FORTRA

GUIDE (Powertech)

Free Linux Antivirus or Enterprise Linux Antivirus: An Evaluation of Linux Antivirus Solutions

The blissful days in which a virus was simply something that made us sneeze or cough are long over. Now, viruses are almost more common in the digital world, and they can wipe out data and destroy businesses. Antivirus solutions have been available almost as long as viruses have. Antivirus software has been on the market since then to help organizations stay secure. But as the software has evolved, so have the choices.

What's the Right Choice: Open Source Linux Antivirus or Enterprise?

One of the biggest choices facing IT and security professionals is whether to rely on open source or enterprise software. Open source solutions come from source code that is made available for users to adopt and modify as they wish. This decentralized approach allows for community driven development, which often results in multiple versions and independent add-ons. Enterprise software is proprietary and created and updated by a known set of developers. These solutions typically have a more focused scope and are made specifically with organizations in mind.

In the Linux world, some still subscribe to the myth that Linux is not susceptible to viruses. This myth is so pervasive that Linux vendors have had to clarify otherwise. For Linux users searching to secure their environment with an antivirus solution, there are a number of additional choices to make. While an organization could deploy software to protect their Linux servers that actually runs on Windows, there are also a number of native antivirus solutions to consider. Security experts recommend organizations use malware protection software that runs natively on their servers' operating systems to avoid security and performance problems caused by Windows-based scanning programs.

Since Linux is a superb open source operating system, layering it with open source applications is an option. However, there are benefits to considering all the options when it comes to choosing software that will safeguard your server. With the variety of native Linux scanning solutions in the market, in addition to the amount of misunderstandings surrounding Linux security, this guide seeks to clarify the perceptions from the reality, enabling you to make an informed decision on how to best protect your organization.

Detection Rates

Two of the best ways to measure the effectiveness of an antivirus solution is through detection rates and performance. Detection rates measure how effective a solution is based on how many pieces of malware it discovers during a certain period of time. Detection rate measurements need to be taken on a consistent basis to account for new viruses that are being introduced into a given environment.

Perception

An antivirus solution guarantees safety. Once antivirus software is installed, that means you're protected from everything.

Reality

Each solution has different detection rates.

Sadly, no solution catches 100 percent of viruses. It's incredibly important to examine the detection rates of both open source and enterprise solutions. The same solution may have vastly different detection rates when on a Windows system versus a Linux system. Typically, enterprise solutions have superior detection rates. Enterprise solutions have tested at least 30 percent higher than open source solutions. Companies creating enterprise solutions can invest in testing by independent labs to verify effectiveness and learn how to improve their results. Such testing may or may not be performed with open source solutions.

Set Up and Performance

An antivirus solution is only performing as long as it is running properly on your system. Efficient and simple set up during installation and updates ensure that an organization's antivirus solution is effective.

There are a few different ways to evaluate performance. First, you have to consider how efficiently a solution runs and detects viruses on a system. A solution isn't useful if it detects a virus after the fact. Secondly, you must assess how much of a burden the solution is on the system itself. Antivirus solutions shouldn't cause a system to slow down to a point of uselessness.

Perception

All antivirus functions the same.

Reality

Set up and performance greatly varies from solution to solution.

Open source solutions may have a limited number of pre-packaged installers. Supporting all these various plat-forms and architectures requires your IT team to compile and package this software. Enterprise solutions are built, tested, and packaged for all the systems in your environ-ment, relieving this burden from your staff.

Enterprise antivirus software is maintained and updated by teams of malware professionals that are constantly updating detection methods for the latest threats and zero-day attacks. You'll immediately receive the latest pro-tection and regularly scheduled updates throughout the product lifecycle, instead of waiting for the open source community to make a change.

Native antivirus software will always have better system performance over Windows-based solutions. Open source solutions can be fast and lightweight, causing little disruption to the system on which they run. Enterprise solutions can be equally lightweight, with the additional perk of having more flexible scanning options, allowing users to choose how and when to scan their systems with minimal impact on system performance. For example, one could decide between on-access scanning, checking for viruses any time a new file is opened or modified, or a full scan performed at night, when users are offline.

Scalability and Optimization

Deciding on an antivirus solution shouldn't be a spur of the moment choice. If you carefully consider the future of your company, you can ensure that your security solutions can serve you for years to come. If your organization is growing fast, you'll need a solution that will scale along with you. Otherwise, you'll be faced with another time-consuming reassessment before you know it.

Perception

Antivirus software is one size fits all.

Reality

Enterprise solutions are much easier to optimize and scale.

Since open source solutions were often created with a singular user in mind, scaling them for a business can be difficult, if not impossible, to do successfully.tInstalling open source software can take a great amount of time and effort. Installing antivirus solutions on additional servers at a large organization at such a slow pace would make a safe expansion difficult and may leave them incredibly vulnerable to security threats.

Additionally, enterprise solutions often take a more holistic approach to security. The current security environment does not allow for a single security solution. While an antivirus tool is a key component, security teams today must rely on a multi-layered approach to provide advanced threat detection and response. Enterprise solutions typically offer options to easily integrate related security solutions so that IT teams can correlate data and have visibility across multiple security solutions. There's no real open source solution with centralized management and reporting, which is a critical component in making antivirus software manageable for IT teams. While there may be different open source options that can handle these different security tasks, integrating them together into a coordinated solution would be unlikely, and could ultimately cost more.

Usability and Support

When assessing usability and support, there are a couple key questions to answer. What kind of environment does your IT team prefer interacting with? Usability preferences can make or break a solution for IT teams. How much time do you want them to spend working with an antivirus solution? If your solution does not come with commercial support, you should be prepared to allow for more time to be spent on security issues in-house.

Perception

All antivirus software looks the same. Antivirus solutions are so common that they're all just essentially plug and play.

Reality

Enterprise solutions are more user friendly.

Open source solutions have different plug-ins to create basic GUIs, which can be difficult to incorporate and insufficient for your organization's purposes. While seasoned members of the IT teams may be proficient enough to use these solutions, other IT employees within the company may struggle if they're expected to interact with it in any way.

Organizations that provide enterprise options have the resources to invest in usability testing, creating a GUI that is intuitive enough for any user. These solutions tend to have more configuration options, allowing IT operations to set alerts, reminders, and more. Since enterprise solutions can integrate without additional tools, this gives the option of having a centralized management console, which gives users a holistic view of what's going on across their entire environment. A more usable antivirus tool makes an IT team that much more efficient when utilizing it.

Cost

Once you've made the wise decision to implement an antivirus solution, there are a few key elements in making your decision of which software to use. One of the biggest factors is that of total cost of ownership. There's a wide range of pricing in the market to consider. It's important to know and consider every aspect of how your solution will affect your budget.

Perception

Open source solutions are free. When it comes down to it, there are really only two options: free open source or enterprise, right?

Reality

No antivirus solution costs nothing.

While open source antivirus solutions may not cost anything to obtain, that doesn't make it free. There are multiple hidden costs that occur after the IT team clicks "download."

One cost of open source technology comes in the form of the labor that it takes to install and manage software. For example, open source solutions must be compiled to suit your organization's needs. This is usually done in house by your own support/IT/development teams or via outsourced vendors. Since these solutions can be used by organizations of different sizes and industries, it can take a great deal of time and effort to package these solutions. Therefore, it may be a long time before your organization can reap the benefit of such a solution.

On the other hand, there are some pre-built packages that are available for open source, but this brings up another cost of open source software. Documentation, resources, and support are available, but there is no central, authoritative location for them. You can expend valuable effort and time researching and tracking down everything you need. One expert spent an entire day simply installing a single open source antivirus solution on one system.

Enterprise solutions have more of a straightforward cost: they come in a variety of price points and plans to support different needs. Enterprise models provide full support throughout the installation and set-up process, which significantly shortens the timeline to going live with your solution. Cost for an enterprise solution includes access to additional resources like documentation or customer assistance portals. Additionally, vendors such as Fortra provide excellent live chat and phone support from system experts.

Functionality also affects pricing for enterprise solutions. On the one hand, there are solutions that offer simple, stand-alone scanning. Price points go up as you add robust functionality and tailor your solution to fit your specific needs, like adding integration with broader suites of security solutions for a more in-depth view of your environment.

This doesn't mean that open source solutions should be discounted entirely. There are cases in which an open source option can be enlisted until a more robust solution is found. After all, any antivirus protection is better than none at all.

Next Steps

Electing to use an open source solution usually means you must pick and choose your priorities. With an enterprise solution, you won't have to. While an open source solution may be the right choice for your business at a certain point, organizations will typically outgrow them more quickly than they'd like to admit.

Of course, the ultimate priority is protection. Viruses can cripple your organization in an instant and take years to fully recover from. An antivirus solution minimizes this risk from the moment it's installed.

Powertech Antivirus provides advanced heuristic analysis and detection, discovering new variants of malware or previously unknown viruses. Additionally, Powertech Antivirus provides quarantine and cleaning with a minimal impact on system performance. If you're ready to see what an enterprise solution can do for your business, request a free trial of Powertech Antivirus today.

FORTRA
Fortra.com

About Fortra
Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.