OCTOBER 2024

Why an Accelerated PC Refresh Cycle Makes Sense Today

Gabe Knuth, Senior Analyst

Abstract: Increasing security vulnerabilities, Windows 11 upgrades, and emerging technologies like artificial intelligence are all affecting end-user device strategy at the same time, making it more challenging than ever to keep up with the pace of change. Often, the role of hardware as a solution to these problems is overlooked, and modernizing old PC and laptop hardware can help overcome these challenges while laying a secure, high-performing foundation upon which to build a modern end-user device strategy. Due to its advanced hardware and services portfolio, Dell is especially well positioned to help simplify IT while modernizing the workplace.

IT Complexity Has Bogged Down PC Refresh Cycles

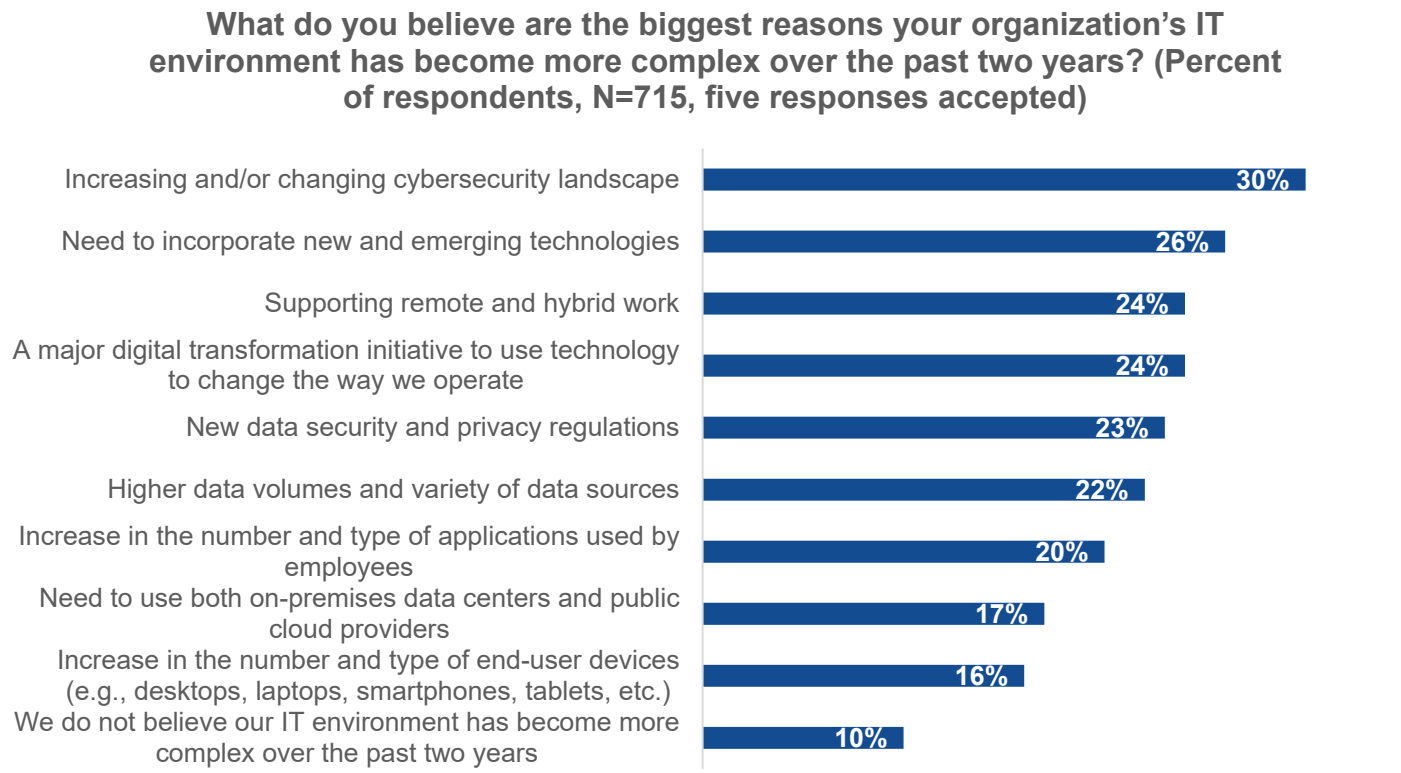
The teams that manage end-user devices such as PCs and laptops are constantly dealing with pressure that extends from all directions. Internally, those take the shape of new application deployments, supporting the needs of specific business units and the demands from end users. Externally, pressure comes from the increased number and volume of security vulnerabilities, the need to upgrade to Windows 11, and, increasingly, all things artificial intelligence.

It's no surprise, then, that 90% of organizations to a research survey from TechTarget's Enterprise Strategy Group say that IT is becoming more complex, with security, incorporating new and emerging technologies, an increase in the number and types of apps, and an increase in devices all featuring prominently (see Figure 1).[1]

Digging into the operational and business challenges specifically associated with PCs and laptops, IT finds itself pulled in many directions at the same time. When a recent research project by Enterprise Strategy Group asked what challenges organizations experienced and which of them was the most significant, responses were evenly distributed, although operational cost for IT staff required to support end users and devices, an increased variety of devices, delivering a consistent user experience, and regulatory/compliance edged out the others as the most significant challenges (see Figure 2).[2]

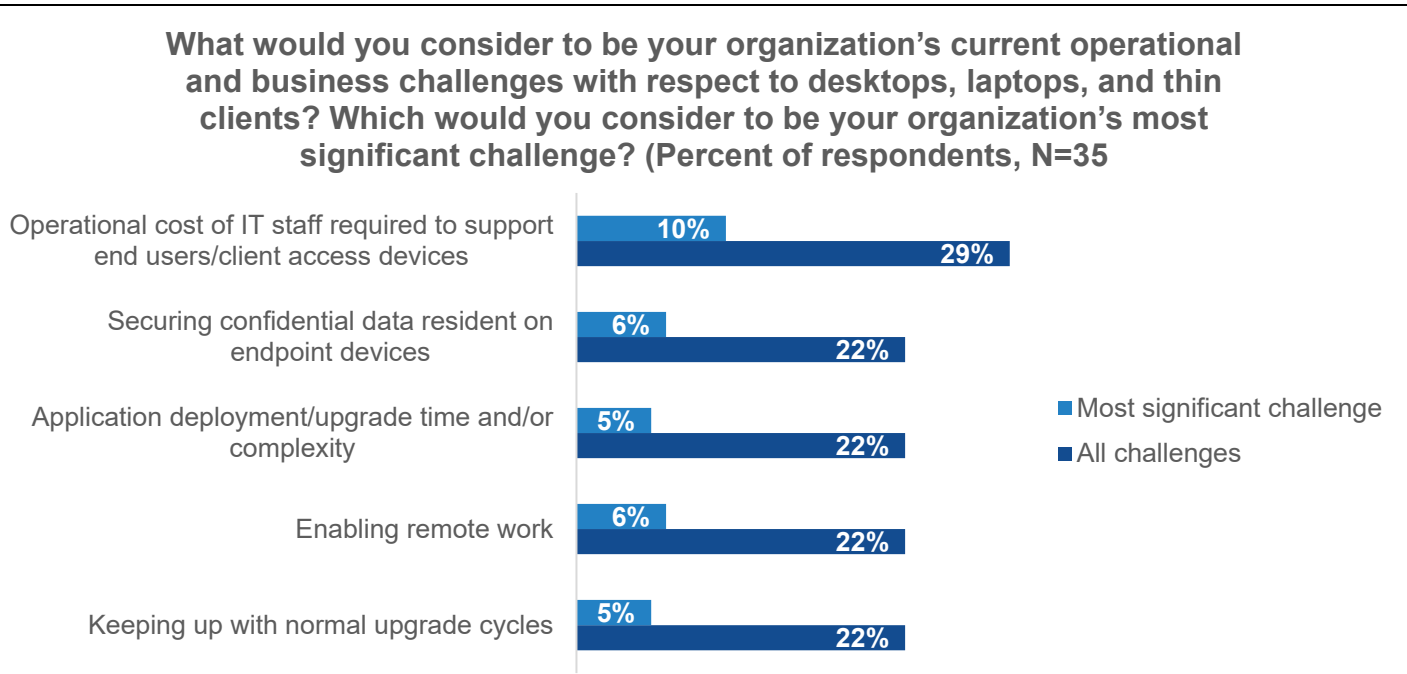
[1] Source: Enterprise Strategy Group Complete Survey Results, *2024 Technology Spending Intentions Survey*, February 2024.
[2] Source: Enterprise Strategy Group Complete Survey Results, *Endpoint Device Trends*, February 2024.

Figure 1. IT Complexity Comes in Many Forms



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 2. Top 5 PC and Laptop-related Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

How a PC Refresh Can Help With Complexity

With so many demands, challenges, and goals, it's tough to find relief. This is where end-user device refreshes can help. In fact, from improving employee productivity and increasing security to enhancing employee experience and reducing cost, the top trends and priorities that most are most influential to end-user device strategies align well with the above challenges (see Figure 3).[3]

Figure 3. Top Priorities Affecting End-user Device Strategy

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While the alignment between challenges, goals, and strategy is clear, there are other considerations that could affect the normal PC and laptop refresh cycle, which is typically between three and five years, based on Enterprise Strategy Group research.[4] Historically, device refreshes have been considered a cost of doing business, and while that may have been the case at one time, the role of the end-user device is more important in achieving business objectives than ever before.

[3] Ibid.
[4] Ibid.

Hardware-based Security Is Critical to Success

For example, improving security amid a constantly changing cybersecurity landscape is a top priority for companies. Attacks have become more sophisticated, but so have the software- and hardware-based approaches for dealing with those attacks. Here are just a few examples of the role hardware can play in improving security:

Secure Boot

Secure Boot is a security standard that ensures a system boots using only software that is trusted by the original equipment manufacturer by validating the operating system, drivers, and firmware against stored cryptographic signatures in the hardware. This ensures that a modern end-user device isn't compromised at the lowest levels of the system and establishes a foundation on which to build additional security layers.

Trusted Platform Module 2.0

The Trusted Platform Module 2.0, or TPM 2.0, is a dedicated chip built into the device's hardware that performs cryptographic key generation and encryption locally on the device. Sensitive data (e.g., passwords, encryption keys, certificates, etc.) are stored in the chip's protected memory, which makes it hard for attackers to gain access to or manipulate that data. TPM 2.0 also factors into the Secure Boot process and ensures that only authorized hardware is connected.

Intel Hardware Shield and Threat Detection Technology

Intel has built a security platform called Hardware Shield that integrates multiple technologies in an effort to protect devices from a variety of threats. At its core is Threat Detection Technology, or TDT, which leverages telemetry from the hardware with machine learning to detect and prevent attacks such as ransomware, cryptojacking, and more. TDT works by monitoring CPU and memory behavior for early signs of malicious activity to report to security software that can take action.

Performance, Efficiency, and AI Capabilities

Of course, the first thing that comes to mind when thinking of hardware isn't security—it's performance. Today, performance is judged as much on speed as it is on efficiency and sustainability, which is why Intel® Core™ Ultra processors are now built on a modular technology that dedicates parts of the CPU to different tasks. For example, there are separate cores dedicated to performance (Performance-cores, or P-cores) and efficiency (Efficient-cores, or E-cores), and the CPU has the ability to move processes between cores, as needed, to deliver the best balance of performance and efficiency.

These CPUs also come with built-in neural processing units (NPUs) for emerging AI workloads that demand local AI processing. These workloads include communications and collaboration, accessibility, and security. NPUs also provide organizations with innumerable ways to improve employee productivity.

Windows 11

With the end of life for Windows 10 quickly approaching (October 14, 2025), Windows 11 deployments are also a huge factor in determining when—and which—PCs should be refreshed. Windows 11 requires the Secure Boot and TPM 2.0 hardware features mentioned above, which means that any devices that don't have both of those features will need to be replaced before October 14, 2025. After that date, Windows 10 will no longer be supported or updated, which increases support and security challenges for IT.

But there's more to updating to Windows 11 than having the latest OS on the latest hardware. Windows 11 helps ensure security through features like disk encryption (BitLocker) and Windows Defender System Guard, which leverages Secure Boot and TPM 2.0 to ensure the device is free from tampering or other malicious modifications.

How Dell Can Help

Dealing with the pressures placed on the organization that simultaneously stem from security, performance, Windows 11 upgrades, and the emergence of AI can be a challenge, and while there may be a clear path forward, the journey itself can be a challenge. Dell plays a significant role in this journey by helping to reduce complexity in procurement and meet sustainability goals while enabling organizations to deploy the latest hardware with the latest security and performance features.

In fact, Dell has built its entire Modern Workplace around three core principles:

1. Delight the end user.
2. Simplify IT.
3. Advance sustainability.

Let's take a look at each of these in more detail.

Delight the End User

For Dell, the modern workplace is a collaborative workspace that ensures users can work from any location without sacrificing productivity, compliance, or security. Dell works closely with partners like Intel® and Microsoft to develop solutions around technologies like Microsoft Copilot, which has resulted in new Copilot+ PCs that further drive productivity and process optimization through the use of local AI processing.

Simplify IT

Dell Trusted Devices offer innovative built-in BIOS-level visibility and tamper detection to help protect against evolving threats. Key features include off-host BIOS and firmware verification and Indicators of Attack and Common Vulnerabilities and Exposures (CVE) Detection. When suspicious activity is flagged, Dell-unique PC telemetry bubbles security alerts up to the OS level for swift action. Dell also have services like Dell Trusted Update Experience, which integrates with unified endpoint management (UEM) providers to optimize the process of updating the BIOS, firmware, and drivers.

Additionally, Dell has leveraged its expertise to build a comprehensive, modular services portfolio that can meet organizations where they are today and help them map out and achieve their goals. These services, including APEX PC as a Service, APEX Managed Device Service, ProSupport, and ProSupport Plus, offer a variety of service levels and price points to help reduce the demand on IT, freeing up resources that can be dedicated to other projects to help the company be more successful.

Advance Sustainability

Dell's focus on sustainability means that customers can rest assured knowing the devices they purchased are being produced in ways that reduce e-waste, increase recycling, and are energy-efficient, both in production and in use. In fact, this year, Dell says that 96.4% of its packaging will be made from recycled or renewable materials, and the products themselves are designed to use recycled materials like plastic, glass, and aluminum.

Dell also has services that can enable and accelerate digital transformation, which helps organizations develop their own more sustainable practices.

Conclusion

There is so much going on today that the role end-user devices play in achieving the overall goals of the business are often overlooked or minimized. Be it through advanced, hardware-based security; support for modern OSes and their capabilities; laying the foundation for artificial intelligence; or simplifying IT through the use of advanced technology or services, there is a lot to be gained from updating hardware and making use of all of the capabilities available today.

Because of this, organizations should prioritize refreshing PC hardware and ensuring the new devices can support the latest features. With their well-earned reputations as trusted providers of technology and services, customers would be wise to consider Dell and Intel® for any PC or laptop refresh initiative.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com