



**astaro**  
internet security

Network Security Whitepaper

**Redundant Security Tools: when  
having two security products makes  
sense**

Version: 1.00

Release date: April 26, 2004

Author: Alan Radding



## Redundant Security Tools: when having two security products makes sense

---

Astaro [www.astaro.com](http://www.astaro.com) [info@astaro.com](mailto:info@astaro.com)  
3 New England Executive Park, Burlington MA, 01803 USA  
Pfinztalstrasse 90, 76227 Karlsruhe, Germany

### Table of Contents

<b>Counter-intuitive IT makes economic and security sense .....</b>	<b>3</b>
<b>Layered security/defense in depth .....</b>	<b>3</b>
<b>Why you want redundant security .....</b>	<b>4</b>
<b>Recommendations .....</b>	<b>6</b>
<b>Selecting additional security tools .....</b>	<b>6</b>
<b>Astaro Security Solutions .....</b>	<b>7</b>
<b>Conclusion .....</b>	<b>7</b>

## *Counter-intuitive IT makes economic and security sense*

Conventional IT wisdom argues for the rationalization and standardization of information systems. Having fewer different systems, vendors, products, and applications for the same functions reduces complexity, which, in turn, lowers costs while improving performance and productivity.

Acting on this wisdom, IT managers consolidate servers and storage as much as possible. They try to standardize on one database management system, one set of application development tools, one middleware vendor, one systems management suite. They rationalize their application portfolios generally by eliminating abandoned, lightly used, and redundant applications.

But they never completely succeed at fully rationalizing their systems; nor do they want to. Different locations require different systems. Different groups within the organization have valid reasons for needing different tools. Culture, skills, budget, timing, geography, and unique requirements all force IT into modifying its desire to standardize and accepting multiple systems.

Security makes a particularly good exception to the urge to standardize all IT systems. Implementing multiple security tools improves security and can actually lower costs. For example, the second tool may have more updated capabilities or new capabilities that the primary security tool lacks and yet cost less to acquire and deploy than the primary tool. In this paper, we will look at why many organizations opt for multiple security tools and suggest ways for you to mix and match security tools to maximize security and minimize cost.

## *Layered security/defense in depth*

Your systems have to operate in a dangerous environment characterized by many types of threats. Threats can involve malicious intruders, viruses, worms, denial of service, spoofing, and more. The source of the threats may be external or internal. And the risks are varied: loss of confidential information, theft of customer data, corruption of systems, disruption of networks and systems, systems failure, and more.

To guard against these multiple and diverse threats, organizations are adopting a layered security strategy often referred to as defense in depth. Defense in depth assumes that no single tool can effectively protect against every threat from every source all the time. As a result, it calls for multiple, often seemingly redundant security tools to be deployed in a layered fashion. It takes advantage of the fact that similar security tools will do the same security task differently, which adds another level of defense, while yet other tools are focusing on other parts of the overall task, which extends the scope of the defensive strategy. In this way a threat that evades one defense is picked up and neutralized by another.

In addition to ensuring there are no gaps in the organization's defenses, such a layered or redundant security strategy can actually lower security costs. This occurs when organizations take advantage of differences in pricing and packaging among the different security product vendors to lower the total security cost.

In the end, a layered defense in depth gives you:

- More complete security by covering all the options
- Flexibility to mix and match tools to meet different threats
- The likelihood of lower cost and easier, faster deployment

For example, an existing firewall may be effective as a firewall but lack other capabilities the organization now seeks, such as a spam blocking or URL filtering. Rather than rip-and-replace the existing firewall, it can augment the firewall with a security tool that includes the new functionality.

Similarly, a high priced enterprise security tool, such as firewall or an intrusion detection system, may be appropriate at a central primary entry point. However, the organization can deploy lower cost departmental tools internally and at secondary entry points for added security and to protect against internal threats. This saves the organization from having to repeatedly incur high fees by rolling out the enterprise tool everywhere protection is desired, even in places where the risk doesn't justify the cost. Although the organization is investing in tools from two different vendors, the total acquisition cost will be lower and the cost of deployment may be lower if the second security tool is easier and faster to deploy, which is often the case.

## *Why you want redundant security*

Redundant security—the use of multiple security tools with overlapping or complementary functionality—can be a smart choice from both a security and economic standpoint. Managers opt for redundant security for one or more of the following reasons: gap coverage, cost savings, new/improved capabilities, and extra defense.

Specifically:

- Gap coverage—the redundant security tool performs essentially the same function as the primary tool but does so in a different way or adds extra functionality that covers gaps in the defense provided by the primary tool. For example, the second tool may bring a more extensive list of virus signatures and provide better virus pattern identification.
- Cost savings—the redundant tool costs less to acquire, deploy, and maintain, allowing it to be deployed in situations that don't justify the investment in the primary security tool.
- New/improved capabilities—the redundant tool addresses new threats that were not apparent when the primary security tool was initially deployed, or the redundant tool

executes certain capabilities in a better way. The second tool, for instance, can bring spam filtering or URL filtering to the primary firewall tool that lacks these additional capabilities.

- Extra layer of defense—the redundant tool provides another layer of defense, which offers another opportunity to thwart a threat

The following table summarizes the reasons for deploying redundant security and the benefits.

Purpose	Description	Benefit
Gap coverage	Fills in areas needing protection not effectively covered by the primary tool	Ensures more comprehensive security coverage
Cost savings	Deployment of less costly tools in non-critical areas	Stretches the security budget by minimizing the need to deploy higher cost tools in every situation
New/improved capabilities	Adds new or improved capabilities, often to address newly emerged threats or take better advantage of changes in technology	Protects the organization from the latest threats
Additional layer of defense	Makes it more difficult for attacks to succeed by adding another defensive hurdle that the threat must overcome	Increases security by providing another opportunity to thwart potential threats

In practice, the redundant tool turns out not to be so redundant after all. It is frequently the case, as noted above, that an organization deploys a primary firewall. While it is effective as a firewall, it will lack important capabilities, such as intrusion detection, spam protection, or URL filtering—capabilities that have become important since the primary firewall was initially selected and deployed. In other cases, the primary tool may have basic anti-virus or web content filtering capabilities but a second tool adds a more extensive, more frequently updated list of virus signatures or URLs. And while it brings important new capabilities to the organization’s defense in depth, the second tool may also be lower in cost or easier to deploy, which makes it all that much better.

## *Recommendations*

Although rationalizing diverse systems and standardizing on a single enterprise selection is generally a good IT practice, there are important reasons, as noted above, to deviate from this practice. Layered security and defense and depth, widely recognized as a more effective approach to security, entail multiple security products that often have some overlapping capabilities. Through the deployment of multiple security tools, organizations can increase their overall security, lower the total cost of security, cover gaps in security defenses, and ensure they have access to the latest functionality and most accurate virus definitions, URL databases, and more.

Leading industry researchers concur: According to International Data Corp. (IDC), a leading technology research firm based in Framingham, MA, "...there will be a strong push toward a layered security ... The layered security approach will combine solutions such as desktop anti-virus, server and gateway (perimeter) anti-virus, content filtering...and firewalls. " Similarly, the layered approach encompasses the deployment of diverse security tools with seemingly overlapping capabilities for economic reasons and to cover security gaps.

## *Selecting additional security tools*

When selecting security products, managers need to keep four critical factors in mind: cost, deployment speed, ease and frequency of updates, and functionality.

- Costs—not every situation requires a costly, industrial strength security solution. Organizations can save money by choosing less costly tools for less critical, lower risk situations. Tools that are easy to deploy and maintain also lower the total cost of ownership.
- Speed of deployment—some security is better than none. Rather than wait until you have the time and budget to deploy a full security solution, organizations can deploy a low cost, lightweight product that can be acquired and deployed immediately.
- Ease of updating, frequency of updating—security threats continuously change. Some security tool vendors update their capabilities and security databases in light of the latest threats much more frequently than other vendors.
- Available functionality—not every security tool provides every capability or executes a given capability well. By mixing and matching tools, the organization can assemble the full range of functionality it requires; say augmenting a basic firewall with spam protection or anti-virus defense or intrusion detection.



## Redundant Security Tools: when having two security products makes sense

---

Astaro [www.astaro.com](http://www.astaro.com) [info@astaro.com](mailto:info@astaro.com)  
3 New England Executive Park, Burlington MA, 01803 USA  
Pfinztalstrasse 90, 76227 Karlsruhe, Germany

There are a number of security products vendors in the market and more enter and leave the market all the time. The following factors will help you find the right security vendor:

- Synergistic capabilities—complements or reinforces what you already have
- Integration with the other security applications—simplifies security administration and lowers overall TCO
- Security track record—look for a vendor with a proven track record in identifying viruses quickly
- Frequent updates to handle the latest threats—the vendor's responsiveness to changes in security conditions and its ability to update its capabilities and security databases quickly and frequently in the face of emerging threats.

### *Astaro Security Solutions*

Astaro Security Linux includes firewall, intrusion protection, virus protection, VPN, spam filtering, and URL filtering as part of its comprehensive solution. These capabilities are all managed from a single, consistent user interface. An integrated update mechanism updates all the security applications in Astaro's comprehensive security offering as well as providing enhancements to the basic security engine. Integrated management will reduce the workload on the organization's system administrators, which will significantly reduce the TCO.

Astaro Security Linux is the best-selling open source-based network security product, and has won numerous awards. Now in its fifth release, it is protecting 20,000 networks in more than 60 countries. Many organizations that have deployed other security solutions find it is highly effective and economical to augment their existing security solution with advanced functionality from Astaro, such as VPN, spam protection, or URL filtering.

### *Conclusion*

Although Astaro, with its comprehensive capabilities—firewall, intrusion protection, virus protection, VPN, spam filtering, URL filtering—can serve as an organization's primary security solution, it also complements any security tool portfolio. With its rich set of capabilities, it can be used to cover gaps in the organization's existing security solution. With its fast, easy deployment and frequent updates, it can supplement the organization's security by addressing the latest threats. Finally, its low cost makes it an ideal choice for areas where more costly tools are inappropriate. Using Astaro under these circumstances enables the organization to achieve greater security at a lower total cost of ownership. A free 30-day evaluation version can be downloaded at [www.astaro.com](http://www.astaro.com) to verify operation in your environment.