

With Windows 10 officially reaching end of life on **October 14, 2025**, time is ticking to ensure your business systems are upgraded and secure. This guide will walk you through everything you need to do to prepare for the transition.

STEP 1: UNDERSTAND WHY UPGRADING IS CRITICAL

- **No Updates:** Windows 10 will no longer receive security updates, leaving systems vulnerable to cyber threats.
- **Compliance Risks:** Many industries require up-to-date systems to meet regulatory requirements.
- **Software Incompatibility:** New applications and hardware may not support older operating systems.

STEP 2: SET A CLEAR PLAN AND TIMELINE

January - February 2025:

- Assess Your Current Environment
 - Inventory all devices running Windows 10.
 - Identify legacy systems or applications requiring special attention.
 - Use tools like Microsoft Assessment and Planning Toolkit or Endpoint Manager, or reach out to your [managed service provider](#).

March - April 2025:

- Evaluate Replace Options
 - **Windows 11:** The logical upgrade for most businesses. Ensure your devices meet minimum system requirements (e.g., TPM 2.0, Secure Boot, and processor compatibility).
 - **Cloud PC or Virtual Desktops:** For businesses shifting to flexible, remote-first models.
 - Linux or Alternative OS: Consider if your workflows don't rely heavily on Windows-exclusive software.

May - June 2025:

- Budget and Procurement
 - Secure budget approval for hardware or software upgrades.
 - Order replacement devices early to avoid supply chain delays.

July - August 2025:

- Test, Pilot, and Train
 - Test upgrades with a small group of users.
 - Address any issues with applications, drivers, or workflows.
 - Train staff on any new features of Windows 11 or replacement OS.

September - October 2025:

- Deploy and Complete
 - Roll out the upgrade organization-wide.
 - Decommission or repurpose old devices securely.

STEP 3: ENSURE HARDWARE COMPATABILITY

- **Hardware Compatibility:** Run the PC Health Check tool to verify if devices can run Windows 11.
- **Software Compatibility:** Ensure all applications and services are supported on the new OS. Contact vendors if needed.
- **Custom Solutions:** Migrate or replace outdated applications that rely on Windows 10 features.

STEP 4: ADDRESS LEGACY SYSTEMS

- If you have systems that can't be upgraded by the deadline:
 - Use virtual machines to run legacy applications temporarily.
 - Isolate unsupported systems from your network to reduce security risks.
 - Develop a long-term replacement plan for critical legacy workflows.

STEP 5: SECURITY AND COMPLIANCE

- Update endpoint protection tools to support Windows 11.
- Review and enhance your cybersecurity policies to align with the new OS.
- Schedule ongoing [patch management](#) for the new environment.

STEP 6: COMMUNICATE WITH STAKEHOLDERS

- Inform your team and clients about the upgrade timeline.
- Share expectations and training resources to reduce resistance.

STEP 7: UTILIZE MICROSOFT TOOLS

- **Microsoft Endpoint Manager:** Streamline deployments across your organization.
- **Windows Autopilot:** Simplify new device setup and configuration.
- **Microsoft 365 Blueprints:** For businesses with Microsoft 365 licenses, [blueprints](#) can fast track your migration with prebuilt templates/policies.

STEP 8: KEEP A CONTINGENCY PLAN

- Maintain backups for critical systems before any upgrade.
- Allocate time for troubleshooting during and after deployment.
- Have an emergency rollback strategy for unforeseen issues.

STEP 9: DON'T WAIT AND SEEK PROFESSIONAL HELP IF NEEDED

- If your team lacks the bandwidth or expertise, consider partnering with an IT service provider like [Next Perimeter](#) to handle the upgrade seamlessly.
- With only 10 months remaining, starting now will ensure a smooth, cost-effective transition without scrambling to meet the deadline.

WINDOWS 10 EOL COUNTDOWN - YOUR MONTHLY CHECKLIST

January:

- Inventory devices and applications
- Identify legacy dependencies

February:

- Finalize replacement OS
- Evaluate hardware requirements

March:

- Secure budget
- Approve upgrade plans

April:

- Begin procurement of hardware and software

May:

- Configure testing environment for pilot group

June:

- Address compatibility issues
- Train IT staff on deployment strategies

July:

- Pilot deployment to the test group
- Collect feedback

August:

- Begin organization-wide deployment
- Monitor for issues

September:

- Complete deployment
- Securely decommission Windows 10 systems

October:

- Complete deployment
- Verify all devices are running the new OS before Windows 10 end of life

We're Here to Help



Phone

888-286-4816

Email

sales@nextperimeter.com

Website

NextPerimeter.com



About Us

Next Perimeter simplifies IT and security for growing businesses by eliminating complexity, boosting productivity, and ensuring seamless, secure experiences.

We streamline onboarding to get new hires up and running on day one, replace outdated systems with cloud-first, zero-trust solutions, and deliver unified IT and security services that protect your business while enabling smarter work.