



intel®

Buyer's Guide

What you need to know to buy PCs for your company

Inside

- 1 Introduction
- 2 Security, manageability top the list of IT needs
- 7 User priorities: Powerful and portable
- 10 Summary and recommendations

Introduction

The choices organizations make when purchasing desktop and laptop computers have never been more important. With hybrid and remote work scenarios expected to dominate the corporate landscape for the foreseeable future, computers have become not only essential tools for getting work done but also lifelines for communicating with colleagues and customers.

We aren't returning to a full-in-office workforce anytime soon, if ever.

- Global Workplace Analytics estimates that between 25% and 30% of the labor force **will work from home multiple days a week** by the end of 2021.
- A **Deloitte study** found that 55% of human resources professionals expect at least half of their workforce to be remote in the future. (Before COVID-19, the number was 13%.)
- **Forrester believes** only 30% of companies will embrace a full return to the office after the pandemic.

IT organizations are under increasing pressure not only to provide employees with adequate compute power and flexibility but also to secure devices that, in many cases, they cannot access directly. Lack of physical access creates new needs for remote management, problem diagnosis, and repair. Time is of the essence, as employees whose computers are out of commission are effectively unproductive.

In the office, IT teams could use endpoint management software to keep track of every device on the internal network and dispatch technicians for quick repairs. In the workplace of the future, though, half the workforce may be disconnected at any given point. That will create new challenges in diagnosing problems and even greater ones in repairing them quickly and economically.

As PCs become more critical to employee productivity, the importance of performance will grow as well.

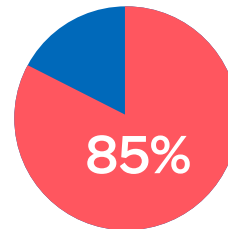
- Many remote workers will participate in videoconferences multiple times per day while having a dozen or more browser windows and applications open simultaneously.
- Computers that slow down, freeze, or behave unpredictably impact productivity and morale. A loss of just five minutes per hour to poor performance adds up to three hours per week and more than 145 hours per year.
- A 2019 **ZenBusiness survey** found that 66% of business professionals reported that working with outdated technology had at least a moderate impact on productivity, and 59% said the same of job satisfaction.
- **Nexthink reported** that 42% of employees say that the quality of the digital workplace influences their willingness to recommend their organization to job seekers.
- A recent **IDC survey** found that 85% of respondents agreed that higher employee engagement translates into a better customer experience, higher customer satisfaction, and increased revenues.

The bottom line is that by providing the best PC technology to get work done, IT can have a direct impact on a company's overall job satisfaction rate—and thus the organization's overall success.

Engagement trifecta

Source: IDC; Market Analysis Perspective: Worldwide Employee Experience Management Strategies

Those who feel that higher employee engagement equates to better customer experience, satisfaction, and increased revenue.



Key Trends on IT's Radar

Better performance

Processors, memory, and storage are faster than ever. IT wants a piece of that action.

Shift cloudward

At the same time, cloud infrastructure can take some of the pressure off desktops and servers.

Aesthetics

IT pros are people too; they want a delightful experience and excellent streaming performance.

BYOD

Growing variations in device form factors create security and manageability challenges.

WFH is the future

Remote employees need good cameras, fast bandwidth, physical security, and safe access to the cloud.

Privacy

The more dispersed the workforce, the bigger a problem this is.

Sustainability

Data centers already consume 1% of the world's electricity, and 5G is expected to gobble up 3.5 times as much electricity as 4G. That makes it an IT problem.

Security, manageability top the list of IT needs

The selection of workplace PCs must balance the need to satisfy user requirements for performance and usability with IT's mandate to secure and control its technology assets. Both groups overlap in their shared interest in provisioning stable platforms. Let's look at each in turn.

Security: Software protection isn't enough

The COVID-19 pandemic brought with it a massive surge in cyberattacks.

- [NCC Group reported](#) that ransomware attacks increased threefold in the second quarter of 2021 compared to the first quarter.
- [IBM said](#) the cost of an average data breach surpassed \$4 million this year, the highest level on record.
- [Lynx Software found](#) that more than one-third of remote workers have been impacted by a cyberattack since the start of COVID-19.

Proliferating vulnerability points created by the shift from managed corporate computers to a dispersed fabric of home-based devices have made the task of securing devices more challenging.

The nature of attacks is also changing. Software-based security is no longer enough to protect an organization from all threats. [Ponemon reported](#) that just 27% of respondents to its 2020 endpoint study believe traditional, signature-based antivirus solutions provide the protection needed to stop serious attacks. It also found that endpoints are the most-attacked IT assets, with 81% of businesses experiencing incidents involving malware.

Secure at the hardware level

Processors with Intel vPro Enterprise for Windows contain several important hardware-based tools to fight against low-level attacks and complement software protections.

Intel **Hardware Shield** helps prevent BIOS attacks by storing an image of the factory BIOS in a location where it can't be reached by the operating system. At boot time it compares the status of the BIOS to the secure image and prevents the PC from starting if they don't match. Hardware Shield also protects against BIOS writes from any other environment.

Intel **Total Memory Encryption** is a feature of Hardware Shield that encrypts all data at the silicon level. This helps protect against attacks in which a bad actor gains physical access to a machine—a scenario that is far more likely with computers at home than in an office.

Intel's **Threat Detection** technology uses machine learning that works with endpoint detection and response (EDR) software like Microsoft Defender to look for anomalies.

"We pull attacks from the wild and run them on our hardware to see if there's suspicious behavior down below," said Mike Nordquist, Strategic Planning and Architecture Director for Business Client Platforms at Intel. "Then we can use the EDR capabilities to decide whether to quarantine, update, or take some other action."

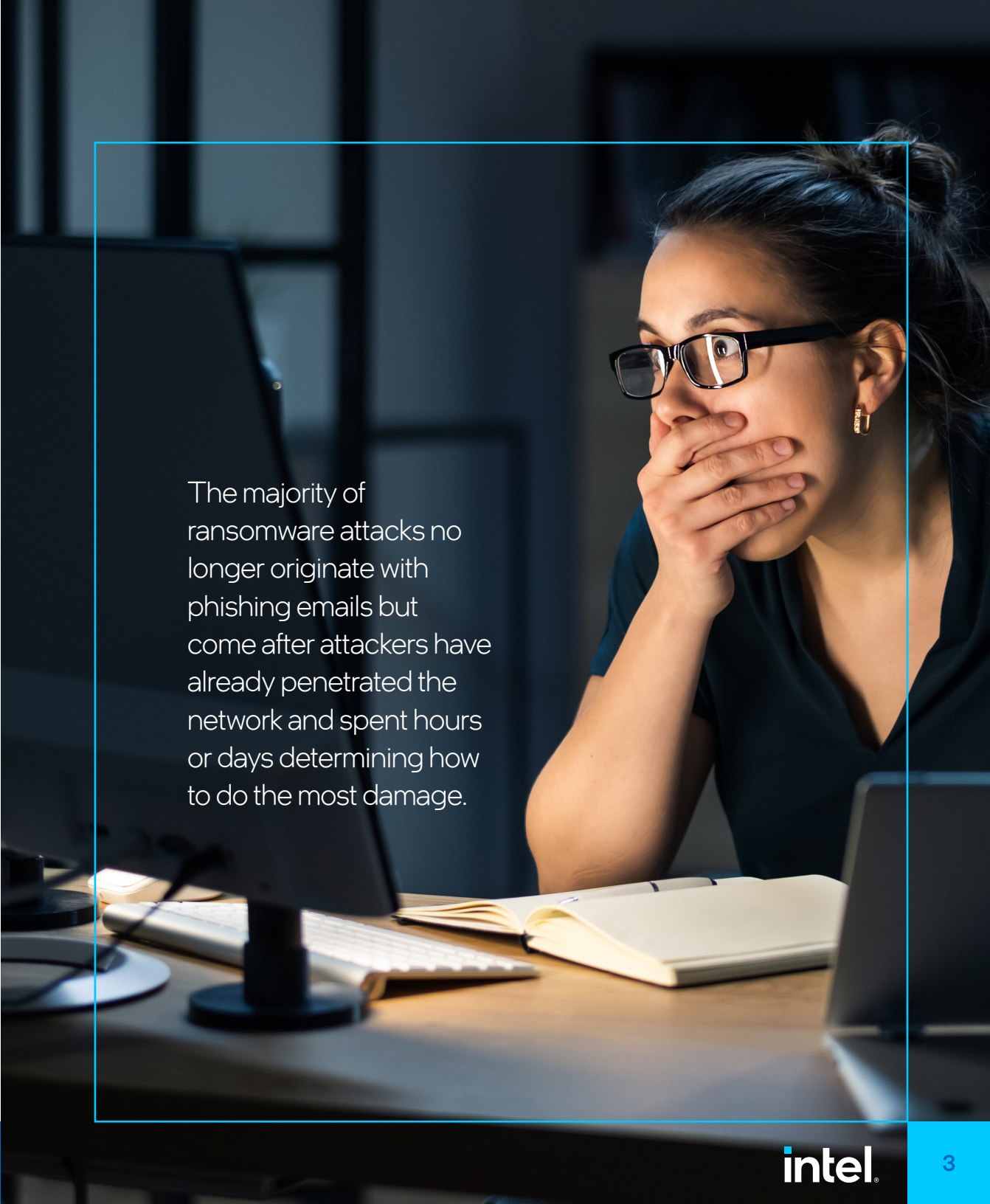
Intel **Accelerated Memory Scanning** is an example of how an extra layer of protection can be applied on top of the encryption that Intel automatically applies to data in memory. Intel AMS uses machine learning algorithms on a graphics processing unit (GPU) to quickly learn the memory characteristics of the computer and continually apply heuristics to look for abnormal activity, greatly reducing the risk of attacks that modify CPU instructions.

The growing volume and intensity of ransomware attacks provide evidence of how cybercriminals can infiltrate a single PC and spread out laterally across the network, ultimately infecting hundreds of endpoints and servers. In fact, the majority of ransomware attacks no longer originate with phishing emails but come after attackers have already penetrated the network and spent hours or days determining how to do the most damage.

The increasing prevalence of work-from-home scenarios has increased the number of attack vectors by orders of magnitude. Corporate firewalls are effective at protecting workers on the business network, but IT has virtually no visibility into devices outside the physical workplace. In the first months of COVID-19, many corporate virtual private networks were overloaded with traffic, prompting some employees to disconnect from the VPN and navigate directly to their preferred software-as-a-service application. This increased the risk to their companies, as employee computers that became infected with malware could contaminate their company networks once they reconnected to the VPN.

Attack vectors also constantly change. Cybercriminals are increasingly targeting their victims' hardware to enable them, in some cases, to take control of PCs without users even knowing. Over the past two years, there has been a surge of attacks on PC basic input/output system (BIOS) software and the similar unified extensible firmware interface (UEFI).

"Antivirus software has come so far in identifying risks that the bad guys have been looking at the easier ways to get in, which is through firmware and BIOS," said Patrick Bohart, director of marketing at Intel.



The majority of ransomware attacks no longer originate with phishing emails but come after attackers have already penetrated the network and spent hours or days determining how to do the most damage.

BIOS/UEFI is embedded in the firmware that is physically attached to the motherboard. Changes at that level can't be detected by software; they must be monitored by other hardware components. A typical BIOS configuration has about 300 settings, providing a bounty of opportunities for exploitation. [Gartner has said](#) that by 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability.

Another example of rapid change is two new types of attacks that evade traditional defenses: memory-based attacks and control flow subversion. Memory-based attacks target the call stack or memory registers of an application in non-repeating ways. Because there is no clear pattern to memory alterations, these attacks resist traditional signature-based malware protection, which relies on pattern matching.

Control flow subversion uses code sequences in authorized modules to divert control flow instructions—which govern the order in which instructions in a program are executed—from the original target address to a new target containing malicious code.

One of the best defenses against these and other vulnerabilities is through a multi-layered security approach that defends at both the hardware and software levels.

Hardware-enhanced security features combined with cloud-based remote manageability provide a combination of more protection and visibility. For example, Intel Control-Flow Enforcement Technology is hardware-based protection against multiple classes of attacks, including memory-based attacks and control flow subversion techniques.

Hardware-based protections augment third-party solutions to help prevent machines from being hijacked and subjected to ransomware or crypto mining. They should be augmented by flexible access controls that enable IT organizations to add such features as biometric and multi-factor authentication. The objective is to harden the system at every potential attack vector, including the physical layer.

Secure computing now begins in the factory. Intel's [Transparent Supply Chain](#) ensures that the sources of equipment and components have been vetted for validity and security throughout the manufacturing process and at every stage of the journey through the supply chain. This protects against vulnerabilities being introduced—unintentionally or otherwise—into components before they are assembled into a finished PC or at any point along the way between assembly and delivery to the end-user.

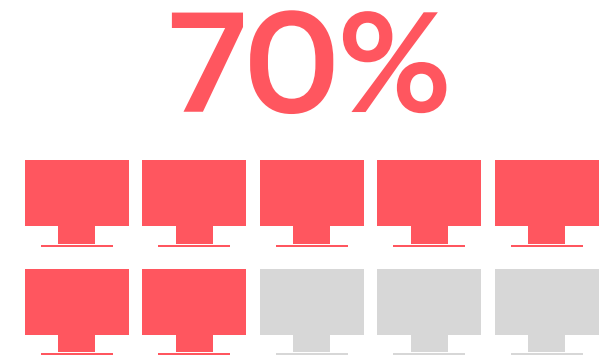
Transparent Supply Chain creates a digital record of the device as it's leaving the manufacturing environment, explains Intel's Bohart.

"It takes snapshots of BIOS, firmware, where it was manufactured, and where it's going," he says. "When the device arrives at the user's home, the provisioning process retakes that snapshot and compares it to the factory. If there's any divergence, the provisioning stops and IT is alerted."

Imminent threat

Source: Gartner Inc.; How to Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds

Percentage of firms expected to experience a breach in 2022 because of a firmware vulnerability:



Managing what you can't see

A global workforce, a mix of device types, and data-intensive applications make managing a modern PC fleet complicated, costly, and time-consuming. Business continuity is at risk when IT doesn't have full visibility into all the devices accessing the corporate network. The proliferation of equipment types, operating systems, and special-purpose devices has made remote, proactive management more challenging.

Remote endpoint management has become an essential capability for all IT organizations, particularly those that administer large populations of mobile and home-based computers. The new hybrid work environment is accelerating the adoption of this technology. Grand View Research expects the global unified endpoint management market to grow more than 32% annually to nearly \$24 billion by 2027. Investments are being fueled by the bring-your-own-device trend, the internet of things, and, more recently, work-from-home.

The global unified endpoint management market is expected to grow more than 32% annually to nearly \$24 billion by 2027.

Features of remote endpoint management

- Automatic distribution and logging of software and security updates to protect against threats
- Remote management over both wired and wireless connections
- Cradle-to-grave device lifecycle management
- Predictive diagnostics to catch problems before they happen
- Running diagnostics and making repairs in the background without disrupting users
- Remote control, even when devices are in standby or sleep mode
- Rebuilds and asset tracking over the network
- Secure power-on for patching and maintenance

Intel Active Management Technology on the Intel vPro platform supports all of these features, either natively or from third-party providers in a complete wireless solution. In addition to remote patching, it provides a cloud-based management console, quick backup, full visibility when recovering remotely, and the ability to download and install patches on user machines without any user involvement.

A platform IT can count on

Given the wide range of devices that IT organizations must support today, it isn't surprising that most prefer to minimize the number of configurations they use. An ad hoc provisioning and maintenance process creates risks that unexpected driver variations may be encountered or that PCs aren't equipped with the latest patches and software updates. The result is increased management complexity and hardware support costs.

Even small changes can create inconsistencies and vulnerabilities that have unintended consequences down the line, though. When purchasing PCs for a large organization, look for guarantees that product configurations will be frozen for a fixed period and that any changes—no matter how small—will be communicated in advance.

Intel Stable IT Platform Program (SIPP), part of Intel vPro Enterprise for Windows, addresses that challenge by aiming to make no major platform changes to hardware, driver, or firmware for 15 months, thus significantly reducing the risk of upgrade incompatibility. The SIPP program has been a cornerstone of the company's strategy to support corporate customers since 2003 and over time has been extended to include additional technologies such as Ethernet, wireless connectivity, Thunderbolt 4, and memory.

Under SIPP, business PCs undergo rigorous design and testing for compatibility with the vPro platform specification. This ensures consistency across OEM-built devices. Intel also engages regularly with OEMs and operating system makers on updated tests and feedback loops.

One way to help ensure stability is with an imaging process that provides a reliable and consistent set of hardware and software features that can be applied to all new machines before they are shipped to users. An image is a master configuration for every computer in the organization. It can be applied to new or recycled machines to give each a reliable and consistent set of hardware and software features. The goal is not to have the latest and greatest features as much as to ensure that all devices can be quickly and easily maintained, repaired, or replaced.

Imaging has other benefits. It enables IT managers to know the exact configuration of every PC in the field so they can optimize support resources and minimize parts inventories. Security is enhanced because patches can be applied to every affected system, often through an automated process. A master image can also be used to restore a PC to a working state in a fraction of the time it would take to load all needed software manually. For example, Intel's [One-Click Recovery](#) can initiate an HTTPS boot to re-image the device. Training and maintenance are also more efficient because fewer system configurations are involved.

PC manufacturers make modifications and updates to their products all the time, often as a cost-saving move when lower-priced components become available. These changes aren't always communicated to customers, even if they are enterprise IT departments.



Imaging enables IT managers to know the exact configuration of every PC in the field so they can optimize support resources and minimize parts.

User priorities: Powerful and portable

The optimal PC user experience combines high performance, vivid graphics, and the flexibility to work anywhere. Here are some key factors to consider in making PC choices that users will love.

Performance is a team sport

Performance today is influenced by many factors other than the CPU. It's also a function of the number of cores used, CPU threading, cache utilization, and the speed of memory and interconnects. An integrated GPU can juice performance by offloading tasks from the CPU. "Including a GPU gives you better form, fit, and function," said Intel's Nordquist. "The PC runs cooler, is less noisy, and is more stable."

Other factors that influence overall PC performance include video processing and network support. Look for native support for the AV1 video coding format, which eliminates the need for an outboard video processor, thereby dramatically speeding up video encoding and decoding, helping improve battery life and lower heat generation.

Sales of PC monitors surged to a record during COVID lockdowns as workers outfitted home offices for maximum convenience, [according to IDC](#). Built-in support for multiple high-resolution monitors on the microprocessor gives users a choice in how they configure displays. Thunderbolt 4 technology also enhances usability by supporting both high-resolution displays and high-performance data transfers through a single port with connectivity that allows multiple devices to be added through daisy-chaining. Thunderbolt is eight times faster than standard USB 3.0 and can charge devices simply and quickly.

Wi-Fi 6/6E is now being widely adopted and should be the standard supported by any new PCs. This high-speed wireless protocol provides greatly improved videoconferencing with ultra-low latency, ultra-reliable connectivity, and up to six times faster speeds at the office (and nearly three times faster speeds at home). Wi-Fi 6 also uses network slicing to allow signals to be dedicated to certain endpoints. That eliminates one of the biggest performance problems of previous Wi-Fi generations, which is the need to share bandwidth.

Mobility experience should match the desktop

Laptop PC sales now outpace desktops by nearly a two-to-one margin, and [Statista forecasts](#) that sales of portable computers will surge to 225 million units in 2021, up more than 60% from four years ago. The shift to hybrid work is expected to accelerate this trend as more users require PCs that can easily move between home and office locations.

Mobile computing has long meant trading off performance and functionality for portability. Older machines limit users' ability to collaborate and multitask. They bog down IT organizations with repairs and performance tuning. Factors such as limited battery life, weight, and processors that sacrifice responsiveness for power efficiency have long inhibited the "work from anywhere" style of today's mobile workforce.

Recent innovations are closing the gap, though. Users should no longer have to compromise on speed or crawl around on airport floors looking for a power source. New laptops are also more than just scaled-down versions of desktop PCs; they are optimized for the uses mobile users need most.

How AI is revving up PC performance

Artificial intelligence is now enhancing user experience by dynamically adjusting system resources. For example, Intel vPro processors use machine learning to improve cache utilization, reducing potential bandwidth bottlenecks. AI also maps out the most efficient use of CPU threads for the characteristics of the applications in use.

Another example of intelligent resource management is Intel's **Performance Maximizer** software, which continually analyzes a PC's workload and makes adjustments such as overclocking the CPU dynamically or shutting down unused functions to reduce cooling demands, extend battery life, and mitigate wear on components.

AI can also help to reduce CPU and GPU stress by applying each processor more efficiently to ensure software, memory, and network stability. Some new processors combine GPU and CPU functionality on the same chipset. This creates a powerful foundation for intelligent task distribution by offloading functions such as repetitive calculations to GPUs, which excel at that task. GPUs provide codex support for such tasks as videoconferencing, for example. Integrated GPUs typically also use less power and create less heat, which aims to provide longer battery life.

Intel's 11th Gen Core Processors introduced such innovations as autonomous dynamic voltage and frequency scaling, which dynamically matches the system-on-a-chip's frequency and voltage to the bandwidth of the workload to deliver the most power-efficient operation. Intel Thread Director—a new hardware feature of [12th Generation Intel Core processors](#)—has been added to assist the OS scheduler to allow the system to make more intelligent and data processing decisions regarding thread scheduling.

These days, mobile users also need platforms optimized for videoconferencing. An onboard Gaussian and Neural Accelerator (GNA) in Intel microprocessors applies neural noise cancellation to reduce background noise and blur videoconference backgrounds for a more secure and professional experience. The availability of these features as part of the microprocessor reduces performance overhead and broadens the range of use case scenarios.

[Intel Evo](#) is a recently introduced design specification that OEMs can use to create laptops that meet the requirements outlined above. The specification

was derived from extensive research into how people use laptops and aims to address the most common frustrations of mobility. To become Evo-certified, candidate laptops must meet these criteria:

- Deliver at least nine hours of battery life on a 1,080-pixel resolution screen
- Wake from sleep in less than one second
- Perform the same whether plugged in or on battery
- Deliver at least four hours of battery life from a 30-minute charge
- Include Wi-Fi 6 and Thunderbolt 4 connectivity

Devices on Intel vPro, an Intel Evo Design include advanced microphone and camera technology for video collaboration as well as thermally efficient form factors and ultra-light portability. Backed by the vPro platform, the devices are also stable, secure, and easy to manage.

Cross-industry validation of rigorous use cases and hardware interoperability help keep systems stable, even in variable system environments.

Be wary of benchmarks

Many PC makers cite benchmark statistics as evidence of machine performance. However, tests in a lab don't accurately represent performance for real-world scenarios. Look for performance measurements that are relevant and address specific needs. For example, the SYSmark benchmark approximates a business/productivity workload on a system, while SPECint and SPECfp focus on the computational performance of the processor.

Intel representative usage guides (RUGs) are an alternative to traditional benchmarks that demonstrate real-world performance on machines running everyday tasks, ranging from video uploads to video collaboration. They capture the end-user experience by simulating actual workflows for use cases like content creation, collaboration/videoconferencing, and productivity applications using the latest software and applications as well as platform capabilities that provide a more comprehensive performance story.

What a modern laptop can do

Partners who are building to the Evo specification are already shipping units with unprecedented combinations of performance and power efficiency. For example:

- **Dell's three-pound Latitude 9520** uses AI to adapt performance levels to use and a PC proximity sensor that detects a user's presence and instantly logs in. It delivers a stunning 34 hours of battery life and charges to 80% capacity in 40 minutes.
- **Lenovo's ThinkPad X1 Titanium Yoga**, which is based on an Intel 11th Gen vPro processor, provides 2,256 X 1,504 video resolution, up to 1TB of SSD storage, and nearly 12 hours of battery life in a unit that weighs less than 2.5 pounds.
- The **HP Elite Dragonfly** starts at less than 2.2 pounds and features such security innovations as a one-button camera mask, privacy screen technology that prevents viewing from an angle, and a battery that charges to 50% in just 30 minutes.

Sustainability

At a time when environmental concerns have never been more pronounced, responsible makers of computers and components are doing everything they can to reduce the carbon footprint of their products.

The issue is top-of-mind for customers as well. Nearly two-thirds of respondents to a recent Forrester Consulting survey of IT leaders found that expanding sustainability initiatives is a critical or high-priority goal and was the most often cited “critical” priority. Top sustainability goals include reducing emissions, ensuring responsible supply chains, achieving net-zero waste, and harnessing renewable energy. The study also found that organizations classified as “high maturity” firms are more likely to avoid partners that don’t engage in sustainable practices, invest in end-of-life refurbishing, or demonstrate corporate transparency.

Sustainability begins in the factory, which is responsible for [more than 80%](#) of the carbon footprint generated by a laptop computer. Factories are major users of power and water, and the manufacturing process for computer products also involves chemicals that could be toxic if introduced into the environment. Reducing emissions involves three critical steps: making the manufacturing process more sustainable, providing for optimum power efficiency in the field, and enabling responsible end-of-life asset retirement.

Green energy initiatives are showing great promise in reducing electrical consumption. For example, Intel derives 100% of its power needs from green sources in the U.S., Europe, Israel, and Malaysia. The company [operates 18 on-site solar plants at its facilities](#) annually. In manufacturing, the company has reduced direct emissions and indirect emissions from the generation of purchased energy by 28% since 2000. It also conserved 7.1 billion gallons of water in 2020 and sends just 5% of total waste to landfills. The company has furthermore set a goal to become 10 times more energy-efficient by 2030.

By working hand-in-hand with component suppliers, PC makers are achieving significant gains in overall efficiency. For example, system-level power consumption for 11th Gen Intel microprocessors is 44% lower than previous generations. Notebook CPU energy efficiency has increased 14-fold since 2010, and initiatives like Evo hold participating vendors to high standards of battery efficiency. By adopting technologies like AMT, manufacturers can reduce the need for customers to send repair technicians out on the road for maintenance.

“If I’m green IT, I can shut off all my devices for the weekend and restart them on Monday,” said Cathy Spence, Senior Principal Engineer at Intel. “The ability to turn machines back on isn’t easy, but it’s a unique feature we enable.”

If sustainability is a concern for your organization, look for companies that are part of the Environmental Protection Agency’s [Green Power Partnership](#). The Global Electronics Council’s [EPEAT Registry](#) also scores individual products according to their sustainability performance.



Intel operates
18 on-site solar
plants at its
facilities.

Summary and recommendations

The process of buying and managing PCs becomes more complex every day. As organizations transform themselves around digital technologies, the choice of reliable, secure, and high-performance PCs will be a critical role for IT organizations. Buyers should look for suppliers with enterprise track records and technology at the core that is built for enterprise use. Among the factors to consider are the following:

- The company uses components from suppliers with a track record of excellence.
- Full supply chain visibility is provided.
- Enterprise-quality support is available.
- Systems support a full range of remote management capabilities, including power-on and automatic update/patch installation.
- There is support for the latest communication technologies, like Thunderbolt 4 and Wi-Fi 6.
- Laptops are Intel Evo-certified.
- Outboard or microprocessor-resident GPUs are included.
- Security is provided down to the BIOS level.

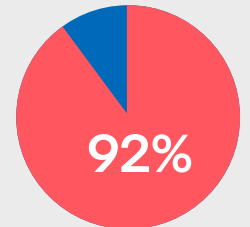
Intel vPro is built for business and it offers the most capabilities for client commercial use cases across the four pillars of performance, manageability, security, and stability. Its effectiveness at meeting the needs of corporate customers has been established by customer feedback and third-party research. Forrester Consulting found that the Intel vPro platform delivers payback in as little as nine months across a composite organization of 100,000 PCs. In addition, 92% of IT professionals who were surveyed said standardizing on vPro made their laptops and desktops more secure, 74% said the adoption of vPro had reduced management costs, and 90% said Intel support and add-on solutions enabled by vPro delivered significant value.

Regardless of the PC platform you choose, look for providers that source components from suppliers that understand the needs of the enterprise—because what’s inside counts.

Better security with Intel vPro

Source: Forrester Consulting

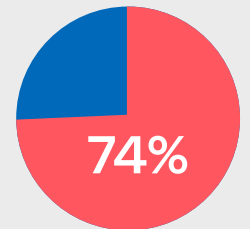
IT pros who feel the vPro platform makes their laptops and desktops more secure



Reduced costs

Source: Forrester Consulting

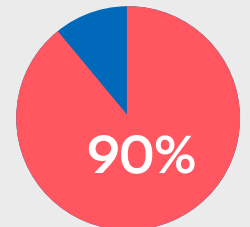
IT professionals who stated the vPro platform has reduced their management costs



Delivering value

Source: Forrester Consulting

IT professionals who believe Intel support and add-on solutions enabled by the vPro platform deliver significant value



Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex.

No product or component can be absolutely secure.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

For more information about the Wi-Fi 6 data presented, visit www.intel.com/wifi6disclaimers

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.