Realtime publishers
"Leading the Conversation"

The Essentials Series: Selecting the Right Network Threat Management Solution

Hidden Costs of Off the Shelf Security Products

sponsored by
NOKIA

by Dan Sullivan

Copyright Statement

Hidden Costs of Off-the-Shelf Security Products

An ever-present challenge facing IT managers is whether to buy a complete solution to a problem or develop a solution in-house using server-based security products. In the case of network security, a business might decide to purchase a server, an antivirus application, an intrusion prevention system (IPS), and a reporting tool to counter threats to the network. Alternatively, organizations can purchase an appliance that consolidates these functions in a single device. At first, a server-based approach might appear more appealing; after all, systems administrators and network managers will have complete control over the server, which is configured to their specification and running applications they hand pick. However, appliances can leverage provider configured and tuned operating systems (OSs), performance-enhancing application programming interfaces (APIs) for security software, and consolidated management and reporting systems. Given these differences, one should consider a number of factors when purchasing security products:

- Long-term cost effectiveness
- Types of hidden costs
- Key management questions regarding building a custom solution (that is, installing software on a server and running it as a network security solution) versus buying a consolidated solution (that is, an appliance)

Businesses will each have specific requirements that need to drive any product evaluation. The goal of this article is to discuss common and long-term considerations when buying off-the-shelf security products.

Long-Term Cost Effectiveness

It does not take long for a novice IT manager to realize that the initial purchase price of any information system is a fraction of its total cost. Nonetheless, the temptation to focus too much on the initial outlay of funds can distort one's perspective. This is understandable. Just as "limited time offers" and calls to "act now" can introduce distorting factors into our reasoning about purchases, the initial price of a product can easily become the focus of decision making. This can be a mistake.

Apparent Advantages of "Do It Yourself"

Consider a "do it yourself" scenario, in which software is installed on general purpose servers, with regards to a collection of security applications. Several considerations make this an appealing option:

- The potential for running the application on commodity hardware, which may reduce initial costs
- The ability to select the best-of-breed application for specific application areas, such as antivirus scanners, anti-spam filters, and IPSs
- The option of purchasing only the functions you need and not paying for applications that will not be used in the foreseeable future
- One still retains the ability to redeploy hardware if requirements change or hardware upgrades are obtained for the security application server

It should be noted that some of these features—such as selecting best-of-breed applications, customizing configurations, and redeploying hardware—may be available from some appliance vendors. The reasons listed previously are compelling reasons to use a cafeteria-style approach to deploying security measures, but there are both obvious and not-so-obvious limitations.

The most apparent limitation is that there is little or no coordination among the products (see Figure 1). For example, with the DIY approach, you have silos of reports each focused on a particular application with little or no coordination with the other tools. Of course, you are free to write applications to scan logs, extract data, apply normalizing transformations, and then store data in a specialized reporting database for use with custom reports—that is, if you have the time and resources.

Another consideration is that firewalls are network security products. You will want visibility into network services such as routing, traffic monitoring, protocols being used, application performance, and so on. Software on a server isolates the security services from these network services and proper management of network security can provide visibility of both.

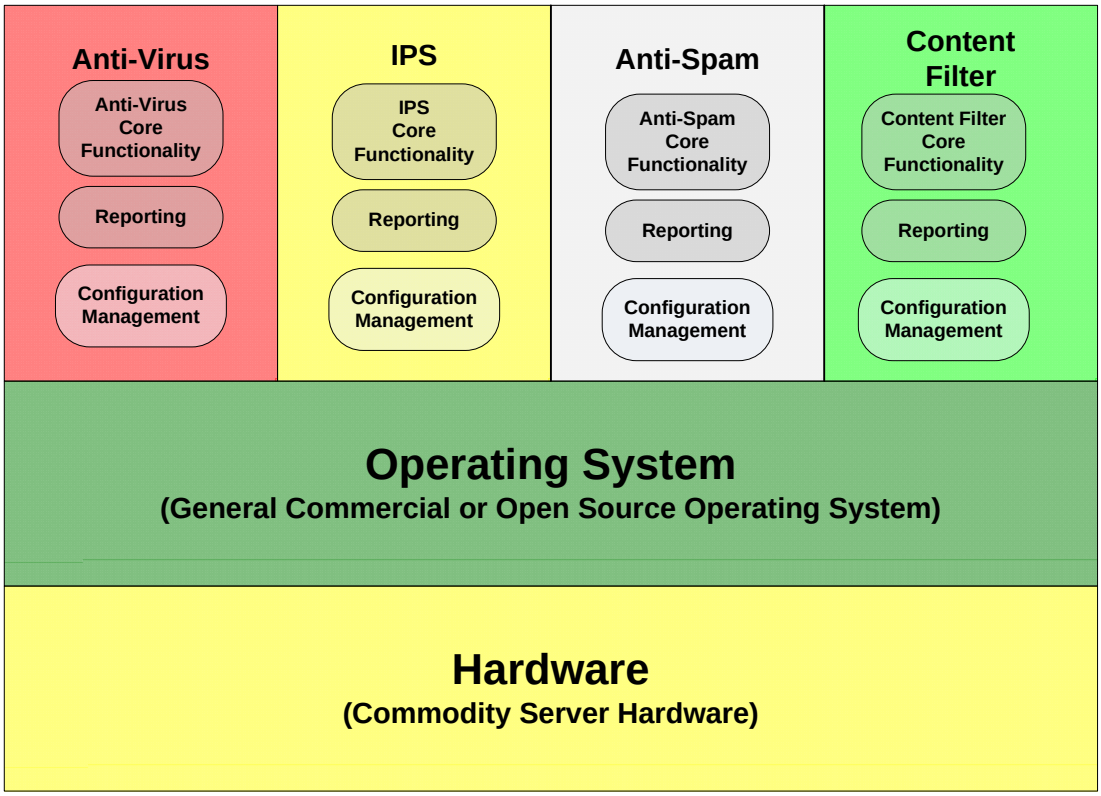

Figure 1: Custom off-the-shelf product deployments might run on a single server but still retain the essential characteristics of a silo approach to security management. As depicted here, the application layer consists of isolated security applications each with separate management and reporting functionality.

Drawbacks to DIY

The drawbacks of the do-it-yourself—deploying security software on a general-purpose server—approach fall into a few categories:

- Limited standardization
- Maintenance overhead
- Support issues

The underlying technical issues of these areas still exist in unified solutions, but they are typically addressed by the vendor, not the customer.

Limited Standardization

Systems administrators can configure their own servers; thus, it would appear that standardization is easy—but this is not always the case. Hardware components may change even if a vendor's model number does not. For example, a server configured with a pair of SCSI drives purchased today may have a slightly different configuration from the same drives purchased in a server ordered 6 months ago. Differences can manifest themselves when configurations designed for one server do not work on another because of differences in dependencies between the two. Another all-too-common problem is that IT staff spends too much time in root cause analysis and updating drivers so that hardware components will work properly together.

Maintenance Overhead

When an IT department configures its own multi-function security device, it is the staff of that department that is responsible for maintaining it. This includes testing patches, running down dependencies between modules, making sure the correct versions of operating system (OS) libraries are in place, as well as fixing misconfigured components. This is not the case with a network appliance. Vendors, who are most familiar with their components and their code, can deploy patches, configuration updates, and new versions of software to all customers. The basic economic principles such as economies of scale and division of labor favor specialized appliances.

In terms of economies of scale, a vendor can spread the cost of designing, testing, and improving security devices over its customer base. This allows vendors to employ production techniques that are efficient at a large scale but not at the scale of a single business customer.

With regards to specialization of labor, an IT department that needs to configure several, perhaps a dozen, custom-configured security devices cannot reasonably dedicate an employee to that task for long periods of time. A vendor with a broad customer base can justify the expense of dedicated teams of employees for extended periods of time to develop expertise and ensure high-quality configurations.

Support Issues

One of the most difficult IT situations to manage is when a customer needs support services from multiple vendors at the same time. Imagine a common scenario: A business runs security software from one vendor and an OS from another vendor on hardware produced by yet another source on the same device, and the systems are not working properly. The first-tier service representative from one vendor might conclude their component is not the problem and the root cause must be elsewhere. The second vendor has the same conclusion about their software. Specialized security appliances are designed to allow security applications to work in concert with the network layer of the OS that is properly configured for the hardware it runs on.

Now, in fairness to the vendors providing components to server-based security solutions, they are right not to try to diagnose a problem outside their realm of expertise, especially with a server that may be configured in ways and for reasons they do not understand. Nonetheless, the problem is not resolved and the customer is left to diagnose the problem themselves or expend time and effort to escalate their issue with both vendors until a solution is found.

These obvious drawbacks of custom solutions, from limited standardization to extra maintenance overhead to vendor support coordination can be reason enough to choose a network appliance approach. They are not the only reasons, though.

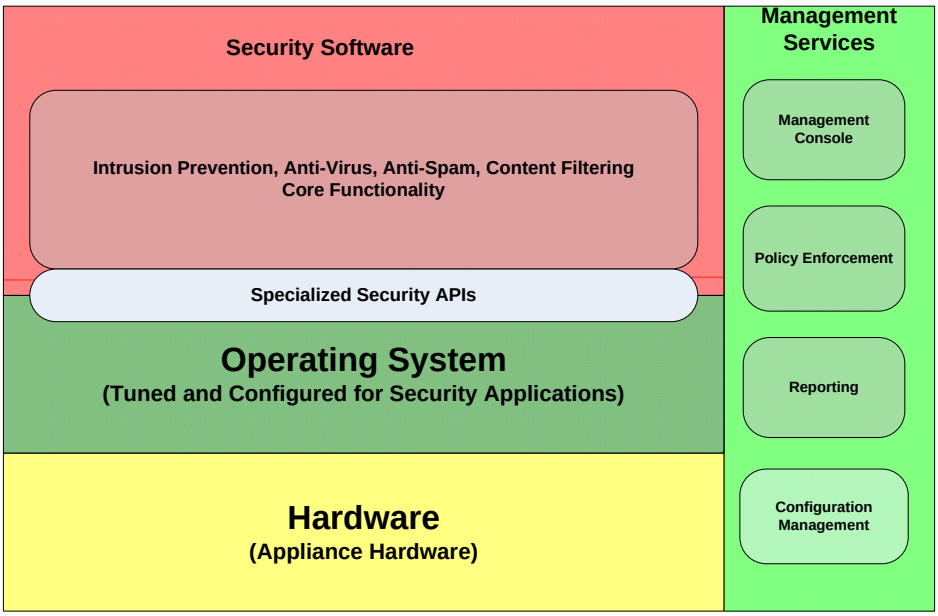

Figure 2: Appliance-based solutions provide a more unified and coordinated approach to security management with shared services at the application layer. In addition, security software can leverage specialized APIs provided by an OS tuned and configured to optimize performance of security applications.

Hidden Costs of Off-the-Shelf Security Products

The hidden costs of combining off-the-shelf security products include increased operational costs and the opportunity costs associated with a server-based solution. These sometimes less-apparent costs should be taken into consideration when calculating the TCO of a custom solution.

Increased Operational Costs

The additional maintenance tasks described in the previous section incur costs in addition to the purchase price of security products. IT staff need to dedicate time to patch and configure systems. Unfortunately, as the complexity of custom solutions increase, so does the likelihood for the need of additional maintenance. Consider the human factors in properly configuring a complex server-based security device. Given the large number of configuration parameters and the range of knowledge required to properly configure the entire device, one can easily introduce configuration errors. Security appliances, however, are based on standardized platforms and application stacks that have been tested before deployment. The risk of misconfiguration is much less with a security appliance than with a server-based security solution.

Opportunity Costs

Another fundamental economic principle that weighs in favor of security appliances is opportunity costs. The time IT staff spends patching, diagnosing, and reconfiguring custom security devices could be better spent on other pressing business needs that cannot be delegated to someone outside the organization. Appliances demand less time of network support staff and thus contribute to more efficient operations.

Summary

The disadvantages of custom off-the-shelf solutions outlined here raise a key management question: Do the benefits of a do-it-yourself approach outweigh the additional costs and risks when compared with a consolidated solution? Many of the advantages of server-based solutions, such as the ability to select only functions needed, are available from some appliance vendors. More importantly, though, is the fact that security devices offer little margin for error. Ironically, maintaining a properly configured server-based solution is challenging and offers opportunities to introduce errors which result in security vulnerabilities. Other drawbacks of the server-based approach include increased operational costs, the opportunity cost of maintaining custom configured servers, and less consolidated reporting and management functions. The long-term management benefits and the assurances of properly configured and tested security appliances are compelling benefits of appliance-based security solutions.