WHITEPAPER

Windows 7 Support Has Ended —
Enterprise Guide to Managing and Securing Devices

February 2020

+44 (0)1452 886982

appguard@csa.limited

Windows 7 Support Has Ended —
Enterprise Guide to Managing and Securing Devices

Support for Windows 7 ended in January 2020. After January 14, 2020, Microsoft no longer provides security updates or support for PCs with Windows 7. If you continue to use Windows 7 after support has ended, your PC will still work, but it will be more vulnerable.

What Risks Must the C-Suite Know?

Some organizations suffered catastrophic breaches in spring 2017 after Windows XP's end-of-life (EOL). Now, Microsoft has ended support for Windows 7, leaving enterprises vulnerable to cyberattacks. Enterprises should break their Windows 7 vulnerabilities into three pieces: OS, driver, and application. An exploit of any one of these three vulnerabilities can lead to catastrophic breaches resulting in financial and reputational damage.

The OS and driver vulnerabilities have the most downside and are the most difficult to mitigate, but are also the least likely to be exploited. Intel started backing off video card driver patches at Windows XP's end of life and Nvidia did so within two years.

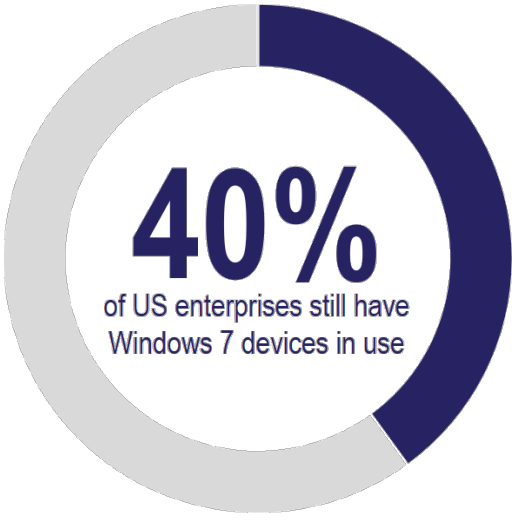
Ask your IT/Sec/Ops team:

If they are monitoring for driver and OS vulnerabilities and exploits, and whether they have capabilities to implement temporary fixes centrally (e.g., disable, host firewall policies, etc.).

This End of Life Affects Enterprises without Windows 7

An enterprise that doesn't have Windows 7 may still be affected by its supply chain, partners, and employees using Windows 7, exposing your organization to higher risks. According to a recent survey by Kollective, about 40% of US enterprises still have Windows 7 devices in use.[1] However, the study did not report the extent of their Windows 7 deployments.

Do we have a robust process to vet partners and vendors, including checking if they still use Windows 7?



1. https://kollective.com/wp-content/uploads/2019/01/6-months-until-end-of-win7_FNL.pdf

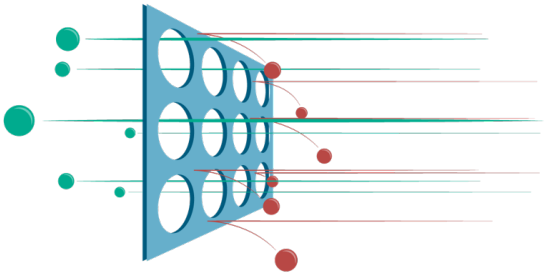
+44 (0)1452 886982
appguard@csa.limited

Most organizations allow employees to remotely access enterprise resources from employee computers via VPN or other client tools.

Have we identified high-risk endpoints in the remote access infrastructure? Each high-risk endpoint should be treated differently. For example, Windows 7 home users might require two-factor authentication and be prohibited from saving files to their PCs.

It's hard to argue against the “better safe than sorry” point. Unfortunately, there are no useful actuarial figures to make an insurance calculation. You won't find patching to the same extent as before end-of-life. Any patches will only include those Microsoft considers *severe*.

Vet your security practices for cybersecurity maturity in terms of hardening endpoints, monitoring threat intelligence, and implementing an emergency workaround



If your organization makes use of good penetration testers already, talk to them about simulating a critical vulnerability workaround exercise

Your infrastructure should enforce network zero trust concepts that can lower exposure from higher-risk partners through reduced access to resources.

TIER	WINDOWS PRO	WINDOWS E3	WINDOWS E5	WINDOWS VIRTUAL DESKTOP
Year 1	*$50*	*$25*	*Free*	*Free*
Year 2	*$100*	*$50*	*$50*	*Free*
Year 3	*$200*	*$100*	*$100*	*Free*

Other Recent End-of-Life Microsoft Products

- Server 2008 R2 and below
- Exchange 2007 and below
- Office 2007 and below
- SQL 2008 R2 and below

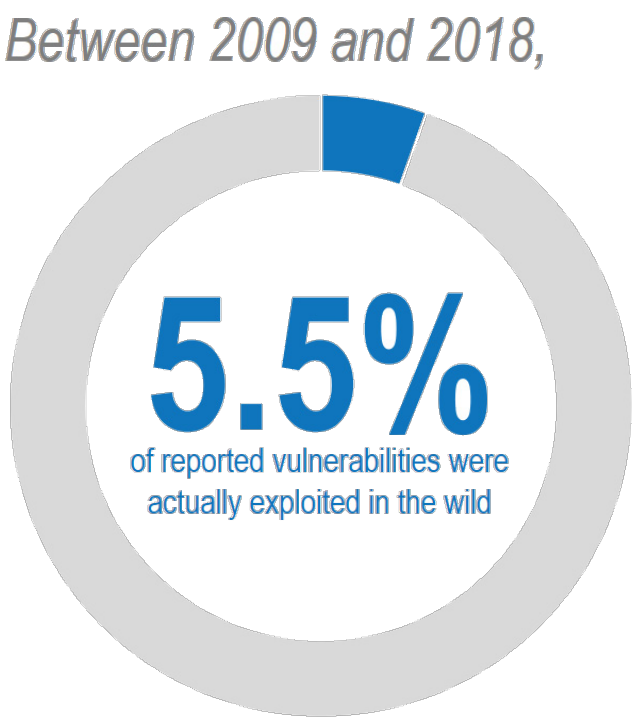
+44 (0)1452 886982
appguard@csa.limited

Patching Apps Becomes More Urgent, If Patches Even Exist

Vendors stop supporting their applications on EOL operating systems. Mozilla Firefox was vague about supporting Windows 7 and Google has committed to support for only 18 months.

Are we tracking patch support for your Windows 7 apps?

Vendors should focus on apps with a history of exploits. Only about 5.5% of reported vulnerabilities between 2009 and 2018 were actually exploited in the wild. They need an excellent threat intelligence service to get this information. And that service will need to stay on its toes because unsupported applications on Windows 7 will attract interest from your adversaries.



Mitigating Vulnerable Applications When Patches Don't Exist or Are Not Implemented

If, like many, your organization struggles to swiftly implement patches, there are other mitigations to those risks. Market analysts who have never worked in IT/Sec-Ops recommend virtual patching. In theory, virtual patches prevent the exploitation of a software vulnerability before a patch can be implemented. The fine print for such tools ought to read: *"the more generic the virtual patch is to the vulnerability, the less effective; the more specific a virtual patch is, the more high-skilled work is required to create, test, and implement it."* The same can be said of anti-exploit features in many endpoint protection agents.

The better approach doesn't try to prevent the application exploit but instead contains the application so no harm can be done if an exploit occurs. When you evaluate such tools, look carefully at how well they handle application updates, patches, and plug-ins. You'll find such life cycle operations make some tools onerous.

What are our plans for mitigating risks from unpatched or unpatchable applications on our Windows 7 devices?

+44 (0)1452 886982
appguard@csa.limited

"Living off the land" attacks are a current cyberattacks trend in which attackers use tools already installed on targeted computers or run simple scripts and shellcode directly in memory. These tools have also been used during lateral movement or to extrude stolen data.

Living off the Land Attacks: Are You Ready?

Instead of sneaking malicious executables onto your Windows 7 devices, your adversaries can use the utilities already running to harm you. Your team should have a plan to prevent attackers from using utilities running on endpoints.

While prohibiting utilities from launching is a step in the right direction, your IT/Sec-Ops personnel may need many of these utilities to make high privilege changes to endpoints. Ask your team:

Can we use suppressed utilities when needed?

If PowerShell were blacklisted, can their IT Asset Management tool (for example, Microsoft SCCM) use PowerShell at any moment without disabling the controls that block it? Also, does using PowerShell, in this example, mean adversaries could use PowerShell while this window is open?

Not all security controls create such a window of vulnerability when IT/Sec-Ops needs to use "controlled" utilities. Context-aware security tools deny the use of risky utilities to all but IT/Sec-Ops designated tools (like SCCM). Ask your team:

Does our cybersecurity stack harden Windows 7 endpoints yet allow IT/Sec-Ops to make changes to them at any time without exposing them to great risk?

Caution about Endpoint Protection Agents

There are at least two features common in most endpoint protection agents that might pose problems with Windows 7. First, some have ransomware roll-back. If struck, this feature restores the PC from an archive stored on it. The storage requirement may exceed available space, which might be why you haven't upgraded to Windows 10.

The second is machine-learning-based behavior analytics. Many agents rely on this feature. It looks for abnormal yet familiar patterns using a machine-learning model built using data from a large community of endpoints. Just how many Windows 7 endpoints have been in these communities? That number gets smaller every month as more enterprises migrate to Windows 10. So does the statistical significance of their observations. Ask your team:

How are we validating the promises of the vendors for Windows 7 protection?

Do public third-party tests include Windows 7?

How may test outcomes differ from Windows 7 and Windows 10 endpoints?

This statistical uncertainty issue might not impact deployments, but implementations may require additional staff to sift through false positives and negatives. Many Windows 10 deployments already do this, despite automated response options. This will lead to higher labor costs to monitor, investigate, and respond to alerts.

Invest in Two-factor Authentication

Windows 7 endpoints are more vulnerable to malware than Windows 10. Credential theft is among the most common post-compromise actions of malware. While two-factor authentications don't prevent adversaries from secretly conducting unauthorized sessions from compromised machines, it makes it very difficult to do so from other machines. And finally, two-factor authentication is portable; it will work on other endpoints.

Do increased Windows 7 risks warrant adopting two-factor authentications?

Network Isolated Windows 7 Devices: Two Considerations

The NotPetya attacks of 2017 crippled seemingly network-isolated Windows XP. The attack used Pass-the-Hash and PsExec to spread from one trusted machine to another rapidly. Well protected enterprises detected NotPetya but could not respond quickly enough. Real-time host-based protection is critical. Ask your team:

What measures are in place to block Windows credential theft in real time?

How can we block remote code execution attacks (PsExec, Remote PowerShell, etc.) in real time?

Are our lateral movement protections real-time (i.e., block) or reactionary (in other words, take action milliseconds or hours later—if the attacks are detected at all)?

Conclusion

If you already have all of this covered, add additional exercises to your next pen test to verify all checks and balances and understand how well personnel understands their roles and how they collectively respond to such attacks.

If you feel your organization is unprepared for these risks, assign someone to investigate how AppGuard can make a meaningful impact. Specifically, look at how AppGuard contains unpatched or unpatchable applications such that they cannot do harm via file, registry, memory, or privileged OS API operations when exploited.

+44 (0)1452 886982

appguard@csa.limited

APPGUARD

A Blue Planet-works Company

How AppGuard Can Help

About AppGuard

AppGuard is a PREVENTION solution, applying a zero-trust approach within the workstations and servers it protects, in real time. AppGuard takes away all applications' ability to harm the operating system.

Protecting Applications with Enforce, Block and Adapt

AppGuard's policy-based, zero-trust solution mitigates application misuse and hijacking risks by:

- *Enforcing policies, so applications do only what they are supposed to do*
- *Blocking actions that do not conform to policies*
- *Adapting in real time to application updates, patches, and other changes to avoid administrative burdens and mitigate unanticipated attack vectors.*

To learn more about AppGuard, visit
www.appguardzerotrust.co.uk

+44 (0)1452 886982
appguard@csa.limited