

Windows End-of-Life

Internal System Audit Report

Your business depends on secure and compliant IT systems. This audit reveals what's at risk, what needs immediate attention, and how to protect your company before Windows EOL creates costly disruptions.

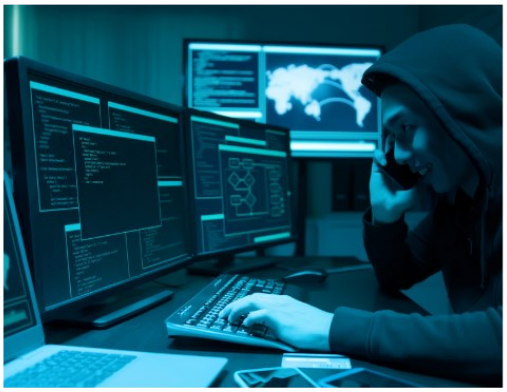
Introduction



Windows end-of-life means no security updates, patches, or support from Microsoft. Operating on outdated systems creates serious security, compliance, and operational risks. This audit is designed to assess the full impact on your business—spoiler: it's bigger than you think.







Executive Summary

Your Systems Are at Risk – Here's What You Need to Know



Windows Versions in Use

[List OS Versions]



Number of Affected Systems

[Number]



Urgency Level:

Extreme—You should have started this process yesterday.



Key Risks Identified:

[Summary of major risks]



Recommended Actions

[High-level recommendations]



Deadline for Upgrade

October [Year] (or sooner if you care about security).

Complete System Inventory & Status

Device Name	OS Version	End-of-Life Status	Risk Level	Upgrade Recommendation
[Device 1]	[OS]	[EOL/Supported]	[Severe]	[Critical Upgrade Needed]
[Device 2]	[OS]	[EOL/Supported]	[Severe]	[Critical Upgrade Needed]
[Device 3]	[OS]	[EOL]	[Critical]	[Severe]
[Device 4]	[OS]	[EOL]	[Critical]	[Critical]

Security & Compliance Nightmare

What's at Risk?



Cyberattacks

Running EOL systems is basically inviting hackers in.



Regulatory Fines & Lawsuits

Non-compliance with HIPAA, PCI, GDPR, and others can cost millions.



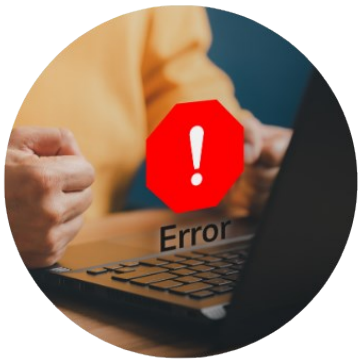
Data Breaches

Sensitive company and client information is now an easy target.



Downtime & Lost Revenue

Unpatched vulnerabilities lead to system failures and lost productivity.



Software & Hardware Incompatibility

Legacy applications will eventually stop working, causing unexpected disruptions.

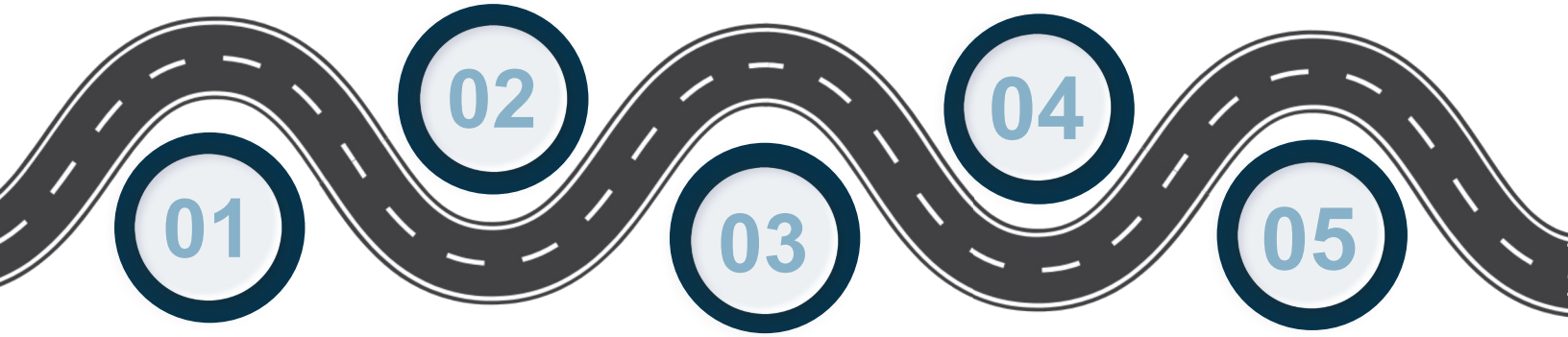


Higher Long-Term Costs

The longer you wait, the more expensive it becomes.

The Action Plan

Upgrading isn't just about security – it's about keeping your business running smoothly.



01 Upgrade to Windows 11

Immediate action needed for security.

02 Replace Legacy Hardware

Future-proof your IT environment.

03 Audit & Update Software

Ensure critical applications work post-upgrade.

04 Implement Additional Cybersecurity Measures

Strengthen defenses.

05 Train Employees

Prevent human errors that could cause downtime.

Migration Strategy

(a.k.a. A Lot More Work Than You Think)

1. Identify and prioritize systems for upgrade/replacement.
2. Back up ALL critical data and applications—hope for no surprises.
3. Test application compatibility (some software WILL break).
4. Develop a phased migration plan to minimize chaos.
5. Implement upgrades, monitor for failures, and provide immediate troubleshooting.
6. Train staff (because someone WILL click the wrong button).

Cost-Benefit Reality Check

Cost of Not Upgrading:

- Potential **millions** in breaches, fines, and lost business.
- Weeks of downtime.
- Angry clients and lost reputation.

Benefits of Upgrading:

- Security, compliance, peace of mind.
- Improved performance and productivity.
- Future-proofing IT infrastructure.
- Avoiding that inevitable “I told you so” moment from your IT team.

Your To-Do List (Or, Just Call Us)

Deadline: NOW.

If this looks overwhelming (spoiler: it is), it’s time to bring in experts.

Contact Newave Solutions to save yourself from the disaster waiting to happen.




NEWAVE
SOLUTIONS