Platform Brief

Intel vPro® with Intel® Core™ Ultra Processors (Series 2)

Empowering organizations to thrive in the age of AI

PCs built on Intel vPro® and powered by Intel® Core™ Ultra processors (Series 2) are designed for seamless technology transitions and address all levels of AI computing

The future of business computing is AI-infused applications across both the user and IT domains. To maximize value from AI, organizations must deploy powerful and efficient PCs optimized for the next wave of productivity, security, and device management applications. The new Intel vPro® platform is built for modern business and the age of AI.

A New Computing Portfolio

Intel aims to meet all organizational computing needs with a portfolio of processors offering different levels of performance and a wide range of AI experiences across mobile and desktop form factors. All processors feature an AI-optimized architecture, where the CPU, GPU, and NPU execute AI tasks as orchestrated by software developers.

Mobile Processors

The new mobile computing portfolio (Table 1) offers solutions for thin and light notebooks, premium thin and light notebooks, high-performance notebooks, and mobile workstations. This enables system manufacturers to deliver AI PCs in scale, with product lines that address multiple price points and various computing personas[1].

- **On-the-go workers** can benefit from thin and light notebooks (Intel® Core™ Ultra Processors 235U/265U) with enhanced CPU cores and integrated Intel® Wi-Fi 7 (5 Gig).
- **Knowledge workers** can be more productive on premium thin and light notebooks (Intel® Core™ Ultra 200V Series Processors) with a new CPU architecture, next-generation Intel® Arc™ graphics, and a higher capacity NPU. These new processors also feature memory on the package and Intel® Wi-Fi 7 (5 Gig).
- **Power users and analysts** may upgrade to new high-performance notebooks (Intel® Core™ Ultra 200H Series Processors) featuring re-designed cores, Intel® Arc™ graphics, integrated Intel® Wi-Fi 7 (5 Gig), and optional Thunderbolt™ 5.
- **Technical creators** with the greatest computational demands can depend on new mobile workstations (Intel® Core™ Ultra 200HX Series Processors) with re-designed CPU cores, support for hybrid graphics, and optional Thunderbolt™ 5.

All products support Thunderbolt™ 4 for high-speed connectivity to peripherals and elegant workspaces via modern docks. In addition, Intel® Dynamic Tuning Technology enables manufacturers to deliver optimized power and performance for any given mobile PC.

Desktop Processors

Intel is bringing its NPU to desktop form factors with a new computing portfolio (Table 2). All processors feature these new NPUs, along with integrated Intel® Graphics, plus wired and wireless connectivity solutions including integrated Intel® Wi-Fi 6E (Gig+), integrated Thunderbolt™ 4, and the Intel® Ethernet Connection with 1 GbE and 2.5 GbE options[1].

As with previous desktop processor generations, the portfolio is organized around three core-count options and three power offerings. Each version of the Intel® Core™ Ultra processor (5, 7, or 9) is available at low power (35 W), standard power (65 W), or higher power (125 W), thus enabling small form factor desktops, all-in-ones, and towers of different sizes:

- **Intel® Core™ Ultra 5**: Up to 14-core processors offering the right performance for most users
- **Intel® Core™ Ultra 7**: Up to 20-core processors for power users
- **Intel® Core™ Ultra 9**: Up to 24-core processors for technical creators using entry workstations

Intel® Arc™ GPU cards, which are also certified with many popular engineering, science, and design applications, can benefit power users and technical creators.

AI for Business

AI empowers people to achieve new levels of productivity no matter the task. Visual and audio effects help employees look and sound their best while collaborating remotely. Personal assistants and large language models promise to streamline daily workflows, meeting preparation, and project management. AI facilitates higher quality work to be done fast in the areas of content creation, data visualization, design, research, and similar tasks common to business

professionals. Thus, Intel's latest offerings can enable better business outcomes everywhere AI PCs are deployed[2].

AI for Security, Security for AI

As security threats become more sophisticated, the need for advanced defense technologies grows as well. While machine learning has been part of security software for a few years, bad actors are now also using AI to attack PCs. Endpoint security solutions must continue to evolve both above and below the OS.

Intel® Threat Detection Technology

Intel® Core™ Ultra processors extend the NPU to third-party security software vendors, enabling their applications to become more effective and efficient at detecting and responding to threats. This can be achieved via native programming or via Intel® Threat Detection Technology.

Intel® TDT helps developers optimally use endpoint computing resources (CPU, GPU, and NPU) to achieve AI-assisted anomaly detection and identification of sophisticated attacks such as ransomware or crypto-jacking. Security software executing locally can lower the latency for threat detection and mitigation. Offloading operations to the NPU frees up CPU bandwidth, which can improve the user experience or create further opportunities to move security functions from the cloud to the endpoint. This end-to-end approach to attack surface reduction helps deliver on the promise of the AI PC.

New Security Engines

All Intel® Core™ Ultra processors incorporate the Intel® Silicon Security Engine for hardware-based authentication of system firmware, and additional security functions will move to the Intel® Silicon Security Engine over time.

Specific products in the new processor portfolio (Intel® Core™ Ultra 200V Series Processors) also integrate the Intel® Partner Security Engine, which is configurable by system manufacturers to support the Microsoft Pluton security processor. Microsoft Pluton targets to deliver hardware-based root of trust, attestation, identity, and other security services to be defined by Microsoft[1].

Windows 11 Security

All Intel® Core™ Ultra processors continue to support the Intel® Converged Security and Management Engine, which houses legacy capabilities such as Intel® Boot Guard for cryptographically verified boot and Intel® Platform Trust Technology, an integrated TPM 2.0 solution compatible with the Trusted Computing Group standard. Both a cryptographically verified boot and a TPM 2.0 solution are Windows 11 requirements.

To achieve Microsoft Secured-core PC compliance, all Intel® Core™ Ultra processors support:

- **Intel® Trusted Execution Technology** for dynamic root of trust
- **Intel® System Resources Defense** for robust system management mode (SMM) protections
- **Intel® System Security Report** for communicating implemented protection policies to the Windows OS

The Intel vPro® platform provides a more secure computing foundation for AI apps and data with a robust set of security features that PC manufacturers must design into every PC bearing the Intel vPro® badge. Table 3 includes a list of all key platform security features.

Services-Ready Endpoints

Intel vPro® platforms support in-band and out-of-band manageability for greater endpoint visibility and availability for remote maintenance.

In-Band Management

Device management applications rely on endpoint data to make the right configuration, maintenance, and servicing decisions. Intel® Device Discovery provides a method for local and remote applications to obtain greater visibility into endpoints, with a robust dataset spanning device profile, history, and capabilities. This includes an inventory of Intel vPro® platform features present and their configuration state. The wealth of data generated by Intel® Device Discovery may be used to generate PC health assessments, determine the security posture of a PC, or learn how to best configure and maintain a device. Greater visibility into endpoints becomes vital as IT operations embrace AI and automation.

Out-of-Band Management

Intel® Active Management Technology helps customers reduce onsite PC repairs via remote access even when a PC is powered down, the OS is unavailable, or the user is not present[3]. Use cases such as wake and patch, boot to BIOS, and OS/image upgrades help customers efficiently manage computing fleets. Keyboard/video/mouse (KVM) remote control allows technicians to remotely manipulate a PC as if they were seated right in front of the machine. Intel® AMT is complemented by Intel® Endpoint Management Assistant and new cloud-native remote management solutions that accelerate the adoption of out-of-band use cases via third-party and stand-alone tools.

Table 4 provides a list of Intel vPro® platform manageability technologies.

The Power of Choice

Organizations that choose Intel® powered AI PCs also benefit from the power of choice, with over 100 AI-infused applications and over 300 features optimized for Intel® Core™ Ultra processors[2]. Intel offers the most robust platform for AI PC development with more AI models, frameworks, and runtimes enabled than any other processor vendor[4]. Organizations that need to create custom applications can lean on over 500 AI models optimized for Intel® Core™ Ultra processors, spanning AI inferencing categories such as natural language processing, diffusion, and computer vision.

Summary

Intel vPro® helps organizations maximize value from AI. Featuring Intel® Core™ Ultra processors, the Intel vPro® platform addresses all levels of AI computing, fuels operational excellence, and helps organizations achieve better business outcomes.

For more information, please visit www.intel.com/vpro.

Product and Feature Tables

Thin and Light Notebooks 12-15 W	Premium Thin and Light Notebooks 8 W / 17-30 W		High Performance 28 W / 45 W	Mobile Workstation 55 W
-----	16 GB Memory on Package -----	32 GB Memory on Package Intel® Core™ Ultra 9 processor 288V 4P + 4LPE 8Xᵉ	Intel® Core™ Ultra 9 processor 285H 6P + 8E + 2LPE 8Xᵉ	Intel® Core™ Ultra 9 processor 285HX 8P + 16E 4Xᵉ
Intel® Core™ Ultra 7 processor 265U 2P + 8E + 2LPE 4Xᵉ	Intel® Core™ Ultra 7 processor 266V 4P + 4LPE 8Xᵉ	Intel® Core™ Ultra 7 processor 268V 4P + 4LPE 8Xᵉ	Intel® Core™ Ultra 7 processor 265H 6P + 8E + 2LPE 8Xᵉ	Intel® Core™ Ultra 7 processor 265HX 8P + 12E 4Xᵉ
Intel® Core™ Ultra 5 processor 235U 2P + 8E + 2LPE 4Xᵉ	Intel® Core™ Ultra 5 processor 236V 4P + 4LPE 7Xᵉ	Intel® Core™ Ultra 5 processor 238V 4P + 4LPE 7Xᵉ	Intel® Core™ Ultra 5 processor 235H 4P + 8E + 2LPE 8Xᵉ	Intel® Core™ Ultra 5 processor 245HX 6P + 8E 3Xᵉ

Table 1: Intel® Core™ Ultra Mobile Processors Eligible for Intel vPro® Enterprise

Low Power 35 W	Standard Power 65 W	Higher Power 125 W
Intel® Core™ Ultra 9 processor 285T 8P + 16E 4Xᵉ	Intel® Core™ Ultra 9 processor 285 8P + 16E 4Xᵉ	Intel® Core™ Ultra 9 processor 285K 8P + 16E 4Xᵉ
Intel® Core™ Ultra 7 processor 265T 8P + 12E 4Xᵉ	Intel® Core™ Ultra 7 processor 265 8P + 12E 4Xᵉ	Intel® Core™ Ultra 7 processor 265K 8P + 12E 4Xᵉ
Intel® Core™ Ultra 5 processor 235T 6P + 8E 3Xᵉ Intel® Core™ Ultra 5 processor 245T 6P + 8E 4Xᵉ	Intel® Core™ Ultra 5 processor 235 6P + 8E 3Xᵉ Intel® Core™ Ultra 5 processor 245 6P + 8E 4Xᵉ	Intel® Core™ Ultra 5 processor 245K 6P + 8E 4Xᵉ

Table 2: Intel® Core™ Ultra Desktop Processors Eligible for Intel vPro® Enterprise

Platform Security Features[1]	
Intel® Virtualization Technology Hardware support for Windows virtualization based security	**Intel® Boot Guard** Supports cryptographically verified boot
Intel® Trusted Execution Technology Dynamic root of trust	**Intel® BIOS Guard** Helps protect firmware residing in non-volatile memory
Intel® System Resources Defense System management mode (SMM) protections	**Intel® Silicon Security Engine** Hardware-based authentication of system firmware
Intel® System Security Report Communicates below the OS security policies to the OS	**Intel® Partner Security Engine[5]** Hardware for executing Microsoft Pluton and other use cases
Intel® Platform Trust Technology Integrated trusted platform module (TPM 2.0)	**Linear Address Space Separation[6]** Helps detect side channel attacks on DRAM contents
Intel® Virtualization Technology with Redirect Protection[7] Hardware-based protection for the OS kernel	**Intel® Threat Detection Technology** Increases the effectiveness/efficiency of security software
Intel® Total Memory Encryption with Multi-Key[7] Full or partial DRAM encryption	**Intel® Control Flow Enforcement Technology** Helps protect against memory safety attacks

Table 3: Intel vPro® Security Features for Windows PCs

Device Manageability Features[1]	
Intel® Device Discovery Remote query of devices to discover features, capabilities, and other data sets important to AI-enhanced IT operations	**Intel® Active Management Technology[7]** Out-of-band device management supporting remote KVM and various other out-of-band use cases
Intel® Innovation Platform Framework (Intel® IPF) Helps local or remote applications interact with Intel platform features and provides the software interface for Intel® Device Discovery	**Intel® Platform Service Record[7]** A set of tamper-resistant ledgers that capture system wear and tear data to help inform reliability assessments and residual value calculations
Intel® Platform Brand Identity[7] Method for remotely identifying Intel vPro platforms and their features	**Intel® Remote Platform Erase[7]** Device sanitization encompassing multiple PC components (SSD, TPM clear, BIOS reset, other)
Intel® Unique Platform ID[7] Creates unique and persistent device ownership credentials to facilitate execution of endpoint services	**Intel® One-Click Recovery[7]** Method for returning a disabled PC to a known good state, using an image stored locally or in the cloud
Intel® Stable IT Platform Program Provides stable hardware with comprehensive platform validation and flexible software updates; includes validation for versions of the Windows 10 and Windows 11 operating systems within the Microsoft servicing period	

Table 4: Intel vPro® Manageability Features for Windows PCs

[1] Feature availability may vary by PC make and model and Windows version installed.

[2] AI features may require software purchase, subscription, or enablement by a software or platform provider, or may have specific configuration or compatibility requirements. Learn more at www.intel.com/aipc.

[3] Remote power-on of an Intel AMT-activated PC is possible when the system is plugged in and has AC power.

[4] Learn more at AI PC Leadership

[5] Available only on Intel Core Ultra processors identified by Intel® Core™ Ultra 200V Series Processors part numbers.

[6] Exclusively available for Intel vPro® Enterprise devices.

[7] Not available on Intel Core Ultra processors identified by Intel® Core™ Ultra 200U Series Processors; feature requires OS enabling.

Performance varies by use, configuration, and other factors. Full details at www.intel.com/performanceindex. Intel technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary.

All versions of the Intel vPro® platform require an eligible Intel processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance and stability that define the platform. See www.intel.com/performance-vpro for details.