Microsoft Pulls Plug on Windows 7 Support—Are You a Sitting Duck?

Posted on January 25, 2020 by Skylor Phillips

The year is 2009. President Obama is inaugurated. Avatar becomes the highest-grossing film of all time. Kanye West interrupts Taylor Swift's speech at the MTV Video Music Awards. And—way down the list of exciting events that year—Microsoft releases Windows 7. While it may not have made as large a splash on the world stage, Windows 7 proved to be a popular, stable, and enduring operating system and still has an estimated 200 million users today.

Sadly, all good things must come to an end. Microsoft ended support for Windows 7 on January 14, 2020, and no longer offers technical assistance, software patches, or security updates as part of its standard product support. If your business is still running Windows 7, you may have noticed that users are now receiving full-page messages warning that the operating system is no longer supported. Yikes!

Dwindling Pool of Sitting Ducks

If you are one of the many businesses that have successfully upgraded your systems to Windows 10, please congratulate yourself on a job well done!

If you still have systems running Windows 7, be aware that you are part of a dwindling pool of sitting ducks. Cybercriminals are aware that many businesses will no longer be applying security updates and software patches to Windows 7 systems. They will likely be targeting these systems with data breach, ransomware, phishing, and other types of cyberattacks. As the pool of Windows 7 users shrinks, your likelihood of being attacked will increase.

What's Holding You Back?

The first step in mitigating Windows 7 risk may be to determine what's keeping you from upgrading.

It may simply be that this risk has not bubbled up high enough in your company's list of competing priorities. If you feel this is the case, consider doing an assessment of the potential costs and customer impacts that could result from a successful **data breach**, ransomware, or phishing attack against your Windows 7 systems. When combined with the fact that Windows 7 attacks are becoming increasingly likely, this can provide the justification needed to upgrade to Windows 10.

You may have concerns that some of your systems or applications will not be compatible with Windows 10. If this is the case, Microsoft offers services under its Desktop App Assure initiative that can help you resolve these issues.

If you have applications that absolutely will not run under Windows 10, it could be time to bite the bullet and find replacements.

Options for Deferring the Inevitable

You may know that you need to upgrade to Windows 10, but just need to buy some time. Here are several options that can help you get by until you are able to upgrade:

1. Strengthen your defenses against external attacks that could potentially compromise your Windows 7 applications. Tools such as Symantec (now Broadcom) Data Center Security (DCS) and Carbon Black Application Control provide security monitoring, malware protection, whitelisting, intrusion detection, and other capabilities to help harden your network and systems against external attacks.

2. For an interim period, Microsoft offers an extended support option that will allow you to continue receiving Windows 7 security updates for up to three years. The annual cost is roughly $50 per device in 2020 and increases to $100 in 2021 and $200 in 2022.

3. If you have Windows 7 applications that don't require internet or internal network connectivity, consider running them on PCs that are disconnected from the network entirely.

4. For applications that will not run under Windows 10, consider finding Linux alternatives.

Upgrade to Windows 10

If you don't have compatibility issues that need to be addressed, or other significant issues that would prevent you from upgrading to Windows 10, we recommend putting together a detailed upgrade deployment plan and executing it as soon as possible.

As part of your planning process, consider taking the opportunity to recycle PCs that are more than five years old and replace them with PCs that are already running Windows 10. This will minimize your software upgrade effort while leaving you with up-to-date hardware.

Businesses have the option to upgrade to Windows 10 Pro or the more expensive Enterprise (or Education) edition. While you should evaluate the costs and benefits that are specific to your company, we generally recommend the Enterprise/Education option due to the longer time between updates and more robust support services.

We Can Help

Tevora's experienced team has in-depth skills and expertise that can help you navigate your path to Windows 10. We'd welcome the chance to be your trusted partner as you take this important

step.

Posted in Uncategorized

California Consumer Privacy Act: What Co…

California Consumer Privacy Act: Assessing…

Recent Tevora Threat Posts

MuleSoft Runtime < 3.8 Unauthenticated RCE (CVE-2019-13116)

October 16, 2019

Smoke and Mirrors | Red Teaming with Physical Penetration Testing and Social Engineering

September 13, 2019

Scout

August 9, 2019

Search for: SEARCH

Recent Posts

Our Response To Covid-19

April 3, 2020

Dear Valued Clients and Colleagues, As the COVID-19 pandemic …

A Preview of the New Cybersecurity Maturity Model Certification (CMMC)

January 31, 2020

What is DFARS? Defense Federal Acquisition Regulation Supplement (DFARS) was …

Privacy Spotlight: Adoriel Bethishou Information Security Analyst and Outdoor Explorer

January 31, 2020

Adoriel Bethishou, Information Security Analyst at Tevora What has been …

Categories

Select Category

Archives

Select Month

Services

- Compliance
- Enterprise Risk Management
- Data Privacy
- Cloud & Security Solutions
- Threat Management
- Incident Response

Industries

- BioTech / Pharmaceuticals
- Energy & Utility Industries
- Entertainment
- Financial Services
- Government Entities
- Healthcare
- Manufacturing & Logistics Industries

Resources

- In the News
- Blog
- Threat Blog
- Events & Press

Who We Are

- Our Commitment
- Careers at Tevora
- Our Brand

Our Clients

TEVORA™