July 2013

Windows® XP–A Compliance and Risk Nightmare in April 2014

Vulnerabilities and Costs Make a Windows Upgrade Mandatory for the Enterprise

Microsoft has announced that it will end active support and "end of life" Windows XP on April 8 2014. This date has been well publicized and telegraphed. However, as the actual date nears, **the highly-negative consequences of continuing to use Windows XP in enterprise** environments **are becoming much clearer.** After that date, IT security risks and compliance issues from continued use will be magnified.

This white paper will consider **three aspects that create a "nightmare"** for the enterprise. These include the **technology threats, potential liabilities/compliance issues,** and **the potential for dramatic cost increases** for end-user computing.

CONTENTS

Sponsored by

intel inside CORE i5 vPro

lenovo FOR THOSE WHO DO.

Windows XP's End of Life Reflects Major Changes in Technology

The end of life (EOL) for technology products is a part of their lifecycle. The technology industry has an unmatched pace of innovation and change. However, **there are unique aspects to Windows XP's EOL that make this an important transition.**

Among the first reasons for moving beyond Windows XP is the simple fact that the era for which it was designed is very different from the present. During Windows XP's design timeframe, mobility was an occasional part of the usage pattern and networking involved only dedicated cables or company controlled WANs. Remote access was commonly achieved via phone lines! The threats PC users faced were quite different, as well. Most attacks were designed more to create aggravation and annoyance than to steal private or valued information. Threat technology was fairly stable, with commonly known methods of defeating malware and viruses. In addition, critical corporate information was often retained in a data center, not on user's PCs. The attributes of the threats faced by end users have changed substantially and created a reality where **Windows XP has such substantial design vulnerabilities that it puts an entire organization and its data at risk.**

Windows XP has such substantial design vulnerabilities that it puts an entire organization and its data at risk.

Windows XP Risk Factors—What Will Keep You Up at Night

There are three aspects that comprise the primary risk factors for continued Windows XP use. These include:

- **Technology risks**
- **Corporate liability/compliance risks**
- **Cost risks**

1. Technology Risks

With respect to technology risks, the most common and well-known issue is that patches to mitigate known vulnerabilities will no longer be provided, effectively **leaving Windows XP-based systems open to exploits** and compromise. Unlike new versions of Windows where security patches are generally delivered within a day of exposure, following Windows XP's EOL date this will not be the case. Without a Custom Support Agreement (CSA) in place, enterprises will not be protected.

CSAs are available from Microsoft under separate contract for Premier Customers at an additional fee. Under the CSA, customers will continue to receive patches for vulnerabilities found in Windows XP. For the enterprise, this presents a very clear situation; either pay hundreds of thousands of dollars for a CSA, or have vulnerable systems in place. Neither option is very attractive.

Without a Custom Support Agreement, customers will not receive patches for newly-discovered Windows XP vulnerabilities.

The next major issue that will arise from Windows XP's EOL is found in Internet Explorer (IE). Newer versions of Internet Explorer, starting with version 9.0, are not supported, meaning that all **vulnerabilities in older versions of IE will represent major risks** going forward.

Further, most peripheral and device vendors will cease to provide new updates or patches to their drivers; some have already started subtly doing this. While this represents less of a security issue, this poses sizable compatibility concerns. The problem here will be user downtime and potentially unusable systems should critical device drivers become flawed or incompatible. Though less likely, old video and printer driver susceptibility to attack could cause a security breach.

An additional area of risk for Windows XP systems is that **many organized hacker groups or organized crime syndicates are developing attacks** in anticipation of unpatched Windows XP systems. The reality is that after a short period of time from the EOL date, **nearly every Windows XP system will be vulnerable,** especially those without a CSA. And based on current NetApplications data that puts the Windows XP installed base at just over 38 percent as of March 2013, this is poses a huge problem.

This adds up to literally thousands of potential vulnerabilities in larger enterprises, with threat vectors likely increasing dramatically in the late spring of 2014.

Speaking of specific new threats, the next generation of malware and virus technologies will be tremendously difficult for Windows XP systems to deal with, even with a CSA. One avenue of attack will be a new generation of Advanced Persistent Threats (APTs), which are basically targeted attacks focused on a very small number of individual endpoints or users that attackers perceive to be vulnerable.

Once these endpoints are compromised, they are used as a "springboard" into the larger IT infrastructure for data theft or industrial espionage. There is already chatter on hacker websites about this kind of attack, according to Dark Reading. In addition, most Windows XP systems depend on anti-virus (AV) solutions for basic protection. At end of life, it is possible that as a cost-saving measure anti-virus vendors will not develop advanced solutions for Windows XP systems.

This adds up to literally **thousands of potential vulnerabilities** in larger enterprises, with threat vectors **likely increasing dramatically** in the late spring of 2014.

Beyond this there are new threat types, primarily those that use object-oriented technology, which may require new versions of AV software. These pieces of malware hide common malware "signatures" within an object that requires the latest AV solutions and technology to detect and remediate. Old AV tools are ineffective as they only focus on the signatures, which are now hidden. Windows XP-based systems will therefore be highly vulnerable to this malware technology.

The next area of concern is the impact of obsolete Windows XP systems on organizations using Mobile Device Management (MDM) tools for security and management. MDM systems typically seek a local agent on the mobile device before allowing access. For Windows XP systems to participate after the EOL date, MDM vendors will have to support it with current agents. This is not a given, and with the potential for Windows XP vulnerabilities, some vendors may not. The decisions of individual MDM vendors have yet to be been made public.

A final technology issue is not a vulnerability, but an incompatibility. New systems based on the 4th generation Intel® Core™ processor family will not run Windows XP. It's unclear why a user would want to bring Windows XP onto a new system, but it is a fact worth noting. Development of a Windows XP image for that new notebook simply won't happen. It's also important to note that Windows XP doesn't support key features found in new Intel processors and chip sets that provide support for new and faster wireless networks, new storage solutions or the improvements in video needed for collaboration and video conferencing.

New systems based on the 4th generation Intel® Core™ processor family will not run Windows XP.

Forgoing the capabilities found in modern processors will frustrate users, as the tools they frequently use will become unavailable in a Windows XP environment.

2. Potential Organizational Liabilities and Issues

With the substantial vulnerability that Windows XP presents after EOL, organizations that don't upgrade face corresponding risks. With the liability from an APT attack or a substantial data breach, it's important to fully consider the potential liabilities and legal issues.

The most substantial liability issue involves the impact that Windows XP may exert with respect to putting an organization into a somewhat indefensible legal position. For example, **the Data Protection Act in the United Kingdom requires that organizations use up-to-date software** to protect critical or private personal and business information. According to the General Services Administration (GSA), **46 U.S. states have data privacy laws** with widely varying non-compliance penalties, each requiring the exercising of due diligence in the protection of private information.

It goes without saying that any breach traced to a Windows XP system would likely be a violation of these statutes. Given the publicity and common knowledge around the Windows XP EOL date and its potential impacts, **using Windows XP may at the very least cast doubt that an organization was being "duly diligent".**

It is also important to understand that this issue will also apply to all remote workers. Organizations may overlook remote/non-office users and leave them with Windows XP-based systems that represent a potential entry point. For this reason, ensure that replacement programs are comprehensive.

Simply put, **the longer you wait, the more you spend.**

3. The High Cost of Keeping Windows® XP

Despite the compelling arguments for migration from Windows XP to Windows® 7 or Windows 8, some organizations, for a myriad of reasons, still may not make the switch. But, in addition to the issues noted above, there are other substantial costs associated with forgoing a migration.

To start with, **the cost of a breach can be substantial.** A recent information breach at Idaho State University that was covered under HIPPA compliance requirements resulted in **a $400,000 payment to settle** the violations. In addition, it is estimated that the cost of notifying those impacted, among other remediation activities, added another $200,000 to the bill. There are also substantial reputational and public relations costs related to breaches. A single breach can impact a company's ability to attract new customers and retain existing ones.

It is somewhat inconceivable that any organization would continue with Windows XP without a CSA. To enter into a CSA, an organization must be a Microsoft Premier Customer. Companies that meet this qualification must then pay a minimum of $200,000 for a CSA, enabling them to receive updates and patches for Windows XP. Assisted support may be avaiable for an additional fee. This amount is definitely not trivial, and more importantly, this cost will rise each succeeding year. Simply put, **the longer you wait, the more you spend.**

The increased costs don't end with the CSA. Based on data from IDC , the cost of administering, supporting, managing and using Windows XP systems is substantially higher than Windows 7 systems.

For example, the **average IT time to handle operational activities** (patches, user administration, security activities, maintaining images, etc.) **is 3.0 hours per PC for a Windows XP system and only 0.9 hours for Windows 7**, based on IDC data. And it doesn't end there. IDC says the **average IT hours per PC for downtime totals 2.9 for Windows XP and 0.6 hours for Windows 7.**

End users are also impacted by Windows XP's additional costs. The cost of end-user non-productivity and wasted time can be quite high, as even mid-level employees may have a fully burdened cost of $800 per day based on a $90,000 salary, and a $200,000 yearly fully burdened cost. So when IDC says the average number of hours spent per PC per year for help desk calls is 4.8 for an Windows XP system and 0.8 for a Windows 7 system, that's $400 of fully loaded employee cost for just that aspect .

When one adds up all of the user tasks in the IDC data, you're looking at Windows XP systems using 9.0 hours per end user per PC, compared to only 1.2 hours for Windows 7. This translates to **one lost day of employee productivity for each Windows XP system** in the organization. If there are 700 XP machines in place, the organization has lost nearly two person years!

IDC also provides calculations that help to illustrate the payback period for migrating from Windows XP. Using their dynamic whitepaper on Windows XP migration, it's easy to calculate the payback period for migration to average between 10 to 17 months . From a financial perspective, the migration from Windows XP, exclusive of the security issues, would appear to be quite easy to cost justify.

If there are 700 XP machines in place, the organization has lost **nearly two person years.**

Summary

The impact of even a few Windows XP systems within an enterprise after the April 8, 2014 EOL date presents such a substantial vulnerability and security risk that it's hard to justify delaying the migration to Windows 7 or Windows 8. With a wholly new set of threats that Windows XP cannot be fully protected from, and the resulting potential for substantial corporate liability, **it's time to get the migration process moving at top speed to meet the deadline.** End users and IT managers should be acting now to put plans in place to have Windows XP machines retired by the EOL date. Prolonging the "agony" will only drive costs up and create unacceptable risks that someone will be blamed for.

Get more information about Lenovo's automated migration solution: In-Place Migration.

Sources

- "Analyzing The Cost of a HIPAA-related Breach Through the Lens of the Critical Security Controls." *Security Trends Blog.* SANS.
- "Begin Preparing For The End...Of Windows XP." *TechWeekEurope UK.*
- "Businesses Nationwide Continue to Grapple with Massachusetts Data Privacy Laws." *PrivacyAssociation.org.* International Association of Privacy Professionals.
- "Hardware Accelerating Everything: Windows 8 Graphics." *MSDN Blogs: Building Windows 8.* Microsoft.
- "Microsoft Gooses Windows XP's Custom Support Prices as Deadline Nears." *Computerworld.*
- "Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea (IDC White Paper)." *Microsoft.com.*
- "Office 2003, Windows XP Support Ends In One Year." *Dark Reading.*
- "Windows XP Decline Stalls as Users Hold onto Aged OS, Flout 2014 Deadline." *Computerworld.*

© 2013 Lenovo. All rights reserved. Lenovo® is a trademark of Lenovo in the United States, other countries, or both. Intel, the Intel logo, and Intel Core are trademarks of Intel Corporation in the U.S. and/or other countries. All other trademarks are the property of their respective owners.

Sponsored by intel inside CORE i5 vPro lenovo FOR THOSE WHO DO.