RJ Systems

Linux System Administration

Home Tech Linux Links Consulting

Linux

vs Windows

Advantages of using Windows:

1. **Ease of use.** Users familiar with earlier versions of Windows will probably also find the more modern ones easy to work with. This is ascribable to everything from the standardised look and feel of almost all programs written for Windows to the way the file system has been presented ever since the days of MS-DOS (disk A:\, disk C:\, etc.). This is one of the main reasons why Windows users are often reluctant to switch operating systems.

2. **Available software.** There is a huge selection of software available for Windows. This is both due to and the reason for Microsoft's dominance of the world market for PC computer operating systems and office software. If you're looking for an application to suit your business needs, chances are that if it exists there will be a Windows version of it available somewhere.

3. **Backwards compatibility.** If you're currently using an older version of Windows and need something more up to date, but you don't want to loose the use of some older programs that are only available for Windows and are critical to your business needs, the chances are good (although not a certainty) that those programs will also work with a newer version of Windows.

4. **Support for new hardware.** Virtually all hardware manufacturers will offer support for a recent version of Windows when they go to market with a new product. Again, Microsoft's dominance of the software market makes Windows impossible for hardware manufacturers to ignore. So, if you run off to a store today any buy some random new piece of computer hardware, you'll find that it will probably work with the latest version of Windows.

5. **Plug & Play.** As an operating system for the average home user, Windows still has an edge over the competition in the area of Plug & Play support for PC hardware. As long as the right drivers are installed, Windows will usually do a good job at recognising new hardware. Other operating systems also offer Plug & Play functionality, but to a lesser degree and more frequently require manual intervention.

6. **Games.** If you crave the latest in PC gaming technology, then you need Windows. A plethora of gaming titles are available for Windows, as well as lots of special gaming hardware that's supported. Some of the most popular games are also available for Linux, and even more for the Mac, but there's really no comparison. It must be said, though, that

not all of the old games that were written for Windows 95 and 98 will also work with XP.

7. **Compatibility with MS driven websites.** After Windows had become the world's most popular desktop operating system, Internet Explorer (IE) became the world's most popular web browser soon after Microsoft began bundling it with Windows 95 in order to squash competition from rival Netscape's Navigator browser. Since Netscape's demise, Microsoft have introduced more and more proprietary features into their web servers that can only be taken advantage of with Internet Explorer. Obviously, these sites are less accessible with other browsers − sometimes not at all. This, coupled with the fact that the latest versions of IE are only available for Windows, has made Windows the only choice for those who want to take full advantage of those websites that use Microsoft's technology.

Disadvantages of using Windows:

1. **High resource requirements.** As opposed to the makers of other operating systems, Microsoft requires its customers to invest the most in their computer hardware: a faster processor (the CPU), more internal memory and a larger hard disk. Microsoft have always maintained that this is due to all the extra functionality that they've added, as demanded by their customers. Actually, few people make use of many of those features, yet everyone is still forced to contend with the additional overhead that is the result. (Ref: *CNN*)

2. **Closed Source.** Troubleshooting problems with Windows would be so much easier for users and support personnel if only they knew what was actually going on. Unfortunately, only Microsoft has full access to its software's source code, and since no log files are generated its users are left to try and deduce what causes their problems by trial and error alone. At best this is time-consuming, while at worst it can make a program impossible to work with. See also: *"Shared Source"*.

3. **Poor security.** Compared to other operating systems, Microsoft security is weak. According to their own developers, their products "just aren't engineered for security." The result is that Windows computers are more likely than other systems to be hijacked and used to distribute everything from spam to pornography (Ref: *Inquirer*) to hate mail. Even worse, any such activity only points to the computer that was compromised: since Windows does not generate log files, the owner has no way of proving anyone else's involvement.
   Another aspect of this issue has to do with internal security from an administrative point of view. Configuring any computer is time-consuming and Windows is certainly no exception. Therefore, it's better if users can be prevented from making changes to certain parts of the system, whether on purpose or by accident. Unfortunately, only with great difficulty is it possible to achieve a level of fine-grained administrative control on Windows systems, which is why it is rarely seen outside of larger organizations. What all this means for businesses is that Windows systems require a lot more time and effort to maintain than other systems. Failure to do so will only result in more lost productivity or worse.

4. **Virus susceptibility.** This subject is usually regarded as part Microsoft's general problems with security. However, the susceptibility of any of Microsoft's operating systems to computer viruses has always been pronounced; nearly all computer viruses target Windows computers and regularly wreak newsworthy havoc. Indeed, if it wasn't for Windows, the multi-million dollar anti-virus industry as as we know it would be virtually non-existant. Viruses on other platforms, save for perhaps the older Mac operating systems, are strictly a rarity. What this means for businesses, is that that they have no choice but to keep investing in anti-virus software for all of their Windows

computers, as well as to keep up with the almost daily release of Microsoft security patches.

5. **Outrageous license agreements.** Most people never bother to read the EULA, or End User License Agreement, that must be agreed to before any Microsoft product − including service packs and security updates − can be used or installed. Most people simply regard these screens as an irritant that must be to clicked through in order to install the product. However, if they did take the trouble to read the EULA, many would probably be a little more than irritated. For instance, Microsoft's EULA for Windows XP was radically ammended for people who installed a security update in mid-2002 that fixed an obvious and potentially dangerous security leak in Windows Media Player. It states explicitly:

   > You agree that in order to protect the integrity of content and software protected by digital rights management ('Secure Content'), Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer.

   So, along with a routine security patch, Microsoft also slipped in this new agreement that gives them the right to install any software on your computer that they see fit − including software that "may disable your ability to ... use other software on your computer". Basically, this amounts to giving Microsoft 'Administrator' rights on your computer (so much for privacy). No doubt Microsoft would say that this measure is only meant to target pirated software, but the EULA is vague insofar that it does not exclude the possibility that software acquired legally from vendors other than Microsoft can be disabled as well. In other words, at the very least, this agreement gives Microsoft the final say on what software may be run on your computer.

   And just in case you think all of this might be a little exaggerated, know that Microsoft has been a big booster of the UCITA − a horrible law that would allow:

   - Software publishers to change the terms of the contract after purchase.
   - Restrictions that prohibit users from criticizing or publicly commenting on software they purchased.
   - Software and information products to contain "back door" entrances, potentially making users' systems vulnerable to infiltration by unauthorized hackers.
   - Software publishers to sell their products "as is" and to disclaim liability for product shortcomings.

   Sound familiar? That's right − they're already doing this! Or, at least they're trying to, despite loads of criticism. Naturally, this is why Microsoft is pushing for a law to be passed that would be on their side. (Ref: *InfoWorld*)

6. **Poor technical support.** Few of Microsoft's support staff truly understand security or high-end enterprise issues, and even less have access to or understand any of the source code. Extremely high-volume accounts get special treatment, but for others the odds of getting good support on truly difficult problems are extremely poor. To make matters worse, the free support provided to end-users has been dramatically reduced over the years. For businesses that depend on Microsoft products, this translates into greater risks and higher costs.
   These days, all Windows users rely heavily on the automated Windows Update system that applies all the necessary patches to Windows computers via the Internet. Unfortunately, this update system is not very reliable; it's had all kinds of problems. Recently, for example, it was giving computers that were in need of critical security

patches a clean bill of health. So much for Microsoft's much vaunted Trustworthy Computing Initiative.

7. **Hostile treatment of legitimate users.** In an effort to curb software piracy, Microsoft includes a scheme in Windows XP that involves sending them a "fingerprint" of your PC's hardware configuration that allows them verify whether your license is still being used on only one PC or not. The moment they detect that your license is running on another machine, your copy of Windows will cease to function. The only way you can get it to work again is by asking them for a new activation code. To some, this may sound reasonable at first, since I'm sure we all agree that software piracy is a bad thing, but what happens if you want to upgrade your entire machine? That's right: you have to call Microsoft for a new code. What's interesting is that Microsoft knows this would really annoy IT managers in big corporations (who normally pay anyway), so they give the bulk licenses a back door round this protection. The rest of us are are considered guilty until proven innocent.
   Another long-time method that Microsoft uses to harass legitimate users is through the Business Software Alliance (BSA). This is a non-profit organization that was set up to fight software piracy and is sponsored by a number of well-known software companies, but mainly by Microsoft. Of course, they spend their time looking for organizations (and even individuals) who they suspect might be using Microsoft's software illegally, but they're equally zealous at targeting those that might not be able to account for all of their licenses in time for an 'official' BSA audit. Actually, unless they are invited to come by to talk about 'software licensing', which is what they like to offer, they have no legal authority to enter onto anyone's premises. Still, that doesn't stop them from sending threats of hefty fines and even jail time − even to those not using Microsoft's products! Again, everyone's guilty until proven innocent. Interestingly, the moment a mea culpa is made, the BSA will arrange for people to buy Microsoft licenses rather than force them to pay fines.

8. **Extortionist prices.** In the past, when Microsoft was asked on numerous occasions why it was raising the price of its Windows licenses yet again, the standard reply was that it was necessary to offset the development costs of their latest version. However, after the the Enron and Worldcom scandles, Microsoft decided to overhaul its reporting structure in an effort to achieve more transparency in its earnings information. The results are quite revealing. What people long suspected was the case is now known to be fact: that Microsoft's profit margin for Windows is huge. According to their earnings report filed with the S.E.C for the third quarter of 2002 (Ref: *S.E.C.*), it was a whopping 85.8% of $2.892 billion in revenues. Their 'Information Worker' division, which includes the Office line of applications, took a 76.8% profit on sales of $2.385 billion. In other words, Microsoft's high prices are mostly 'monopoly tax'. Interestingly, though, while their server division also turned a profit, all the others ones operated at a loss. It looks like Microsoft is using the profits from its monopoly divisions to pay its way into new markets.

9. **Additional expenses.** After setting up a series of Microsoft computers, or even a single one for that matter, sooner or later customers invariably find themselves in need of additional software. For example, a virus scanner is mandatory nowadays, but many also believe a spyware blocker is essential as well. But, that's just the cheap stuff. If you run a Windows-based website, for instance, you may find yourself investing a lot of money in development tools, most of which are Microsoft products. The costs of applications that can run on your web site are usually higher than that of other systems. For example, you can find loads of free scripts and applications to run services such s web boards, chat rooms, web statisics and email for Linux-based web sites, but you won't find many free applications in the Microsoft world.

10. **Poor stability.** For people who are used to dealing with Windows, rebooting and re-installing are such a regular occurance that most don't even give it a second thought. However, that is by no means an excuse for such poor performance: Windows should not freeze up and reboot simply because Word or Internet Explorer was being used. And yes, this is because Microsoft products are full of bugs − no matter what Bill Gates says (Ref: *Cantrip Corpus*). Nevertheless, it seems most people have become largely desensitized on this issue − as if it's a natural consequense of the complexity involved. But, it doesn't have to be that way: every other major operating system available today has a better track record.

11. **Vendor lock-in.** Also referred to as 'vendor dependence', Microsoft is infamous for promoting brand loyalty among its customers in this manner. One way for a vendor to establish lock-in is for it to gain control of both sides of an otherwise open and standard client/server model by adding proprietary extensions to the standard communications format. Customers can then no longer switch to cheaper, alternative client or server ssoftware without losing fuctionality, having to finance a complete migration to different products, or both. Microsoft, being a manufacturer of applications and operating systems for both workstations and servers, is in the ideal position to create such situations. Indeed, they have taken this concept and made it into a fine art. For the customer, poor quality and high prices are inevitably the result.

12. **Backwards incompatible file formats.** A well-known drawback of using Microsoft applications such as Office (Word, Excel, etc.), is that their file formats are not backwards compatible. For instance, this means that a document created in the MS Word 2002 format cannot be interpreted in any way by someone using Word 97. Microsoft has always maintained that this is because of all the new features that have been added to each new document format, but the truth is that it would have been easy for Microsoft's developers to create a common file format that would have allowed all versions of Word to simply ignore any new and unrecognised formatting features. No, they chose to do things differently because their method is the one that keeps their customers upgrading. How does this work in practice? Well, most businesses buy into Microsoft's product lines because they believe everybody else does. An important benefit is that, if all the latest versions are used, they will always be able to read files sent to them by other organizations that also use Micosoft's products. Everything's fine until the next version of the software hits the market. Customers then find that, first of all, the longer that upgrade has been available and they delay buying it, the more often they'll find themselves receiving documents in the new file formats that they can't read. Second, if they postpone their move to the new version for too long, Microsoft will no longer consider them eligible for a cheaper upgrade option and force them to buy a whole new license instead. Finally, upgrading the applications often forces you to upgrade the entire operating system as well.

13. **Poor support for older hardware.** Legacy support for older hardware is gone in Windows 2000 and Windows XP. Microsoft claims this was necessary to increase the overall stability of their systems, but if other systems with excellent reputations for stability include much better support for older hardware, where does this leave Microsoft's argument?

14. **Poor remote access.** As opposed to many of the alternatives available, MS-DOS, and thus Windows after it, were never designed with remote access in mind. That's not to say that it isn't done − it is, because it's a great way to save on administration costs − it's just that the solutions have always left something to be desired. They're unreliable, insecure (especially via the Internet), expensive, need too much bandwidth or require extra Microsoft network components to work. Invariably, it's a combination of these characteristics.

15. **High Total Cost of Ownership (TCO).** The fact that Microsoft charge so much initially for their software is one thing, but what most salesmen fail to mention is that, if you want to stay with this platform in the future and keep all the benefits (application and file format compatibility), you'll have to upgrade every two to three years. Also, Microsoft make upgrading more expensive for customers who lag behind. The other major reason for the high TCO, is the intensive maintenance required by modern Windows systems. Vital Microsoft security patches are published so often, that it seems even Microsoft can't always keep up. As a result, their systems were also affected when the Slammer worm struck in late January 2003. They would not have suffered this humiliation if they had only remembered to install one of their own security patches many months earlier (Ref: *News.com*).

Last modified: 2017-08-02, 17:31