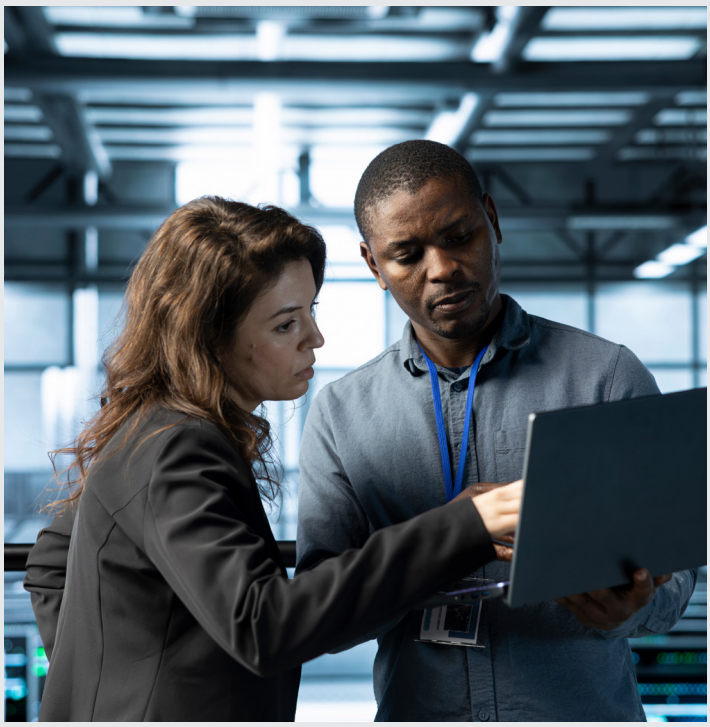
sonet.io

White Paper

Windows 10 End-of-Life: A Strategic Guide for IT Leaders Who Can't Migrate (Yet)

Windows 10 will reach end-of-support on October 14, 2025. While Microsoft offers paths forward: migrating to Windows 11 or paying for Extended Security Updates (ESUs). Both options present significant cost, complexity, and operational burden. For organizations still dependent on legacy Windows 10 apps or running large fleets of non-Windows 11-compliant devices, these paths don't solve the core issue: how to maintain secure, compliant, and uninterrupted access to business-critical systems.



This paper explores a third option: modernizing how applications are delivered altogether. Sonet.io provides a browser-based delivery platform that allows enterprises to keep running Windows 10 apps securely, without rewriting software or replacing hardware. It eliminates the cost, risk, and time of traditional migration strategies while future-proofing the business for whatever comes next.

The Scope of the Problem

As of April 2025, over 50% of desktop Windows devices globally still run Windows 10 [source: StatCounter]. That means hundreds of millions of endpoints will face a critical deadline this fall.

Microsoft's official guidance is clear: upgrade to Windows 11 or pay for ESUs to continue receiving security updates. But both choices carry a high price. ESUs cost $61 per device in year one, then

double in cost each subsequent year [source: Microsoft]. Meanwhile, upgrading to Windows 11 often requires replacing devices outright, an investment of $800-$1,500 per endpoint.

For many enterprises, especially those with custom-built or tightly integrated Windows 10 apps, neither option is viable. Mission-critical applications may require significant rewrites to run on Windows 11. Budgetary timelines don't align with a massive hardware refresh. And many IT teams are already stretched thin managing security, compliance, and user support.

The Hidden Risk of Doing Nothing

While expensive, the cost of inaction is even higher.

Running unsupported operating systems opens the door to serious security vulnerabilities. Without regular patches and updates, Windows 10 becomes a soft target for ransomware, zero-day exploits, and lateral attacks. According to IBM, the average cost of a data breach in 2024 was $4.88 million [source: IBM Cost of a Data Breach Report].

For regulated industries like healthcare, finance, government, the implications are even more severe. Failing to maintain a secure IT environment can lead to regulatory penalties, increased insurance premiums, and lost customer trust. Even if nothing happens immediately, the moment an audit occurs or a breach is discovered, the lack of proactive planning becomes a liability.

Why Traditional Solutions Aren't Built for This Moment

Extended Security Updates (ESUs) were designed to buy time, not to be a long-term strategy. They don't help with app compatibility, they don't modernize your stack, and their costs increase year over year. At scale, this becomes unsustainable. And this is only an option for 3 years.

Migrating to Windows 11 sounds straightforward until you factor in hardware incompatibilities and legacy applications. Many older devices don't meet Windows 11's TPM 2.0 and Secure Boot requirements. Replacing those devices early can divert millions from innovation budgets.

Rewriting Applications is rarely fast or cheap. Refactoring complex systems to support Windows 11 while maintaining integrations, workflows, and performance can take months or years. For most IT leaders, the risk, cost, and distraction aren't justifiable.

A Third Option: Modern App Delivery via Sonet.io

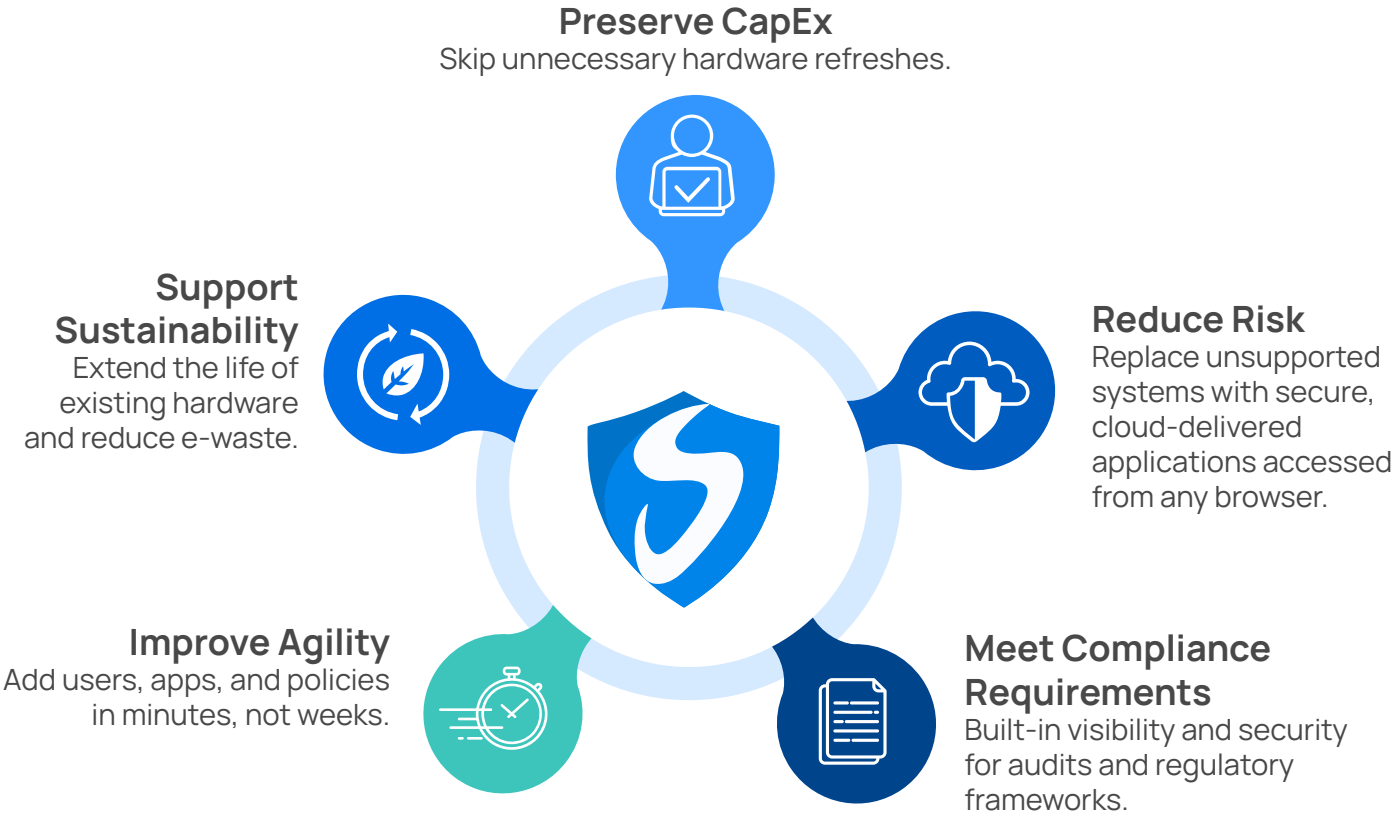
Sonet.io offers a strategic alternative: keep your existing apps and devices, and deliver them securely through the browser.

Instead of rewriting software or replacing hardware, Sonet.io enables organizations to provide zero-trust, browser-based access to any application, Windows 10 or Windows 11, web or legacy, cloud or on-prem. No VPNs, no endpoint agents, no proxies, and no infrastructure to manage.

Security is built in, not bolted on: every session is protected with granular access controls, session recording, and DLP. Applications are isolated from the device, and corporate data never touches the endpoint. Compliance becomes easier, not harder.

Business Impact

The benefits of this approach go far beyond avoiding a migration project:



Next Steps

If you're managing a fleet of Windows 10 systems or running business-critical legacy apps, now is the time to explore a different approach.

Start with a pilot. Identify your most important use cases. Validate performance and security in your environment. Sonet.io can be deployed in under an hour and works alongside your existing systems.

Don't wait until the deadline forces a rushed migration or an unpatched system becomes your weakest link.

Schedule a Demo

Contact Us :
sales@sonet.io.

Download the Solution Brief

sonet.io

Work Securely From Any Device

sales@sonet.io

Find us online at **sonet.io**

3031 Tisch Way, 110 Plaza West
San Jose, CA 95128