White Paper

Public Sector Client Computing

Maximizing Your PC Investments

Best practices for the public procurement of PC client devices

Authors

Bryon Wirtz
Government Segment Sales Manager, CCG Sales

Larry Rother
Director, Public Sector Commercial Client

Table of Contents

Executive Overview

The technology procurement landscape, always complex, is becoming more so as AI adoption accelerates. The government's responsibility to appropriate funding optimally and transparently creates immense pressures, especially when critical missions and citizen services hang in the balance. These pressures lead to ambiguity without clear direction amidst disparate industry advice. By using guidance from one of the world's leading digital computing providers, Intel, governments can better leverage technology to meet the expectations and needs of their constituents and operate efficiently.

Background

As a PC technology provider for over 50 years, Intel has seen many different public procurement processes and their corresponding outcomes. Intel has recognized three recurring themes in procurement processes that have helped government agencies and departments meet, or even exceed, their PC procurement objectives and come within or even under budget. This document will review those best practice concepts and cut through the noise to simplify each government entity's journey towards an optimal PC procurement outcome.

Intel's Public PC Procurement Best Practice Observations:

PCs are a critical part of modernization / digital transformation efforts – think of the client device as a strategic procurement element, not just something to refresh at the lowest cost, but rather an asset that can help an organization meet its goals.

Not all PC characteristics should be considered equally – device security and system performance should be foundational considerations, and needs can vary by device usage.

Use the organization's RFP structure/procurement process to ensure needs are met at the best value – aim for vendor-neutral device specifications along with clear award-scoring methodology to incentivize fair and open competition aligned with stated objectives.

Check out **TABLE 1** for a summary of Intel's procurement recommendations aligned to the above concepts.

Observations:

PC Clients Are a Critical Part of Modernization and Digital Transformation

As the world adapts to AI's increasing presence and technology plays a growing role in daily life, many governments around the globe are undertaking massive digital transformation and modernization efforts. Whether a department or agency is exploring artificial intelligence (AI), Internet of Things (IoT), or even preparing students to be the workforce of the future, the PC is a critical element in those endeavors. Today, more than ever, PCs are needed for the creation, interpretation, and processing of data required to provide citizen services and deliver mission outcomes to public and private stakeholders.

While data fuels technology and digital transformation, PCs also have a central role. As the primary interface between humans and technology, PCs are a critical element of transformation models. Whether deploying or designing digital modernization frameworks, public sector entities will surely include the client device in their project scopes and objectives. In fact, to optimize the end-user computing environment, it makes sense to start by reexamining and refreshing the client fleet. Doing so simplifies adopting transformative innovations, keeping pace with regulatory changes, and deploying the latest operating systems. Microsoft's October 2025 end of support for Windows 10 makes PC refresh an especially timely topic. Windows 11 is the most secure Windows yet. PCs still using Windows 10 after that date may become more vulnerable to ever-evolving security risks[1], and many older devices may not meet the minimum hardware requirements to upgrade. Organizations will need to upgrade both OS and supporting hardware to avoid potential disruptions.

Learn more about **Microsoft Windows 10 End of Support here**

Not only is the PC critical for advancing transformation initiatives and goals, but even steady-state environments might not be so steady. It is essential to ensure that devices continue to be an asset rather than a hindrance by refreshing the organization's fleet in a timely manner. The "if it isn't broken, don't fix it" mentality for devices that are responsible for citizen and defense services (and their data) around the globe gets to be a harder and harder position to take without calculated risks.

Another consideration is that the rapidly changing threat landscape means **security will remain a top focus**. Security in every aspect of the infrastructure and compute endpoints must be a priority without compromising performance. This reality calls for resilient, proactive device management strategies and solutions to maintain security for a dispersed workforce.

As the world saw during the July 2024 massive global PC outage, caused by a faulty software update, swift and efficient remediation tools are essential. These tools help organizations return to normal operations quickly when the unexpected happens, as it surely will. Security solutions and PC hardware resiliency now play key parts in many disaster recovery plans, as organizations have realized how essential maintaining a healthy PC fleet is to mission success.

Waiting too long between device refresh cycles can lead to increased total-cost-of-ownership impacts, primarily due to increased support costs, productivity loss, and increased security vulnerability exposure. Intel's IT department recommends a 3- to 4-year refresh cycle when the devices are meeting a department's needs on a day-to-day basis.[2]

When preparing for a refresh, organizations should carefully consider the performance and security requirements of likely use cases, which may differ across departments and agencies. Tables 1 and 2 offer lists of specific technologies to help government agencies and departments optimally meet these varied requirements.

Learn more about **Modernizing Windows Client Management**

The PC is a strategic IT asset that can impact an organization's ability to meet mission goals and serve its citizens at the levels needed to be relevant in an increasingly complex and data-driven global environment.

Not All PC Characteristics Are Equal

A car analogy illustrates the difference between critical procurement considerations and "nice-to-have" specifications. Buying a car requires evaluating many features. Most prospective buyers would agree that a car's engine function and safety rating are significantly higher in importance than the car's paint color. The same concept applies in PC procurement. The screen display size, among other choices, does not mean much if the device leaves the user and/or organization exposed to increased security vulnerabilities or if the device does not work for its intended usage. Therefore, Intel recommends **device security** and **system performance** as critical salient characteristics that should weigh heavily in an organization's procurement framework. (Note: The latter concept is covered in the third section of this document.)

End-user computing innovations are driving new efficiencies and modernizations in the public sector, including:

Industry-specific trends	New end-user capabilities required	IT issues in meeting the requirements
▪ Growing use of AI and computing at the edge ▪ Need to deploy new, mission-focused services or support new learning models ▪ Need to increase productivity and efficiency ▪ Rising security threats and privacy concerns ▪ Growing use of geographic information systems (GIS)	▪ Cost-effective performance at varying levels ▪ Hardware-based, resilient manageability and disaster recovery solutions ▪ Ability to adopt AI tools seamlessly ▪ End-to-end data security and privacy protection, supply chain assurance ▪ Mobility for field employees, students, teachers	▪ Budget constraints ▪ Complex procurement cycles, rapidly changing requirements ▪ Vendor lock-in and choice ▪ Evolving geopolitical landscape and regulations, supply chain uncertainty ▪ Aging, complex infrastructure

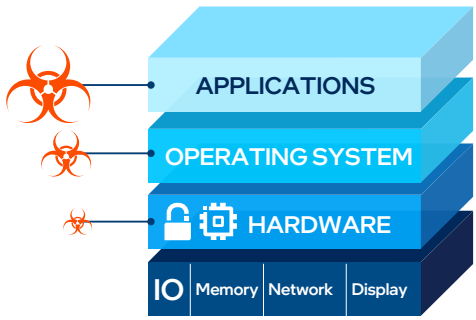
Why Device Security Matters

News of major security breaches suggests that security can no longer be an afterthought in PC purchase decisions. The public sector remains a top target. Particularly as remote and hybrid work have surged, end-to-end security from the cloud to the edge and employee devices has become paramount.[3]

In 2025, the public sector faced a significant rise in cyberattacks, with the global average weekly cyberattacks per organization reaching an all-time high of 2,683 in a 17 percent increase over 2024.[4] This highlights the need for stronger cybersecurity measures. While the focus typically has been on security software to protect assets, and security software remains key, sophisticated attackers increasingly are looking for vulnerabilities that may exist at the firmware level.[5] One recent survey found that 85 percent of public sector respondents agree that a security breach of their organization could endanger lives, especially if critical or emergency services go down.[6] This trend suggests that in designing an upcoming PC purchase, the security of edge devices (including PCs, personal devices, and IoT) likely will rank at or near the top of the priority list. Hardware-based security features further harden security defenses and can be an important consideration for government agencies and departments deciding when devices need to be refreshed. These features play an indispensable part in addressing emerging security threats.[7]

As noted earlier, cyberattacks have been moving deeper into the hardware and even into the supply chain. Because counterfeit components bring significant risk, the protection of the supply chain has become an increasingly important consideration.[8,9] IT decision-makers purchasing PCs face challenges in confirming the provenance of their processors. Many of these frameworks and tenders, aiming at enhancing supply chain security, use the country of origin (COO) to determine where a product is sourced.[10] However, the COO often does not address where the components of a product come from, or what happens to a device during shipping and warehousing after it has been assembled.

Building these considerations into an organization's PC procurement framework will help to minimize device vulnerabilities and maximize the potential return on PC investment.



Learn more about the **hardware-enabled security provided by Intel® technologies here**

Learn more about **Intel vPro® Security here**

Why System Performance Matters

When it comes to spending public funds optimally and efficiently, it's critical that systems match their intended usage to avoid the inefficient use of limited resources. PCs are designed for a wide range of uses, so thoughtful consideration of the workloads needed to meet mission goals must be mapped to the right hardware to achieve the best use of resources. IT decision-makers should consider the overall device experience when making technology decisions. This includes both the persona and workload/application usage. Adequate system performance is critical to achieving the expected experience.

Examples of Common Usage Personas

Mainstream | Premium | High Performance

Operation and Administration	Field-Based Critical	Mission Execution	Data Analysts and Research
▪ Multitasking ▪ Video Collaboration ▪ Productivity	▪ Limited Connectivity ▪ Battery Life ▪ Situational Responsiveness	▪ Processor Speed ▪ Screen Size ▪ Battery Life ▪ Anywhere Productivity	▪ Performance ▪ Application Compatibility ▪ Data Privacy

Intel recommends aligning device usage models with their matching system performance needs. See **Table 1** for additional information on how to drive this alignment.

As mentioned previously, different agencies and departments have varying usages for PCs, ranging from simple data entry to powerful workstations in charge of highly complex modeling. New usages are also emerging with the fast adoption of artificial intelligence (AI). Organizations are deploying AI to optimize IT operations and improve operational outcomes. For end users, some AI workloads run in the cloud and others, like inference for generative AI, run best on a PC. For this reason, many workloads operate a hybrid model where part of the processing is done in the cloud and part is done on the device. A new class of PCs has been introduced with a processor architecture specially optimized to run AI workloads locally. They are called AI PCs and include a CPU, GPU, and NPU, the latter being specifically designed for AI tasks. This "xPU" architecture enables faster and more efficient processing of AI workloads locally on the device rather than relying on cloud services. The benefits are lower latency (no round trip needed to the cloud and back), better privacy (data remains local), enhanced productivity (automate repetitive tasks), and better battery life (with AI-powered features that optimize energy consumption). This example demonstrates the tight connection between experience and performance.

Leveraging the PC to support AI workloads offers several advantages:

- **Lower latency and swift response times**—to facilitate more real-time AI experiences.
- **An additional layer of privacy and security**—possible because data is processed locally.
- **Increased personalization and customization**—attainable when models are customized using data specific to the individual.
- **Potential cost savings (lower SaaS cost)**— achievable as AI and machine learning become ubiquitous in client apps.
- **Offline and field-based decision-making**—running workloads locally eliminates the need for a network connection and enables high-quality decision-making right where the device is.

Understanding the different underlying technology needs for each workload is critical to maximizing the value of an organization's technology investments. Intel recommends ensuring procurement frameworks outline the performance needs for the devices in accordance with their usages. While there are hundreds of device use cases, above are four widely utilized usage personas that help guide an expected device performance level. Referencing these use cases can assist IT decision-makers with ensuring that vendor RFP responses match their planned usage and user experience and will best meet mission objectives most effectively.

RFP Recommendations for Performance Benchmarks

Documenting performance requirements is a fundamental step in designing any tender or RFP. In the past, physical metrics such as frequency and core counts were used as proxies for performance. However, these no longer accurately represent system performance. Some hardware specifications (such as TOPs) can be misleading. Intel recommends the use of commercial benchmarks that provide **verifiable performance outcomes** running specific meaningful workloads. To make an informed purchasing decision, it is essential for buyers to conduct benchmarks that reflect their unique usage patterns and requirements.

With the emergence of AI and multiple processing units on a PC, considering benchmarks that attempt to model real usages and track system-wide performance can lead to highly relevant information.

CAUTION: Not all benchmarks represent overall system performance in an enterprise environment. Some measure specific aspects of a system that may or may not be relevant to an organization, so care must be taken when weighing how to use benchmark scores. Intel and BITKOM recommend using benchmark tests that are:

1. Real, **Relevant,** and **Popular,** representative of the actual intended usage of the device
2. **Reproducible,** not predicting an outcome, and up to date
3. **Reliable,** with unbiased and quality input[11]

This document groups benchmarks into four categories that cover system performance: productivity, professional software, AI and machine learning, and battery life. Intel recommends using a basket of benchmarks to evaluate overall performance, as illustrated below.

Real-World Commercial Benchmarks

Productivity	**Procyon® Office Productivity**	The benchmark from UL Solutions uses Microsoft Office applications to measure Windows PC and Apple Mac performance in office productivity tasks.
	CrossMark	CrossMark is an easy-to- run native cross-platform benchmark that measures the overall system performance and system responsiveness using models of real-world applications.
	Web XPRT4	WebXPRT will run a series of tests to measure your browser's HTML and Javascript handling, as well as tasks like photo manipulation and face detection.
Professional	**Spec Workstation 4.0**	The benchmark targets the diverse needs of engineers, scientists, and developers who rely on workstation hardware for daily tasks by including a comprehensive set of tests.
	Procyon® Photo Editing	This multi-platform benchmark measures performance using Adobe® Lightroom® Classic and Adobe® Photoshop® in a typical photo editing workflow that includes batch processing and image retouching.
	Procyon® Video Editing	The UL Procyon Video Editing Benchmark uses Adobe Premiere Pro in a typical video editing workflow.
AI & Machine Learning	**MLPerf Client**	This is a benchmark for Windows and macOS, focusing on client form factors in ML inference scenarios like AI chatbots, image classification, etc.
	Procyon® AI Text Generation	This benchmark provides a more compact and easier way to repeatedly and consistently test AI performance with multiple LLM AI models.
	Procyon AI Image Gen	This benchmark provides a consistent, accurate, and understandable workload for measuring the inference performance of on-device AI accelerators.
	Procyon AI Computer Vision	This benchmark measures the performance of dedicated AI processing hardware and verifies inference engine implementation quality with tests based on common machine-vision tasks.
Battery Life	**Procyon Office Productivity Battery Life**	This benchmark uses Office apps to simulate a working day. The benchmark uses Word, PowerPoint, Excel and Outlook to run workloads in a loop and can factor in different screen brightness levels.
	Mobile Mark 30	This is an application-based, performance-qualified battery life benchmark. In addition to reporting battery life, the Index provides an easy-to-understand composite score that factors in both performance and battery life.

Benchmark results can come from multiple sources and be interpreted differently. Intel recommends running benchmarks directly, whenever possible, to guarantee the most consistent and realistic results. Aspects to be aware of when looking at benchmark databases include the following:

- What is the system hardware configuration? System configuration can significantly impact scores, even more so for benchmarks that examine a specific workload on a specific device.
- How was the benchmark run? Benchmarks can be run from different OS images with different applications running in the foreground and background. Other settings, like screen resolution and battery/performance, can greatly impact results.
- How is the database populated? Suppose anyone can submit results to a database. In that case, the average score is likely shifted lower because benchmarks will be run in a wide variety of unknown configurations, leading to scores spreading out and generally shifting lower.
- How many results are available? Too few results may result in skewed results due to a small sample size's ability to influence the average. Many results also tend to shift scores lower as described in 3 above.

How should a government agency or department put its performance needs and expectations into a request for proposal (RFP)? Intel aligns with the worldwide industry best practice of using system performance benchmarks as outlined by the BITKOM technology consortium and the OECD organization.

"The continuous evolution of computer technology has made it increasingly difficult to compare the performance of individual systems only in terms of technical specifications. For instance, a processor with a higher clock rate does not necessarily provide more processing power. The fact that clock rate (frequency) alone is no longer sufficient to compare the performance of different processors from different manufacturers with distinct internal architecture has led to the development of tests, so-called benchmarks, to improve the comparability of the performance. The restriction to certain technical peculiarities of system components no longer suffices to make an informed decision in the context of an award process ."[12]

Bitkom, Vendor-Neutral Tendering of Notebooks

The BITKOM industry consortium represents more than 2,200 ICT companies, including major technology vendors like Intel, AMD, and NVIDIA, as well as government agencies, with the purpose of creating one voice for optimal public IT procurement frameworks.[13] The consortium has published vendor-neutral procurement frameworks that meet strict European Union (EU) legal standards and that can also scale around the globe as best practices.

Check out BITKOM's **latest 2022 product-neutral tendering of notebooks here** and their **2022 desktop version here**

Learn more about **BITKOM by visiting their site here**

Using system performance benchmarks is BITKOM, OECD's, and Intel's recommended path to compare systems and align performance needs with device usages.

"Contracting authorities should avoid using brand names when procuring computers and favour the use of technical standards and benchmarks to allow comparisons of the performance of computers and their components."[14]

OECD, Good Practices for Procuring Computers and Laptops in Latin America

The OECD is an international organization with 38 members currently that works to promote economic development and build better policies for better lives.[15]

Check out **OECD's Good Practices for Procuring Computers and Laptops in Latin America here**

For the usage personas outlined previously, Intel recommends using the CrossMark benchmark, which meets the criteria for trusted benchmarks and is grounded in real-world business applications and workloads. This means that the CrossMark benchmark measures the system performance and responsiveness in scenarios most reflective of actual device usage. Table 1 shows how organizations can use the CrossMark system benchmark scores to set measurable and enforceable performance expectations by device usage model, helping ensure the optimal use of limited resources.

The CrossMark benchmark was developed and continues to be managed by a non-profit industry consortium, BAPCo, which works with over 30 countries to create informed PC procurement specifications.[16,17] BAPCo even has a government network program where qualifying government agencies or associations can provide benchmark development feedback, obtain free licenses, and receive priority technical support.[17]

Learn more about the **BAPCo Government Network program here**

To learn more about the latest CrossMark benchmarks, read the **CrossMark 2022 white paper here**

Government entities will achieve the optimal value from public funds by prioritizing device security and system performance benchmarks above other component features.

Benchmarks Best Practices Summary

- Use a suite of benchmarks to ensure a complete system performance assessment.
- Run benchmarks with a clean OS and again with a full IT image installed.
- Know what the benchmark does and does not measure.
- Understand how to interpret results, especially 3rd party databases.

The Importance of Sustainable Technology

While security and performance are top priorities of IT decision-makers, 70 percent say that defining their environmental, social, and governance (ESG) strategy and expanding on sustainability initiatives is a high or critical priority.[18] This finding, from a Forrester study commissioned in 2024, makes sense as decision-makers frequently are tasked with helping their organizations meet ESG goals.

When evaluating options and assessing the overall carbon footprint, it is beneficial to consider the full lifecycle of the product as well as energy efficiency based on real-life applications. Each phase of the lifecycle matters, from sourcing and manufacturing to packaging, device usage, and finally, reuse or recycle options.

Intel recommends the following procurement considerations for decision-makers:

- Take a lifecycle approach: analyze emissions at every level of the product lifecycle.
  - Verify manufacturing carbon footprint at the OEM website.
  - Analyze energy efficiency—opt for trusted benchmarks and labels like ENERGY STAR.
  - Consider the repairability of the system/components you are choosing.
  - Verify what recycling/takeback options are available at the end of the device lifecycle.
- Leverage industry-recognized standards like EPEAT and TCO that can help reduce complexity when making decisions. These labels take a lifecycle approach to sustainability and are independently verified.
  - Note that 98 percent of Intel vPro® devices registered on EPEAT are Silver or better.[19]
- Choose remote manageability capabilities to reduce emissions associated with IT operations—reducing desk-side visits/truckrolls can avoid significant emissions.
- Opt for trusted suppliers—look for suppliers committed to reducing emissions and environmental impact.

The Importance of Securing Supply Chain Integrity and Reliability

Ensuring the manufacturing provenance of hardware is critical for organizations to minimize financial losses, reputation damage, system downtime, and downtime during recovery due to counterfeit-related hardware risks. When evaluating options, consider devices that provide a digitally attestable chain of custody of each chip's progress through the chip manufacturing process.

The Intel® Assured Supply Chain (Intel® ASC) program is a specialized client system-on-chip (SoC) solution that provides a digitally attestable chain of custody of each chip's progress through the chip manufacturing process.

Intel ASC leverages a pre-determined end-to-end silicon manufacturing corridor for Intel vPro-eligible SKUs. Each SKU has an Intel ASC identifier embedded at the silicon level. IT organizations can use industry tools to read this identifier and view the list of specific locations where the CPU has been manufactured.

Intel ASC encompasses every step in the silicon manufacturing process, including fabrication, die prep and sort, assembly, test, and warehousing. By safeguarding the supply chain, Intel enhances the stability of its products, offering businesses confidence in the authenticity and dependability of their hardware investments.

To learn more about Intel® Assured Supply Chain, read the **product brief here** and **FAQ here**.

How to Use the RFP Structure to Ensure the Organization Gets Optimal Value for Needed Purchases

Once PC procurement is treated as a strategic investment decision, with device security and system performance as paramount considerations, the organization can adopt evaluation criteria for an RFP based on these considerations. This helps to ensure that proposals received will meet or even exceed expectations.

Setting up a successful procurement cycle begins with aligning the budget to organizational priorities and objectives. Then the RFP structure should reinforce the identified objectives, from minimum requirements that all device submissions should meet to maximum system costs. The RFP scoring system can be a useful tool that sets the organization up to achieve optimal value systems from vendors by creating requirements that work together to provide the best solution at the cost. Table 1 provides an example.

Conclusion

Intel believes that client procurement outcomes for the public sector are maximized when the PC is treated as critical for mission and citizen services outcomes, and when hardware-based device security and system performance benchmarks are built into RFP structures as key decision elements.

Table 1: Intel's Optimal Value PC Specification Recommendations

The structure below is an example only of structuring device security and system performance into an RFP; each department/agency should evaluate its unique procurement objectives.

Example structure: The highest-scoring system within budget is awarded the bid; overachievement points are set for critical device security and system performance.

Common Use Cases						
Specification Category	**Eval. Type**	**Over-Achievement Award**	**Operation and Administration**	**Field-Based Critical**	**Mission Execution**	**Data Analysts and Research**
General Usage Description			▪ Multitasking ▪ Video Collaboration ▪ Productivity	▪ Limited Connectivity ▪ Battery Life ▪ Situational Responsiveness	▪ Highest Processor Speed ▪ Screen Size ▪ Battery Life ▪ Anywhere Productivity	▪ Performance ▪ Application Compatibility ▪ Data Privacy ▪ AI Training and Fine-tuning
Typical Form Factor for Usage Model			▪ Notebook ▪ 2 in 1 ▪ Desktop	▪ Notebook ▪ 2 in 1	▪ Notebook ▪ 2 in 1 ▪ Mobile Workstation	▪ Mobile Workstation ▪ Stationary Workstation
System Performance	Min	Extra X points for every X% incremental points beyond the minimum	▪ Procyon Office Productivity ▪ CrossMark ▪ Minimum score of XX points			
AI Performance	Min	Extra X points for every X% incremental points beyond the minimum	▪ MLPerf Client ▪ Procyon® AI Text Generation ▪ Procyon AI Image Gen ▪ Minimum score of XX points	When evaluating AI Performance, first establish the parameters you want to measure, what AI engine to target (CPU, NPU, GPU) and the desired level of precision (Int8, FP16, FP32), then define the minimum score requirement.		
Device Security	Min	Extra points X for hardware-based below-the-OS security capabilities	Security capabilities that ensure platform integrity and trusted execution along with application and data protection and threat detection are recommended. Security requirements should be determined based on needs and priorities and may consider industry standards such as FIPS, NIST and DFARS. To learn more about technology solutions that strengthen device security, see **Intel Security solutions.**			

For additional considerations, reference **TABLE 2** and the BITKOM framework. Check out **BITKOM's latest 2022 product-neutral tendering of notebooks paper here**

Check out **BITKOM's product-neutral tendering of desktops paper here**

Table 2: Intel® Technologies to Consider for your PC Investment

Technical Capability	Recommended Intel® Technologies	Nonproprietary Value	Intel Advantage
Performance (Architecture)	Performance Hybrid Architecture	CPU architecture that utilizes different types of cores within the same CPU complex.	The enhanced architecture of Intel® Core™ Ultra processors allows workloads to be placed on different types of core types based on how PCs are actually used: Performance cores (P-cores) are designed to handle the most demanding business workloads. Efficient cores (E-cores) are ideal for handling the typical IT tasks that run in the background of business PCs– with minimal impact to user experience.
Performance (Platform Stability)	Intel® Stable IT Platform Program (Intel® SIPP)	Platform validation that aims for zero changes to key system components for at least 15 months or until the next generational release.	Maintains platform stability throughout the buying cycle, aiming for zero hardware changes for 15 months from first availability or until the next generational release. A full corporate platform validation program for devices running Windows 10 and Windows 11 .
Security	Intel vPro® Security	MITRE ATT&CK framework mapping for hardware-based security features.	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Intel vPro® Security provides the only real-time PC fleet hardware security visibility aligned with MITRE ATT&CK threat mapping.[20]
Security (Threat Detection)	Intel® Threat Detection Technology (Intel® TDT)	Intelligent security capabilities that provide AI- and hardware-based monitoring of applications to help improve detection of advanced cyber exploits such as polymorphic malware, file-less scripts, cryptojacking, ransomware, and other targeted attacks – in real time, with minimal end-user impact.	Intel® Threat Detection Technology (Intel® TDT) with Anomalous Behavior Detection (ABD) provides hardware-based monitoring of applications to identify early indicators of attacks, while also leveraging the GPU to offload the high compute requirements.
Security (Platform Protection)	Intel® Platform Trust Technology (Intel® PTT)	Hardware-based method to help store keys, passwords, and digital certificates securely and enable trusted boot and seamless platform updates.	Intel PTT offers capabilities of discrete Trusted Platform Module 2.0 (TPM 2.0) to help store keys, passwords, and digital certificates securely and enable trusted boot and seamless platform updates. Intel PTT supports BitLocker for hard drive encryption and supports all Microsoft requirements for firmware TPM (fTPM) 2.0.
Security (Hardware-hardened Security)	Intel® Total Storage Encryption (Intel® TSE)	Hardware-based, inline storage encryption capability providing security hardening and accelerated performance for Microsoft BitLocker.	Strengthens data protection without compromising performance by offloading disk encryption workloads from the CPU to a dedicated SoC-based hardware engine. Intel TSE safeguards encryption keys below the operating system layer, reducing the attack surface and helping prevent key exposure from software-based attacks through the use of hardware-wrapped keys. Uses AES256 encryption, incorporating postquantum–resistant design principles to help ensure long-term resilience. Works seamlessly with Microsoft BitLocker on supported versions of Windows.
Manageability	Intel® Fleet Services with Intel® Active Management Technology (Intel® AMT) Available with Intel vPro only For Windows only Requires provisioning before use	Software-as-a-service product designed to provide easy-to-use, below the OS, out-of-band manageability including the ability to execute full , graphical remote control of computing endpoint over an Ethernet or Wi-Fi connection, regardless of OS state and power state.	Software-as-a-service product hosted by Intel that is designed to provide IT professionals with an easy-to-use, Intel-hosted solution for leveraging hardware-level management of Intel vPro platforms, eliminating the need to run your own server. Intel vPro Fleet Services, with only a few steps, brings complete remote manageability to an entire organization, allowing administrators access to devices remotely from anywhere, including those with a non-responsive OS. Intel® AMT builds on the DASH standard to enhance the features and scale to enterprise-class deployments.
Connectivity	Intel® Wi-Fi 7 (5 Gig)	High-speed Wi-Fi 7 wireless connectivity to access channels in 6 GHz and 5 GHz bands, supporting industry standard IEEE 802.11 BE.	Wireless connectivity that's faster than many wired networks at speeds exceeding 5 Gbps. Discrete Wi-Fi 7 support means you can access high-speed Wi-Fi channels in the 6 GHz and 5GHz bands and count on lightning-fast responsiveness with 60 percent lower latency than Wi-Fi 6.[21]
Sustainability	EPEAT Standard Support ENERGY STAR 9.0 Support	The device must meet the criteria set for EPEAT ecolabel at silver or above level. The device must meet energy-efficiency criteria set by the ENERGY STAR organization.	98% of Intel vPro devices registered on EPEAT are Silver or better, with 80% achieving Gold certification.[22] Up to lower total energy consumption on Series 3 Intel® Core™ Ultra-based notebooks than ENERGY STAR 9.0 requirements.[23]

(continued on next page)

Table 2: Intel® Technologies to Consider for your PC Investment *(continued)*

Technical Capability	Recommended Intel® Technologies	Nonproprietary Value	Intel Advantage
Supply Chain	Intel® Assured Supply Chain (Intel® ASC)	Supply Chain solution that provides a digitally attestable chain of custody of each chip's progress through the chip manufacturing process.	The Intel® ASC program is a specialized client system-on-chip (SoC) solution that provides a digitally attestable chain of custody of each chip's progress through every step of the chip manufacturing process . It leverages a pre-determined end-to-end silicon manufacturing corridor for Intel vPro-eligible SKUs. Each SKU has an Intel ASC identifier embedded at the silicon level. IT organizations can use industry tools to read this identifier and view the list of specific locations where the CPU has been manufactured. Intel ASC encompasses every step in the silicon manufacturing process, including fabrication, die prep and sort, assembly, test, and warehousing. By safeguarding the supply chain, Intel enhances the stability of its products, offering businesses confidence in the authenticity and dependability of their hardware investments.

Contact your Intel representative for more available technologies to meet your needs.

Learn more about Intel's solutions by going to: https://www.intel.com/content/www/us/en/government/public-sector-solutions-overview.html

Where to Find Resources Found in This Document:

Hardware-Enabled Security Provided by Intel® Technologies	https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-security/overview.html
Intel vPro® Security Overview white paper	https://www.intel.com/content/www/us/en/content-details/838959/white-paper-intel-vpro-security-overview.html
Intel® Artificial Intelligence Overview and Solutions	https://www.intel.com/content/www/us/en/artificial-intelligence/overview.html
Intel® Assured Supply Chain product brief	https://www.intel.com/content/www/us/en/content-details/850997/content-details.html
Intel® Assured Supply Chain FAQs	https://www.intel.com/content/www/us/en/content-details/851002/content-details.html
Intel vPro® Manageability Overview white paper	https://www.intel.com/content/www/us/en/content-details/874011/content-details.html
Intel Customer Spotlight	https://www.intel.com/content/www/us/en/customer-spotlight/overview.html
Microsoft End of Support for Windows 10	https://www.microsoft.com/en-us/windows/end-of-support
Modernizing Windows Client Management	https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/modernizing-windows-client-management.html
Verizon 2025 Mobile Security Index	https://www.verizon.com/business/resources/reports/mobile-security-index/
Cyber Security Report 2026	https://engage.checkpoint.com/security-report-2026-gsem/items/report-cyber-security-report-2026?utm_campaign=dg_ps_26q1_amer_all_mesh-mix-cyber-sec-report-26-ggl-lg_en-gsem&utm_source=google-dg&utm_medium=cpc&utm_term=checkpoint+cyber+security+report&utm
NIST: Hardware Security Failure Scenarios	https://doi.org/10.6028/NIST.IR.8517

(continued on next page)

Where to Find Resources Found in This Document: (continued)

CrowdStrike: CrowdStrike and Intel Partner with MITRE Center for Threat-Informed Defense in PC Hardware-Enabled Defense Project	https://www.crowdstrike.com/en-us/blog/crowdstrike-intel-partner-mitre-center-for-threat-informed-defense-hardware-enabled-defense-project/
SMT: The Growing Threat of Counterfeit Electronic Parts in the Critical Infrastructure Supply Chain of the United States and Allies	https://smtcorp.com/counterfeit-electronic-components/
Microsoft: New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats	https://www.microsoft.com/en-us/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/
UK Government: Cyber Security and Resilience Bill	https://www.gov.uk/government/collections/cyber-security-and-resilience-bill
BITKOM: Vendor-Neutral Tendering of Notebooks	https://www.bitkom.org/sites/main/files/2023-08/itk-beschaffung-lf-notebooks-eng-online.pdf
BITKOM: Product-Neutral Tendering of Notebooks	https://www.bitkom.org/sites/main/files/2023-09/ICT-Procurement-Product-Neutral-Tendering-of-Notebooks-2022.pdf
BITKOM: Product-Neutral Tendering of Desktop PCs	https://www.bitkom.org/sites/main/files/2023-09/ICT-Procurement-Product-Neutral-Tendering-of-Desktop-PCs-2022.pdf
BITKOM Website	https://www.bitkom.org/EN
OECD: Good Practices for Procuring Computers and Laptops in Latin America	https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/good-practices-for-procuring-computers-and-laptops-in-latin-america_fd40f69d/cdf11f4d-en.pdf
BAPCo Government Network Program	https://bapco.com/about/#bgn
CrossMark® White Paper	https://bapco.com/wp-content/uploads/2024/03/crossmark_white_paper_v1.2.pdf
Forrester Study: Meet Sustainability Goals Through Strategic PC Purchasing	https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2024-12/intel-sustainability-tlp.pdf

Notes

[1] "End of support for Windows 10, Windows 8.1, and Windows 7," Microsoft, https://www.microsoft.com/en-us/windows/end-of-support.

[2] Dustin Ciscoe, et al,"Modernizing Windows Client Management," Intel, July 2024, https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/modernizing-windows-client-management.html.

[3] "2024 Mobile Security Index," Verizon, 2024, https://www.verizon.com/business/resources/T61b/reports/2024-mobile-security-index.pdf.

[4] "Cyber Security Report 2026," Check Point, 2025, https://engage.checkpoint.com/security-report-2026-gsem/items/report-cyber-security-report-2026?utm_campaign=dg_ps_26q1_amer_all_mesh-mix-cyber-sec-report-26-ggl-lg_en-gsem&utm_source=google-dg&utm_medium=cpc&utm_term=checkpoint+cyber+security+report&utm.

[5] Peter Mell, Irena Bojanova, "Hardware Security Failure Scenarios," NIST, November 13, 2024, NIST Interagency/Internal Report (NISTIR) – 8517. https://doi.org/10.6028/NIST.IR.8517.

[6] Verizon, "2024 Mobile Security Index," 19.

[7] Brad Moon, Joel Spurlock, Benjamin Sherwood, "CrowdStrike and Intel Partner with MITRE Center for Threat-Informed Defense in PC Hardware-Enabled Defense Project," CrowdStrike, February 25, 2025, https://www.crowdstrike.com/en-us/blog/crowdstrike-intel-partner-mitre-center-for-threat-informed-defense-hardware-enabled-defense-project/.

[8] "The Growing Threat of Counterfeit Electronic Parts in the Critical Infrastructure Supply Chain of the United States and Allies," SMT, November 9, 2023, https://smtcorp.com/counterfeit-electronic-components/.

[9] Microsoft Security Team, "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," Microsoft, March 30, 2021, https://www.microsoft.com/en-us/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/#:~:text=Firmware%20provides%20fertile%20ground%20to,a%20security%20threat%20versus%20firmware.

[10] Cyber Security and Resilience Bill, UK government, September 30, 2024, https://www.gov.uk/government/collections/cyber-security-and-resilience-bill.

[11] "Product–Neutral Tendering of Notebooks," BITKOM, 2022, https://www.bitkom.org/sites/main/files/2023-09/ICT-Procurement-Product-Neutral-Tendering-of-Notebooks-2022.pdf.

[12] "Vendor–Neutral Tendering of Notebooks," BITKOM, 2018, https://www.bitkom.org/sites/main/files/2023-08/itk-beschaffung-lf-notebooks-eng-online.pdf.

[13] https://www.bitkom.org/EN/About-us/About-us.html

[14] "Good Practices for Procuring Computers and Laptops in Latin America," OECD, June 13, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/good-practices-for-procuring-computers-and-laptops-in-latin-america_fd40f69d/cdf11f4d-en.pdf.

[15] https://www.oecd.org/en/about/members-partners.html

[16] "Crossmark®," BAPCo, 2022, https://bapco.com/wp-content/uploads/2024/03/crossmark_white_paper_v1.2.pdf.

[17] https://bapco.com/contact/bgn/

[18] "Meet Sustainability Goals Through Strategic PC Purchasing," Forrester Consulting, September 2024, https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2024-12/intel-sustainability-tlp.pdf.

[19] See intel.com/performance-vpro for detailed information. Results may vary. Based on data in the EPEAT Registry as of October 30, 2025, hosted by the Global Electronics Council, for computing client products in the market 2019-2025. Data is global and covers Desktop, Integrated Desktop Computer, and Notebook form factors. Intel, AMD, Apple, Arm, Dual, MediaTek, and Snapdragon devices are compared. Visit www.epeat.net/about-epeat to learn more about the registry.

[20] As of March 2026, among x86-based systems, Intel is the only silicon provider to enable query of PC fleets for hardware security configuration status and MITRE ATT&CK-aligned mitigations to help support real-time security posture and risk assessment. No product or component can be absolutely secure. See intel.com/vpro for details.

[21] Intel® Wi-Fi 7 (5 Gig) products enable up to 60% lower latencies vs. Wi-Fi 6 products claim is based on Intel engineering simulations of congested network environments. Performance varies by use, configuration, and other factors. For details on performance claims, learn more at www.intel.com/performance-wireless.

[22] Based on data in the EPEAT Registry as of October 30, 2025, hosted by the Global Electronics Council, for computing client products in the market 2019-2025. Data is global and covers Desktop, Integrated Desktop Computer, and Notebook form factors. Intel, AMD, Apple, Arm, Dual, MediaTek, and Snapdragon devices are compared. Visit www.epeat.net/about-epeat to learn more about the registry.

[23] Based on OEM design implementation as measured by data relative to one HP laptop tested and may not be characteristic of all platforms on the market. Platform configuration and implementation have obvious impact to overall platform power as it applies to power measurements for these government regulations. See intel.com/performanceindex for details.

Printed in USA 0426/LR-BW/MIM/PDF Please Recycle