

Reducing Risk Through Linux*

Table of Contents:

2 It's About the Risk

2 The Benefits of
Closed Source

3 Public vs. Private Goods

3 Intelligent Design
vs. Evolution

4 Software—Asset or Service?

4 Free. As in Free Markets

5 Open Source: Less Risk



It's About the Risk

Linux provides a lower-cost, more flexible solution than Windows, but CIOs can't afford these benefits if they are accompanied by an increase in risk. Fortunately, Linux is not only better and cheaper, but also less risky, than Windows.

The adoption of the Internet demonstrates that businesses can and do trust a public good for a key piece of their IT infrastructures. So there is a precedent, and the adoption of Linux could easily follow the same pattern as the adoption of the Internet.

Software decisions are risky. They result in major multi-year resource commitments, both financial and human, and can shape the future of your enterprise. This is particularly true regarding foundational operating system (OS) software for desktops and servers. Even if software were free, CIOs wouldn't be employed for long if the OS software they chose were not reliable, functionally rich, secure and above all else, cost-effective. For CIOs, the decision to commit to open source software isn't about ideology; it is very often about minimizing risk.

Conventional wisdom has long maintained that proprietary software is less risky, a perception that's frequently true. After all, specific vendors (complete with buildings, employees and press releases) back up most proprietary products. But open source software can also reduce the risk inherent in a software decision. Linux*, for example, provides a less expensive, more flexible solution than Windows*, but CIOs can't afford these benefits if they are accompanied by an increase in risk. Fortunately, Linux is not only better and cheaper, but also less risky than Windows.

The Benefits of Closed Source

One of the attractions of a proprietary software solution is its perceived safety. Proprietary software may cost more, but IT managers believe the cost is well worth it if it eliminates the risk of buggy software, weak support or lack of a large supporting ecosystem. This is particularly true when considering desktop and server operating systems.

Microsoft has long been perceived as the safe choice for operating systems. Windows, in particular, is perceived as stable and the

most functionally rich. While Microsoft requires customers to give up a certain amount of control, in return it assures IT executives that their needs will be met not just today, but far into the future. There is nothing inherently wrong with this value proposition, but is it the best choice for a competitive business or a cost-conscious government agency?

The cost an organization is willing to incur to avoid risk depends on two questions: What's the cost? and How much risk? The total cost of ownership (TCO) of Windows compared to Linux is easy to calculate, and Novell® has been calculating the hard-dollar ROI of our SUSE® Linux Enterprise solutions for years; it's clear that Linux is less expensive, even in the long term. The risk, on the other hand, is much harder to assess. The risk must ultimately be evaluated by the IT executives accountable for the OS decision. They must ask themselves whether their decision could negatively impact the business, causing that decision to be second-guessed by other executives, publicly criticized and, to one extent or another, penalized. Ultimately, executives' jobs can be on the line when they make these decisions—and if not their jobs, certainly their credibility and influence in the organization. As the old saying goes, no one ever got fired for buying IBM, or in the more recent past, Microsoft.

The risk, or mitigation thereof, relies on the level of trust IT executives can place in Microsoft's ability to fulfill their expectations over the long term versus the level of trust they can place in Linux and its vendors. It's the latter that is often problematic for CIOs—how can they trust software that no one owns to run their critical applications?

However, this approach isn't so far-fetched. In fact, IT shops already trust the Internet, a similar public good, for their networking infrastructure.

Public vs. Private Goods

Open source software is a *public good*, while proprietary software is a private good. This distinction is at the heart of the economics and the risk of open source versus proprietary software.

A public good has two characteristics that differentiate it from a private good. First, one person's consumption of a public good does not interfere with another's ability to consume the same good. For example, gasoline is not a public good because once someone has burned a tankful in her car, another person can't burn it in his. One's consumption of a particular piece of software, on the other hand, does not in any way prevent others from consuming the same piece of software. But this is true of both closed and open source software. The second criteria for a public good applies to open source only: consumers cannot be excluded from consuming it. So while proprietary software is based on a license that dictates who can and cannot use the software, open source, by virtue of its open source license, is freely available to anyone. So open source software, like broadcast television, clean air and Central Park, is a public good.

But are public goods as trustworthy as private goods? In one striking example, the business world has said "yes."

The early days of online services were dominated by proprietary service providers such as Compuserve, Prodigy and AOL, while business-to-business Electronic Data Interchange relied on commercial value-added networks. These proprietary services and networks have since been largely replaced by the Internet, which meets the two criteria for a public good. One person's

use of the Internet doesn't prevent another from using it, and no one can be excluded from its use (which is why governments have so much troubling controlling spam and online gambling and pornography).

The adoption of the Internet, even for critical roles such as ATM networks, demonstrates that businesses can and do trust a public good for a key piece of their IT infrastructures. So there is a precedent, and the adoption of Linux could easily follow the same pattern as the adoption of the Internet.

Intelligent Design vs. Evolution

The Internet has proven itself to be very trustworthy, but will the same be true over time for Linux? How can software built by a group of global developers (who almost never meet face-to-face) be reliable?

Software has traditionally been developed according to a waterfall development methodology. Developers create a grand system design to meet the requirements laid out in a requirements document. Pieces of code are written to meet the specs of the design, and the code is tested according to a test plan designed to ensure it meets the specs. This process is analogous to the Intelligent Design theory of human origins, the theory that an intelligent designer created humans according to a divine design. (For some development projects, it seems as if the waterfall approach requires divine intervention to succeed!)

In contrast, the development of open source is more analogous to the Theory of Evolution. Someone creates a piece of code for a specific purpose, but the code is immediately thrown into a jungle where it must compete with alternative approaches to solving the same problem. The best pieces of code survive and thrive, being extended and applied to new purposes not originally conceived. This chaotic process of creation, competition, survival and expansion happens

Just as the reliability of the Internet is due to its redundant, chaotic, complex structure, Linux is more reliable because of its redundant, chaotic, complex development process.

When it comes to mitigating risk, the amount a software vendor is able to charge for access to the asset up front is only part of the equation—it's the quality of the ongoing support and maintenance services that the customer must rely on.

Open source provides a freer market, which gives customers alternatives for ongoing Linux support and services, something not available for Windows.

Whereas CIOs at one time had trouble justifying to their Boards any decision to adopt open source solutions, the day is rapidly approaching when Boards will recognize that open source can actually reduce risk.

over and over. The result is a more robust, hardened, structured, modular and secure solution than any one designer, no matter how intelligent, could have developed alone.

Just as the reliability of the Internet is due to its redundant, chaotic, complex structure, Linux is more reliable because of its redundant, chaotic, complex development process.

Software—Asset or Service?

But Linux is still software. It could have bugs or security vulnerabilities, and it might “break.” Besides which, there is always new hardware or new software functionality up the stack that has to be supported and new functional requirements that must be added over time. Who is going to fix, support and update this public good so it will keep pace with these changes? With Windows, it is always clear whom to hold accountable. The CIO has “one throat to choke,” and it’s in Redmond. How many throats does the Linux community have? And where are they?

Proprietary software is sold up-front as an asset. The software vendor is charging the buyer for access to software, into which the vendor has invested development dollars that they are looking to recoup. In contrast, open source vendors can’t charge for the software asset itself, because it is a public good, accessible to all. Open source generates no revenues from the sale of the actual software asset.

But IT shops pay for more than just the use of the software, since the license agreement itself does not give the CIO the easy-to-reach throat to choke when things go wrong. Besides the software asset, ISVs sell the

ongoing support, promising to take calls, provide onsite support, distribute patches and provide access to future upgrades. This is the ongoing set of services that ensures the continued usefulness of the asset over time.

When it comes to mitigating risk, the amount a software vendor is able to charge for access to the asset is only part of the equation—it’s the quality of the ongoing support and maintenance services that the customer must rely on. So how can a CIO make sure this ongoing support will always be available for Linux?

Free. As in Free Markets

With Windows, IT executives have only one choice for the ongoing software maintenance and support. If CIOs trust Microsoft to provide good support and to consistently do what’s in the best interest of its customers, this is not a problem. However, if CIOs begin questioning Microsoft’s ability to support them in the future, they have no recourse. Even if the software asset itself is of good quality, any weakness in ongoing software maintenance and support may cause real problems for customers. Unfortunately, because it’s closed source, the CIO has no alternative.

Companies that use open source software, such as Linux, avoid these risks. Novell has long had a world-class technical support service that is second to none. One reason this will continue is that Novell understands its SUSE Linux Enterprise customers have alternatives, so it must earn their loyalty anew each day. Because Linux source code is freely accessible, a free market can provide alternatives to Novell support services. Novell understands that a dissatisfied customer represents an opportunity for a competitor to step in. Not so with Microsoft and Windows. In this way, open source provides a freer market, which gives customers alternatives for ongoing Linux support and services, something not available for Windows.

Open Source: Less Risk

Contrary to conventional wisdom, Linux can actually reduce enterprise IT's risk compared to Windows. This is the case not because of the virtue of open source ideology, but is simply the result of hard-nosed economics.

First, Linux is a public good, one that is not controlled by one company and can seem chaotic and unmanaged. That is why, like the Internet, it is so robust and reliable. Linux replaces a single point of failure—a proprietary software developer—with a public good supported by a global community.

But CIOs still need accountability. Open source provides a freer market than closed

source does by enabling competition among software service and support suppliers. The result is the accountability CIOs demand without the inflexibility they despise. The open source process better aligns customers' and vendors' incentives.

Over time, conventional wisdom will catch up with the underlying economics. Whereas CIOs at one time had trouble justifying to their executive boards any decision to adopt open source solutions, the day is rapidly approaching when those same boards will recognize that open source can actually reduce risk. Such is the case today with Linux. Soon, executives will understand that Windows is just too risky.

www.novell.com



Contact your local Novell
Solutions Provider, or call
Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA