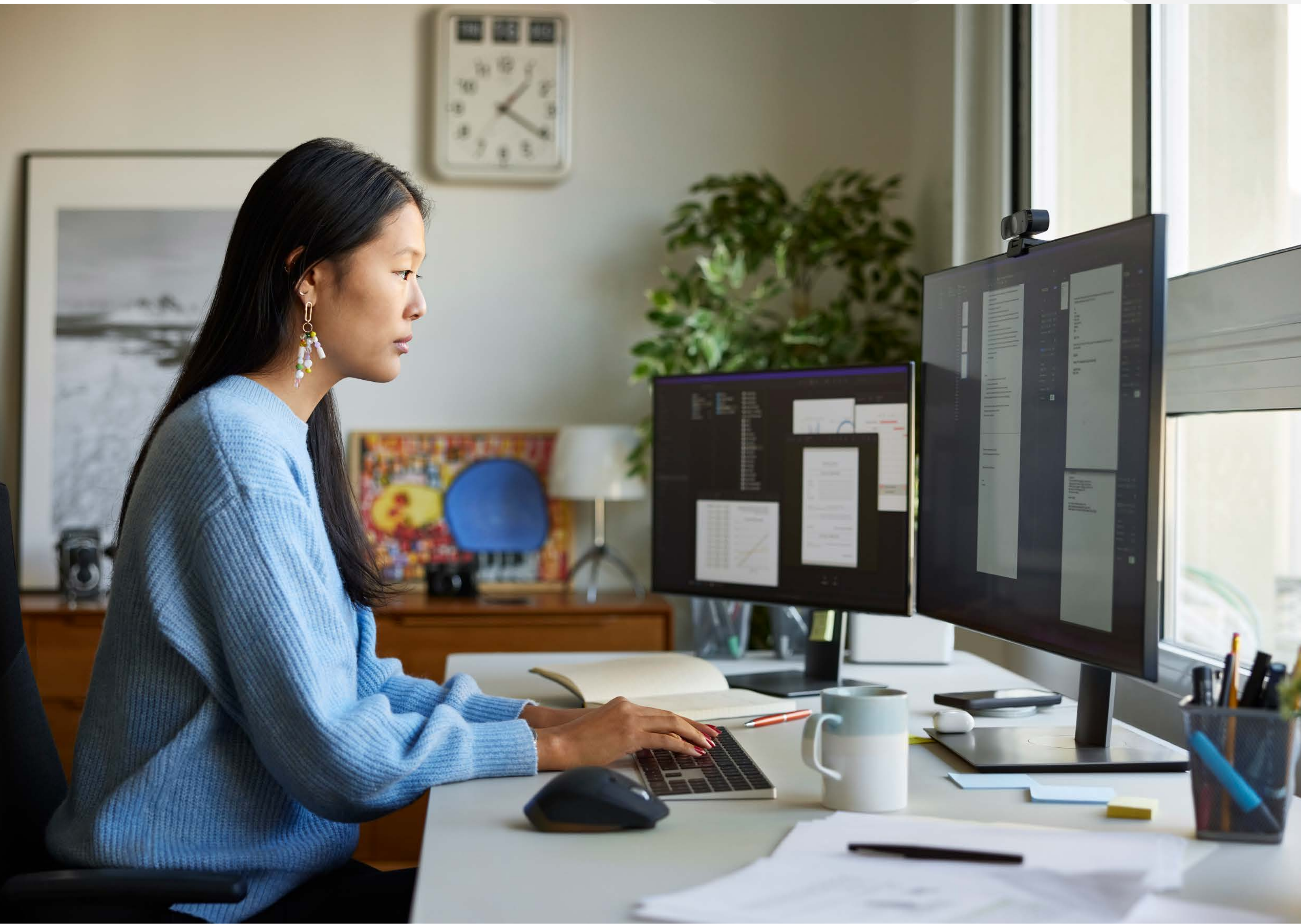
opentext™

GUIDE

What to do before Windows 10 support ends: A practical step-by-step guide

Support for Windows 10 ends October 2025.
Learn how you can stay secure, compliant, and ready with help from OpenText Core Endpoint Backup.



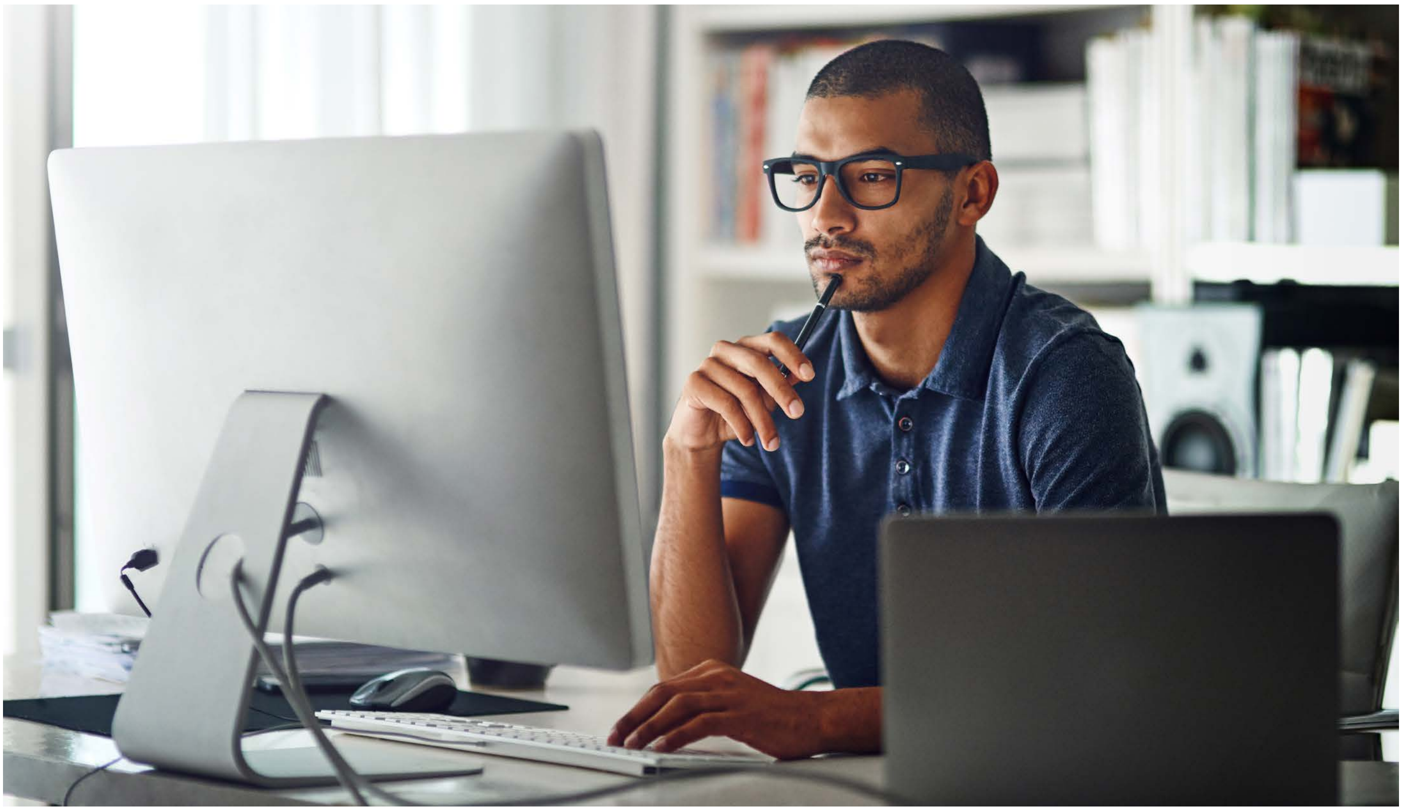
Windows 10 reaches its end-of-support on Oct. 14, 2025. After this date, Microsoft will no longer deliver security updates or patches, leaving millions of devices vulnerable to new threats.

For managed service providers (MSPs), resellers, distributors, and SMBs, this isn’t just a technical milestone. It’s a business-critical moment. Unsupported systems can put customer data at risk, break compliance requirements (including Cyber Essentials in the UK), and jeopardize cyber insurance coverage.

Insurers increasingly demand evidence of secure, up-to-date systems and robust data protection plans. Without a clear strategy for Windows 10 EOL, businesses could face higher premiums, denied claims, or even lose coverage altogether.

But it’s not all bad news. This moment also represents an opportunity to modernize IT security, improve data protection, and strengthen trust with customers. For channel partners, it’s a chance to offer real value by helping clients stay secure and compliant, with minimal burden on internal resources.

This guide will walk you step by step through what you need to do before Windows 10 support ends—from device assessment to upgrade planning and, crucially, ensuring reliable endpoint backup. You’ll also learn how OpenText™ Core Endpoint Backup offers an easy, low-touch, cost-effective solution that keeps your data secure, compliant, and insurance-ready, even on aging or remote devices.



Here’s what you need to do.

System upgrade

- Upgrade all systems to Windows 11 before Oct. 14, 2025
- Decommission or isolate any devices that cannot be upgraded
- Document the upgrade process (dates, devices, responsible personnel)

Security controls

- Enable multi-factor authentication (MFA) for all critical systems and accounts
- Use endpoint detection and response (EDR) tools
- Ensure firewalls and antivirus are active and updated
- Apply security patches regularly (automated if possible)

User and access management

- Implement least privilege access for all users
- Review and remove inactive or unnecessary accounts
- Conduct regular password audits and enforce strong password policies

Documentation and policies

- Maintain an incident response plan (IRP)
- Keep a cybersecurity policy updated and accessible
- Document employee cybersecurity training sessions

Testing and monitoring

- Perform regular vulnerability scans
- Conduct penetration testing at least annually
- Monitor logs and alerts for suspicious activity

Insurance-specific actions

- Review your cyber insurance policy for specific tech requirements
- Confirm your coverage includes ransomware, data breaches, and business interruption
- Keep a record of all compliance efforts in case of a claim

Why Choose OpenText Core Endpoint Backup?

Preparing for Windows 10 end-of-life isn't just about upgrading hardware or OS licenses. It's about protecting your data, maintaining compliance, and keeping cyber insurance valid.

OpenText Core Endpoint Backup makes that easy. It's designed for MSPs, resellers, and SMBs who need a low-touch, affordable, and powerful way to secure endpoints, even aging devices.

With cloud-based backup, simple deployment, and strong encryption, you can protect critical data, reduce risk, and deliver true peace of mind to your customers.

Don't wait until October 2025 to act. Transition smoothly and stay protected now.

Learn more about OpenText Core Endpoint Backup and start protecting your customers today.