KB

IT PROS: WHY YOU SHOULD CHOOSE AI PCS FOR YOUR NEXT PC REFRESH

December 2024

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

DELL Technologies

Executive Summary

The traditional refresh cycle for business PCs (desktops, laptops) — typically about four years, and a bit longer for small businesses — is projected to result in even more new PC deployments in 2025. Key drivers include:

- **Post-Pandemic Refresh:** PCs deployed during the sudden shift to remote/hybrid work at the start of the global pandemic in mid-2020 are now ripe for replacement.
- **Windows 10 EOS:** Microsoft Windows 10 will reach its formal End-of-Support (EOS) in October 2025, after which cybersecurity updates and technical support will no longer be provided.
- **An AI-Enabled Future:** Generative AI is rapidly transforming business processes and workflows, creating new opportunities to leverage AI capabilities integrated directly into edge devices like PCs rather than exclusively in the cloud.

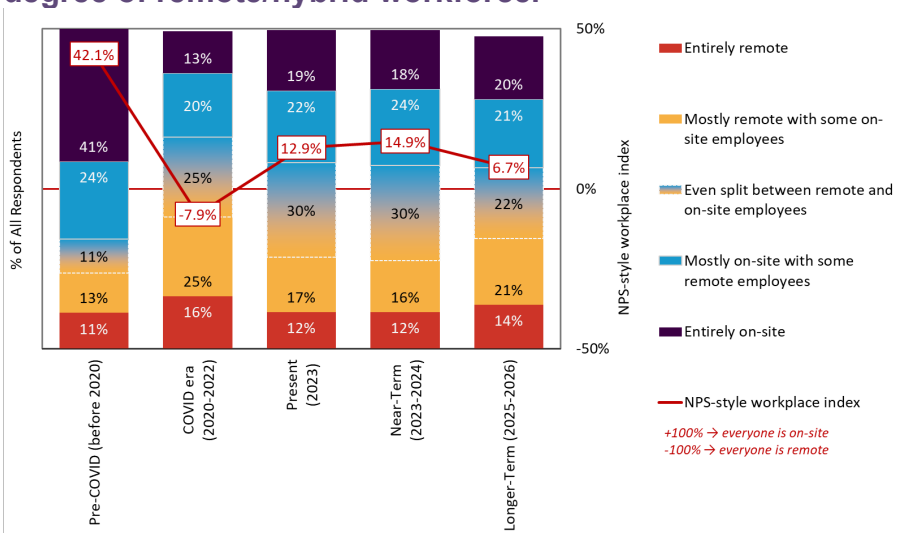
For the millions of business PCs that IT professionals will be refreshing in 2025 and beyond, Aberdeen identifies six reasons to choose an **AI PC** over a traditional PC for your next refresh or new deployments.

AI PCs are purpose-built to support artificial intelligence-enabled capabilities directly on the endpoints, *making users more productive* at key business tasks, *enabling IT Pros to be even more efficient* at managing and supporting remote/hybrid devices, and *reducing downside cybersecurity and regulatory compliance risks*.

Post-Pandemic Refresh

Although on-site workplace policies have been rebounding post-pandemic, four out of five organizations still have at least some degree of remote/hybrid workforce (see Figure 1).

Figure 1: About 80% of organizations still have at least some degree of remote/hybrid workforce.



Source: Aberdeen *Future of Workplace* study, May 2024

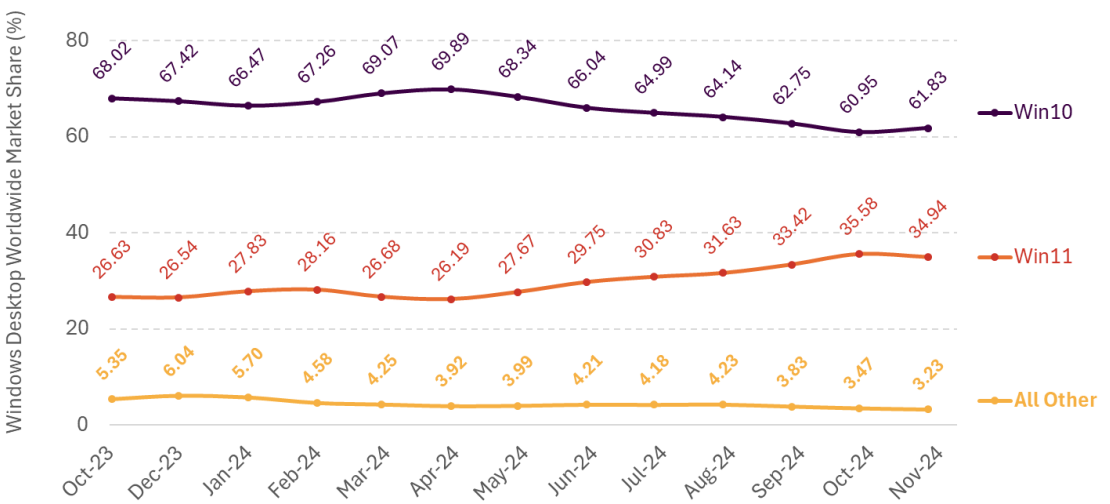
The traditional refresh cycle for business PCs (desktops, laptops) is typically about four years, and a bit longer for small businesses. Technologies initially put into place on an "emergency" basis at the beginning of the global pandemic in mid-2020 need to be revisited with an eye toward a more planful and experience-based approach to supporting the modern workforce. On today's enterprise endpoints this includes **secure login** capabilities, hard drive **encryption**, **remote monitoring and management (RMM)** capabilities, advanced **endpoint security**, and automated **patch management** solutions.

Modern enterprise endpoints typically include *secure login* capabilities, hard drive *encryption*, *remote monitoring and management* (RMM) capabilities, advanced *endpoint security*, and automated *patch management* solutions.

Windows 10 EOS

Microsoft Windows 10 will reach its formal End-of-Support on October 14, 2025, after which cybersecurity updates and technical support will no longer be provided. Just 10 months before EOS, over 3 of 5 (62%) PCs are still running Windows 10 (see Figure 2). Many of these PCs will not meet the minimum system requirements for running alternative versions or upgrading to Windows 11 (e.g., CPUs, RAM, TPM, firmware, graphics, storage, and display), providing extra incentive for an endpoint upgrade.

Figure 2: Just 10 months from its formal EOS, more than 3 of 5 (62%) PCs are still running Windows 10.



Source: Adapted from *Statcounter Global Stats*; Aberdeen, December 2024

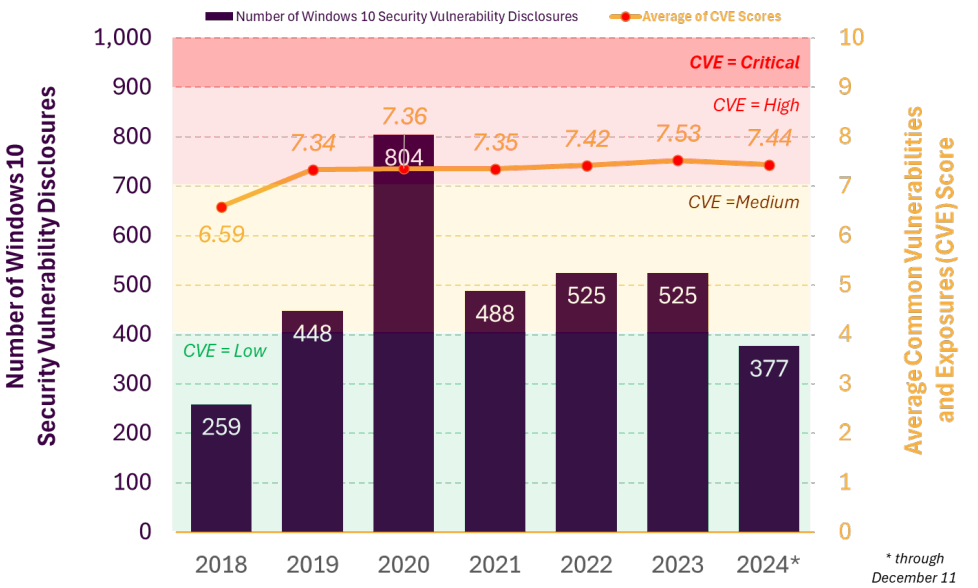
The empirical data in Figure 2 reflects some distinct movement in 2024 toward Windows 11 — a 10% decline in Windows 10, a 30% increase in Windows 11, and a 40% decline in all other versions (Windows 8.1, Windows 7, Windows Vista, Windows 8, and Windows XP) — which the formal Windows 10 EOS date is expected to accelerate.

Even so, note that all of the "all other" versions, still representing more than 3% of all Windows deployments, reached their respective EOS between 2014

and 2023. This means that even known cybersecurity vulnerabilities are no longer being updated, leaving those systems at some degree of risk.

To put this in perspective, Windows 10 has had over 3,100 cybersecurity vulnerability disclosures between 2019 and 2024, with average Common Vulnerability and Exposure (CVE) scores in the "High" category (Figure 3).

Figure 3: Windows 10 has had >3,100 cybersecurity vulnerability disclosures between 2019-2024, with "High" average CVE scores.



Source: Adapted from *stack.watch*; Aberdeen, December 2024

In Aberdeen's recent research, respondents reported that cybersecurity incidents affecting **confidentiality**, **availability**, and **compliance** were all too common. Over the previous 12 months:

- About 4 in 9 (43.9%) experienced an incident affecting **data confidentiality/privacy** — including incidents involving *structured data (records)*, *unstructured data (files)*, and *ransomware*.
- About 3 in 5 (61.4%) experienced an incident affecting **availability** — including incidents resulting in unplanned downtime or slowdown for *endpoints*, *networks*, and *back-end systems*.
- Nearly 2 in 5 (38.6%) experienced an incident affecting **regulatory compliance** — e.g., a finding or observation that was substantial enough to require prompt remediation or a committed plan for remediation.

This highlights the importance of keeping enterprise PCs properly configured, patched, and up to date — and in general, of moving away from Windows 10.

In addition to active cybersecurity updates and technical support, Windows 11 offers enhanced security features compared to Windows 10 based on its *hardware-backed* security features, which help protect against malware and other threats.

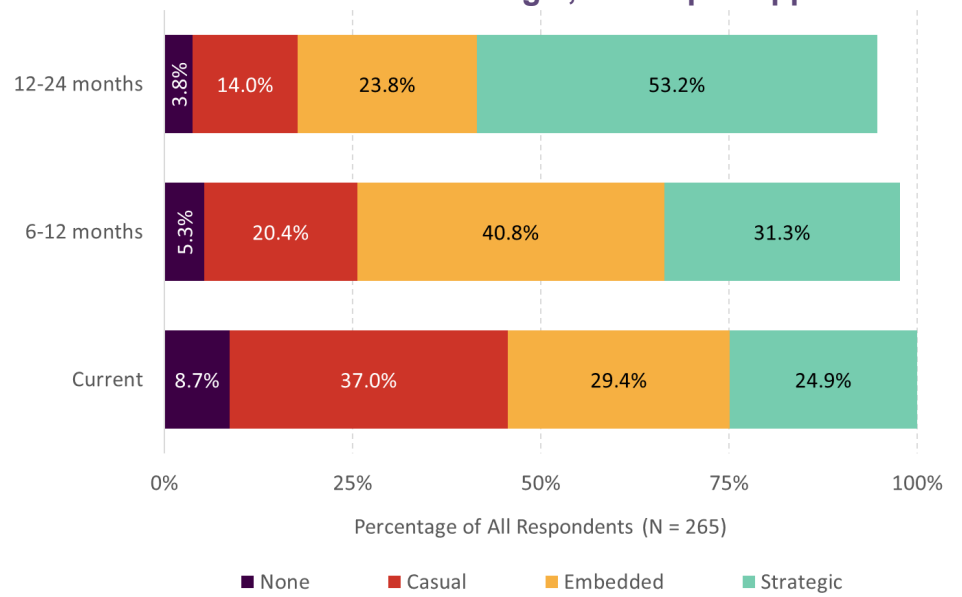
IT Pros understand the importance of keeping enterprise PCs properly configured, patched, and up to date. In general, this means moving away from Windows 10 before its formal EOS.

An AI-Enabled Future

In Aberdeen's 2024 *AI Infrastructure study*, organizations see their adoption of artificial intelligence moving rapidly from the *casual use of free tools* by individuals for ad hoc business needs to *strategic applications* developed in-house or based on commercially available platforms (see Figure 4). In between these two scenarios is the adoption of products and services that embed AI and machine learning capabilities (e.g., monitoring and alerting, predictive modeling, chatbots) as value-added features.

For organizations of all sizes, AI adoption is projected to move rapidly from casual, individual use of free tools to strategic, developed applications.

Figure 4: Adoption of AI is projected to move rapidly from casual, individual use of free tools to strategic, developed applications.



Source: Aberdeen AI Infrastructure study, September 2024

Given the high likelihood of an AI-enabled future, here are six reasons to choose an AI PC over a traditional PC for your next refresh or new deployments:

- **Cybersecurity and Compliance.** AI PCs integrate advanced hardware and software capabilities to detect and protect against endpoint security threats more effectively than traditional PCs. They can run AI-related applications locally, keeping your sensitive data on the device and reducing the risk of exposure.
- **Technology.** AI PCs have specialized hardware accelerators — including CPUs, GPUs (graphics processing units), and NPUs (neural processing units) — designed to handle AI workloads more efficiently than traditional PCs. Processing AI workloads locally yields faster speed and lower latency than relying exclusively on cloud-based AI

computing. AI PCs are already compatible with a wide variety of data types, LLMs, and AI frameworks for flexible application development.

- **User Enablement and Convenience.** AI PCs offer a smoother and more responsive experience for modern users than traditional PCs, thanks to the dedicated hardware and software optimized for AI-related workloads. AI-powered features are rapidly becoming established for use cases such as creativity, personal assistance, collaboration, and cybersecurity — with tremendous investment, innovation, and adoption still to come.
- **Business Enablement.** Organizations of all sizes are leveraging AI for innovation, operational efficiencies, and improved customer experiences across diverse departments and use cases. Embracing AI PCs allows you to take full advantage of a rapidly growing ecosystem of AI-powered applications and workflows.
- **Strategic.** AI PCs are part of a broader "AI Everywhere" vision — a shift towards integrating AI capabilities directly into devices and platforms, making AI more accessible and enabling organizations to adopt a distributed AI strategy. Investing in AI PCs over traditional PCs creates opportunities for today, and ensures that your IT infrastructure is ready for the future of work.
- **Cost.** AI PCs can run AI-related workloads locally, reducing operational costs for cloud-based AI computing, processing, and storage. In addition, compared to traditional PCs the advanced capabilities and future-proof nature of AI PCs are expected to contribute to a longer useful life and higher residual value.

In Aberdeen's view, choosing an AI PC over a traditional PC has advantages in several areas, including *cybersecurity and compliance*, *technology*, *user enablement and convenience*, *business enablement*, *strategic* value, and overall *cost*.

Summary and Key Takeaways

With respect to your organization's PCs (desktops, laptops), over the next several months it's highly likely that *"a change is gonna come."* Whether driven by a **post-pandemic refresh**, the formal **Windows 10 End-of-Support**, or the rapid realization of an **AI-enabled future**, IT professionals have an important choice to make for their next PC refresh or new PC deployments.

AI PCs are purpose-built to support artificial intelligence-enabled capabilities directly on the endpoints, *making users more productive* at key business tasks, *enabling IT Pros to be even more efficient* at managing and supporting remote/hybrid devices, and *reducing downside cybersecurity and regulatory compliance risks*.

In Aberdeen's view, choosing an AI PC over a traditional PC has advantages in several areas, including **cybersecurity and compliance**, **technology**, **user enablement and convenience**, **business enablement**, **strategic** value, and overall **cost**.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research (a division of Spiceworks Ziff Davis), with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to **inspire** critical thinking and **ignite** data-driven business actions.

ABERDEEN STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

DELL Technologies