

Buying criteria for email security – what’s right for you?

A Sophos white paper

February 2006

Faced with the growing volume and complexity of threats at the email gateway, organizations are looking for security solutions that offer better protection. The availability, expertise, and productivity of IT resources must be balanced against budgets, flexibility, and control. This paper helps IT administrators make an informed decision by comparing software solutions, appliances, and managed services, and looks briefly at the choices offered by Sophos.

Overview of gateway security

The email gateway is the focal point for message handling and can represent a major security challenge for enterprises today. The overriding objectives of email management are to deliver clean, wanted inbound email and clean outbound messages that comply with company and regulatory policy. The recent exponential growth in malware, spam, and blended threats, combined with the pressure to optimize resources and comply with legislation, is persuading many organizations of the need to review their security solutions. Some will have attempted to maximize performance by selecting best-of-breed point solutions. Others will have opted to simplify administration and budgeting by choosing a single vendor solution. Neither of these strategies will necessarily provide the best and most cost-effective protection – business requirements and resources need to be carefully evaluated before selecting a particular solution.

IT departments can choose from the following:

- An appliance, which combines hardware and software in a dedicated device
- A software solution
- A managed service, which delegates message handling to a third party.

Each approach provides a different set of benefits, risks, and disadvantages which must be reviewed in the context of the organization’s needs. Key to any decision is what level of involvement is required by the IT department in installing and maintaining hardware and software, and in monitoring and controlling the message stream. Other factors include the deployment of capital and operating budgets together with headcount, training, and investment strategies.

An in-house solution might seem the obvious choice to an organization with an established IT department and network infrastructure. In this case, the pros and cons of both software and appliance-based solutions need to be weighed against the productive use of IT resources and total cost of ownership.

A business that wants to minimize IT support should balance the benefits, risks, and costs of using an appliance or outsourcing to a managed service.

Evolving threats

The threat landscape is growing in complexity, driven by collaboration between virus writers and spammers. Their efforts are increasingly targeting individuals and organizations with the objective of commercial gain. The use of spyware, such as keyloggers, and phishing attacks allow spammers to access passwords and steal confidential information. Denial of service and zombie attacks can also compromise unprotected computer networks: the former denies legitimate users access to an email or web server, while the latter hijacks computers so that they can be clandestinely used to spam thousands of others. More details can be found in the Sophos white paper *The growing scale of the threat problem*¹.

Optimizing gateway protection

In evaluating the likely effectiveness of a particular type of gateway security solution, organizations first need to assess their risk profile, the availability and allocation of resources, and the support offered by the solution provider.

Risk assessment

Organizations require an insight into the volume of messages they need to process and what to protect against. Enterprises lacking this information, or wanting to improve their levels of protection, should review their vulnerability to a wide spectrum of email-borne threats. In addition to protecting against the security threats posed by malware and targeted attacks, organizations should ensure protection against potentially unwanted applications and spam, which threaten productivity. Threats are also becoming faster moving, often using a combination of techniques in new ways to evade detection – all of which means that protection should be regularly reappraised.

Balancing resources and requirements

When reviewing which type of email security solution to use, an organization needs to take into account the following business structure and investment factors:

- Size, expertise, and productivity of IT department
- Infrastructure capacity
- Policy regarding capital and operational budgets
- Policy regarding outsourcing.

Other business needs will determine what is required from a specific solution, for example:

- Simplicity of operation
- Degree of flexibility and control
- Failure contingency
- Scalability.

Email security appliances

Appliances have become increasingly popular in the last few years as a simple means of delivering security – and appliance products now cover a wide variety of security applications. Early products often provided disappointing results, but the latest appliances can deliver improved performance and security, and a better user experience. According to analysts IDC, by 2007, 80% of all network security solutions will be delivered via a dedicated appliance.²

Benefits

An appliance integrates hardware and software components in a single package that is straightforward to acquire and deploy with minimal IT support.

- **Management:** The best appliances offer management insight and control as well as remote assistance and real-time monitoring – combining key benefits of software solutions and managed services.
- **Performance:** Unlike a software solution, the performance of an appliance is optimized for a specific operating system and hardware.
- **Purchasing:** The hardware element of an appliance is normally purchased outright, while the software, maintenance, and support is conventionally licensed. Acquiring an appliance means there is no need to source and maintain a separate email server.
- **Deployment:** Appliances are usually quick and easy to install, with the best solutions offering plug-and-protect usability. Setup should be simple, but settings and rules can have varying degrees of configuration and flexibility.

An appliance typically aims to provide a “set and forget” experience, with the best providing automatic updates and upgrades.

- **IT support and productivity:** The ultimate appeal of appliances to organizations is that they require little or no IT expertise to set up and maintain. Even organizations with a dedicated IT department can benefit from using an email security appliance, as it can free up IT manpower to focus on tasks other than email management.
- **Cost of ownership:** Once an appliance is installed, the savings in additional hardware and IT support can lead to significantly lower costs.

Disadvantages

An appliance will be less attractive to organizations wanting a wide range of flexibility and control, particularly if advanced policy enforcement features are required.

- **Flexibility:** A consequence of simplicity of installation and operation can be a reduction in flexibility and customization capability, even though a good appliance will minimize these drawbacks. However, an appliance will in general provide less flexibility with regard to policy enforcement than a software solution.
- **Continuity of service:** Uptime is not guaranteed, so organizations should ensure that an appliance includes system redundancy to protect against the failure of hard disks and power supply.
- **Funding:** Buying an appliance requires capital budget to be available. An organization wanting to fund the full security package via its operating budget may find leasing the hardware problematic.

Software solutions

Despite the growth in popularity of appliances, software solutions remain the right choice where a high degree of flexibility and control is required. The advanced features of software solutions, and the need for hardware integration, demand a greater level of in-house IT expertise and reliable support from vendors.

Benefits

Organizations can choose a fully integrated solution from a single vendor, or mix and match different solutions for different tasks. The advantages are:

- **Flexibility:** Software solutions typically offer much more flexibility and control than appliances or managed services. Feature-rich, they allow organizations a high degree of fine-tuning of virus and spam filters, as well as a wider range of policy setting.
-

- **Advanced features:** Sophisticated software solutions provide administrators with a greater degree of control over aspects of policy and compliance, and give users more control of their email.
- **Scalability:** Advanced software solutions are highly scalable, limited only by hardware capacity.

Disadvantages

The penalty of highly configurable and customizable software is that installation and maintenance are very labor-intensive.

- **IT support:** Products can be relatively sophisticated and difficult to set up and deploy. Therefore, IT support costs are likely to be higher than with an appliance or managed service.
- **Hardware requirements:** As with any software purchase, hardware will also need to be acquired, and maintained with appropriate storage and backup.

Managed services

Organizations outsourcing their message handling aim to remove the worries of securing and managing email, and minimize the in-house resources required.

Benefits

A single contract, with no hardware or software to purchase, and very few IT resources required, can be very cost-effective for some organizations.

- **IT support:** Minimal support is required from IT, as all maintenance and updating is done by the service provider.
- **Flexibility:** A high degree of flexibility is available if traffic, quarantining, or archiving requirements change.

Disadvantages

The risks of using a managed service are similar to those associated with any outsourced service.

- **Control:** Direct visibility and control of the mail stream is not possible.
- **Targeted attacks:** The client organization cannot take direct action in response to a specific threat, such as a zombie attack.

Choosing the right solution

Factors which should prompt an organization to review its email security include:

- Declining spam catch rates
- Increased exposure to blended threats

- Insufficient time to protect against new threats
- Growing administrative burden at the gateway
- Unsatisfactory support from an existing vendor
- Poor experience with a first-generation appliance.

Early adopters of appliances have found that performance often does not meet expectations. First-generation appliances can contain a patchwork of solutions from different vendors and are difficult to coordinate and manage.

Reliability, convenience, and flexibility

Most organizations want to minimize the time spent on administering email, but the principal consideration must be to choose a solution that provides the most robust and reliable threat protection. Whether opting for software, an appliance, or a managed service, it is critical to choose a solution with a straightforward and effective management interface.

The levels of customization and policy enforcement available from a software solution tend to be much greater than those offered by either a managed service or an appliance, but realization of these benefits is heavily dependent on IT resources. In contrast, an appliance is a self-contained system requiring minimum support. As such, it will benefit organizations with few IT resources, or will enable those with good IT support to release manpower to focus on tasks other than email management.

A managed service offers the convenience of unlimited flexibility if capacity requirements change. The hardware elements of both appliances and software solutions mean that capacity can only be increased by adding a unit or substituting a bigger model.

The Sophos range of solutions

Whether organizations are looking for a simple but effective solution to email security or a flexible solution with a wide range of control, Sophos offers a choice. Sophos Email Security Appliances provides a plug-and-protect experience, with identical levels of protection to Sophos PureMessage software, which delivers advanced features for organizations wanting more flexibility and control. Both products use the same robust anti-virus and anti-spam engines and are backed by the expertise and technology of SophosLabs™ – a global network of threat analysis labs.

- **Sophos Email Security Appliance:** The Sophos appliance is the latest generation of enterprise-class gateway solutions, designed to deliver superior email protection

in a compact and easy-to-manage format. Its web-based management console provides complete visibility and control of the email infrastructure, simplifying administration and enhancing the decision-making process. Maximum uptime is ensured by built-in system redundancy and diagnostics, together with automated capacity optimization. The appliance also has many of the benefits normally associated with a managed service – it is continuously monitored by Sophos and receives anti-virus and anti-spam updates automatically.

- **Sophos PureMessage:** Based on a scalable architecture, PureMessage integrates into an existing infrastructure, enabling complete email management in a UNIX or Windows®/Exchange environment. A range of tools simplifies administrative tasks, while a centralized quarantine and powerful web-based administrative interface enable single-point management of multi-server systems. The end-user interface and spam digests allow end users to review quarantine contents easily. PureMessage also includes powerful content scanning controls and incorporates a rich policy environment to support complex security and regulatory compliance requirements.

Summary

In looking for a solution to their email security, organizations have a variety of options. They can choose between the delegation of protection to a managed service, the ease of use and manageability of an appliance, or the flexibility of a software solution. Organizations must evaluate the advantages and disadvantages of each, but whichever solution is ultimately chosen, the overriding criterion is that it needs to be reliable and robust, providing total protection against today's increasingly complex threats.

To find out more about how Sophos and our products can protect your organization, visit www.sophos.com.

Sources

- 1 <http://www.sophos.com/virusinfo/whitepapers/>
- 2 IDC, Worldwide Threat Management Security Appliances 2005-2009 Forecast and 2004 Vendor Shares: Security Appliances Remain a Well-Oiled Machine, 2005.

About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2006. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM