How Windows XP End of Support Will Impact Your Business

What You Must Do to Keep Your Business Secure

Daniel J. Haurey
Exigent Technologies LLC

t: 877-EXIGENT – (877) 394-4368
e: CONTACT@EXIGENT.NET
w: www.exigent.net

About This White Paper

With the Windows XP end of support date right around the corner (April 8, 2014), many companies are still struggling with what the planned end of support means for their business.

Even with Microsoft's extension for providing anti-malware signatures through July 14, 2015, there are significant security risks and hacker threats that can affect your business. This can lead to data theft, among other serious issues.

In this white paper, you will learn:

- What Microsoft means by "Windows XP End of Support"
- The key risks of not migrating to a newer version of Windows
- Potential solutions and migration paths for to keep your business secure

Windows XP, long the standard operating system in offices across the world, is nearing the end of its lifecycle. In June of 2008, Microsoft announced that it would stop officially supporting the Windows XP platform on April 8, 2014.[1] On that date, the software giant will stop offering most support, updates, patches, and security bulletins for what is still the most widely used business operating system of all time. And with many companies still months, if not longer, away from a full migration, confusion seems to be the word of the day.

This white paper explains what the Windows XP end of support (also known as "end of life") entails, what it means for businesses, and offers some alternatives and solutions for companies looking to mitigate those problems. This is not a definitive guide, and speaking with your IT provider or a managed IT services firm can pinpoint your exact needs best, as well as plotting the optimal course and schedule for your migration. Use this white paper as a starting point to begin a dialogue with someone who specializes in the migration needs of your business.

What is Windows XP End of Support?

Windows XP end of support is the term for Microsoft's policy of ending official support for a product after a given quantity of time since the product was released.

According to Microsoft's Malware Protection Center, "After April 8, 2014, Windows XP users will no longer receive new security updates, non-security hotfixes, free or paid assisted support options, or online technical content updates from Microsoft."

Microsoft will continue to provide updates for their anti-malware signatures for Windows XP users through July 14, 2015, but there will be no security updates. This presents a big security risk to Windows XP users.[2]

> Hackers and other criminals have been stockpiling malware for over a year in preparation for the day Windows XP is no longer supported. They are ready to unleash it on unsuspecting XP users.

Microsoft's End of Support Process

Introduced in 2002 (a year before Windows XP was released), this product lifecycle was meant to make the migration and upgrade process reliable, stable, and transparent. Per Microsoft's XP end of life micro-site: "In 2002 Microsoft introduced its Support Lifecycle policy based on customer feedback to have more transparency and predictability of support for Microsoft products."[3]

The product lifecycle for business products like Windows XP, Server 2003, and the Office 2003 suite hinges on a two-part, 10-year cycle.

---

1 http://windows.microsoft.com/en-us/windows/end-support-help

2 http://blogs.technet.com/b/mmpc/archive/2014/01/15/microsoft-antimalware-support-for-windows-xp.aspx

3 http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx

Part I: The initial five years represent mainstream support. During this phase, Microsoft not only provides security updates, but also regular "hotfix" patches (small software updates meant to solve specific problems or bugs found in the main product), as well as major overhauls and redesigns like the Service Packs that most Windows users are familiar with. This can be compared to a warranty period on a car purchase - if something goes wrong, Microsoft will usually take care of it.

Part II: The next five years is the Extended Support Phase. During this period, Microsoft will continue to provide security patches and bulletins, and in some cases will still provide hotfixes for their product, though not for all bugs and not for all products. This is the phase in which Windows XP and Office 2003 are currently. Also during this time, Microsoft continues to provide paid support, but no longer offers complimentary support to licensed product owners.

At the end of the Extended Support phase, Microsoft stops releasing all updates and no longer provides any kind of mainstream support for Windows XP, including security updates, bug fixes, and phone or email support. On April 8, 2014, Windows XP and Office 2003 will reach this point and will no longer be officially supported, though Microsoft will continue supplying anti-malware signatures until July 2015.

At the end of the Extended Support phase, Microsoft stops releasing all updates and providing any kind of mainstream support for that product, including security updates, bug fixes, and phone or email support. On April 8, 2014, Windows XP and Office 2003 will reach this point, and will no longer be officially supported. Additional software from Microsoft for the Windows XP platform will likewise no longer be released or supported, for the most part. Microsoft has stated that it will continue to provide updates to Microsoft Security Essentials, its consumer XP security suite, until July 14, 2015. For enterprise customers, Microsoft has committed to providing security updates to System Center Endpoint Protection, Forefront Client Security, Forefront Endpoint Protection and Windows Intune running on Windows XP.

Otherwise than that, Microsoft will no longer update any other XP related software. Microsoft will also no longer have Security Essentials or its enterprise security suite for XP available for download or purchase.[4] So, if your business does not yet have Security Essentials installed[5] and will not be ready to migrate off of Windows XP by April 8, 2014, we strongly suggest installing a copy as soon as possible or contact your managed IT services provider for guidance.

Why is XP End of Support Important?

Many businesses put off migrating to newer software because it is not entirely clear what "end of support" means in regards to their operations. Many companies never deal with Microsoft directly for equipment and software support, instead working through third-party support companies like managed IT service firms and contractors. This tends to create an atmosphere that downplays the

[4] http://www.zdnet.com/microsoft-to-extend-windows-xp-anti-malware-updates-one-year-7000025215/

[5] http://windows.microsoft.com/en-us/windows/security-essentials-download

role Microsoft has in maintaining, securing, and supporting their business operations. While it is entirely possible that no one at your company has ever picked up the phone and dialed Microsoft's support number, or sent a quick email to one of Microsoft's support desks, Microsoft still plays an invaluable support role for all organizations using Microsoft products.

Much of this support is invisible to end users and difficult to quantify. For example, Microsoft sets and enforces operability standards on software manufacturers. This can include creating a guideline for how PDF documents are handled, or the technical process that occurs in the event of a crash. Other benefits are much easier to put a number on. By mid-January 2014, Microsoft had already released four new security bulletins, all rated important, and most of which are set to download and install silently. This is on top of the hundreds of security bulletins and patches it has released over the course of the Windows XP and Office 2003 lifetimes. **When April 8, 2014 rolls around, all of this will stop and businesses that have not migrated will be exposed, no matter who handles their direct support.**

There are two primary reasons why XP end of life is so critical for businesses to pay attention to: the risks of not migrating to a newer operating system, and costs of not migrating.

Risks

The largest security risk will be in the form of "zero-day" exploits. These exploits are new and never before seen, and are called zero-day because they do most of their damage on the first, or zeroth, day that they are released into the wild.[6] Usually, these exploits are found quickly and patched or otherwise invalidated. Once XP end of life occurs, however, security patches will no longer be forthcoming, and zero-day will stretch on until the last Windows XP machine is upgraded or disposed of.

The largest security risk will be in the form of "zero-day" exploits. These exploits are new and never before seen, and are called zero-day because they do most of their damage on the first day that they are released into the wild.

In fact, the risk is even worse than it seems. While threats for active software with a long lifespan tend to come out organically and irregularly, many security experts believe that hackers and other criminals have been stockpiling malware for at least the last year in preparation for the day XP is no longer supported. Instead of letting exploits be caught, identified, and corrected, there is now a huge pool of viruses and other malware that will catch individuals and businesses using XP completely off guard with no chance of future patches or security updates.

This problem is exacerbated since many third-party companies that provide software for Windows XP will stop providing updates at the same time as Microsoft. While several major anti-virus suites have promised to provide updates beyond April 8th, they will still be unable to close vulnerabilities in Windows XP itself, and will be playing a constant game of catch-up as malware writers continue to exploit the same vulnerabilities with programs just different enough to slip past the virus filters. In short, keeping an XP system secure will be like trying to keep a boat afloat by constantly plugging new holes with your fingers - eventually you run out of fingers.

---

6 http://www.pcworld.com/article/2046839/zero-day-forever-move-away-from-windows-xp-now.html

Costs

Besides the costs of potential security breaches and malware infestations, holding on to Windows XP past the end of life date carries some very serious and very expensive costs. For companies large enough to be on Microsoft's radar, the maker of Windows XP has stated off-the-record that they will likely continue to provide support on a paid contract model. The price of this paid support is estimated in the range of $100,000 to $300,000 per year or more, which puts it squarely out of the budget for most small and mid-size businesses. Non-Microsoft support companies are jumping in to fill the gap left by the departing software maker, but their support options are limited. Most range in price from $15 to $50 per XP device, and they don't have the ability to actually update the operating system. The best they can do is monitor for threats and try to block those threats from entering the system.

Companies using specialized software built on XP can also face tremendous costs. As third-party software vendors move their operations to Windows 7, 8 and 8.1, they will also stop providing XP-centric updates. That means companies that realize they need a critical patch or software update can end up paying huge sums for a custom solution, assuming the vendor is even willing to provide that service. Unless your company's infrastructure has reached its pinnacle and there is no possible way you will need to upgrade any of your third-party software, maintenance will likely become significantly more expensive for XP-based software.

Besides the costs of potential security breaches and malware infestations, holding on to Windows XP past the end of life date carries some very serious and very expensive costs.

Post-Windows XP Options and Migration Path

Businesses looking for a way forward past the April 8th deadline have several options available to them. The most obvious path forward is a migration to the next version of the Windows operating system, however it not the only choice. In this section we will explore several potential options that may be right for your company.

Windows 7

Windows 7 represents the most straightforward and simple upgrade path for most businesses. The operating system is visually and functionally very similar to Windows XP, making transitioning your team very easy. Windows 7 also has a long history in business, and has been in use by many companies large and small for many years. Most large vendors that provide third-party software have had ample time to upgrade their products to Windows 7. That means support is strong, and there is plenty to choose from among vendors.

The main drawback of migrating to Windows 7 is that Microsoft has already scheduled the end of life for that operating system on January 14, 2020.[7]

Windows 8/8.1

The new flagship product from Microsoft, Windows 8.1, has received some criticism for being a sharp deviation from the classic Windows interface. That could mean that it takes some time for your staff to get used to the new interface, but there is a way to make the interface look like Windows 7, something your users might be more comfortable with.[8] Underneath the cosmetic changes, however, is a great operating system that has been optimized from the top down for performance. The addition of several new features has actually made Windows 8 a powerful business system, and well worth a look as a replacement for Windows XP. Additionally, Windows 8 is scheduled to be supported until January 10, 2023.

The biggest drawback for Windows 8 for business use is the relative newness of the operating system. It hasn't been really tested in a commercial setting.[9] Some third-party software companies do not fully support Windows 8/8.1, but they will likely have to do so soon. If your business requires specialized software, such as point-of-sales systems, electronic record keeping, etc., check with your IT provider to see if Windows 8/8.1 will work with your other software.

Non-Windows Migration Paths

As with any major business decision, there are plenty of non-obvious options, such as switching to Apple OS X, which has been proven in business environments for years and can make a good replacement for Windows. Each potential option comes with a host of positives and negatives that are beyond the scope of this white paper to fully explain. If you may think that a non-Microsoft migration solution may work for you, or if you have any questions, speak to your managed service provider or managed IT company about possible alternatives.

Getting Rid of Old Equipment

If your current computers cannot effectively handle a more recent operating system, you will need to upgrade your equipment. It is important to remember what steps to take before throwing out any old PCs.

1. Make sure to start with a full backup of each machine. Often, it is easier to create a full disk image instead of backing up individual files; however, if you plan on moving to a new OS you will need to back up the files individually.

---

[7] http://windows.microsoft.com/en-us/windows/lifecycle

[8] http://blog.laptopmag.com/make-windows-8-like-windows-7

[9] http://www.informationweek.com/windows-8/windows-8-adoption-slows-ahead-of-windows-81/d/d-id/1111758?

2. After backing up all of your data, do a full inventory of the software on the computer, since any unique programs that your company uses will need to be re-installed on the new machines.

3. Finally, the most important step is to have your IT team or managed services provider remove the hard drive from each machine to keep in storage. Remember that wiping a hard drive or reformatting it is not always enough to completely wipe all of the data, so make sure to either keep old hard drives stored away safely or destroy them.

Your Next Steps

As with any major technology change, the Windows XP migration can present a challenge and an opportunity. Since staying on Windows XP is no longer an option, organizations can use this time to set themselves up for a successful future. While migrating can seem like a huge challenge, leveraging this forced upgrade to your advantage can give you a major boost in productivity and ensure that your company data is safe from security hacks and breaches.

The decisions your organization makes today regarding your technology use can seriously impact the way you do business in the future. Use this opportunity to jump ahead rather than fall behind. To evaluate the best options for your organization, please contact us for an assessment of your existing technology infrastructure. We will evaluate it for security risks and recommend efficient, cost-effective options that will help your company develop a comprehensive understanding of what your technology use looks like now, where potential problems may be hiding, and how to move forward in a manner that benefits your organization.