Windows XP EoL: The risk of not migrating

AppSense®

You are the technology

Windows XP EoL:
The risk of not migrating

Executive summary

Risks:

- Windows XP will become a soft target to exploit when security patches cease to be issued by Microsoft
- Windows XP still has many vulnerabilities both known and unknown
- Speculation exists whether “black hat” attackers are holding back exploit code for un-published vulnerabilities to release once End of Life occurs. AppSense believes this is likely.
- Simply maintaining up to date anti-virus on Windows XP will not suffice
- Network exploitable vulnerabilities still being found
- In the first quarter of calendar year 2013, NIST.gov published 28 network exploitable vulnerabilities affecting Windows XP

Recommendations:

- Re-evaluate risk profile of delaying Windows 7 migration
- Avoid paying for custom end of life Windows XP support, instead invest in rapid migration to Windows 7
- Avoid security risks both known and unknown with a rapid migration to Windows 7
- Utilize specialist migration solutions to rapidly migrate user persona, security policies and user data to new Windows 7 desktop

Preface

For the 50% of businesses that have not yet migrated towards Windows 7, an important date looms in exactly one year from today. Windows XP End of Life (EoL) occurs on April 8th 2014.

What this means for end users and businesses alike is that the mainstay of desktop computing for the past 10 years will cease to be supported by Microsoft, unless the customer invests in a very expensive End Of Life custom support agreement, in some cases reaching millions of dollars over multiple years.

In these agreements, Microsoft do not negotiate price, and compounding this is the fact that analysts are reporting hefty price hikes beyond previous Windows 2000 EoL support agreements.

For more information and a breakdown of the staggering cost and structure of these support agreements, please refer to the datasheet *“Windows XP EoL: The cost of not migrating”.*

Windows XP EoL: The risk of not migrating

The risk of not migrating

The impact for businesses that choose to stay on Windows XP beyond April 2014 without a support agreement is that business risk will have increased significantly. Hackers and malware creators alike will be specifically targeting Windows XP, safe in the knowledge that any major Windows XP system issue or vulnerability that is exploited after this point in time will not be fixed, even if it is a security compromise issue at the scale of Nimda or Code Red.

Today we face increased risk from organized crime in addition to the seemingly inane motivations of the past, delivering malware in the form of viruses, Trojans, keyloggers and botnets. While these don't always rely on a system vulnerability to gain access, many do and as such we cannot assume that anti-malware tools will always be able to protect us. Ultimately without regular patch updates, Windows XP stands to become a soft target in the digital war between IT departments and organized crime.

AppSense, with its partners, can help in multiple ways to help accelerate Windows 7 deployment – making a project operationally successful and delivered in lower cost with less time required.

AppSense's solutions help to solve:

- Migration of the user persona
- Migration and centralization of distributed endpoint data
- Application compatibility situations relating to Windows 7 User Account Control
- Securing the desktop – utilizing Trusted Ownership, whitelisting and blacklisting to prevent malware execution

Why wouldn't you migrate?

At todays date, industry analysts place the total number of desktops migrated towards Windows 7 anywhere between 45% to 60% of the total Windows PC installed base (PCIB). A true number is fairly difficult to accurately ascertain.

The remaining 55% of desktops generally fall into one of several groups:

1. **Businesses that want to migrate though haven't moved quickly enough**

   Organizations in this group are likely just about to start their migration or are in the process of migration right now. They may be still looking around for options to ensure that the migration occurs smoothly with as minimal cost and disruption as possible.

2. **Businesses that for one reason or another cannot migrate**

   Organizations in this group already accept that they will have to purchase an EOL support contract, to ensure that their risk is mitigated. This is likely due to application dependency and/or compatibility issues.

3. **Businesses that don't see what the fuss is about.**

   This group may have the perception that everything in Windows XP that could have been exploited, probably already has. They may also believe that this is a "Y2K like" overhyped fuss and that they have effective anti-malware controls in place to mitigate anything else that could occur.

Windows XP EoL:
The risk of not migrating

A soft target or not?

Since the massive security issues caused by worms such as Nimda or SQL Slammer, Microsoft has made security its number one focus with major initiatives such as the Windows XP SP2 security update addressing many known and unknown security vulnerabilities.

From a product standpoint, successive versions of Windows have implemented increasing levels of security features that make it harder to exploit, with the success evidenced in recent malware infection rate reports (Microsoft, 2012).

From a process standpoint Microsoft as a company has made tremendous advancements in the way it responds to and manages security related incidents.

Testament to Microsoft's efforts in security since Nimda, there has never been such a widespread security incident of that magnitude. Though as security professionals know, despite all this advancement in security no platform is secure. It could just as easily occur again without proper processes and technology to patch and secure the platform.

Therein lies the challenge. Without patches being released, can the platform still remain secure just relying on anti-malware? And can your business afford to take the risk?

According to NIST.gov, between the 3-month period of January 2013 and 31st March 2013, Microsoft released 34 high severity updates for the Windows XP platform. Of these, 28 of them are exploitable via the network. It should also be noted that some of these vulnerabilities can be exploited even when up-to-date anti-virus is in place.

Anti-virus itself is only intended to be a last line of defense – to detect and cleanup the mess once the malware has been executed on the system and completed its payload actions. Even then, it falls short in many areas outside of its scope of control or ability to respond in a timely manner. A recent New York Times article shares that *"…By the time its products are able to block new viruses, it is often too late. The bad guys have already had their fun, siphoning out a company's trade secrets…"* (Perlroth, 2012).

Adding weight into this is a Microsoft report (Microsoft, 2012) that also underscores malware infection rates of Windows XP are double that of Windows 7. The Windows XP platform itself is inherently insecure in comparison to its successors.

Many industry watchers agree with this standpoint; that organizations choosing to run Windows XP past the EOL date do so at a much higher business risk standpoint. Many also assert that that cybercriminals may even step up their attacks (Sheldon, 2012) and that "black hat" attackers may hold back exploit code for un-published vulnerabilities for release post April 2014.

A reasonable risk assessment emerges then; the moment support patches stop for Windows XP on April 8th 2014 a major layer of defense for the operating system disappears.

It's at this moment Windows XP becomes a soft target for relatively easy attack.

Windows XP EoL: The risk of not migrating

Recommendations

AppSense recommends that organizations choosing the “wait and see” approach reconsider their stance and migrate towards Windows 7 (or Windows 8) as soon as possible to avoid paying for an expensive End of Life support agreement.

Rationale:

- Vulnerabilities continue to be found: The stance that all vulnerabilities have been found is also a fallacy as has been disproven with NIST.gov data. With 28 network based vulnerabilities of a high risk nature underscores the need to migrate rapidly.
- A significant threat exists: With the level of infection that occurs around the Windows XP platform, the potential and installed base of Windows XP, arguably still as high as 43%, is a significantly high enough installed base for cybercriminals to target.

Conclusion

Significant security risks exist for companies that choose to stay on Windows XP that are not intending to purchase a Microsoft EOL support agreement.

AppSense, in combination with its partners, offers solutions to help companies, large and small migrate rapidly and seamlessly towards Windows 7.

Utilizing the power of solutions such as DesktopNow and DataNow enables companies to seamlessly gather all the user related persona and data assets, centralize them and stream back into a new desktop without user disruption.

Aside from the lower operating cost savings associated with managing Windows 7 versus Windows XP, AppSense can further increase operational and capital cost savings during the course of (and post) the migration.

For more information on the cost of custom support for Windows XP please refer to the datasheet *“Windows XP EoL: The cost of not migrating”*

For more information on how AppSense enables a faster, smoother and more cost effective migration please refer to the AppSense and Windows 7 migration at: http://go.appsense.com/wp_windows7_migration.html

For more information on how AppSense helps companies achieve up to a 284% ROI and a net payback of 5 months please refer to the Forrester TEI whitepaper at: http://go.appsense.com/Website_Asset_Forrester_Study.html

For more information on DesktopNow and DataNow please visit http://www.appsense.com

References:

NIST.gov, Advanced search for Windows XP vulnerabilities. Web, searched April 1st 2013.

Perlroth, Nicole, “Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt”, New York Times. Web. December 31st 2012.

Microsoft, “Microsoft Security Intelligence Report Volume 13 English”, Microsoft, Web (PDF), November 8th 2012.

Sheldon, Robert, “Windows XP End of Support: What are the risks for users?”, TechTarget, Web, November 2012.

appsense.com

Twitter:
@appsense

email us:
iwanttoknowmore@appsense.com

About AppSense

AppSense, the people-centric computing company, is the leading provider of user virtualization technology that transforms organizations into productive mobile workforces securely governed by IT. AppSense enables companies to embrace consumerization in the enterprise by independently managing all aspects of the user experience across mobile devices and desktops. Our user virtualization technology reduces IT complexity and improves the deployment, management and migration of multi-platform desktop and mobile environments. The company is headquartered in New York, NY with offices around the world. For more information visit www.appsense.com

All other trademarks are the property of their respective owners. The information in this document is believed to be correct at time of printing but no representation or warranty is made as to its accuracy or completeness.