A **TrendLabs** Security in Context Paper

TREND MICRO™

Managing Your Legacy Operating Systems

What Will Life Be Like After Windows XP?

Microsoft has been supporting Windows® XP for over a decade but will stop doing so after April 8, 2014. Users will no longer receive security updates, nonsecurity hotfixes, free or paid assisted support options for Windows XP, and online technical content will no longer be updated.

The looming end-of-support date means that corporate systems that still run Windows XP may face serious consequences. This paper discusses the technology threats, potential liabilities and compliance issues, and increased user computing costs enterprises may face if they continue to use the operating system (OS).

Windows XP in Today's OS Market

Figure 1 shows the Windows XP worldwide usage rate's slow decline in the past year. Though the OS's share significantly declined, Windows XP still has a very strong market foothold. Microsoft has been in command of the client OS market for 20 years now. Based on an IDC study, nine out of every 10 PCs still run on Windows OSs.[1] A Spiceworks survey also found that, as of December 2013, 76% of IT professionals still supported Windows XP. Among them, 97% supported the OS on desktops while 68% did so for laptops.[2]

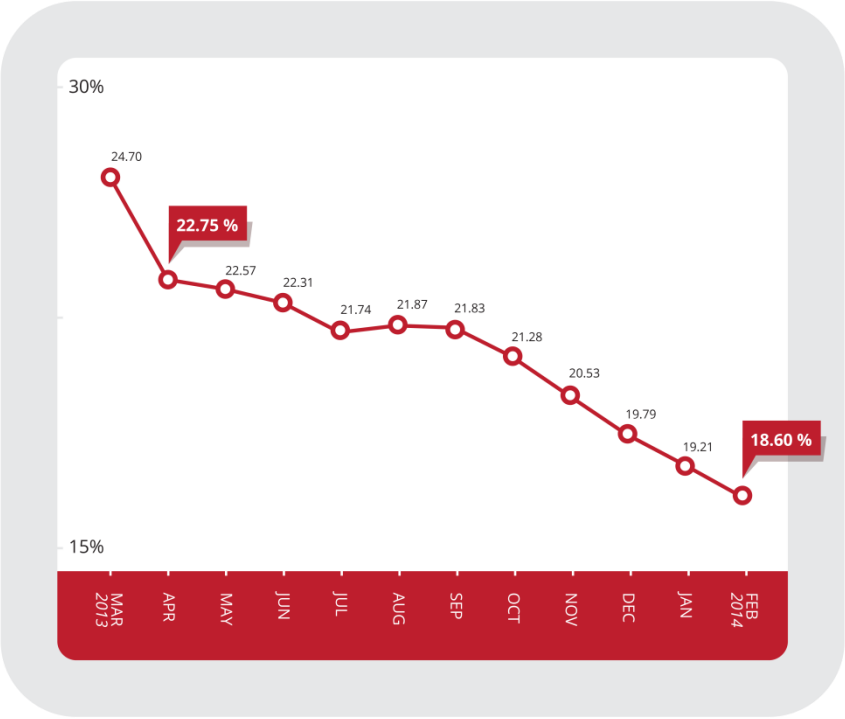

Figure 1: Windows XP market share from March 2013 to February 2014
Source: StatCounter.com

[1] Al Gillen, Randy Perry, and Nancy Selig. (May 2012). "Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea." Last accessed March 21, 2014, http://download.microsoft.com/download/2/2/A/22A70C6F-71F7-4984-8404-4FBA665B27D8/WHITEPAPER%20--%20IDC%20MSFT%20-%20Migration%20from%20XP%20to%20Win7.pdf.

[2] Spiceworks. (December 2013). "Getting Over Your XP: Windows XP End-of-Life and Why Breaking Up Is Hard to Do." Last accessed March 21, 2014, http://www.spiceworks.com/voit/reports/windows-xp-end-of-life/.

Windows XP is still widely used despite the looming end of support for the OS. Microsoft has ended support for Windows versions before but never for one that remains in use. One possible factor for its continuing dominance could be the 2008 economic crisis when companies suffered from insufficient cash flow, layoffs, and cost reductions.[3] The five-year gap between Windows XP and its successor, Windows Vista, may not have compelled companies enough to upgrade as well, leading to a slow desktop replacement cycle.

The data in Figure 1 is disconcerting, as a large portion of the desktop market will remain vulnerable to an increasingly larger number of threats. When Windows XP was first introduced in 2001, mobile use was rare and networking was accomplished using wired connections. Network access was obtained via company-controlled networks and remote access was commonly achieved via phone lines. The PC threats back then were also mostly designed to annoy users and waste their time rather than to steal critical data. Simply put, the need to migrate from Windows XP is due to the fact that the era for which it was designed has long passed.

[3] Barbara Kiviat. (September 16, 2013). *Time*. "Explaining the Financial Crisis: Why Do We Still Not Know What Happened?" Last accessed March 21, 2014, http://business.time.com/2013/09/16/explaining-the-financial-crisis-why-do-we-still-not-know-what-happened/.

Why Is It So Hard to Migrate?

Despite the pressing urgency, migrating to another OS is not as easy as some might believe. IT professionals anticipate challenges that come with a major OS upgrade. A Dell study revealed that migration caused the respondents headaches.[4] Challenges such as application compatibility (41%) and user training and support (33%) were mentioned. Upgrading also involved purchasing new hardware, which could also pose problems for seamless transition.

Will Windows XP Suffer the Same Fate as Java 6?

After the Java™ 6 end of life (EOL) last February 2013 when Oracle stopped providing security updates to fix vulnerabilities, attackers immediately went after unpatched versions of the software. A few months after Java 6's EOL, attackers attempted to exploit CVE-2013-2463, which affected certain versions, including Java 6.[5] Because Java 6 was no longer supported at the time, Oracle did and will not release security updates for its users. Even worse, the exploit used was integrated into the Neutrino Exploit Kit, which can lead to more successful future attacks.

Java 6 could serve as an example of what would likely happen to Windows XP users after April 8, 2014. Windows XP threats are about to become significantly deadlier. However, common code between Windows XP and newer Windows OS versions may serve as "clues" for spotting vulnerabilities that need patching.

In sum, today's threats have substantially changed, creating a reality wherein Windows XP vulnerabilities can put an entire company and its data at risk. To protect against vulnerabilities for which software patches will no longer be made available, using a vulnerability protection solution such as Trend Micro™ OfficeScan™ Intrusion Defense Firewall is advisable. Vulnerability shielding works on the premise that exploits take a specific or definable network path to and from an application in order to use a vulnerability. It is, therefore, possible to manipulate the network layer through rules to control the communications being made to the targeted software.

[4] Dell Inc. (September 2013) "Migrating Away from Windows XP: A Survey of IT Professionals." Last accessed March 21, 2014, https://www.kace.com/resource-center/resources/analyst-reports/Migrating_Away_from_Windows_XP_A_Survey_of_IT_Professionals.

[5] Gelo Abendan. (August 27, 2013). *TrendLabs Security Intelligence Blog*. "Java 6 Zero-Day Exploit Pushes Users to Shift to Latest Java Version." Last accessed March 21, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/java-6-zero-day-exploit-pushes-users-to-shift-to-latest-java-version.

What Potential Technology Risks Will Companies Face?

An October 2013 Microsoft announcement claimed that the number of Windows XP infections may rise 66% after support for the OS ends, which means attackers are likely to take advantage of windows of exposure.[6] Attackers will try to find vulnerabilities in Windows XP by reverse-engineering security updates for newer Windows OS versions. Cybercriminals may even be "hoarding" exploits to launch once support for Windows XP ends.[7]

Internet Explorer® (IE) poses other risks that will arise once support for Windows XP ends. No version of the browser later than IE 8 is compatible with the platform, which means users who will continue to use the OS will be left behind. They can, of course, use alternative browsers. However, simply switching browsers may not be 100% foolproof against browser exploits.

Another possible technology risk is that vulnerable endpoints may be used as launch pads for next-generation malware that obsolete systems might find difficult to deal with. Targeted attack campaigns often use software exploits to get in to systems, rendering enterprises at risk of data theft or espionage, and any PC running Windows XP is an obvious weak point from attackers' point of view.

What Is the Cost of Not Migrating?

Not scrapping and replacing legacy systems and software involve significant corporate risks, including potentially unpredictable costs and consequences. However, a seemingly valid contention—sticking with Windows XP means users would not have to learn how to use a new OS because are already familiar with the interface and developers know the platform inside out—also exists.

So why bother switching? First off, IT administrators should consider the financial cost of maintaining Windows XP after support for it ends. Companies that need to stick with systems running the OS are likely to avail of custom support services, which require becoming Microsoft Premier Online customers.

The costs do not end with availing custom support services though. Based on the previously cited IDC study, administering, supporting, managing, and using Windows XP systems is substantially more expensive than doing the same for Windows 7 systems. As shown in Table 1, the average amount of IT time spent on handling operational Windows XP versus Windows 7 system activities is also higher.

---

[6] Gregg Keizer. (October 30, 2013) *Computerworld*. "Windows XP Infection Rate May Jump 66% After Patches End in April." Last accessed March 21, 2014, http://www.computerworld.com/s/article/9243660/Windows_XP_infection_rate_may_jump_66_after_patches_end_in_April.

[7] Dan Worth. (March 10, 2014). *V3.co.uk*. "Hackers Hoarding Windows XP Exploits for Cut-Off Bonanza." Last accessed March 21, 2014, http://www.v3.co.uk/v3-uk/analysis/2333009/hackers-hoarding-windows-xp-exploits-for-cut-off-bonanza.

Table 1 Average Amount of IT Time Spent on Operational Activities	
Windows XP	**Windows 7**
Operational Activities	
3 hours	0.9 hours
Downtime	
2.9 hours	0.6 hours
Amount of Time Lost by User per Year	
9 hours	1.2 hours

Source: IDC and Microsoft

What If Immediate Migration Is Impossible?

If companies have to maintain their Windows XP systems, using a whitelisting approach to keep a more secure corporate environment is recommended. Trend Micro™ Endpoint Application Control™ controls applications that run on endpoints. This additional layer of protection prevents the installation and execution of any unwanted, untrusted, or malicious applications on endpoints and is simple to manage and deploy with an endpoint security solution such as Trend Micro OfficeScan.

Figure 1: To support a layered approach to security, Endpoint Application Control is easy to integrate with Trend Micro Complete User Protection solutions to deliver multiple layers of interconnected threat and information protection.

Upgrading OSs, if possible, should be the immediate course of action. However, for some, it may be necessary to keep Windows XP going even after support ends. The following are some best practices for system administrators of companies that need to keep using the OS. Although these tips will not solve existing problems, following them can help your company avoid future problems.

- **Virtualize your Windows XP environment.** This will provide an additional layer of security and more efficient management.
- **Use a Read-Only Domain Controller (RODC) such as Windows 2008, 2008 R2, 2012, or 2012 R2 on Windows XP LAN.** For effective management, using a domain controller on the same LAN switch to which any Windows XP systems are connected is recommended. By keeping the domain controller in read-only mode, your system administrators can still effectively remotely manage Windows machines without affecting the security of your entire network.
- **Implement the strongest possible security group policy settings to Windows XP machines.** Recommendations should fit your company's requirements. It is strongly recommended though to use Specialized Security-Limited Functionality (SSLF) group policy settings. More information on best practices for group policy settings can be found in the "Windows XP Security Guide" and the "Threats and Countermeasures Guide."[8]
- **If possible, do not allow Windows XP machines to communicate outside the internal network.** Manually provide updates to third-party software, if and when needed. If communicating outside the internal network is unavoidable, use a Web proxy or an application-layer firewall.
- **Consider using alternative browsers.** Because using IE may be unavoidable, only use it if a site will absolutely not work with any other browser.
- **Use an intrusion prevention system (IPS) device on the LAN.** You can do this either on the Switched Port Analyzer (SPAN) port or between the LAN switch and the rest of the network.

"The existence of even a few Windows XP systems within an enterprise after support ends presents substantial vulnerability and security risks that would make it hard to justify keeping them. With an increasingly larger number of threats that the OS cannot be fully protected from and the resulting potential for substantial corporate liability, it is highly recommended that Windows XP no longer reside in enterprises."

—Edward Ray, senior cyberthreat researcher

8 Microsoft. (2014). *Microsoft Download Center.* "Windows XP Security Guide." Last accessed March 21, 2014, http://www.microsoft.com/en-us/download/details.aspx?id=962; Microsoft. (2014). *Microsoft Download Center.* "The Threats and Countermeasures Guide." Last accessed March 21, 2014, http://www.microsoft.com/en-us/download/details.aspx?id=24696.

Trend Micro will also extend endpoint protection support for Windows XP users to help make the transition to newer Windows OS versions less complex. Extended support for business endpoint protection products, OfficeScan and Trend Micro™ Worry-Free Business Security™, will run until January 30, 2017.[9] As an OfficeScan plug-in, Intrusion Defense Firewall will also provide stronger endpoint protection by supplementing highly effective client-level security with network-level Host Intrusion Prevention System (HIPS) to protect endpoints against vulnerabilities.

To combat targeted attacks, meanwhile, Trend Micro™ Deep Discovery provides advanced threat protection and identifies evasive threats in real time. It also offers in-depth analyses and actionable intelligence to assess, remediate, and defend themselves against targeted attacks.

[9] Trend Micro Incorporated. (2014). "Trend Micro's Official Statement for Windows XP End of Support." Last accessed March 21, 2014, http://esupport.trendmicro.com/solution/en-us/1101907.aspx.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud