Microsoft

Windows XP Support Has Ended – Why It Concerns You

Protect

Detect

Respond

Windows XP support has ended - why it concerns you

Windows XP Service Pack 3 (SP3) and Office 2003 reached end of extended support on 8. April 2014. Microsoft no longer provides public support for these products, including security patches, non-security hotfixes, incident support or online technical content updates.

Running Windows XP SP3 may expose organizations to potential risks, such as security & compliance risks or lack of Independent Software Vendor (ISV) & Hardware Manufacturers support.

To mitigate the risk of cyberthreat and to protect their IT infrastructure, enterprise and public sector organizations are strongly recommended to migrate away from Windows XP to Windows 7 or Windows 8 and to implement an appropriate patching regime to ensure a good security hygiene.

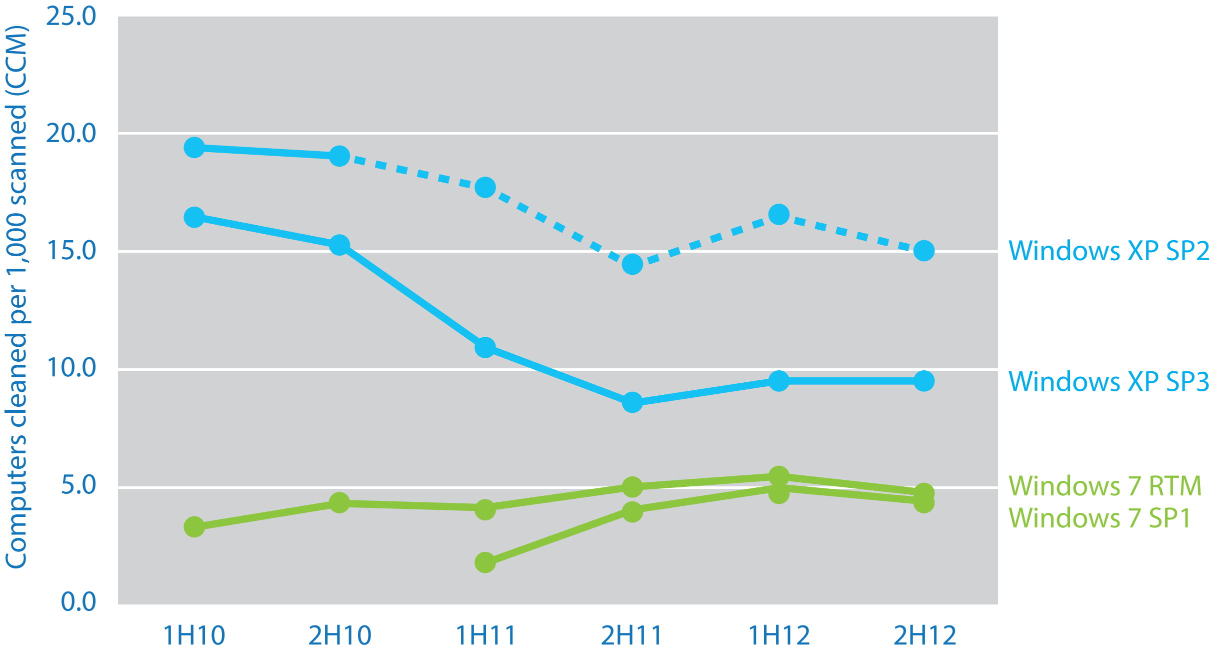
Windows XP great in its time – but times have changed

It has been twelve years since the release of Windows XP and the world has changed so much since then. Internet usage has grown from ~361 million to more than 2.4 billion users. We have witnessed the rise of the internet citizen with members of society connected through email, instant messaging, video-calling, social networking and a host of web-based and device-centric applications. As the internet becomes more and more woven into the fabric of society, it has also become an increasingly popular destination for malicious activity (as evidenced in the Microsoft Security Intelligence Report.) Given the rapid evolution, software security has had to evolve to stay ahead of cybercrime. To help protect users from rapid changes in the threat landscape, Microsoft typically provides support for business and developer products for 10 years after product release, and most consumer, hardware, and multimedia products for five years after product release.

Per our long established product support lifecycle, Windows XP SP3 users no longer receive new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates. This means that any new vulnerabilities discovered in Windows XP will not be addressed by new Microsoft security updates. From now it is significantly easier for attackers to successfully compromise Windows XP-based systems using exploits for unpatched vulnerabilities. In this scenario, antimalware software and other security mitigations are severely disadvantaged and over time will become increasingly unable to protect the Windows XP platform.

We can get insight into what happens to malware infection rates once a platform goes out of support by looking at Windows XP Service Pack 2 (SP2) as an example. Support for Windows XP SP2 ended on 13. July 2010. Although this platform benefited from numerous security enhancements when it was released, today it has a much higher malware infection rate than Windows XP SP3 or any of the newer Windows operating systems. As the figure on the next page illustrates, computers running Windows XP routinely experience a significantly higher malware infection rate than computers running any other supported version of Windows. Much of the elevated infection rate on Windows XP can be attributed to the fact that some of the key built-in security features included with more recent versions of Windows are not present in Windows XP. Windows XP, designed in a different era, simply can't mitigate threats as effectively as newer operating systems, like Windows 7 and Windows 8.

As the threat landscape has evolved over the past twelve years since the release of Windows XP, so has software security. There are many new security features today in more modern operating systems that can better protect users from criminal activity including:



- Kernel improvements:

Recent versions of Windows include a number of security-related improvements to the Windows kernel, making it harder for cybercriminals to use standard hacking techniques, such as exploiting buffer overflows or predict memory location of code.

- Real-Time Malware Protection:

In Windows 8, Windows Defender provides real-time protection against malware and potentially unwanted software out of the box.

- BitLocker Drive Encryption:

Introduced in Windows Vista, BitLocker Drive Encryption enables users and administrators to encrypt entire hard drives, protecting data on lost or stolen computers from unauthorized access. Windows 7 introduced BitLocker To Go, providing full disk encryption for removable volumes. In Windows 8, BitLocker can more easily be deployed and managed.

- User Account Control (UAC):

Introduced in Windows Vista, User Account Control helps prevent unauthorized changes to a computer by enabling user accounts to run without administrator permissions except when needed to perform administrative tasks. UAC was streamlined in Windows 7 and later operating systems, providing an improved user experience.

- AppLocker:

Introduced in Windows 7, AppLocker can be used by IT departments to restrict the programs users can execute by defining powerful and flexible rules. In Windows 8, administrators can restrict Windows Store apps in addition to legacy Windows applications.

- UEFI Secure Boot:

Introduced in Windows 8, UEFI Secure Boot is a hardware based feature that is required on all Windows 8 certified devices. It helps prevent unauthorized operating systems or firmware from running at boot time by maintaining databases of software signers and software images that are pre-approved to run on the individual computer.

- Trusted Boot:

The Trusted Boot feature in Windows 8 verifies the integrity of Windows startup files, and includes an Early Launch AntiMalware (ELAM) capability that enables the antimalware software to start before any third party software. By starting the antimalware solution early and within the protected boot process, the operation and integrity of the antimalware solution can be better guaranteed. As part of the boot process, Windows also runs Measured Boot, which allows third-party software on a remote server to securely verify the security of every startup component in a way that would be very difficult for malware to forge. If any tampering with the Windows boot process or the antimalware's ELAM driver is detected, Trusted Boot will repair the system by restoring the original files.

Over and above all the security mitigations and features that are available in more modern operating systems, security development practices have also evolved greatly over the past decade, but so has the threat landscape. See the table on the next page showing the key threats present during the time of release of Windows XP, Windows Vista, Windows 7 and Windows 8.

Key Threats

- Internet was just growing
- Mail was on the verge

1995

Windows 95

- -

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

Key Threats

- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure ”by default” configuration (Windows features and IE)

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

Key Threats

- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)

2012

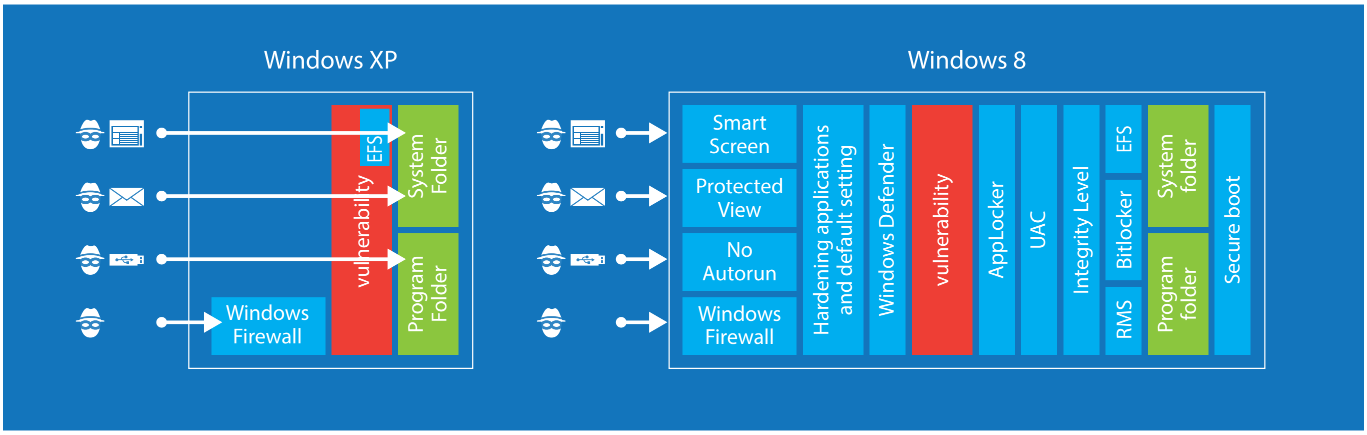
Windows 8

- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (w/ELAM)
- Measured Boot and Remote Attestation Support
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Picture Password, PIN
- Dynamic Access Control
- Built-in Anti-Virus

The risk of Windows XP not being supported any more

As cybercriminals are very well aware that XP does not receive any longer security updates, it can be assumed that exploits will be targeted and leveraged quickly. In addition, the new operating system offers new opportunities for telecommuting, sharing of documents and information, working with mobile solutions and connect with cloud services without impacting your security.

The effect of this is that today's cyberthreats are significantly better contained in Windows 8 than in Windows XP.



Vulnerability of Windows XP compared to windows 8

The risk is real, and it is not only about security. Further risks include:

- Unsupported business software

Since security fixes and support for Windows XP ended on April 8, 2014, Independent Software Vendors have already stopped testing new software versions on Windows XP and new releases of critical business software may require Windows 7 at minimum.

- Unsupported hardware

Hardware Vendors and OEM's have also stopped testing new devices on Windows XP. Many currently shipping computers will not support XP and device drivers are not available.

- Increases support costs

Software Assurance no longer provides support so customers needing support on XP will be required to have XP Custom Support Agreement (CSA) in place. Additional cost will include an Enrollment Fee, and a Per Device Fee.

Additional benefits for migration

Organizations that have migrated to Windows 7 or 8 are enjoying the benefits of a much improved user, and management experience. One of the great advantages of the migration is the opportunity to transform outdated, manual processes. Real, tangible cost savings are realized as a natural outcome of the capabilities of Windows 8 Enterprise.

- Anywhere Connection

Give people secure, hassle-free access to data, applications, and colleagues. They need to stay productive anywhere, anytime, and on a variety of devices.

- Personalized Experience

Enhance productivity by giving people personalized experiences that anticipate their needs, remember their preferences, and adapt to their unique workstyle.

- Intelligent Infrastructure

Deliver enterprise-grade solutions designed to help you maintain security, streamline management, and cut costs.

- Desktop Deployment Planning Services (DDPS)

Plan and prepare for an efficient and successful Microsoft Office deployment by taking advantage of comprehensive planning services delivered through prequalified partners.

- Microsoft App Accelerate Program (MAAP)

Test the product and service capabilities in a lab environment, define requirements for the new deployment, conduct a pilot, and then fully deploy the Solution for Flexible Workstyle.

- Windows To-Go

As bring-your-own-device (BYOD) and mobility scenarios become increasingly common, businesses need new and more flexible ways to help users be productive wherever they are. Windows To Go is a new feature for enterprise users of Windows 8 that enables users to boot a full version of Windows from external USB drives on host PCs. Windows To Go drives can use the same image that enterprises use for their desktops and laptops, and can be managed the same way. Offering a new mobility option.

- Reduced cost

„IDC's analysis shows that supporting older Windows XP installations, compared with a modern Windows 7-based solution, saddles organizations with a dramatically higher cost. Annual cost per PC per year for Windows XP is $870, while a comparable Windows 7 installation costs $168 per PC per year. That is an incremential $701 per PC per year for IT and end user labor costs."

(Source: „Mitigating Risk: Why Sticking with Windows XP is a Bad Idea." IDC White Paper, May 2012.)

We are aware that there may be a lot of challenges with the transition to new systems, and have therefore developed a number of tools that will make it easier to migrate solutions to a modern platform.

Plan and execute your Windows XP migration

Windows XP was a great operating system in its time and provided value to a large number of people and organizations around the world for over a decade. But all good things must come to an end. We hope this information reinforces the importance of migrating to a modern operating system with increased protections, and instills a sense of urgency onto organizations that have still deployed Windows XP.

The support and maintenance for windows XP has ended – It is crucial that that enterprises, public sector organizations and consumers migrate to systems to Windows 7 or 8: our new, modern operating systems that have been made for the future, both in terms of new usages such as touch and mobile computing, but importantly also due to the heightened security.

Elements to a Secure Environment – Becoming Resilient Towards Modern Cyberthreats

This whitepaper is part of a series of papers on achieving resilience towards modern cyberthreats. It follows the “protect – detect – respond” framework. In short, the framework is based upon the assessment that against modern attackers it is not enough to apply protective measures but that we need to be prepared to contain potentially successful intruders, detect them, respond to the incident and have the capability to recover. Threat information is the foundation for all activities and provides awareness during each step.

Protect

Detect

Respond

- **Protect** systems from compromise through a combination of training, implementation, and assessments. Focus efforts on:
- **Detect** active attacks or compromised systems before they become pervasive in the customer.
- **Respond** to an intrusion once it is detected.

For More Information Please Visit:

Microsoft Security:
http://www.microsoft.com/security

Windows XP end of support:
http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

Security Intelligence Report:
http://www.microsoft.com/security/sir/default.aspx

This document is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.