

# Astaro OrangePaper

## Open Source Security Myths Dispelled

Author: Angelo Comazzetto

*Astaro Product  
Evangelist*



Date: 2007-09-25

| <b>Content</b>  | <b>Page</b> |
|---|-------------|
| Introduction .....  | 2           |
| Myth One: Open Source Software Is Too Risky for IT Security .....         | 2           |
| Myth Two: Open Source Software Is Free .....                              | 4           |
| Myth Three: Open Source Vendors Add Little Value to OSS Projects .....    | 6           |
| Myth Four: Proprietary Solutions Are More Reliable than Open Source ..... | 7           |
| Myth Five: Open Source Security is too Complex for Small Businesses ..... | 8           |
| Conclusion .....  | 10          |

## Introduction

Open Source Software (OSS) is computer software whose source code is available to the general public with relaxed or non-existent [intellectual property](#) restrictions (or arrangement such as the public domain), and is usually developed with the input of many contributors. In the security space, this type of development also brings the expertise of multiple persons to bear on the design and architecture of a software program, making it robust and capable of doing the job for which it is being designed. The openly viewable nature of the source of a program means that if possible problems are found, they can be quickly addressed and altered to adapt, again with the supervision of more than one company / programming team. When choosing between proprietary and open source security solutions, many organizations are misled by open source myths. As a result, they ask the wrong questions when evaluating their options and unnecessarily limit their IT solutions.

Is it risky to trust mission-critical infrastructure to open source software? Why should we pay an open source vendor when open source is supposed to be free? Will a shift to open source add complexity to our IT infrastructure?

These questions all arise from open source myths that this paper will explain and dispel, allowing IT decision makers to focus on more important organizational issues: return-on-investment, ease-of-use, agility, reliability, and control.

## Myth One: Open Source Software Is Too Risky for IT Security

Many IT decision makers have a knee-jerk reaction to OSS, especially when it comes to security. They believe OSS is most appropriate for do-it-yourself technology geeks working in their basements. It might be fine for a company with an obsessive technology savant on staff, but for the rest of us, OSS is unproven, complex, and risky.

That's the myth. The reality is that OSS is already part of most IT infrastructures. A recent [Network World magazine article](#)<sup>1</sup> looked at the state of open source adoption within the enterprise and found it widely pervasive. "Most of the packaged security appliances for everything from firewalls to

---

<sup>1</sup> <http://www.networkworld.com/supp/2007/ndc2/031907-open-source-security-side-code.html>

security information management are built on the same BSD Unix and Linux distributions as the application servers you build yourself," according to the article.

A recent [Forrester Research report](#)<sup>2</sup> further argued that enterprises should seriously consider open source options for mission-critical infrastructure. "Although fewer than half of the large enterprises in Europe and North America are actively using or piloting open source software, a majority of those are using it for mission-critical applications and infrastructure," the report said. The debate about open-source vs. proprietary solutions has long been discussed, and generally open-source critiques attack the stability of the platforms as not ready for widespread adoption due to their ever-changing natures as they evolve from more contributions to their features and code. They also criticize open-source for requiring so many patches to stay secure.

The truth is that while many open-source network security programs are continually evolved, this is usually a direct result of research done and progress made by the open-source programming community. The resulting projects and programs reflect current trends and the needs created by them, offering programs with cutting-edge functionality built for today's Internet. The argument that open-source must be unreliable since it requires so many patches is countered with the explanation that by having so many individuals and companies continually examining and working with the source code of these projects, potential vulnerabilities and design flaws are uncovered much faster than with programs build on proprietary code. Open-Source platforms are as a result considered more secure than many of their proprietary counterparts, since the frequency of the updates offered keeps the windows of vulnerability and susceptibility to an absolute minimum.

Besides the already successful generally acknowledged open-source projects like Linux (an open-source operating system with many distributions), and Apache (one of the world's most successful web servers), open source security software already common in enterprise settings includes OpenSSL, an encryption tool, Snort, an intrusion detection engine, and Exim, a fast and reliable Mail Transfer Agent.

Many of these applications are also used today within commercial security products, for instance the Astaro Security Gateway, an all-in-one security appliance which uses many of those OSS projects for its protection

---

<sup>2</sup> <http://www.forrester.com/Research/Document/Excerpt/0,7211,38866,00.html>

mechanisms. Astaro, who has been developing and selling this product since 1999, has not only won several “Best Security Solution” awards from publications like SC Magazine and at industry trade shows like Linuxworld, but also further proved their reliability by receiving ICSA certification and Common Criteria compliance. Key design elements such as deploying the solution in a fully secured or “locked down” configuration ensures that only what is enabled and configured will be operational on the device, with all other traffic being logged and dropped. Further, a complete built-in self-monitoring system continually checks the health of all system components enabling the system to fix many problems on its own (e.g., by restarting specific processes), and offering alerts and notifications for hundreds of possible events, ensuring those responsible for the device remain informed regarding its status.

Many forays into open source security are implemented successfully, only to suffer setbacks as the result of improper maintenance. The ability to correctly patch and update the various facets of a solution that uses OSS is crucial to maintaining security as well as stability, since otherwise issues can arise from having un-patched components that are susceptible to attack or disruption. The Astaro Up2Date feature (which is standard in every ASG installation) allows users to download, verify, and apply patches, feature additions, and pattern updates via an automated system. This removes the need for administrators to remain constantly vigilante in ensuring their open-source solution is properly maintained, as all components of the Astaro environment can be updated accordingly via this automated process.

## Myth Two: Open Source Software Is Free

Another myth is that open-source is free of charge, and as such generic open source implementations can save thousands of dollars. A common question that open source vendors face every day is “why should we pay for something we can go download for free?” Certainly, OSS can be downloaded for free but that is where “free” begins and ends. There are certainly other advantages to OSS, such as strong community support, continuous upgrades, and the ongoing improvement of projects by those using them. All of these advantages are technically free to any user, but someone must manage, evaluate, and then support whatever open source product your organization adopts. If your organization would rather concoct its own OSS security suite from scratch, then it is possible to do so, however be prepared to invest vast amounts of IT capital into such an effort. Not only must a company install and configure

individual projects, but actually blending multiple projects together, all working with the correct interoperation and harmony, and being maintainable with regards to security patches and other upgrades, is a vastly complex task.

For example, while installing an Intrusion Detection component along with a VPN solution on the same platform is technically possible, however it takes a much more detailed understanding of many different factors in order to ensure proper processing of the traffic, so for example the VPN tunnel traffic is first decrypted, and then run through the IDS engine ensuring that encrypted traffic handled by the tunnel does not contain malicious payloads. Making things operate together is an essential component in deploying an effective security system.

Open source products tend to be created by developers for developers. These creators thrive at the command-line level and enjoy developing their own work-arounds and add-ons. In a typical enterprise setting, however, most organizations would rather not have their limited IT resources devoted to customization and decentralized management. Most OSS developers are driven by technical enthusiasm, not commercial pressures. That being the case, how do you get them to work on the more mundane things, such as interoperability, documentation, and GUIs, for non-technical end users?

A final issue is accountability. If homespun open source security fails, who is to blame? Is it the software itself? Perhaps, but what if it was configured improperly? Is it some other product within your infrastructure that has created a conflict? It's possible, but you'll need to search through bulletin boards or wait for an expert within the community to respond to the question you post to find out. Is it your own IT staff member who managed the project? After all, that's the exact person you will have to ask to get an answer. As the cliché states, 'you get what you pay for.'

With commercial products like the Astaro Security Gateway, the traditional negatives of using a fully free open-source project are countered with full documentation and technical support for all areas of the product, and reinforced with resources like how-to guides, training sessions, and a searchable knowledgebase. Astaro removes the need for open-source platform knowledge, and provides a network security firewall, web and email filtering, full VPN capability, IDS, and much more, that can be totally configured using a graphical user interface with minimal security knowledge and no command-line or Linux knowledge required.

## Myth Three: Open Source Vendors Add Little Value to OSS Projects

There is sometimes a perception that paying for open source-based products is a waste of money, since acquiring the same projects a company bases a product on can be done for free (see Myth #2) and as such companies that attempt to commercialize OSS do not really add anything substantial to the offering that justify the costs they demand. Also, some question the legality of charging money for products based on the work of others. This myth is partially based on a common misunderstanding of open source licenses. Under the most common of open source licensing, known as the GPL, vendors are free to distribute and sell OSS if they follow the rules of the license and *add value*. In various products, vendors not only harness existing projects and code-bases in order to build their solutions, but then contribute back to the community in offering features, performance improvements, financial support, and more. This further evolves the community, so that it benefits from the commercialization and can continue to evolve. Examples of this are the many versions of Linux, the Apache web server, and the popular Netfilter firewall project.

Companies that commercialize open-source software and add value such as documentation, guides, interfaces, interoperability and more, create a solution known as “mixed source” or “hybrid” solutions; a blend of both open-source and proprietary components. These solutions give customers the best of both worlds; they are based on a solid open source foundation, while also offering the support, documentation, QA testing, and upgrades. This provides a final level of polish that makes the solution stable, manageable, and realistically deployable at more companies than an open-source-only solution.

Mixed-source vendors also add checkmark features to products that ensure they’re appropriate for real-world enterprise settings and not just development scenarios. Failover, redundancy, auditing, reporting, intuitive GUIs and other similar capabilities tend to be overlooked by developers who focus on technical challenges rather than business ones. Documentation and associated help for many open-source projects can also be quite vague, as again the technical nature is understood by the developer(s), but poorly (or not at all) communicated to the end-user. Mixed-source not only brings these projects to the masses, but can add the necessary reference material to allow everyday use of their features and workings.

One of the key value propositions that mixed-source vendors bring to the table is usability and integration. OSS often tackles narrow technical challenges, and bringing together disparate projects into a workable, interoperable security solution is a demanding chore.

[Astaro Corporation](#) is such a mixed-source vendor. Their Astaro Security Gateway product is a Unified Threat Management platform that weaves together powerful open-source programs, licensed technologies (like Anti-Virus engines), and proprietary code.

All these components are joined together into a fully integrated solution by Astaro's patent pending Content Filtering Framework, which are completely managed under a single graphical user interface (GUI).

## Myth Four: Proprietary Solutions Are More Reliable than Open Source

As mentioned at the start of this paper, the reliability and dependability of OSS is called into question by closed-source proponents. If today's security solutions – open source and proprietary alike – start with the same Linux or Apache foundation, then those tasked with securing the world's networks disagree with this premise. If security experts trust open source, why shouldn't you?

Proprietary solutions do present many advantages such as providing technical support, training, pushed updates, integration via APIs, and innovative GUIs. Today however, these same advantages are being added to lower-cost OSS alternatives by mixed-source vendors. Adding to this is the fact that the open source community actively resists much of what customers dislike about proprietary solutions, such as vendor lock-in, high initial costs, lack of feature upgrades/additions, and escalating maintenance contracts. Open-source licenses discourage the kind of secrecy that has plagued proprietary software for decades, secrecy that has led to vulnerabilities and the inability to enhance or customize the software.

When something goes wrong in an open source security project, distributors cannot deny, hide or downplay the issue. The OSS community actively polices itself and discourages anything other than openness.

A specific example is the Netfilter project, an open-source packet filtering solution. Netfilter provides stateful firewalling, NAT and load balancing. The project has grown to more than 93,000 lines of code contributed by more than 700 developers, and each line of code was examined by many experts before it

was accepted into the core project and distributed to end-users in the “stable” release.

Astaro themselves utilize this project, and give back to the community that develops it via financial support and codebase reviews.

## Myth Five: Open Source Security is too Complex for Small Businesses

There is some truth to this myth. Projects like Snort (a popular open-source Intrusion Detection project) are certainly designed with expert users in mind – and they may work poorly (or not at all) if users are not familiar with their approach and implementation possibilities. Even if implemented correctly, an end-user must then ensure the program remains updated, and continues to work correctly with the rest of the network security programs that are deployed. Fortunately, more and more software vendors are adapting open source projects to the demands of the market, making them very flexible and capable of being deployed in diverse network scenarios with ever-increasing ease.

There is also a second myth at work here. Proprietary solutions don’t necessarily lack complexity. The idea that open source is an all-or-nothing commitment is false. Proprietary vendors who follow the traditional shrink-wrap model work a lot harder to lock customers into their product lines. They won’t guarantee interoperability with competing products, and for those features they don’t offer, they’ll point you to equally expensive partner solutions. Moreover, many users of proprietary solutions are bemoaning a new datacenter problem: appliance overload. Even those proprietary vendors with a broad range of security offerings tend to deliver them as separate, standalone products. These many layers add cost and complexity to the IT infrastructure, as well as presenting multiple points of failure that could undermine security if even one appliance is mis-configured or out of date.

With mixed-source solutions, your organization can put together a best-in-class security lineup without the associated costs or complexity. You also gain the flexibility to change your security posture as you see fit, without fear of breaking contracts, voiding warranties, worrying about interoperability, or throwing away existing investments by being forced to abandon legacy products that still work perfectly fine.

Astaro addresses this by bringing together all areas of their product with their easy-to-use graphical user interface “WebAdmin”, now in its seventh

generation. The company has re-tooled their already powerful solution using AJAX technology and a layout developed in specific response to user feedback, allowing management of all their product areas with a degree of simplicity whose only shortfall is hiding the true complexity of the tasks it is performing. WebAdmin for example will take just a few mouse clicks by a user seeking to enable and configure SSL road-warrior VPN access, and turn that input into dozens of command-line file creations and edits, start and stop services, and otherwise implement the feature. The user saves hours of researching, syntax learning, troubleshooting, and testing, leaving them free to focus on the features Astaro offers and how to best utilize them at the company.

WebAdmin bridges the gap between the open-source knowledge required to successfully implement advanced security tools, and the network configuration knowledge needed to deploy them correctly. Astaro stresses that only security concepts need to be understood, which means anyone can take advantage of the massive security benefits and enterprise-class tools, with no previous open-source knowledge necessary. For instance the setup of the intrusion protection module just requires you to select the appropriate types of servers, applications and operating systems that should be protected, without requiring any knowledge about attack patterns or protocols used. (See Figure-1 below).

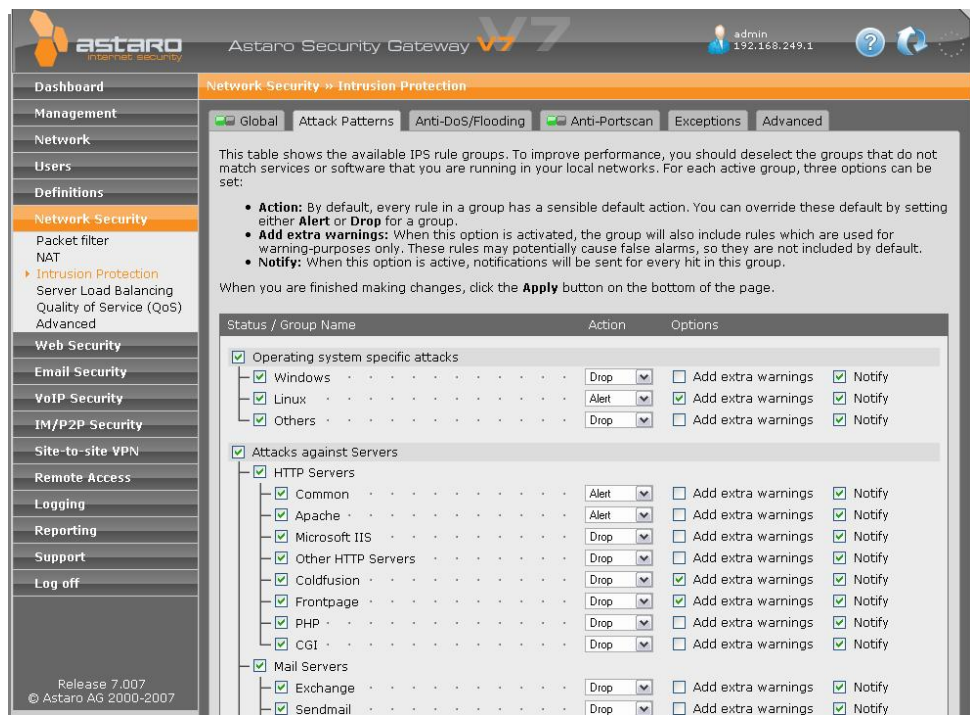


Figure 1: Managing 1000s of SNORT-rules with just a few mouse-clicks

## Conclusion

At the root of a myth there usually exists some level of truth or situation that caused the myth and then propagated its spread. The basis of this truth is then twisted and diluted, then sometimes lost amongst incorrect opinions or common misconceptions. Open-source is steeped in history and capability, and remains daunting to those that have not been educated in this exciting area of development. This massive community has created some truly remarkable tools; however it continually faces various reactions to adoption of their ideas and projects. This situation is mostly due to their community focusing more on creation than marketing, and as such end-user awareness suffers.

Mixed-source security solutions give customers the best of both worlds – the low cost and reliability of open source and the technical support, training, and user-friendly interfaces of proprietary products. These are no longer just tools for the gifted.

Astaro takes advantage of over 300 objects derived from as many as 80 individual open source projects, and is continually evolving. Astaro Security Gateway, Astaro's innovative combination of best-of-breed OSS security projects and a proprietary, intuitive management interface has resulted in the most powerful, easy-to-use, and secure UTM appliance on the market – delivered with the lowest total cost of ownership. Astaro's technology has received numerous industry awards and recognition and continues to gain market share, protecting over 30,000 networks in 60 countries.

The Astaro Security Gateway is available as a software appliance (running on any Intel-compatible PC), as a virtual appliance (running in VMWare environments), or as a rack-mountable hardware appliance.

For more information please visit [www.astaro.com](http://www.astaro.com).

## Sources:

1. "You're Already Using Open Source Security," by Joel Snyder, *Network World*, 03/19/07, <http://www.networkworld.com/supp/2007/ndc2/031907-open-source-security-side-code.html>
2. "Open Source Becoming Mission-Critical In North America And Europe," by Michael Goulde, Forrester Research, 09/11/06, <http://www.forrester.com/Research/Document/Excerpt/0,7211,38866,00.html>

## Contact

**Europe, Middle East,  
Africa**

Astaro AG  
Amalienbadstrasse 36  
76227 Karlsruhe Germany  
T: +49 721 255 16 0  
F: +49 721 255 16 200  
emea@astaro.com

**The Americas**

Astaro Corporation  
3 New England Executive  
Park  
Burlington, MA 01803  
USA  
T: +1 781 345 5000  
F: +1 781 345 5100  
americas@astaro.com

**Asia Pacific Region**

Astaro K.K.  
12/F Ark Mori Building  
1-12-32 Akasaka Minato-ku  
Tokio 107-6012, Japan  
T: +81 3 4360 8350  
apac@astaro.com

[www.astaro.com](http://www.astaro.com)

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2007 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.