Introduction
Windows 7 enjoyed a good run as one of Microsoft’s more widely used and well-received operating systems (OSes), but the venerable OS passed its sunset date in January. As of Jan. 14, 2020, Microsoft no longer provides security updates or support for Windows 7.

Windows 7 was in service for years. After the initial release of Windows 7 in 2009, Windows 7 Service Pack 1 came out in 2011. Then there was a platform update released in 2013. Microsoft began preparing to sunset Windows 7 as early as 2014 when the company started to withdraw retail sales. Then in 2016, PCs with Windows 7 pre-installed were no longer available.
For any organization that has not yet migrated, now is clearly the time to upgrade to Windows 10. Continuing to use Windows 7 even now after sunset date has passed and support has expired is an option, but not an advisable one. PCs and laptops running Windows 7 will still operate, but there will be no technical support, no updates to features and functions, and no security updates. Windows 7 systems will continue to run, but at dramatically reduced capacity and greatly increased risk.

The U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) issued an alert in October of 2019 (Alert AA19-290A: Microsoft Ending Support for Windows 7 and Windows Server 2008 R2) to Microsoft Windows users regarding critical security vulnerabilities. The CISA alert reads, “On January 14, 2020, Microsoft will end extended support for their Windows 7 and Windows Server 2008 R2 operating systems. After this date, these products will no longer receive free technical support, or software and security updates.”

The CISA alert further recommends organizations should:

1. **Upgrade to a newer operating system.**
2. **Identify affected devices to determine breadth of the problem and assess risk of not upgrading.**
3. **Establish and execute a plan to systematically migrate to currently supported operating systems or employ a cloud-based service.**

Even Microsoft itself recommends moving to a new laptop or PC specifically configured to optimize Windows 10, stating on its website, “For most Windows 7 users, moving to a new device with Windows 10 will be the recommended path forward. Today’s PCs are faster, lightweight yet powerful, and more secure, with an average price that’s considerably less than that of the average PC eight years ago.”

**Make the Move to Windows 10 Pro**
Many of the updates to Windows 10, including the updates pushed out on a regular basis, represent a significant boost to efficiency
The latest security services protect sensitive data, devices, user identities, and intellectual property.

and productivity. Windows 10 Pro can help modern workers drive productivity with functions like:
— Remote Desktop, which provides access to all files, folders, and apps from virtually anywhere and any device.
— Windows Hello2, which is an enterprise-grade alternative to passwords designed for mobile devices. It uses a PIN, biometrics, or companion device as identity validation factors.

Moving to Windows 10 can also greatly improve security effectiveness, and is a driving factor in migration plans. According to a recently released report from 1E entitled, “Windows 10 2020: Beyond the Migration,” 82 percent of the responding organizations indicated security is a primary factor in deciding to migrate from Windows 7 to Windows 10.

Continuing to operate Windows 7 now that support has expired can expose networks and individual systems to greater risk of security breaches. The older OS no longer receives security updates and patches, essentially leaving the door open for infiltrators.

Besides being a current, actively supported, continuously updated OS, Windows 10 Pro also brings to bear several additional security functions, including high-quality management tools to help organizations stay up-to-date with the latest security services to protect sensitive data, devices, user identities, and intellectual property. Those tools include:
— The Windows Defender series, including Smart Screen, Application Guard, Device Guard, Exploit Guard, and Credential Guard.
— Bitlocker3, an enterprise-grade solution that protects sensitive information and ensures regulatory compliance, even when devices are lost or stolen.
— User account control, which protects against malware.

Windows Defender gives you control over virus protection, account protection, firewalls, app control, and device security.
Security is clearly the primary threat, but not the only one. Using an unsupported OS like Windows 7 will increase the likelihood of malware attacks and other cybersecurity threats, as there are no more current updates or security patches. Systems rapidly become hobbled by unpatched vulnerabilities and software bugs, and are subject to data breaches, loss of data integrity, reduced data availability, and a general reduction of productivity.

**Carefully Configured for Optimal Operations**

Enterprise organizations that opt for the simplified migration route of moving to pre-configured Acer desktop and laptop systems are selecting the most cost-efficient and operationally efficient model. Acer ensures organizations are working with high productivity solutions designed for SMB organizations with improved security features and enhanced controls to ensure optimization of organizational resources.

Moving to Windows 10 and opting for upgrading to Acer mobile and desktop systems pre-loaded and pre-configured with Windows 10 conveys a variety of benefits, including:

- **simplified migration path**
- **improved productivity**
- **significantly improved security posture**

Acer’s systems—like the TravelMate P6—have Windows 10 Pro pre-installed. Combined with Acer’s extended battery life and vastly improved Wi-Fi performance, systems like the TravelMate P6 are uniquely suited for today’s mobile Enterprise environments.

**Systems like the TravelMate P6 are uniquely suited for today’s mobile Enterprise environments.**
Other Acer systems pre-configured with Windows 10 Pro include:
— TravelMate series: P6, P4, X5, and X3
— Veriton M and Veriton Z desktop systems
— Veriton X and Veriton N mini-PCs

Acer’s full range of systems are pre-loaded with Windows 10 to ensure immediate productivity.

**Now is the Time**
Not moving to Windows 10 is not an attractive option. Among the many migration paths available to organizations, adopting preloaded and preconfigured Acer mobile and desktop systems stands as the most efficient and cost-effective option. So, now that the end date of Jan. 14, 2020 has come and gone, organizations should make their migration and upgrade plans right away.

To learn more about Acer systems configured with Windows 10, please visit: acer.com/ac/en/US/content/windows-10-pro.