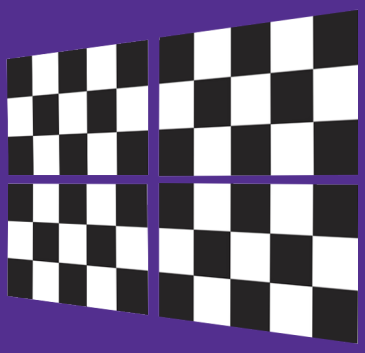

The Critical Shift: Navigating the End of Windows 10

LeapFrog®

The Critical Shift: Navigating the End of Windows 10

As the end of life (EOL) for Windows 10 rapidly approaches in October 2025, businesses must face critical decisions regarding their IT infrastructure. As the most popular operating system among businesses, with a global market share that has floated around 30% the past year, this transition will have significant financial implications. Companies will need to upgrade not only their software but potentially their hardware as well, impacting budgets worldwide.

What does this mean for me?

While Windows 10 will continue to function after the EOL date, there will be several negatives to continuing usage:

- No longer receive security updates, increasing your vulnerability to cyber attacks
- No longer receive bug fixes
- No more technical support
- Newer applications (apps) and software may not be compatible
- Slower and overall poor system performance, decreasing productivity

Some of these negatives might appear as minor inconveniences, but continuing to use Windows 10 can cost catastrophic amounts of revenue and reputational damages if your company experiences a breach, hack, or ransomware attack. As Emmett (Trey) Hawkins, CTO of Leapfrog Services, states, **"The largest attack surface for any business is its computers."**

What are the benefits of upgrading to Windows 11?

Windows 11 brings several important improvements over Windows 10, making it more secure, faster, and easier to use. It has stronger security features, like built-in protections against malware and ransomware, along with better hardware-based security. Performance is also improved with faster start-up times, better use of system resources, and longer battery life for laptops. Additionally, it supports Android apps, expanding its functionality. With future updates focused on Windows 11, it's a more future-ready option than Windows 10.

So, what's the dilemma?

Microsoft requires essential hardware and specific computer processors to run Windows 11. For reliable Windows 11 operation, computers need a multi-core processor, an 8th-gen Core CPU or above, 4GB of RAM, and a TPM 2.0 chip — Microsoft lists the hardware requirements.

What are my options?

With the EOL for Windows 10 approaching next year, IT leaders need to take action. Upgrading to Windows 11 isn't just about new features; it's about securing your organization and staying ahead of potential risks. Organizations can pursue a range of responses below to avoid business disruption:

Option 1 – Slowly integrate New Hardware with Windows 11 into an infrastructure with Older Hardware and Windows 10

- Running two different operating systems in a single environment is a challenge for your IT team. Successfully managing components that don't run universally takes more time and effort. It's also riskier for your IT environment when some computers are less secure than others.

Option 2 – Switch to a Virtual Desktop Infrastructure (VDI)

- If it's impractical to replace older computers, a good option to consider is switching to a Virtual Desktop Infrastructure, or VDI, as part of your digital transformation. VDI, also referred to as Desktop as a Service, is a centralized, super-secure, and high-performing platform with the latest technology that allows users to access a company's servers, files, apps, and services from any device. Microsoft's Modern Desktop platform includes the benefits of cloud-based management, improved security, and streamlined user experiences.

Option 3 – Replace all outdated equipment and upgrade to Windows 11

- In addition to being able to run all the Windows 11 security features while keeping workers productive, newer devices can run the latest, most effective security tools, especially Endpoint Detection and Response (EDR). Leapfrog considers EDR a must-have tool to meet updated industry standards and cyber insurance requirements.

Incorporating these necessary upgrades into your 2025 budget

Waiting until the last minute to migrate from Windows 10 could lead to rushed decisions, missed budgets, and technical debt. Planning now can help mitigate risks and ensure a seamless transition. As a best practice, IT leaders should start working with their business partners to establish a clear plan for upgrading or replacing systems.

Finding the right balance between security and productivity is a puzzle as old as the PC. In this case, keeping older computers and/or older software can cost you both.

Unfortunately, it can be a paradigm shift to consider buying all new computers for your IT environment in a single year.

"Most organizations follow the traditional three-year or five-year lifecycle planning model, which replaces a percentage of the organization's computers each year — it makes sense when the priority is managing cash flow. But the traditional model is no longer ideal because it may not be enough to keep companies secure," says CTO Trey Hawkins.

The new lifecycle model moves from time-based lifecycle planning to security-based lifecycle planning. Today, the priority is to replace computers based on their ability to keep companies secure rather than their age.

As the EOL for Windows 10 draws near, the decision to upgrade to Windows 11 becomes increasingly critical. The risks associated with continuing to use an unsupported OS are substantial, from security vulnerabilities to decreased productivity. By understanding the benefits of Windows 11 and carefully considering the available options, IT leaders can make informed decisions that balance security, productivity, and financial considerations. Planning and proactive upgrades will ensure a smooth transition and safeguard your organization against future threats.

Leapfrog offers outsourced managed IT and cybersecurity services that fit easily into your business model. With over 25 years of MSP, MSSP, and CyberRisk Management experience, we help a broad array of companies simplify their IT operations while improving their security and resiliency. Our services are scalable, aligned, and built on a proven methodology, and our culture (we call it "Frogma") is built on Integrity, Service, and People so you get personalized, best-in-class support.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to take your IT and cybersecurity services to the next level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329