/mailguard-signup to request a 14-day free trial of MailGuard.

MailGuard Pty Ltd

68-72 York Street,
South Melbourne
Victoria, 3205
Australia

Freecall: 1300 30 44 30 within Australia/NZ
Tel: +61 3 9694 4444 from overseas
Fax: +61 3 9011 6110

www.mailguard.com.au