

Getting the Most out of Your PC Investment in the Public Sector

Best practices for the public procurement of PC client devices

Authors

Christina Daubeneck

World Wide Government Client Sales

Ulrich Norf

World Wide Government Client RFP
Support Manager

Executive Overview

The technology procurement landscape is complicated, and the government's job of spending public funds 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. However, if you follow a few key learnings from the leading worldwide technology provider, Intel, you'll be on track to optimize your procurement process.

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 reoccurring themes in procurement processes which 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 your journey towards an optimal PC procurement outcome.

Table of Contents

Executive Overview	1
Background	1
Intel's Public PC Procurement	
Best Practice Observations:	1
PC Clients Are a Critical Part	
of Modernization and Digital	
Transformation	2
Not All PC Characteristics Are Equal	2
Why Device Security Matters	3
Why System Performance	
Matters	3
Common Device Usage	
Personas	3
Notebook Usage Personas	3
Desktop Usage Personas	3
RFP Recommendations for	
Performance Benchmarks	3
Use Your RFP Structure to	
Ensure You Get the Optimal	
Value for What You Need	4
Conclusion	4
Table 1: Intel's Optimal Value PC	
Specification Recommendations	5
Table 2: Intel® Processors to	
Consider for Performance Needs	5
Table 3: Intel® Technologies to	
Consider for Your Security Needs	6
Where to Find Resources	
Found in This Document:	7
Works Referenced	8

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 you meet your 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 your RFP structure / procurement process to ensure your 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 progresses into the Fourth Industrial Revolution where technology becomes an integral part of life, many governments around the globe are undertaking massive digital transformation and modernization efforts. Whether your 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. PCs are needed even more today for the creation, interpretation, and processing of data required to provide citizen services and deliver mission outcomes to public and private stakeholders.

A common connection point between the emerging technologies and information and communication technology (ICT) trends is data, and PCs are still at the center. Consequently, the PC is a critical element of transformation models; deploying or designing digital modernization frameworks would be remiss to not include the client device in the overall project scope and project objectives. In fact, according to Intel's "Optimize End-User Computing with Comprehensive Modernization" white paper, **"optimizing the [end user computing] environment often starts with reexamining and refreshing the client fleet...making it easier to adopt transformative innovations, stay abreast of regulatory changes, and deploy the latest operating systems,"** which is a timely assertion given Microsoft's end of support for Windows 7 in January 2020.^{1,2} PCs still using Windows 7 may become more vulnerable to ever-evolving security risks.

[Read the Modernization White Paper here](#)

[Learn more about Microsoft EOL 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 make sure that your devices continue to be an asset rather than a hindrance by refreshing your 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. Waiting too long between device refreshes 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-year refresh cycle when the devices are meeting your department needs on a day-to-day basis.³

When preparing for a refresh, consider carefully the performance and security requirements of likely use cases, which may differ across departments and agencies. Tables 1, 2 and 3 offer lists of specific technologies that can help you meet these varied requirements optimally.

For more refresh details check out the [Intel IT white paper, "Business Investment Strategy for Device Refresh" here](#)

[Learn more about the total-cost-of-ownership concept as it relates to the Intel vPro® platform here](#)

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



Not All PC Characteristics Are Equal

To demonstrate the importance of critical procurement considerations versus nice-to-have specifications, let's look to a car analogy. When buying a car, there are a lot of features to consider, but most likely you are not evaluating the paint color as more important than the safety rating and/or the car's engine function. The same concept applies in PC procurement; the size of the screen display, among other choices, does not mean much if the device leaves you 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 procurement characteristics** which should weigh heavily in your process design framework (we will cover the latter concept in the third section of this document).

A wide variety of factors drive a need for end-user computing innovation in the public sector. These may include:

Industry-specific trends

- 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)

New end-user capabilities required

- Cost-effective performance at varying levels
- End-to-end data security and privacy protection
- 3D graphics for analysts, GIS users, and other data-rich applications
- Mobility for field employees, students, teachers

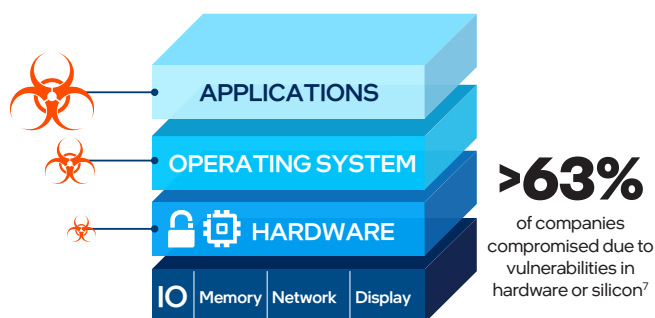
IT issues in meeting the requirements

- Budget constraints
- Complex procurement cycles
- Diverse user requirements
- Aging, complex infrastructure
- Need to manage field offices and schools with limited or no IT
- Need to protect confidential data

Why Device Security Matters

News of major security breaches suggests that security can no longer be an afterthought in PC purchase decisions. Particularly as remote working has surged, end-to-end security from the cloud to the employee laptop has become paramount.⁴ In the public sector alone, from the last quarter of 2019 through the first quarter of 2020, the number of disclosed security incidents increased 73 percent.⁵

Cybercrime damages are expected to top \$6 trillion annually by 2021.⁶ 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. One recent survey found that 63 percent of companies have been compromised due to a vulnerability in hardware or silicon.⁷ This trend suggests that in designing your next PC purchase, the security of your “edge devices” (for example, PCs, personal devices and IoT) should be of the utmost importance. Building these considerations into your PC procurement framework will help to minimize device vulnerabilities and maximize the potential return on your PC investment.



Learn more about the **hardware-enabled security** provided by Intel® technologies [here](#)

Check out **TABLE 3** [for device security solutions from Intel aligned with CIO and CISO priorities.](#)

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. Just as you probably don't want to drive a jet plane to and from work every day or drive a scooter for a cross-country family vacation, you don't want to buy a PC that does not match its intended use.

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. The underlying technology needs for the workloads are different, so to spend your budget effectively and efficiently, Intel recommends ensuring your procurement framework outlines the performance needs for the devices in accordance with their usages. While there are hundreds of different device use cases, here are six widely utilized usage personas which help guide an expected device performance level. Referencing these use cases can assist

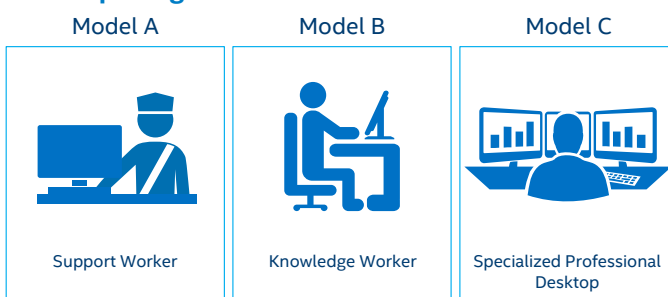
with ensuring your vendor device submissions match their planned usage and user experience and therefore match the necessary resources required.

Common Device Usage Personas

Notebook Usage Personas



Desktop Usage Personas



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

RFP Recommendations for Performance Benchmarks

How do you put your performance needs and expectations into a request for proposal (RFP)? **Intel recommends following the worldwide industry best practice of using system performance benchmarks** as outlined by the BITKOM technology consortium below:

“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.**”⁸

The BITKOM industry consortium represents more than 2,000 ICT companies including major technology vendors like Intel and AMD, as well as government agencies, with the purpose of creating one voice for optimal public IT procurement frameworks.⁹ The consortium has published vendor-neutral procurement frameworks which meet strict European Union (EU) legal standards and which can also scale around the globe as best practices. **The use of system performance benchmarks is BITKOM and Intel's recommended path forward to compare systems as well as align performance needs with device usages.**

Check out BITKOM's **latest 2018 vendor-neutral tendering of notebooks here** [↗](#) as well as **their 2019 desktop version here** [↗](#)

Learn more about **BITKOM** by visiting their site here [↗](#)



CAUTION, not all benchmarks are good benchmarks (just like not all consumer reviews of cars should be considered truthful). Intel and BITKOM recommend using benchmark tests that are:

1. **Relevant** and 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 input⁸

For Intel-recommended benchmarks, which also align with the BITKOM benchmark guidance, explore the white paper **"The Role of Benchmarks in the Public Procurement of Computers."** [↗](#)

For the usage personas outlined previously, Intel's recommendation is to use the SYSmark benchmark, which not only meets the criteria for trusted benchmarks but is also grounded in real-world business applications and workloads, meaning the SYSmark benchmark measures the system performance in scenarios most reflective of actual device usage.¹⁰ **Table 1** reflects an example of how you can use SYSmark system benchmark scores to set measurable and enforceable performance expectations by device usage model, helping ensure the optimal use of limited resources.

The SYSmark benchmark was developed and continues to be managed by a non-profit industry consortium, BAPCo, which is currently working with over 60 countries to create informed PC procurement specifications.^{10,11} 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.¹¹

Learn more about the **BAPCo Government Network program here** [↗](#)

To learn more about the new latest SYSmark benchmarks, **read the SYSmark 2018 white paper here** [↗](#) and the **SYSmark 25 white paper here** [↗](#)

Achieve the optimal value from public funds by prioritizing device security and system performance benchmarks above other component features.



Use Your RFP Structure to Ensure You Get the Optimal Value for What You Need

Once PC procurement is treated as a strategic investment decision, with device security and system performance as paramount considerations, adopt evaluation criteria for your RFP that are based on these considerations so that you receive proposals meeting or even exceeding your expectations.

Setting up your procurement cycle for success begins with making sure that you set a budget aligned with your priorities and objectives. Then your RFP structure should enforce your 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 you up to achieve optimal value systems from your vendors by creating requirements that work together in concert to provide you with the best solution for 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 below structure is an example only of structuring device security and system performance into an RFP; please evaluate your unique department/agency/procurement objectives.

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

			NOTEBOOK			DESKTOP		
SPECIFICATION CATEGORY	EVAL. TYPE	OVER-ACHIEVEMENT AWARD	DEVICE USAGE MODEL 1 High Mobility, Field Staff 	DEVICE USAGE MODEL 2 Regular Mobility, Department Employees 	DEVICE USAGE MODEL 3 Specialized Professional Mobile 	DEVICE USAGE MODEL A Entry Performance, Shared Devices 	DEVICE USAGE MODEL B Optimal Performance, Knowledge Worker 	DEVICE USAGE MODEL C High Performance, Specialized Professional Desktop 
General Usage Description			Light office productivity needs; entry systems	Optimal productivity & security; flexible, mid-range systems	Highest compute & visual performance for specialized applications, best in class compute & security	Light office productivity needs; entry systems	Optimal productivity & security; flexible, mid-range systems	Highest compute & visual performance for specialized applications, best in class compute & security
Typical Form Factor for Usage Model			2 in 1	2 in 1, Notebook	Notebook, Mobile Workstation	Mini/SFF	Mini Tower	Tower
System Performance	Min	Extra X points for every X% incremental points beyond the minimum	SYSmark 2018 System Performance score of min. 750 overall points	TBD - Evaluate your current notebook install base performance and any incremental or different needs you might have for performance. Then check out the BAPCo SYSmark dashboards here to determine a minimum threshold that meets your device usage needs.		SYSmark 2018 System Performance score of min. 750 overall points	TBD - Evaluate your current desktop install base performance and any incremental or different needs you might have for performance. Then check out the BAPCo SYSmark dashboards here to determine a minimum threshold that meets your device usage needs.	
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 Intel's recommended base security standards and specifications see Intel® Security Essentials white paper here .					

For additional considerations, reference [TABLES 2 and 3](#) and the BITKOM framework.

Check out [BITKOM's latest 2018 vendor-neutral tendering of notebooks paper here](#)

Check out [BITKOM's vendor-neutral tendering of desktops paper here](#)

Table 2: Intel® Processors to Consider for Performance Needs

NEED	RECOMMENDED INTEL® TECHNOLOGY	NON-PROPRIETARY VALUE PROPOSITION	INTEL COMPARATIVE ADVANTAGE
Entry System Processors	Intel® Pentium® processor Intel® Celeron® processor Latest available Generation Intel® Core™ i3 processor	Check out the BAPCo system performance results for Intel-based systems here . Review the latest Intel products here .	Great value, excellent price/performance return along with the quality you'd expect from Intel.
Mid-Range System Processors	Latest available Generation Intel® Core™ i5 processor Latest available Generation Intel® Core™ i7 processor		Excellent performance & user experience along with greater stability and security features for business computing.
Premium Business Processors	Latest available Generation Intel® Core™ i5 vPro® processor Latest available Generation Intel® Core™ i7 vPro® processor		The Intel vPro® platform is a set of hardware & technologies (beyond just the CPU) utilized to build premium business computers. The platform offers performance, stability, manageability, and security features. Learn more here .

Table 3: Intel® Technologies to Consider for Your Security Needs

SECURITY CAPABILITY	RECOMMENDED INTEL® TECHNOLOGY	NON-PROPRIETARY VALUE PROPOSITION	INTEL COMPARATIVE ADVANTAGE
Threat Detection	Intel® Threat Detection Technology (Intel® TDT)	Silicon-level telemetry and machine learning to help our industry partners improve the detection of advanced cyber threats & exploits.	Intel TDT is a set of technologies that harness hardware telemetry and acceleration capabilities to help identify threats and detect anomalous activity. TDT provides advanced threat protection against ransomware and crypto mining without compromising performance.
BIOS Defense	Intel® Runtime BIOS Resilience	Hardware-enhanced protection for system UEFI/BIOS; minimizes risk of malware injection by protecting the critical underlying SW responsible for running the PC.	There are software mechanisms for defending against firmware attacks, but they lack the hardware protection of Intel Runtime BIOS Resilience. Protects against SMM (system management mode) attacks. <i>Intel Runtime BIOS Resilience is exclusive to Intel® vPro branded platforms.</i>
Platform Protection	Intel® Platform Trust Technology	Provides platform credential storage and key management used by the operating system.	Meets requirements for firmware Trusted Platform Module (fTPM) 2.0.
Platform Protection	Intel® Trusted Execution Technology (Intel® TXT)	Dynamic Root of Trust Measurement (DRTM) that allows a VMM/OS to check system integrity before loading.	Intel TXT demonstrates Intel's commitment to help secure platforms at all layers in the computing stack.
Platform Protection	Intel® Virtualization Technology (Intel® VT-x) & Intel® Virtualization Technology for devices Intel® VT-d)	Hardware virtualization technologies which enable new Windows 10 Enterprise software capabilities out of the box.	Intel VT-x, VT-d demonstrates Intel's commitment to help secure platforms at all layers in the computing stack. <i>Intel vPro branded platforms are validated for VT-x, VT-d.¹²</i>
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.	Intel SIPP delivers a more stable platform resulting in predictable transactions for business customers. SIPP's comprehensive offering includes CPU, chipset, firmware, and drivers for LAN/WLAN, Thunderbolt™, memory, and storage components. <i>Intel vPro branded platforms require Intel SIPP eligible processors. Intel SIPP is available on other systems as well.¹³</i>
Manageability/ Recovery	Intel® Active Management Technology (Intel® AMT)	Hardware manageability features enabling better discovery, repair, and protection of wired or wireless connected computers regardless of operating system or power state.	Intel AMT is a superset of the industry standard DASH specification with 10+ years of innovations, including remote KVM, which allows a technician to remotely maintain, diagnose, and repair a LAN/WLAN-connected PC as if they were sitting right in front of it. Practical use cases include wake and patch, system recovery, and remote re-imaging. <i>Intel AMT is exclusive to Intel vPro branded platforms.</i>
Secure Sourcing	Intel® Transparent Supply Chain	Certificate-based mechanism to trace components from manufacturing point to confirm authenticity.	Intel Transparent Supply Chain demonstrates Intel's commitment to help secure platforms at all layers in the computing stack.
Hardware-hardened security	Intel® Control Flow Execution Technology (CET)	CPU-level security capabilities to help protect against common malware attack	Intel CET is designed to protect against the misuse of legitimate code through control-flow hijacking attacks.
Hardware-hardened security	Intel® Total Memory Encryption (TME)	Protects data against exposure via physical attack on memory, such as cold-boot attacks.	Intel TME protects encryption keys and data stored on system memory during active or sleep state by fully encrypting all physical memory of a system. <i>Intel TME is exclusive to Intel vPro branded platforms.</i>

Contact your Intel representative for even 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:

Intel White Paper: Optimize End-User Computing With Comprehensive Modernization	https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/optimize-end-user-computing-white-paper.pdf
Microsoft End of Life Plans for Windows 7	https://www.microsoft.com/en-us/windowsforbusiness/end-of-windows-7-support
Intel IT White Paper, Business Investment Strategy for Device Refresh	https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/enterprise-mobility-pc-upgrade-strategy-guide.pdf
Intel White Paper: The Economic Case for the Intel® VPro™ Platform	https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/total-cost-of-ownership-white-paper.html
BITKOM Website	https://www.bitkom.org/EN
BITKOM: Vendor Neutral Tendering of Notebooks	https://www.itk-beschaffung.de/EN/Guidelines/Vendor-neutral-tendering-notebooks
BITKOM: Vendor Neutral Tendering of Desktop PC's	https://www.itk-beschaffung.de/sites/beschaffung/files/2020-01/200128_lf_desktop-pcs_en.pdf
BAPCo System Benchmark Performance Dashboard	https://results.bapco.com/dashboard
BAPCo Government Network Program	https://bapco.com/contact/bgn/
SYSmark White Paper: 2018 Benchmarks	http://bapco.com/wp-content/uploads/2018/08/SYSmark_2018_White_Paper_1.0.pdf
SYSmark White Paper: 25 Benchmarks	https://bapco.com/wp-content/uploads/2020/07/SYSmark25WhitePaper.pdf
Intel White Paper: The Role of Benchmarks in the Public Procurement of Computers	https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/role-of-benchmarks-white-paper.pdf
Intel Brief: Optimizing PC Refresh	https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/optimizing-pc-refresh-brief.html
Forrester Consulting Thought Leadership Paper Commissioned by Intel: How PCs Will Drive The Future of Work	https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/how-pcs-drive-future-of-work-study.html?wapkw=forrester%20future%20of%20work
Intel White Paper: Intel® Security Essentials: A Built-in Foundation with Security at the Core	https://software.intel.com/content/www/us/en/develop/articles/intel-security-essentials-a-built-in-foundation-with-security-at-the-core.html

Works Referenced

- ¹ Bartley, Andrew, et al. Optimize End-User Computing With Comprehensive Modernization, Intel, 2018, <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/optimize-end-user-computing-white-paper.pdf> ↗
- ² "Support for Windows 7 Is Ending." Software Asset Management – Microsoft SAM, www.microsoft.com/en-us/windowsforbusiness/end-of-windows-7-support ↗
- ³ A Business Investment Strategy for Device Refresh, Intel IT, 2014, <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/enterprise-mobility-pc-upgrade-strategy-guide.pdf> ↗
- ⁴ Verizon, Data Breach Investigations Report, 2020, <https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report> ↗
- ⁵ McAfee Labs, COVID-19 Threats Report, July 2020, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf> ↗
- ⁶ Global Cybercrime Damages Predicted to Reach \$6 Trillion Annually by 2021, Cybercrime Magazine, October 2020, <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> ↗
- ⁷ BIOS Security – The Next Frontier for Endpoint Protection, A Forrester Consulting Thought Leadership Paper Commissioned by Dell, June 2019, <https://www.delltechnologies.com/ja-jp/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf> ↗
- ⁸ "Vendor–Neutral Tendering of Notebooks," BITKOM, 2018, <https://www.itk-beschaffung.de/EN/Guidelines/Vendor-neutral-tendering-notebooks> ↗
- ⁹ <https://www.bitkom.org/EN/About-us/About-us.html> ↗
- ¹⁰ http://bapco.com/wp-content/uploads/2018/08/SYSmark_2018_White_Paper_1.0.pdf ↗
- ¹¹ <https://bapco.com/contact/bgn/> ↗
- ¹² VT-x, VT-d is available on other systems as well.
- ¹³ Only time-to-market platforms can support Intel SIPP.



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

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See specific resources referenced for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

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

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice.

Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. Intel provides these materials as-is, with no express or implied warranties.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

Any forecasts of requirements for goods and services are provided for discussion purposes only. Intel will have no liability to make any purchase pursuant to forecasts. Any cost or expense you incur to respond to requests for information or in reliance on any forecast will be at your own risk and expense.

Statements in this document that refer to Intel's plans and expectations for the quarter, the year, and the future, are forward-looking statements that involve a number of risks and uncertainties. A detailed discussion of the factors that could affect Intel's results and plans is included in Intel's SEC filings, including the annual report on Form 10-K. Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See <http://www.intel.com/content/www/us/en/processors/processor-numbers.html> for details.