Windows 10 end of life

With Microsoft® ending support for Windows® 10 on Oct. 14, 2025, businesses face critical decisions. This FAQ answers common questions about security risks, compliance, insurance implications, and how OpenText™ Core Endpoint Backup can help protect data when devices can't be upgraded in time.

1. Why do we need to upgrade from Windows 10 to Windows 11?

Microsoft ends support for Windows 10 on Oct. 14, 2025. After this date, devices running Windows 10 will no longer receive security updates, bug fixes, or technical support. This exposes the company to cybersecurity risks and compliance issues.

2. What are the risks of staying on Windows 10?

- Security vulnerabilities: No patches or updates means increased exposure to malware, ransomware, and data breaches.
- Compliance issues: Many regulatory frameworks (e.g., ISO, GDPR) require up-to-date and supported software.
- Software incompatibility: New applications and updates may not support Windows 10, leading to productivity loss.
- Vendor support: Third-party vendors may stop supporting Windows 10, affecting critical business tools.

3. What are the benefits of Windows 11?

- Enhanced security: Built-in hardware-based security features like TPM 2.0 and Secure Boot.
- Improved performance: Faster boot times, better memory management, and optimized for hybrid work.
- Better integration: Seamless compatibility with Microsoft 365®, Teams, and cloud services.
- AI readiness: Windows 11 is optimized for AI-powered tools and workflows.

4. Can we upgrade existing machines or do we need to replace them?

It depends on the hardware:

- Devices that are eligible for upgrade include machines with:
  - TPM 2.0
  - Secure Boot capability
  - UEFI
- Ineligible devices: Older machines that must be replaced to meet Windows 11 requirements.

A full audit should be conducted to identify which machines qualify for upgrade and which need replacement.

5. Will my cyber insurance company deny my claim if do not upgrade to Windows 11 by Oct. 14, 2025?

Yes, your cyber insurance company **could deny your claim** if you **fail to upgrade to Windows 11 by Oct. 14, 2025**, especially if you're still using Windows 10 or older systems after that date.

Here's why:

1. Windows 10 support ends Oct. 14, 2025

Microsoft will officially stop providing security updates and support for Windows 10 on that date. Running unsupported software is considered a cybersecurity liability

2. Cyber insurance policies are getting stricter

In 2025, insurers are increasingly denying claims if businesses:

- Use outdated or unsupported software.
- Lack multi-factor authentication (MFA).
- Don't regularly patch vulnerabilities.
- Fail to document cybersecurity training or incident response plans.

3.Insurance Implications

Failing to upgrade to Windows 11 could be seen as **negligence**, which may:

- **Void your cyber insurance coverage**
- **Lead to claim denials**
- **Increase your premiums**

What you should do

- **Upgrade to Windows 11 before Oct. 14, 2025**
- **Document the upgrade process** as part of your cybersecurity compliance
- **Review your cyber insurance policy** to confirm what's required
- **Consult your insurer or IT provider** to ensure you're meeting all obligations

Would you like help reviewing your current system setup or preparing a checklist to stay compliant?

Contact us >

Copyright © 2025 Open Text • 08.25 | 288-000019-001

opentext™