



The Ultimate Guide to **Navigating Windows 10 End-of-Life**



Introduction

Windows 10 has been a staple in businesses worldwide, but its time is coming to an end. On **October 15, 2025**, Microsoft will officially discontinue support, leaving organizations with critical decisions to make. Without security updates and support, companies risk compliance issues, cybersecurity threats, and operational disruptions.

This guide will help you understand your options and take the right steps to ensure a smooth transition.

CHAPTER 1:

What Windows 10 End-of-Life Means for Your Business

Microsoft's decision to end support for Windows 10 means businesses can no longer rely on security patches, bug fixes, or technical assistance. This presents significant risks, including:

- **Increased Security Vulnerabilities:** Without updates, businesses become prime targets for cyberattacks, malware, and ransomware.
- **Compliance & Regulatory Risks:** Many industries require supported, secure software to meet legal and regulatory standards.
- **Software & Hardware Incompatibility:** New applications and peripherals may no longer work with Windows 10, leading to potential productivity loss.

Organizations must assess their risk exposure and develop a proactive plan to avoid disruptions.



CHAPTER 2:

Your Options for Moving Forward

Many companies will need to choose between these three paths:

1. **Upgrading to Windows 11** – The most straightforward approach if your hardware supports it.
2. **Paying for Extended Security Updates (ESU)** – A temporary fix for those unable to upgrade immediately.
3. **Adopting Desktop as a Service (DaaS)** – A long-term cloud-based alternative that eliminates the need for hardware refreshes.

Each option has cost, security, and operational implications, and organizations should carefully weigh their choices.



CHAPTER 3:

Windows 11 Upgrade Considerations

Windows 11 introduces new security and performance enhancements but comes with **strict hardware requirements**.

What Microsoft Says You Need vs. What You Actually Need

	Microsoft's Official Minimum Requirements	Real-World Minimums for Viable Performance
Processor	1+ GHz with 2 or more cores on a compatible 64-bit processor or SoC (<u>full list of approved CPUs</u>)	2+ cores at 1+ GHz (approved CPUs)
RAM	4 GB minimum	8 GB minimum
Storage	64 GB minimum	100 GB recommended
TPM	TPM version 2.0 (<u>Enable TPM 2.0 guide</u>)	TPM 2.0

In most modern business environments, the bare minimum specs won't cut it. While Microsoft's requirements may technically allow an upgrade, the day-to-day performance may not be adequate—especially with modern workloads and multiple apps running concurrently.

DaaS and Virtualization Requirements

When moving to DaaS or a virtual desktop infrastructure (VDI), the numbers shift slightly:

For Virtualized Desktops:

- **vCPU:** Minimum 2 vCPU (4 vCPU preferred for power users)
- **RAM:** 8 GB minimum (16 GB for heavier applications)
- **Storage:** 85 GB to 125 GB depending on applications, data, and performance tuning

Note: These numbers apply to persistent virtual desktops. For **session-based DaaS**, which often runs Windows Server OS skinned to resemble Windows 10/11, hardware demands can differ significantly and are shared across users.

To determine upgrade eligibility:

- Use **Microsoft's PC Health Check tool**.
- Check your **existing hardware lifecycle**.
- Identify systems that require **replacements or upgrades**.

If a majority of your devices are not upgrade-eligible, alternative solutions such as DaaS should be explored.



CHAPTER 4:

The True Cost of Extended Security Updates (ESU)

Microsoft's **Extended Security Updates (ESU)** provide a temporary solution for businesses unable to upgrade. However, this comes at a price:

- **Cost Estimates:**
 - **\$30-\$65 per device per year**, depending on licensing agreements.
 - Prices may increase in subsequent years.
- **Limited Availability:**
 - ESU is only confirmed for **one year**.
 - No guarantee of continued support beyond 2026.

While ESU provides a short-term security net, businesses should not rely on it as a long-term solution.

CHAPTER 5:

The Case for Desktop as a Service (DaaS)

Desktop as a Service (DaaS) provides a flexible alternative to upgrading hardware. With DaaS, users access a **cloud-hosted Windows 11 environment** from any device, reducing IT complexity and costs.

Key Benefits:

- **No Hardware Upgrades Required** – Extend the life of existing devices.
- **Built-in Security & Compliance** – Continuous updates and threat protection.
- **Scalability & Flexibility** – Supports remote and hybrid workforces.
- **Lower Total Cost of Ownership (TCO)** – Reduces IT overhead and capital expenses.
- **Sustainability Advantages** – DaaS supports sustainability by extending device lifespan, allowing businesses to repurpose older devices while still providing employees with a modern desktop experience. This helps reduce **e-waste** and minimizes the need for frequent hardware refreshes.
- **Energy Efficiency** – By reducing reliance on physical servers and on-premises infrastructure, DaaS lowers both **energy consumption** and **hardware demands**.
- **Remote Work & Carbon Reduction** – Many DaaS solutions, including UCaaS and CCaaS, enable **remote work**, decreasing the need for commuting and reducing **carbon emissions**.

Organizations looking for a future-proof IT strategy should strongly consider adopting DaaS.





CHAPTER 6:

Preparing Your Business for the Transition

A successful transition from Windows 10 requires a well-structured plan. Businesses should:

1. **Conduct an IT Asset Audit** – Identify Windows 10 devices, their specifications, and their upgrade eligibility.
2. **Develop a Migration Plan** – Decide on a phased or full migration strategy.
3. **Test Software & Hardware Compatibility** – Ensure critical applications work on Windows 11 or DaaS environments.
4. **Train Employees** – Provide guidance on new OS features and any workflow changes.
5. **Monitor & Optimize** – Continuously assess performance and security post-migration.

Proper planning will ensure minimal disruptions and a seamless transition.

CHAPTER 7:

FAQs and Common Objections

Businesses often have questions about Windows 10 end-of-life. Here are some of the most common concerns:

- **Can I keep running Windows 10 past October 2025?**
 - Technically, yes, but it will be **highly risky** due to lack of security updates.
- **What if my business software isn't compatible with Windows 11?**
 - Work with vendors to secure updates or explore virtualization solutions like DaaS.
- **How do I justify the investment in DaaS to leadership?**
 - Highlight **cost savings, security improvements, sustainability benefits,** and **future scalability** as key business advantages.

CONCLUSION:

Take Action Now

Waiting until the last minute to plan for Windows 10 end-of-life can be costly and risky. Whether you choose to upgrade, extend support, or move to DaaS, having a strategy in place is crucial.

Ready to start your transition?

Contact us for a free assessment and consultation today!



**Schedule a
Consultation**

