PLATFORM BRIEF

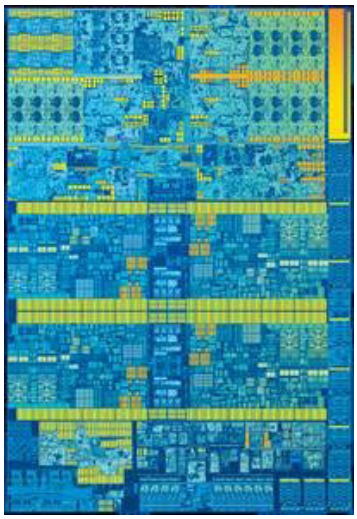
Intel® Xeon® Processor E3-1200 v5 and
E3-1500 v5 Product Families and Intel® C230
and CM230 Series Chipsets

Internet of Things

Intel® Xeon® Processor-Based Platforms for Internet of Things (IoT) Solutions

(Intel® Xeon® Processor E3-1505M v5, E3-1505L v5, E3-1515M v5, E3-1275 v5, E3-1225 v5, and E3-1268L v5)

Harness the Performance, Features, and Edge-to-Cloud Scalability to Build Tomorrow's IoT Solutions Today



Product Overview

Intel is proud to announce its Intel® Xeon® processor E3-1200 v5 and E3-1500 v5 product families. Manufactured on the latest 14 nm technology, these processors offer dramatically higher CPU and graphics performance as compared to the previous generation, a broad range of power options, and new advanced features to boost edge-to-cloud Internet of Things (IoT) designs. The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families also maintain a standardized thermal envelope for 95W and 35W land grid array (LGA) workstation products, remaining consistent with the previous processor generation. Additionally, Intel Xeon processors are introducing ball grid array (BGA) parts for mobile workstation computing needs under the Intel Xeon E3-1500 v5 product family. The BGA parts are 45W (35W cTDP) and 25W.

The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families deliver quad-core processing and intelligent performance capabilities, including Intel® Turbo Boost Technology[1] 2.0, and Intel® Hyper-Threading Technology.[2] Additionally, they boost performance to integer/matrix-based calculations through Intel® Advanced Vector Extensions 2 (Intel® AVX2).

The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families offer numerous advancements over the previous generation, making them ideal for a wide range of IoT applications, including industrial control and automation equipment, retail devices, and military, aerospace, and government systems.

Power-Efficient Performance

The new Intel Xeon processor E3-1200 v5 and E3-1500 v5 families make a powerful difference on the efficiency front as well. The improved technology promises up to 35 percent[3] faster CPU for theS-Series and up to 26 percent[4] for the H-Series, and faster graphics of up to 49 percent[5] for S and up to 22 percent[6] for H. And these families achieve these enhancements using the same or similar thermal design power (TDP) as the prior generation.[7]

Develop more flexible designs with up to 40 percent more high-speed I/O than previous generations and tap into faster memory performance with new memory support for DDR4 1.2V up to 2133, 64GB max capacity with 8GB density. The workstation products support error-correcting code memory to detect and correct single-bit memory errors to keep a system up and running.

Other important features include Intel AVX2, which provides optimized instructions to drive enhanced performance on floating point–intensive apps,[8] and Intel® Ready Mode Technology[9] for PCIe* storage for improved data reliability and greater levels of performance, responsiveness, and expandability.

Stunning Visual Performance

The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families utilize the new Gen9 and E3-1500 v5 graphics engine, which improves graphic performance by up to 49 percent[5] for the S Series and up to 22 percent[6] for the H Series. The improvements are demonstrated through faster 3-D graphics performance and rendering applications at low power. Video playback is also faster and smoother thanks to the new multiplane overlay capability. The new generation offers up to three independent audio streams and displays, Ultra HD 4K support, and workload consolidation for lower BOM costs and energy output.

Users will also enjoy enhanced high-density streaming applications and optimized 4K video conferencing with accelerated 4K hardware media codecs HEVC (8-bit), VP8, VP9, and VDENC encoding, decoding, and transcoding. Together, the stunning visual performance enhancements add up to more immersive computing experiences.

Broad Design Range

Intel Xeon processors deliver the best experience for computing- and graphics-intensive environments. Applications span multiple industries and solutions ranging from medical workstations and CAT scans, to industrial controller solutions and military and aerospace applications.

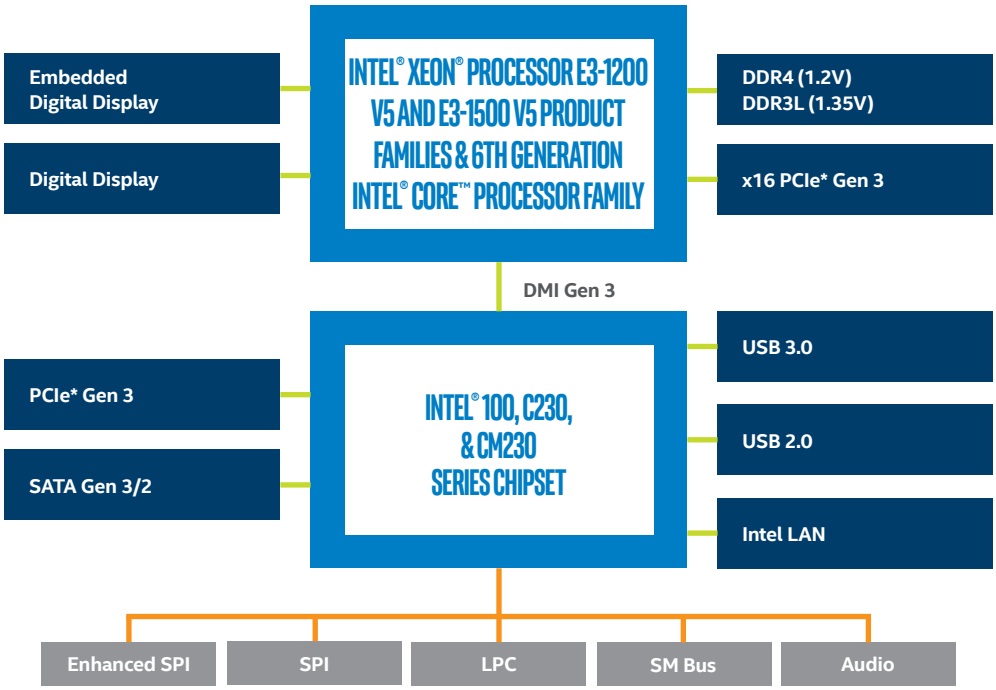
Operating system support ranges from small-footprint real-time operating systems (RTOSs) to feature-rich OSs to optimize choice, flexibility, and OS investment protection.

The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families enable more flexible designs with configurable I/O offering additional high-speed ports compared to the previous generation. More high-speed input/output (HSIO) means improved flexibility, increasing from 18 to 26 total HSIO ports,[10] from up to eight PCIe 2.0 to 20 PCIe 3.0 ports,[10] and from up to six USB 3.0 to 10 USB 3.0 ports.[10] The LGA parts are paired with the Intel® C230 series chipset while the BGA parts are paired with the Intel® CM230 series chipset.

Advanced Security and Manageability

The Intel Xeon processor E3-1200 v5 and E3-1500 v5 product families protect IoT systems and data at rest and in flight through hardware- and software-based security hardening. Keep increasingly connected devices more secure and enhance the firmware trusted platform module (TPM) with Intel® Platform Trust Technology (Intel® PTT), Intel® Software Guard Extensions (Intel® SGX) to protect data while in use, Intel® Memory Protection Extensions (Intel® MPX) to protect memory from buffer-overload attacks, and Intel® Boot Guard to securely boot machines.

Intel® vPro™ technology[11] allows you to remotely configure, diagnose, isolate, and repair an infected PC—even if it is turned off. In addition to helping secure the IT environment, hardware-based KVM Remote Control enables you to address issues remotely by seeing what users see.



KEY FEATURES

INTEL® BUILT-IN VISUALS

NEW Gen9 graphics with embedded DRAM: Supports the latest graphics APIs DirectX* 12 (Windows* only) and OpenGL* 4.5 for improved 3-D rendering performance at low power.

NEW Accelerated 4K hardware media codecs: Enhances high-density streaming applications and optimized 4K videoconferencing with HEVC (8-bit), VP8, VP9, and VDENC encoding, decoding, and transcoding.

Intel® HD Graphics: Plays HD video with exceptional clarity; permits viewing and editing of even the smallest image details.

Intel® Quick Sync Video: Delivers excellent videoconferencing capability, fast video conversion, and fast video editing and authoring.

Intel® Clear Video HD Technology: Provides visual quality and color fidelity enhancements for spectacular HD media playback.

Ultra HD 4K support: Provides stunning display resolutions,[12] now up to 4096x2304 pixels, and supports performance across three independent displays with audio.

Multiplane overlay: Enables faster, smoother, higher-quality video playback and improved 3-D graphics.

Intel® Iris™ Pro Graphics (GT4e): Access a broad range of 3-D rendering capability options that fit low-, medium-, and high-performance applications.

PERFORMANCE

Intel® Advanced Vector Extensions 2 (Intel® AVX2): Provides optimized instructions to deliver enhanced performance on floating point–intensive apps, adding 256-bit integer instructions and new instructions for Fused Multiply Add (FMA), which delivers better performance on media and floating-point computations.

Intel® Turbo Boost Technology[1] 2.0: Dynamically increases the processor's frequency, as needed, by taking advantage of thermal and power headroom when operating below specified limits.

Intel® Hyper-Threading Technology[2]: Delivers two processing threads per physical core; highly threaded applications can get more work done in parallel, completing tasks sooner.

NEW Additional HSIO: Increases flexibility from 18 to 26 total HSIO ports,[10] from up to eight PCIe* 2.0 to 20 PCIe 3.0 ports,[10] and from up to six USB 3.0 to 10 USB 3.0 ports.[10]

NEW Faster memory performance: Offers new DDR4 memory support, including new support for DDR4 1.2V up to 2133, 64GB max capacity with 8GB density.

Intel® Smart Cache: Dynamically allocates shared cache to each processor core, based on workload, reducing latency and improving performance.

Error-correcting code: Detects multiple-bit memory errors; locates and corrects single-bit errors to keep a system up and running.

KEY FEATURES

SECURITY

Intel® Identity Protection Technology (Intel® IPT) with multifactor authentication (MFA): Provides enhanced security by verifying the boot portion of the boot sequence; protects your one-time password (OTP) credentials and PKI certificates and adds a layer of encrypted second-factor authentication for online transactions.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[13]: Access a fast, secure AES engine for a variety of encryption apps, including whole-disk encryption, file-storage encryption, conditional access of HD content, Internet security, and VoIP. Consumers benefit from protected Internet and email content, plus fast, responsive disk encryption.

Intel® OS Guard: Protects the OS kernel and prevents use of malicious data or attack code located in areas of memory marked as user-mode pages from taking over or compromising the OS kernel. Intel OS Guard is not application-specific and protects the kernel from any application.

NEW **Intel® Platform Trust Technology with BIOS Guard:** Safeguards credential storage and key management, while helping reduce BOM cost and board space.

NEW **Intel® Software Guard Extensions (Intel® SGX):** Allows application developers to protect sensitive data from unauthorized access or modification by rogue software running at higher privilege levels[14]; secures data while in use in a Windows* or Linux* environment.

Intel® Data Protection Technology (Intel® DPT) with Intel® Boot Guard: Prevents unauthorized software and malware takeover of boot blocks critical to a system's function, thus providing added level of platform security based on hardware.

NEW **Intel® Memory Guard Extensions (Intel® MPX):** Identifies errant pointer usage which, if left undetected, puts an application at risk of data corruption or malicious attack via buffer overruns and overflows. By adding extensions to the underlying architecture, Intel MPX achieves improved performance over software-based solutions.

Intel® Secure Key[8]: Generates high-quality keys for cryptographic (encryption and decryption) protocols, and provides quality entropy that is highly sought after for added security.

BIOS Guard: Augments existing chipset-based BIOS flash protection capabilities targeted to address the increasing malware threat to BIOS flash storage; protects from modification without platform manufacturer authorization, helps defend the platform against low-level denial of service (DOS) attacks, and restores BIOS to a known good state after an attack.

VMCS shadowing: Allows a Virtual Machine Manager (VMM) running in a guest (nested virtualization) to access a shadow VMCS memory area using the normal VMRead/VMWrite instructions, reducing overhead for a more natural and responsive user experience and allowing users to take control of their personal and professional data and apps while being protected by game-changing security.

POWER EFFICIENCY

Integrated Memory Controller: Supports DDR4 and offers stunning memory read/write performance through efficient prefetching algorithms, lower latency, and higher memory bandwidth as compared to previous generations.

Intel® Power Optimization and processor c-states: Increases periods of silicon sleep state across the platform ingredients—including the CPU, chipset, and third-party system components—to reduce power.

PCI Express* 3.0 interface: Offers up to 8 GT/s for fast access to peripheral devices and networking with up to 16 lanes[15]—PCI Express ports can be configured as x1, x2, x4, x8, and x16 depending on motherboard designs.

Intel® Ready Mode Technology[9]: Provides quick access to your PC with applications that are up-to-date and constantly connected.

Intel® Intelligent Power Technology: Reduces power consumption through automated energy efficiency.

Automated low-power states: Adjusts system power consumption based on real-time processor loads.

Fully integrated voltage regulator: Simplifies power delivery by integrating legacy power delivery on to processor package/die.

KEY FEATURES

INTEL® VPRO™ TECHNOLOGY

Intel® Active Management Technology (Intel® AMT): Remotely monitors, maintains, updates, upgrades, and repairs PCs through hardware and firmware technology for remote out-of-band management.

Intel® Trusted Execution Technology (Intel® TXT)[16]: Protects embedded devices and virtual environments against rootkit and other system-level attacks. Using an industry-standard TPM 1.2 to store keys and other protected data, this portion of Intel® vPro™ technology boots the BIOS, operating system, and software into a "trusted" execution state, verifying the integrity of the virtual machine and protecting the platform from unauthorized access.

Intel® Virtualization Technology[17]: Allows one hardware platform to function as multiple "virtual" platforms; offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

SUSTAINABILITY

Green technology: Manufactured with lead-free and halogen-free component packages

Conflict-free: Products do not contain conflict minerals (tin, tantalum, tungsten, and/or gold) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo (DRC) or adjoining countries

SOFTWARE OVERVIEW

The following independent operating system and BIOS vendors provide support for these platforms.

OS VENDOR	OPERATING SYSTEM (TARGETED FOR SUPPORT)	DISTRIBUTION	SUPPORT	BIOS
Microsoft	Windows* 10 (64b)	Microsoft	Intel/Microsoft	American Megatrends Inc. Insyde Software Phoenix Technologies Byosoft
	Windows* 8.1 Au (64b)	Microsoft	Intel/Microsoft	
	Windows* Embedded Industry 8.1 (64b)	Microsoft	Intel/Microsoft	
	Windows* 7 Pro (32/64b)	Microsoft	Intel/Microsoft	
	Windows* POSready 7 and WES7* (32/64b)	Microsoft	Intel/Microsoft	
Linux*	Fedora* Distribution (64b)	Open Source		
	Ubuntu*, SUSE*, Red Hat Enterprise (64b)	Canonical Ltd.*, Attachmate Group, Red Hat, and Open Source		
	Yocto* Tool-Based Embedded Linux* (64b) Distribution	Yocto Project* Community		
Google	Chromium* (Chrome*) (64b)	The Chromium Projects*	Google	
RTOS	Wind River VxWorks 7* (64b)	Wind River Systems		

Not all features are supported. Contact your local Intel representative for more information.

INTEL® XEON® PROCESSOR E3-1200 V5 AND E3-1500 V5 PRODUCT FAMILIES FOR INTERNET OF THINGS SOLUTIONS

	CORE FREQUENCY (GHz)							
PROCESSOR NUMBER	CORES/ THREADS	BASE FREQUENCY	1 CORE TURBO (MAX)	INTEL® SMART CACHE	THERMAL DESIGN POWER	PACKAGE	INTEL® AES-NI	INTEL® AVX
Intel® Xeon® processor E3-1275 v5	4C/8T	3.6 GHz	4.0 GHz	8M	80W	LGA1151	Yes	Intel® AVX2
Intel® Xeon® processor E3-1225 v5	4C/4T	3.3 GHz	3.9 GHz	8M	80W	LGA1151	Yes	Intel® AVX2
Intel® Xeon® processor E3-1268 v5	4C/8T	2.4 GHz	3.4 GHz	8M	35W	LGA1151	Yes	Intel® AVX2
Intel® Xeon® processor E3-1505M v5	4C/8T	2.8 GHz	3.7 GHz	8M	45W (cTDP 35W)	BGA1440	Yes	Intel® AVX2
Intel® Xeon® processor E3-1505L v5	4C/8T	2.0 GHz	2.8 GHz	8M	25W	BGA1440	Yes	Intel® AVX2
Intel® Xeon® processor E3-1515M v5	4C/8T	2.8 GHz	3.7 GHz	8M	45W (cTDP 35W)	BGA1440	Yes	Intel® AVX2

			INTEL® VPRO™ TECHNOLOGY			
PROCESSOR NUMBER	INTEL® TURBO BOOST TECH 2.0	INTEL® HYPER-THREADING TECH	INTEL® VIRTUALIZATION TECH	INTEL® ACTIVE MANAGEMENT TECH 9.0	INTEL® TRUSTED EXECUTION TECH	ERROR-CORRECTING CODE
Intel® Xeon® processor E3-1275 v5	Yes	Yes	Yes	Yes	Yes	Yes
Intel® Xeon® processor E3-1225 v5	Yes	No	Yes	Yes	Yes	Yes
Intel® Xeon® processor E3-1268 v5	Yes	Yes	Yes	Yes	Yes	Yes
Intel® Xeon® processor E3-1505M v5	Yes	Yes	Yes	Yes	Yes	Yes
Intel® Xeon® processor E3-1505L v5	Yes	Yes	Yes	Yes	Yes	Yes
Intel® Xeon® processor E3-1515M v5	Yes	Yes	Yes	Yes	Yes	Yes

INTEL® CHIPSETS FOR INTERNET OF THINGS SOLUTIONS

PRODUCT	PRODUCT CODE	PACKAGE	FEATURES
Intel® C236 Chipset	Not in mark system yet. Using plug GL82C236.	FC-BGA13	Supports ECC and Intel® Active Management Technology 11.0; up to eight SATA ports (6 Gbps); 14 total USB ports (up to 10 USB 3.0); up to 20 PCI Express* x1 Gen 3 ports; 1x16, 2x8 or 1x8+2x4 PCI Express graphics support; memory channels/DIMM per channel = 2/2
Intel® CM236 Chipset	Not in mark system yet. Using plug GL82CM236.	FC-BGA13	Supports ECC and Intel® Active Management Technology 11.0; up to eight SATA ports (6 Gbps); 14 total USB ports (up to 10 USB 3.0); up to 20 PCI Express* x1 Gen 3 ports; 1x16, 2x8 or 1x8+2x4 PCI Express graphics support; memory channels/DIMM per channel = 2/2

intel.com/iot

1. Requires a system with Intel® Turbo Boost Technology. Intel Turbo Boost Technology and Intel Turbo Boost Technology 2.0 are only available on select Intel® processors. Consult your system manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit http://www.intel.com/go/turbo.
2. Available on select Intel® Core™ processors. Requires an Intel® HT Technology-enabled system. Consult your PC manufacturer. Performance will vary depending on the specific hardware and software used. For more information, including details on which processors support HT Technology, visit http://www.intel.com/info/hyperthreading.
3. Measured by Intel on systems with Intel® Xeon® Processor E3-1268L v5 and Intel® Xeon® Processor E3-1268L v3 using SPECfp2006 (1-copy).
4. Measured by Intel on systems with Intel® Core™ i7-6820EQ processor and Intel® Core™ i7-5700EQ processor using SPECfp2006 (1-copy).
5. Measured by Intel on systems with Intel® Xeon® Processor E3-1268L v5 and Intel® Xeon® Processor E3-1268L v3 using 3DMark11*.
6. Measured by Intel on systems with Intel® Core™ i7-6820EQ processor and Intel® Core™ i7-5700EQ processor using 3DMark11.
7. Based on industry-standard cooling solutions. Actual TDP may vary.
8. Intel® Advanced Vector Extensions (Intel® AVX) are designed to achieve higher throughput to certain integer and floating point operations. Due to varying processor power characteristics, utilizing AVX instructions may cause, a) some parts to operate at less than the rated frequency and, b) some parts with Intel Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you should consult your system manufacturer for more information. Intel® Advanced Vector Extensions refers to Intel® AVX, Intel® AVX2 or Intel® AVX-512. For more information on Intel Turbo Boost Technology 2.0, visit http://www.intel.com/go/turbo.
9. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.
10. Actual number of ports available may vary by processor number and system configuration. Please refer to the specifications corresponding to the processor number of interest or consult your system vendor for more information.
11. Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro.
12. On eDP/DP at 24bpp and 60Hz.
13. Intel® AES-NI requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.
14. No computer system can be absolutely secure. Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.
15. Actual number of ports available may vary by processor number and system configuration. Please refer to the specifications corresponding to the processor number of interest or consult your system vendor for more information.
16. No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, and Intel® TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security.
17. Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary, depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

0316/KK/CMD/PDF ♻ Please Recycle 333023-002US