

Managed appliances: security solutions that do more

The complexity of dealing with enterprise security continues to grow, placing increasingly heavy demands on the IT department. Vendors have attempted to meet the challenge with solutions that strive to let the IT administrator do more with constrained resources and less time. But these have turned out to be at best only partial solutions. This paper introduces the concept of the managed appliance, highlighting how they serve a specific purpose (i.e. email or web security), and how they free up time while providing improved security, visibility and peace of mind better than any other type of security solution available today. It explains how managed appliances score over conventional appliances in the fundamental principles of efficient security management: reduced daily administration, an enhanced overall user experience, and proactive vendor support.

Managed appliances: security solutions that do more

In today's increasingly connected world, the challenges to maintaining business continuity seem never-ending. Shifting operational priorities, complex and evolving networks, and mounting internal and external security risks have led to an increasingly volatile environment. Nowhere is this more evident than in the IT department where success is expected despite daunting project scopes, tight timeframes, and perpetually strained resources – money, staff, and most significantly, time.

So how are today's IT administrators addressing the challenge of providing cost-effective, full-scope security while ensuring that administrators have time for other, more strategic priorities? The answer is that they are increasingly choosing appliance-based security solutions on the assumption (based on vendor promises) that appliances are easier to set up and use than software.

“
Just 7.91% of the overall IT budget in North American and European enterprises will go to security in 2007. 48% of respondents also identified security initiatives as a major theme for the IT organization.

”
Forrester Research, Jan 2007¹

Easily adaptable to any network infrastructure, and built on a maintenance-free operating system, appliances are, indeed, a natural form-factor for security solutions. But do they actually fulfill the promise of effective security with less effort? Do they enable better strategic management by providing better visibility and control? Or are they simply software on a box, offering no realizable benefit beyond a hardened operating system? Are they, in fact, simply a modern-day version of the emperor's new clothes?

Appliances defined

According to Gartner, an appliance is “a computing entity that delivers predefined service(s) through an application-specific interface, with no accessible operating software.”²

True appliances require a high level of integration between the hardware and software on a dedicated device. An appliance is not simply pre-installed software imaged onto a generic or re-branded server. It is a single package that is straightforward to acquire and deploy, minimizes the degree of configuration required during installation, requires minimal IT support and alleviates the need to manually patch, configure, and maintain the underlying operating system.

Conventional appliances: a promise broken

In response to the growing demand for simpler security solutions, vast numbers of appliances have flooded the market. However, most are not fulfilling the promises of overall time and resource savings. Further, not all devices marketed as appliances are actually appliances. They fall short of Gartner's definition offering neither the predefined service(s) through an application-specific interface nor the vendor-maintained infrastructure – in many cases, the vendor simply pastes the software onto the hardware. These appliance-like solutions in reality require substantial time to install, configure and manage.

“Most appliances fall short of Gartner's definition offering neither the predefined service(s) through an application-specific interface nor the vendor-maintained operating software.”

Those solutions which try to solve non-specific problems or pull together non-integrated fragments of solutions, frequently lack simplicity. As vendors work to get product to market quickly, they invest little thought in developing solutions that will reduce administrator effort, bringing together disparate functionality, delivering it on a single server and calling it an appliance. The absence of integrated design impacts the manageability of the device and usability suffers dramatically.

However, the ultimate criticism of today's appliances is their failure to build confidence that they are doing what they should. So although the burden of installation might be reduced to some degree, and although some appliances do offer

some flexibility if traffic, quarantining, or archiving requirements change, this does not constitute a promise fulfilled. Unless the administrator can also have confidence in the appliance's performance and availability, it has not delivered its true potential.

The managed appliance: the ideal solution

Into this field of incomplete solutions enters the managed appliance, bridging the entire spectrum of IT concerns and delivering clear benefits in measurable time savings and peace of mind. It adds value in critical areas such as system health monitoring, tracking of and assisting with anomalous traffic behavior, and one of the most time-consuming administrative tasks – internal help desk support.

The 'managed' part of a managed appliance becomes apparent when one looks at two aspects of its design: how it reduces day-to-day administrative overhead and saves time, and how it is supported by the vendor both proactively and reactively.

Day-to-day administration

Determining the time saved in any IT process can be difficult to measure. Yet such assessment becomes important when evaluating the added value of a security solution. All aspects of an appliance's design contribute toward its overall impact on administration and an experienced security vendor's insight into the latest network security issues can translate into more effective policy creation and deployment and better overall user experience.

Streamlined installation

An appliance should be ready to perform within minutes of being taken out of the box,

without the administrator having to read tomes of documentation. A well-designed managed appliance provides easy access to an array of features that makes this possible. For example:

- Configuration wizards can save a great deal of time and effort, minimizing data entry and offering access to targeted help topics when relevant.
- Automatic verification of network settings will ensure that the appliance is configured correctly the first time.
- Automatic detection of user authentication systems such as Active Directory® servers help pre-configure the appliance for the local environment and reduce the amount of time needed for installation and configuration.

Finally, many administrators want clear confirmation that the appliance is indeed in regular, scheduled contact with the vendor's security and software update services.

“*Managed appliances do more than simply cut down on administrative overhead – they engender the sense of confidence that comes from knowing that they are operating as expected and will continue to do so.*”

Instant policy set-up

Security policy optimization is a balance between efficiency and control. Achieving the right balance should be the vendor's challenge, not the administrator's. Vendors with extensive expertise in dealing with threats and who truly understand the challenges currently faced by IT departments will offer the optimal combination of powerful default

settings and easily accessible (but not excessive) customization options, available through a wizard-based interface.

Task automation/elimination

There are myriad tasks and events that administrators should never have to do manually: download threat definition updates, back up configuration data, archive logs, upgrade software, synchronize with LDAP servers for authentication and policy enforcement, and many more. Yet most security solutions, including appliances, fail to deliver even these most basic time-saving functions. One of the key differentiators of managed appliances is that they are designed to reduce or eliminate as many of these tasks as possible, without forcing compromises in other areas, such as acceptable use policies, protection of confidential business data and overall visibility and control.

Easier access to information

Easy access to relevant, actionable information is the critical foundation to any appliance interface. The administrator should only require a single graphic user interface (GUI) to manage all functions of the appliance, and should never need command line access for any task. Frequently accessed information – such as protection status, traffic patterns, throughput and system health – should be visible from a central dashboard. When more detail is required, the administrator should also be able to navigate the interface quickly using as few clicks as possible, regardless of the starting point or desired destination.

By providing quick, intuitive access to information, through a point-and-click interface with drill-down capabilities, and separate off-box archiving, a managed appliance makes it easy to carry out in-depth investigation.

Better reporting and visibility

When done properly, a good reporting system helps paint a clear picture of network traffic and enables better enforcement of security policies. A good reporting system also helps administrators plan for the future, by watching and predicting the impact of traffic on the overall network, not just the appliance. A managed appliance goes beyond the narrower scope of functionality addressed by traditional appliances by providing visibility into how it is affecting or being affected by upstream and downstream components.

“
If the vendor truly understands the core deliverable of a managed appliance – simplified security management – and has invested appropriately in the design and development process, this will be evident in the overall administrative experience.
”

Ongoing vendor support

A key area in which managed appliances score over other solutions, whether hardware- or software-based, is in the redefinition of the role of the vendor as an extension of an organization's IT department. Managed appliances do more than simply cut down on administrative overhead – they engender the sense of confidence that comes from knowing that they are operating as expected and will continue to do so. This is achieved by the vendor committing to both local and remote monitoring, and offering high standards of proactive and reactive support – offering an agreed service level that provides the clearest differentiation between a traditional appliance and a managed appliance.

Local monitoring and alerting

In order to focus valuable time on other more mission-critical activities, administrators should be able to avoid interacting with non-strategic systems such as security appliances unless a condition exists that cannot be resolved automatically.

To achieve this goal, the role of the managed appliance is clear:

- Keep track of what's going on – a comprehensive array of built-in sensors will monitor system performance and availability and should cover traffic anomalies, security updates and hardware performance (e.g. temperature or capacity), and more.
- Try to fix the problem if one arises – e.g. initiate an FTP backup of logs or quarantine to make space for new traffic.
- Alert the administrator to take some action if necessary – e.g. investigate downstream mail servers for queue delays, or isolate a spyware-infected client computer for cleanup.

Proactive support

Where managed appliances really stand apart from the crowd is in the domain of proactive support. With alerts being sent to the vendor as well as the administrator, the vendor is able to confirm that appliances are being updated on schedule and remotely monitor the health and performance of the appliance.

In addition, the ability to initiate contact and offer high-quality technical support even before the customer is aware there might be a problem, means that the vendor is able to prevent costly service interruptions, stop important data from being lost and avert critical failures that might occur at a later time if the condition were to go unnoticed. For example, if the FTP server that archives log and configuration data becomes unavailable, the vendor can contact the administrator directly.

Similarly, if a condition occurs that can fatally interrupt system performance or availability (e.g. failing hard drive or defective power supply), the normal operating environment can be rapidly restored with the vendor dispatching a replacement part or unit as soon as possible.

Reactive support

As well as looking for proactive support, appliance users will have many occasions where they look to the vendor to react quickly to specific requests. Changes to the network infrastructure, evolution of policy, or training a new administrator unfamiliar with the appliance, might lead the administrator to want help and guidance from the vendor and it is in the response to this type of request that the vendor of a managed appliance again differs from other appliance vendors.

Traditional support can come in different forms: built into the appliance and accessible via the GUI, in an online knowledgebase on the vendor's website, via email, or via live online or telephone contact with support engineers. But for a managed appliance vendor, there is an additional layer of reactive support that surpasses the speed and quality of support associated with traditional appliances and represents the responsibility assumed by the vendor for ensuring appliance uptime and availability.

This extra layer involves on-demand remote assistance, through which the vendor can log onto the customer's appliance and troubleshoot it remotely. Naturally, this service should be heavily guarded by security, leaving the customer with ongoing control over the remote session and giving them access to detailed logs of any modification made by the vendor.

Summary

The challenges faced by organizations in maintaining network security while protecting business information and client confidentiality have become increasingly complex and time-consuming. Dealing with emerging security issues while trying to accomplish more strategic initiatives is an increasingly fine balancing act for IT administrators. Organizations that seek reduced administrative effort without compromising security or business practices now have a new choice: managed appliance solutions. Retaining insight and control, avoiding costly down-time, and ensuring efficient, effective and reliable security can only be achieved by working with vendors that understand the challenges facing IT departments, and offer solutions that add real value beyond security.

The Sophos solution

Sophos managed appliances for email and web security provide the performance, reliability, insight and support that IT administrators need, freeing up time to focus on their business and not on their infrastructure. Every Sophos appliance is built on a robust, easy-to-install platform that features a highly intuitive, easy-to-use management console for quick access to relevant, actionable information. They include time-saving features such as automated installation and configuration, automatic updates to threat definitions and software every five minutes, an advanced alerting system, remote heartbeat monitoring and on-demand remote assistance. In addition, all appliances come with 24/7 proactive technical support.

Sources

- 1 Trends 2007 “Security budgets increase: The transition to information risk management begins”, Forrester Research. Base: North American and European enterprises
- 2 Neil MacDonald, Thomas J Bittman, Martin Reynolds, Brian Gammage, Findings: Not all appliances are appliances, Gartner, 12 Sep 2006

For more information on Sophos managed appliances, visit www.sophos.com

About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years’ experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

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

© Copyright 2007. 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