JANUARY 2025

Securing the Endpoint: How Dell Helps Balancing AI Adoption With Cyber Resilience

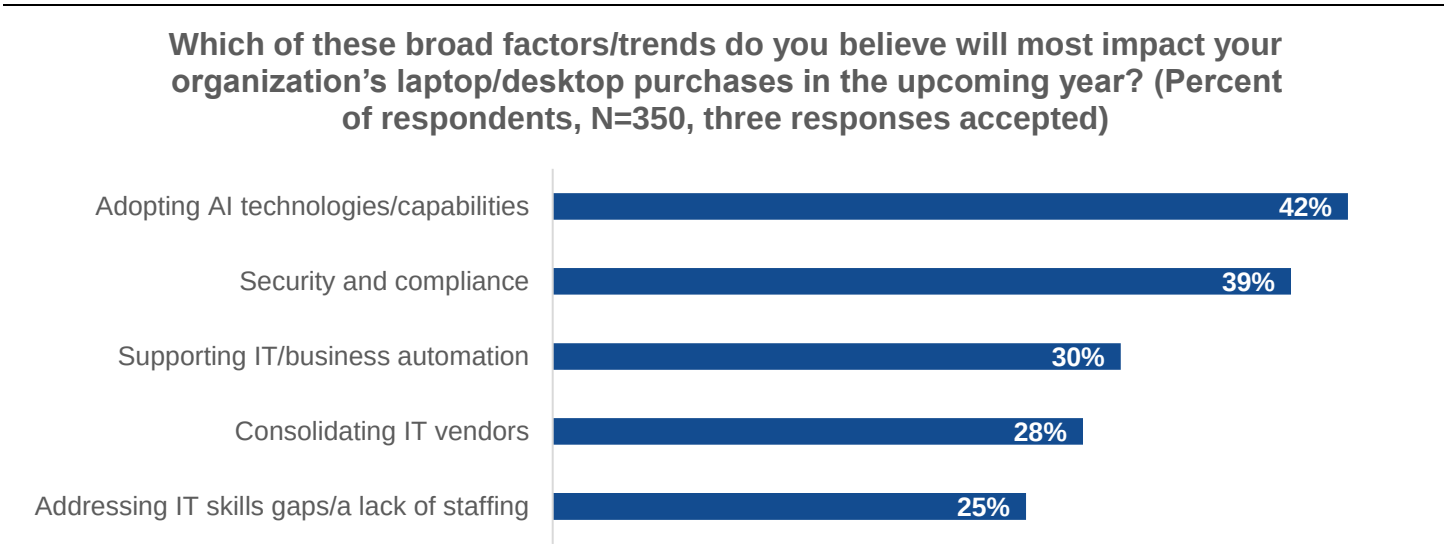
Gabe Knuth, Senior Analyst

Abstract: The role of endpoint security is growing as AI adoption by both organizations and cybercriminals grows. Recent research from Informa TechTarget's Enterprise Strategy Group highlights the dual pressures IT teams face: managing sophisticated cyberthreats while enabling transformative innovations.[1] This paper explores how Dell's combination of below-the-OS security, secure supply chain practices, and comprehensive services positions it as a trusted partner for organizations looking to strengthen their security posture.

Overview – The Problem

As organizations face constantly evolving cybersecurity threats, security is often the cornerstone of any technology decision. This is as true in the cloud and data center as it is at the PC, where, according to a recent Enterprise Strategy Group research project commissioned by Dell, security is among the top features influencing desktop and laptop purchases (see Figure 1). What's most notable about this is that organizations have given adopting AI technologies and capabilities a similar level of priority, underscoring that organizations are facing challenges integrating transformative technologies like AI while safeguarding endpoints from increasingly sophisticated cyberthreats.

Figure 1. Top 5 Factors Affecting Endpoint Purchases



Source: Enterprise Strategy Group, a division of Informa TechTarget

[1] Source: Enterprise Strategy Group Custom Research commissioned by Dell, *Client Trends and Competitive Landscape*, June 2024. All Enterprise Strategy Group research references and charts in this showcase are from this research study unless otherwise noted.

Of course, this is expected. AI is already proving to be transformational in a user-facing capacity, so its ascent up the priority ladder was all but a sure thing. But all the things that AI does for user productivity, creativity, and the business in general also apply to the bad actors, which means this tandem of AI adoption and security (or the trio, if you count compliance separately) are likely joined in lockstep forever.

While AI usage and concerns are still being defined by many organizations, security-related challenges are well established, such as:

- Keeping up with hardware and software upgrade cycles (cited by 32% of respondents).
- Securing confidential data on laptops and desktops (29%).
- Enabling hybrid work (27%).
- Supporting a growing end-user workforce (27%).
- Addressing patch management (20%).
- Managing unauthorized application usage or configuration changes (17%).

These "classic" challenges, coupled with the emergence of AI and the increasing sophistication and volume of attacks, paint an unenviable picture for IT. In truth, it's not possible to block everything, so it's important to leverage all the tools available to stay ahead of the challenges of today and the ones that are coming down the road.

What Can Organizations Do?

To address these challenges, organizations need to take advantage of security features that can help them expand on their current initiatives. Often, this means looking beyond basic security measures and end-user training, choosing instead to focus on a broader, multi-layered approach that can help improve long-term cyber resilience.

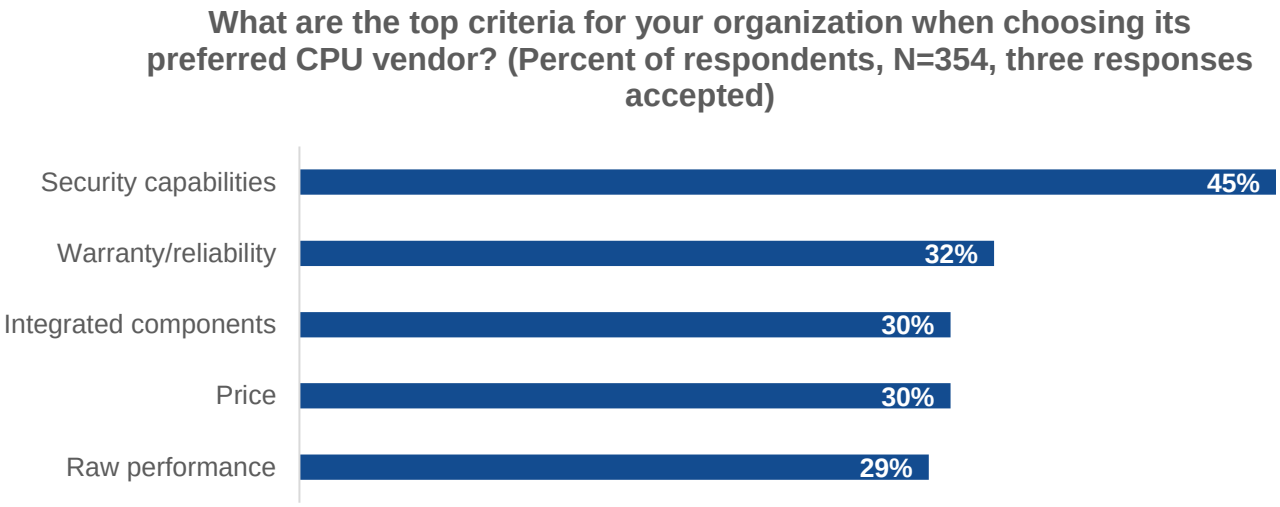
One of the layers that is often overlooked (or at least minimized) is the role that hardware-level, or "below-the-OS," security plays. Hardware-based security reduces the overall attack surface of a machine, which can mitigate attacks before they have a chance to become entrenched. Stronger foundational security complements software-based configuration, analysis, and remediation tools, which reduces the load on IT resources that are constantly analyzing detected issues and alerts.

If the hardware is so powerful, then why is it so often overlooked? Too often, hardware is seen as a commodity—a necessary evil that requires patching and maintenance or, worse, is deployed and forgotten altogether. The reality, however, is that each generation of chipsets comes with more advanced security capabilities that can protect against both firmware and hardware-level attacks. More recently, hardware has built-in security measures that can work with in-OS security tools to detect anomalous behaviors deep within applications.

While updating a device or its firmware was historically perceived as something done only when it was outdated or having a problem, the reality is that those updates often improve overall security posture, especially since these updates are for end-user devices! It's for this reason that security capabilities tops the list of criteria for choosing a CPU vendor (see Figure 2).[2]

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

Figure 2. Top 5 Factors in CPU Vendor Choice



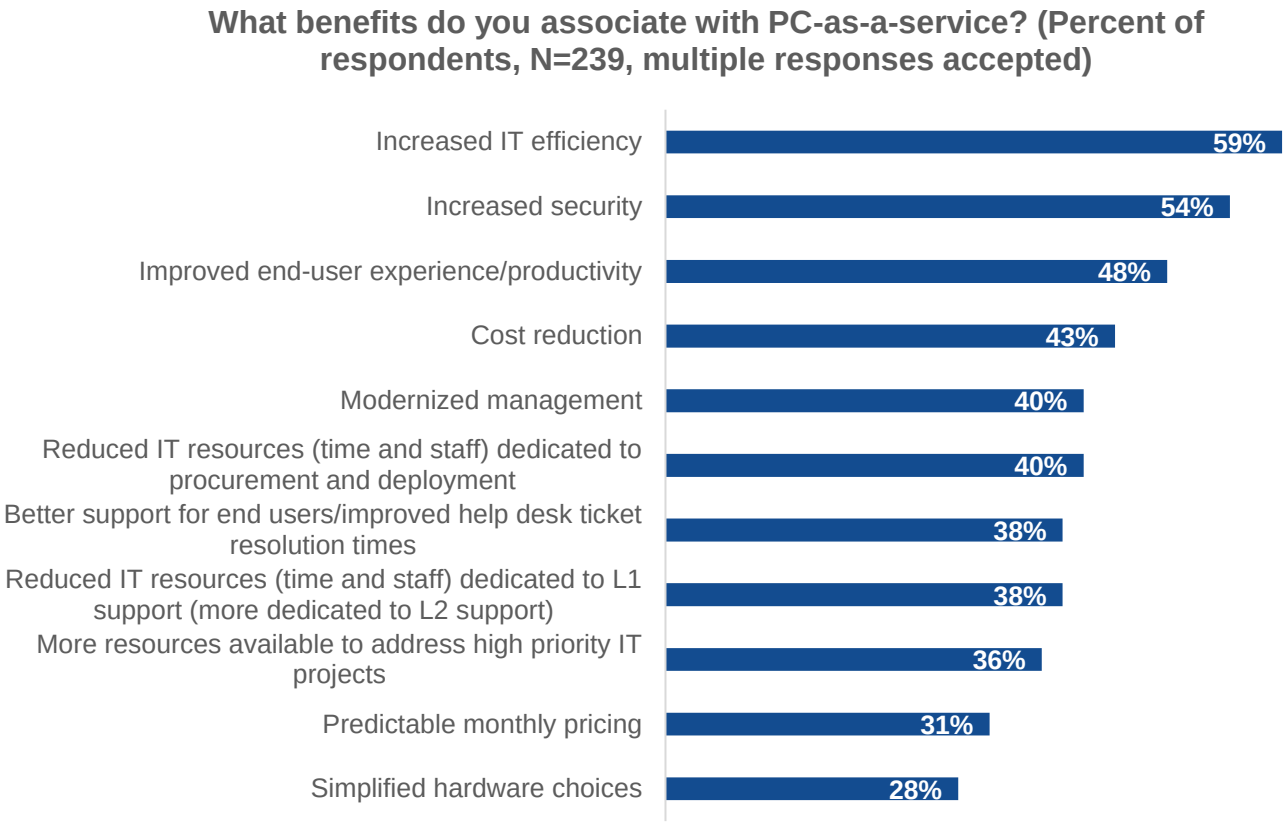
Source: Enterprise Strategy Group, a division of Informa TechTarget

There are also elements of security that are not often considered by admins, such as supply chain security, which was cited by 40% of organizations as one of their top laptop/desktop PC procurement challenges (behind cost management, growing end-user demands, and fulfillment speed).

Altogether, this highlights the need for organizations to work with vendors that can demonstrate a dedication to hardware and supply chain security. This will help with procurement, for sure, but recalling the 32% of organizations that struggle with keeping up with normal upgrade cycles or the 20% that said patch management was a challenge suggests that organizations could use help with the day-to-day security tasks as well.

Considering this, it's not surprising to see that companies are increasingly leaning on managed services like PC as a Service (PCaaS). PCaaS simplifies procurement and support by offering varying devices and service levels at a monthly operation cost. The survey asked respondents that use PCaaS about the key benefits they associate with it, and increased IT efficiency (59%), increased security (54%), and improved end-user experience/productivity (48%) all featured prominently in the results (see Figure 3), showing that there is the potential for services to play a key role in a multi-layered security approach, too.

Figure 3. PCaaS Has Widespread Benefits, Including Increased Security



Source: Enterprise Strategy Group, a division of Informa TechTarget

How Dell Can Help

As a leader in every area discussed thus far (AI, security, user experience, and more), Dell is in a unique position to help customers meet their goals. Dell understands that security must be comprehensive through the entire device lifecycle, from the supply chain to recycling. Dell maintains strict control over its supply chain, ensuring security and availability through diverse, global chip manufacturers, facilities, and distribution channels.

Its commercial PCs and laptops feature below-the-OS security through Dell Trusted Device and Dell SafeBIOS, a suite of capabilities that protects the integrity of the device down to the BIOS and firmware levels. This feature, paired with Intel core silicon, means Dell commercial devices deliver comprehensive hardware-level security that minimizes the attack footprint of each device. This combination of Dell Trusted Devices powered by Intel processors is one of the reasons Dell is recognized as a leader in endpoint security. Dell also includes its own software to ensure device firmware, BIOS, and drivers stay up to date, which is especially important for those organizations that struggle with unauthorized app usage and patch management.

Finally, Dell offers a flexible array of services to support organizations overwhelmed by the growing demands of endpoint security management. ProSupport and ProSupport Plus provide advanced technical assistance and predictive issue resolution, ensuring devices remain secure and operational with minimal downtime. For organizations looking to simplify IT operations further, Dell's APEX PC-as-a-Service (APCaaS) delivers an all-encompassing solution by bundling hardware, software, and lifecycle services into a predictable, subscription-based model.

This holistic approach—combining a sophisticated supply chain, cutting-edge hardware, robust software, and flexible services—gives organizations the head start they need to overcome the security issues associated with today's endpoints by enabling IT teams to maintain a strong security posture, even in the face of increasing complexity and resource constraints.

Conclusion

Security is a constant challenge for IT teams, and it's only becoming more challenging as the same technology that bolsters business helps the bad actors, too. But it doesn't have to be a losing battle. Even as emerging trends like AI climb the list of priorities, it's important to stay focused on the need for comprehensive endpoint security. Organizations can take meaningful steps to address their challenges by building a multi-layered approach that leverages hardware, software, and services.

Often, this involves working with trusted partners, which is why Dell's portfolio stands out. Dell's focus on hardware-level security, end-to-end lifecycle protections, and flexible service offerings ensures that customers have the tools and support they need to address both day-to-day security tasks and long-term strategic goals of improving security while still adopting—and deriving value from—emerging technology. In short, Dell's solutions are well suited to meet the demands of modern IT environments.

In a world where AI and security are becoming equally critical priorities, organizations must adopt strategies that make the endpoint both a tool for productivity and a key element of an organization's cybersecurity objectives. Dell's ability to combine these priorities into a unified approach makes it a natural choice for organizations that value innovation, reliability, and peace of mind.

For more information, visit dell.com/endpoint-security.

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