

Still Using Windows 10?

Business risks, practical options, and a safer path forward



The short version: Windows 10 standard support ended October 14, 2025. Without an appropriate Extended Security Updates (ESU) plan, the operating system no longer receives standard security updates from Microsoft.



Why continued use creates business risk

- **Security exposure:** Newly discovered Windows vulnerabilities may remain unpatched.
- **Insurance and compliance:** Unsupported systems may complicate audits, coverage requirements, or the defense of a claim.
- **Compatibility and cost:** Vendor support will decline while troubleshooting, workarounds, and incident response become less predictable.

Your options

Option	Best fit	Important limitation
Upgrade to Windows 11	Compatible PCs in good condition	Confirm hardware and application compatibility first.
Replace the device	Older or incompatible hardware	Requires budget, setup, and a planned user transition.
Use commercial ESU	A short transition window	Security updates only; not full support or a permanent solution.
Isolate or retire	Legacy systems or unnecessary devices	Isolation reduces exposure but does not make the device supported.

Your Windows 10 Action Checklist

- ✓ Inventory every Windows 10 device and check Windows 11 and application compatibility.
- ✓ Prioritize high-risk systems, then set an upgrade or replacement date.
- ✓ Use ESU only as a documented, time-limited bridge and ask your IT provider to validate completion.

WANT TO LEARN MORE?

Not ready to talk? Visit calpcc.com for practical IT and cybersecurity articles, guides, and resources.

READY FOR HELP?

Call (415) 897-0078 to talk through the right next step for your business.