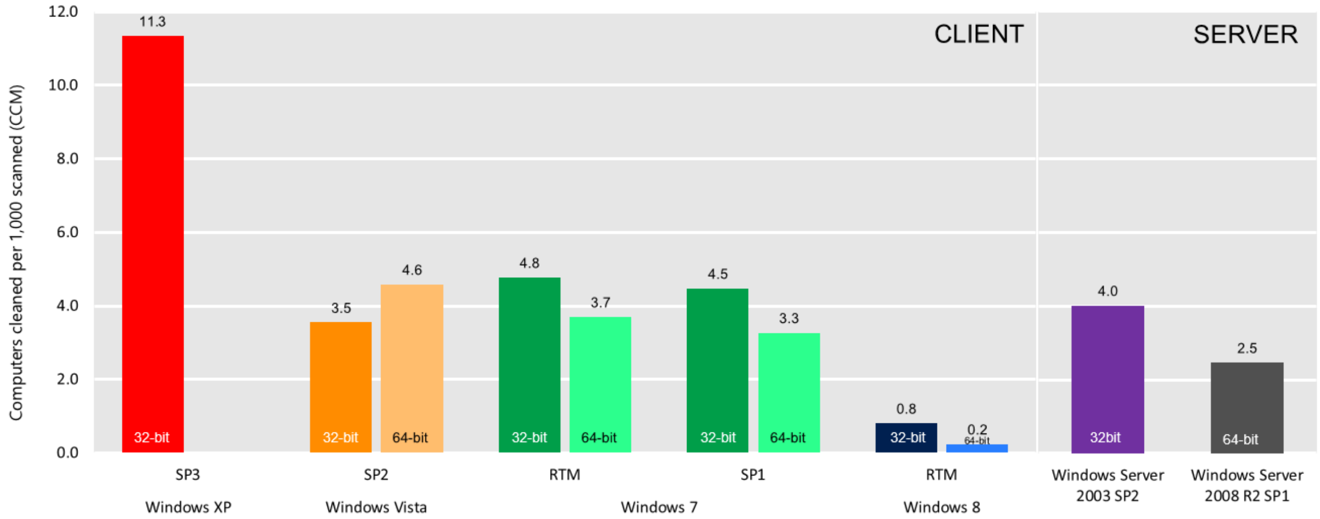
The risk of running Windows XP after support ends

Support for Windows XP ends April 8 2014

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. This means that any new vulnerabilities discovered in Windows XP after its end of life will not be addressed by new security updates by Microsoft. Moving forward, this will make it 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 and will become increasingly unable to protect the Windows XP platform.

Windows XP is already significantly more likely to become infected with malware, as shown in Microsoft's Security Intelligence Report covering the second half of 2012[1]:



www.microsoft.com/sir

What is the risk of continuing to run Windows XP after support ends?

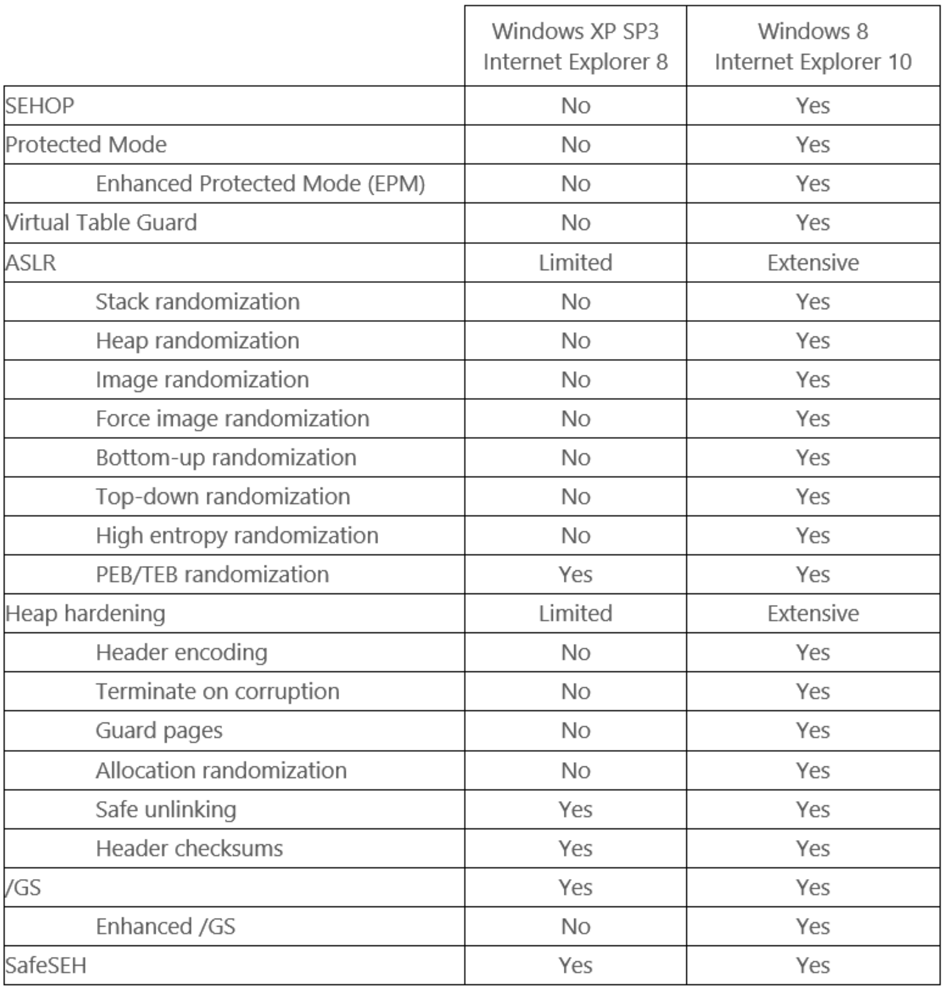
One risk is that attackers will have the advantage over defenders who choose to run Windows XP because attackers will likely have more information about vulnerabilities in Windows XP than defenders. When Microsoft releases a security update, security researchers and criminals will often times reverse engineer the security update in short order in an effort to identify the specific section of code that contains the vulnerability addressed by the update. Once they identify this vulnerability, they attempt to develop code that will allow them to exploit it on systems that do not have the security update installed on them. They also try to identify whether the vulnerability exists in other products with the same or similar functionality.

The very first time after April 2014 that Microsoft releases security updates for supported versions of Windows, attackers will reverse engineer those updates, find the vulnerabilities and test Windows XP to see if it shares those vulnerabilities. If it does, attackers will attempt to develop exploit code that

[1] www.microsoft.com/sir

can take advantage of those vulnerabilities on Windows XP. Since a security update will never become available for Windows XP to address these vulnerabilities, Windows XP will essentially have a “zero day” vulnerability forever. How often could this scenario occur? Between July 2012 and July 2013 Windows XP was an affected product in 45 Microsoft security bulletins, of which 30 also affected Windows 7 and Windows 8.

Windows XP security mitigations were state of the art when they were developed many years ago. But we can see from data published in the Microsoft Security Intelligence Report that the security mitigations built into Windows XP are no longer sufficient to blunt many of the modern day attacks we currently see. The table below compares the mitigation features supported by Internet Explorer 8 on Windows XP Service Pack 3 with the features supported by Internet Explorer 10 on Windows 8. As this table shows, Internet Explorer 10 on Windows 8 benefits from an extensive number of platform security improvements that simply are not available to Internet Explorer 8 on Windows XP:



	Windows XP SP3 Internet Explorer 8	Windows 8 Internet Explorer 10
SEHOP	No	Yes
Protected Mode	No	Yes
Enhanced Protected Mode (EPM)	No	Yes
Virtual Table Guard	No	Yes
ASLR	Limited	Extensive
Stack randomization	No	Yes
Heap randomization	No	Yes
Image randomization	No	Yes
Force image randomization	No	Yes
Bottom-up randomization	No	Yes
Top-down randomization	No	Yes
High entropy randomization	No	Yes
PEB/TEB randomization	Yes	Yes
Heap hardening	Limited	Extensive
Header encoding	No	Yes
Terminate on corruption	No	Yes
Guard pages	No	Yes
Allocation randomization	No	Yes
Safe unlinking	Yes	Yes
Header checksums	Yes	Yes
/GS	Yes	Yes
Enhanced /GS	No	Yes
SafeSEH	Yes	Yes

For more information, check out these resources

Microsoft Security Blog: http://blogs.technet.com/b/security

Windows Springboard Series Blog: http://blogs.windows.com/windows/b/springboard

Software Vulnerability Exploitation Trends whitepaper: http://aka.ms/exploits