DealersEdge®

SPECIAL REPORT

The End of Windows 10 Support

October 16, 2024

Table of Contents & Topic Abstracts

As Microsoft phases out support for Windows 10, dealerships are at a crossroads. How will this shift impact your operations, security, and overall efficiency?

In this webinar, Erik Nachbahr, Founder and President of Helion Technologies and a Certified Information Systems Security Professional (CISSP), breaks down what this transition means for your dealership, how to avoid costly mistakes, and strategies to manage this significant technological disruption smoothly.

The takeaways from this workshop are:

- ☺ The end of Windows 10 Support: Why this change is happening and why it's more than just another software update.
- ☺ The Cost of Waiting: The real risks of delaying upgrades, including exposure to cybersecurity threats, operational downtime, and potential regulatory penalties.
- ☺ Your Next Steps: Practical, actionable strategies for a seamless transition to Windows 11, ensuring business continuity and security.

With Windows 10 support ending on October 14, 2025, dealerships face security risks and regulatory violations.

Unsupported systems become vulnerable to cyberattacks, endangering customer data and breaching the FTC Safeguards Rule.

Upgrading to Windows 11 ensures compliance, protects operations, and maintains customer trust, helping avoid potential breaches, fines, or legal issues.

Windows 11 offers enhanced security over Windows 10 with hardware-based features like Trusted Platform Module (TPM) technology for encrypting sensitive data and next-gen cryptographic technology to prevent breaches. Biometric multifactor authentication, including facial recognition and fingerprint scanning, strengthens defenses against unauthorized access.

These upgrades align with regulatory frameworks like the FTC Safeguards Rule, making Windows 11 essential for dealerships to protect customer data, prevent disruptions, and maintain compliance, even if devices are lost or stolen.

Upgrading to Windows 11 is essential as Windows 10 support ends in 2025. With 72% of users on Windows 10, timely action avoids hardware shortages, rising costs, and compliance risks. Many older PCs can't support Windows 11's security features like TPM chips, requiring new machines. Used PCs are risky, with potential component issues, higher maintenance, and compliance challenges.

Early upgrades ensure security, operational continuity, and customer trust while meeting regulatory standards.

Microsoft Support Ends

The end of support for Windows 10 on **October 14, 2025**, presents significant challenges for dealerships that continue to use the outdated operating system.

Why does that matter?

After this date, Microsoft will no longer release security patches or offer technical support, leaving systems vulnerable.

Because they are easy targets, cybercriminals actively search for businesses still running unsupported software.

Without regular updates, any discovered security flaws remain unaddressed, increasing the likelihood of a successful attack.

Dealerships are particularly attractive to attackers due to the valuable customer financial data they store.

Regulatory Compliance Concerns

The FTC Safeguards Rule mandates that businesses maintain secure, up-to-date systems to protect consumer data and continuing to use Windows 10 after its end-of-support date on October 14, 2025, violates this regulation.

Without security updates, systems become increasingly vulnerable, exposing dealerships to potential breaches and legal consequences.

Transitioning to Windows 11 ensures your dealership remains aligned with regulatory expectations, safeguarding both operations and customer trust while avoiding penalties.

Neglecting to upgrade could result in significant fines or legal issues if a data breach occurs.

Windows 11: The Next Generation

So, what does Windows 11 offer over Windows 10?

As far as your day-to-day experience goes, not a whole lot. However, what happens behind the scenes is what counts and big change is a security boost.

New hardware-based security functionality

Windows 11 introduces a suite of advanced security features that make it a significant upgrade from its predecessors. One key enhancement is the integration of new hardware-based security functionality.

This includes Trusted Platform Module (TPM) technology, which ensures that devices meet the latest security standards by encrypting sensitive data that makes data unreadable unless you have the security keys to get in.

Next gen cryptographic technology

Next-generation cryptographic technology plays a pivotal role, safeguarding information through highly secure encryption algorithms that protect against data breaches.

Its cryptographic key storage and device authentication provide an additional layer of protection, ensuring that only verified devices can access dealership networks.

This feature enhances data security by securely storing encryption keys in protected hardware environments.

Biometric Multifactor Authentication

Additionally, biometric multifactor authentication combines technologies such as facial recognition and fingerprint scanning with traditional passwords.

This layered approach makes unauthorized access significantly more difficult, fortifying defenses against cyberattacks.

These improvements align with regulatory compliance frameworks, helping businesses meet FTC Safeguards Rule requirements and other security standards.

For dealerships handling customer financial data, these security upgrades are essential.

Windows 11's encryption technology mitigates risks of operational disruptions caused by cyberattacks and ensures personal data remains inaccessible to unauthorized parties, even if devices are lost or stolen.

The Windows 11 Rush

These forward-looking security features emphasize the importance of upgrading to Windows 11 before the Windows 10 support ends, ensuring a seamless transition while maintaining the highest level of security.

Because **72%** of Microsoft users are on Windows 10 and with cyber threats continually evolving, transitioning to Windows 11 is crucial to maintain security and compliance.

Delaying upgrades could result in hardware shortages and increased costs as the deadline approaches, further complicating the process and demand for Windows 11 equipment outstrips supply.

Action taken now ensures that dealerships avoid vulnerabilities and compliance issues, maintaining operational continuity and customer trust.

Old or Used vs. New PCs

Couldn't old PCs be upgraded to Windows 11? The answer is "Maybe" because upgrading to Windows 11 introduces hardware challenges, and many older PCs lack the capabilities to support the new security functionalities.

Specifically, Windows 11 requires TPM (Trusted Platform Module) chips and other advanced hardware features to enable encryption, device authentication, and biometric security.

As a result, approximately 25% of existing PCs cannot be upgraded to Windows 11, forcing dealerships to invest in new machines.

Can used PCs be purchased to keep the cost down?

Erik is of the opinion that dealerships should avoid purchasing used PCs, because these often come with

hidden risks such as compromised components, unsupported software, may lack essential features like TPM chips, licensing issues and higher maintenance costs.

Relying on outdated hardware could expose dealerships to cyber risks and compliance violations, particularly as Windows 10 reaches its end of life in 2025.

Have a Plan

Planning hardware upgrades early allows dealerships to spread the capital investment over time, avoid supply chain delays and ensure a smooth transition to Windows 11 that maintains both operational efficiency and data security compliance.

Inventory your PCs now

Inventory your current PCs now to determine compatibility with Windows 11.

This preparation helps avoid unexpected gaps in hardware and prevents reliance on outdated systems using unsupported Windows 10 software.

I addition to incurring an increased cyber security risk, continuing with unsupported software can lead to regulatory non-compliance, violating FTC Safeguards requirements.

Waiting too long could result in supply shortages or backorders, leaving dealerships without essential equipment during the transition.

This is not plug and play

Transitioning to Windows 11 requires more than just installing the new operating system because the enhanced security features that make Windows 11 appealing, such as biometric authentication and cryptographic technology, do not activate automatically.

For dealerships, this means additional steps must be taken to ensure these protections are properly configured and utilized.

Appropriate Security policies

Security policies need to be established and aligned with the specific features available in Windows 11.

These policies should define how encryption, multifactor authentication, and access controls will be managed across the organization.

Improper setup or lack of enforcement could leave dealerships vulnerable to attacks, undermining the very purpose of the upgrade(transcript)(transcript).

Staff must be trained

Being proactive in setting policies and training staff ensures that dealerships can fully leverage Windows 11's capabilities, enhancing security and maintaining compliance from day one.

Without proper training, there is a risk that users may disable or bypass essential security features, compromising the network.

Having a trained staff is a critical component of a successful rollout because employees must understand how to navigate the new security protocols, including how to use multifactor authentication systems effectively.

Additionally, IT personnel should receive specific training, such as Windows 11 certifications, to ensure

that installations are configured correctly and that critical security measures remain active. Erik noted that it takes a couple of hours for trained personnel to swap out PCs.

Misc.

Erik noted during the Q&A portion that dealers should refrain from using the home version of Windows 11 operating system because it lacks security features found in Microsoft PRO and does not support "Active Directory" centralized security.

Conclusion

Planning for the transition to Windows 11 is essential, as demand for compatible PCs with TPM chips is expected to surge in 2025.

As the Windows 10 support deadline of October 14, 2025, draws closer, prices for hardware are already climbing due to increased demand and supply chain challenges.

Acting proactively ensures dealerships can secure necessary devices at reasonable prices *before the rush* intensifies.

Erik Nachbahr

Enachbahr@heliontechnologies.com

443.610.7640

For Slides: Marketing@heliontechnologies.com

For A Complementary Cybersecurity Assessment Please Visit:
www.HelionTechnologies.com/it-assessment

This DealersEdge Special Report was adapted from a webinar presentation featuring Erik Nachbahr of Helion Technologies

DealersEdge is a member supported organization.
For information on how to gain access to the recordings and other resources connected to this topic please visit www.dealersedge.com/freetrial