Intel Xeon 6248 processor

Artikel	21238331
Herstellernummer	BX806956248
EAN	0735858410533

Intel

Intel® Trusted-Execution-Technik
Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt werden.

Intel® Directed-I/O-Virtualisierungstechnik (VT-d)
Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

Intel® Virtualisierungstechnik (VT-x)
Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

Intel® 64
In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

Cache
Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Intel® Turbo-Boost-Technik
Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

Max. Turbo-Taktfrequenz
Die max. Turbo-Taktfrequenz ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor unter

Verwendung der Intel® Turbo-Boost-Technik und, falls vorhanden, der Intel® Turbo-Boost-Max-Technik 3.0 und des Intel® Thermal Velocity Boost arbeiten kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Execute-Disable-Bit
Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireninfektionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

Intel® Hyper-Threading-Technik
Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

Intel® vPro™ Plattformqualifizierung
Die Intel vPro® Plattform ist eine Reihe von Hardware- und Technologien, die zum Erstellen von Business-Computing-Endpunkten mit erstklassiger Leistung, integrierter Sicherheit, moderner Verwaltbarkeit und Plattformstabilität verwendet werden.

Intel® VT-x mit Extended Page Tables (EPT)
Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

Erweiterte Intel SpeedStep® Technologie
Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

Intel® Speed Shift Technology
Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

Intel® Deep Learning Boost (Intel® DL Boost)
Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

Befehlssatzerweiterungen
Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

Intel® Run-Sure-Technik
Die Intel® Run Sure-Technik umfasst RAS-Funktionen („Reliability, Availability, Serviceability“, Zuverlässigkeit, Verfügbarkeit, Wartungsfähigkeit), die für eine hohe Zuverlässigkeit und Plattformstabilität sorgen, um die Betriebszeit von Servern, auf denen geschäftskritische Workloads ausgeführt werden, zu maximieren.

Intel® Turbo Boost Max-Technik 3.0
Intel® Turbo Boost Max-Technik 3.0 identifiziert den/die Kern(e) mit der besten Leistung und liefert an diese Kerne erhöhte Leistung, indem sie die Taktfrequenz nach Bedarf steigert und dabei Strom- und Temperaturreserven verwendet.

Anzahl der UPI-Links
Intel® Ultra Path Interconnect (UPI) Links bedeutet ein Punkt-zu-Punkt-Hochgeschwindigkeit-Interconnect-Bus zwischen den Prozessoren, der erhöhte Bandbreite und Leistung über Intel® QPI bietet.

Anzahl der AVX-512 FMA-Einheiten
Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

Intel® Resource Director Technology (Intel® RDT)
Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

Intel® Speed Select Technology – Leistungsprofil
Es besteht die Möglichkeit, den Prozessor an drei spezifischen Betriebspunkten zu konfigurieren.

Intel® Speed Select Technology – Grundtaktfrequenz
Diese Technik ermöglicht es Nutzern, die garantierte Grundtaktfrequenz auf bestimmten Kernen (Kerne mit hoher Priorität) zu erhöhen, indem die restlichen Kerne (Kerne mit niedriger Priorität) eine niedrigere Grundtaktfrequenz erhalten. Dadurch wird die Gesamtleistung erhöht, indem die Frequenz auf den kritischen Kernen erhöht wird.

Intel® Volume Management Device (VMD)
Intel® Volume Management Device (VMD) bietet eine allgemeine, robuste Hot-Plug- und LED-Management-Methode für NVME-Solid-State-Laufwerke.

Persistenter Intel® Optane™ DC Speicher unterstützt
Der persistente Intel® Optane™ DC Speicher stellt eine revolutionäre Ebene von nichtflüchtigem Speicher dar, der zwischen dem Arbeits- und Datenspeicher angesiedelt ist, um eine große und kostengünstige Speicherkapazität zu liefern, die mit DRAM-Leistung vergleichbar ist. Dank der großen Speicherkapazität auf Systemebene bei Kombinierung mit traditionellem DRAM unterstützt der persistente Intel Optane DC Speicher die Wandlung von Workloads mit beschränktem Speicher: Cloud, Datenbanken, In-Memory-Analysen, Virtualisierung und CDN-Anwendungen (Netzwerke zur Inhaltsbereitstellung).

Mode-based Execute Control (modusbasierte Ausführungssteuerung, MBEC)
Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

Intel® TSX-NI
Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

Zusammenfassung

Intel® Trusted-Execution-Technik
Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt werden.

Intel® Directed-I/O-Virtualisierungstechnik (VT-d)
Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

Intel® Virtualisierungstechnik (VT-x)
Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

Intel® 64
In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

Cache
Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Intel® Turbo-Boost-Technik
Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

Max. Turbo-Taktfrequenz
Die max. Turbo-Taktfrequenz ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor unter Verwendung der Intel® Turbo-Boost-Technik und, falls vorhanden, der Intel® Turbo-Boost-Max-Technik 3.0 und des Intel® Thermal Velocity Boost arbeiten kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Execute-Disable-Bit
Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireninfektionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

Intel® Hyper-Threading-Technik
Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

Intel® vPro™ Plattformqualifizierung
Die Intel vPro® Plattform ist eine Reihe von Hardware- und Technologien, die zum Erstellen von Business-Computing-Endpunkten mit erstklassiger Leistung, integrierter Sicherheit, moderner Verwaltbarkeit und Plattformstabilität verwendet werden.

Intel® VT-x mit Extended Page Tables (EPT)
Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

Erweiterte Intel SpeedStep® Technologie
Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

Intel® Speed Shift Technology
Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

Intel® Deep Learning Boost (Intel® DL Boost)
Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

Befehlssatzerweiterungen
Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

Intel® Run-Sure-Technik
Die Intel® Run Sure-Technik umfasst RAS-Funktionen („Reliability, Availability, Serviceability“, Zuverlässigkeit, Verfügbarkeit, Wartungsfähigkeit), die für eine hohe Zuverlässigkeit und Plattformstabilität sorgen, um die Betriebszeit von Servern, auf denen geschäftskritische Workloads ausgeführt werden, zu maximieren.

Intel® Turbo Boost Max-Technik 3.0
Intel® Turbo Boost Max-Technik 3.0 identifiziert den/die Kern(e) mit der besten Leistung und liefert an diese Kerne erhöhte Leistung, indem sie die Taktfrequenz nach Bedarf steigert und dabei Strom- und Temperaturreserven verwendet.

Anzahl der UPI-Links
Intel® Ultra Path Interconnect (UPI) Links bedeutet ein Punkt-zu-Punkt-Hochgeschwindigkeit-Interconnect-Bus zwischen den Prozessoren, der erhöhte Bandbreite und Leistung über Intel® QPI bietet.

Anzahl der AVX-512 FMA-Einheiten
Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

Intel® Resource Director Technology (Intel® RDT)
Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

Intel® Speed Select Technology – Leistungsprofil
Es besteht die Möglichkeit, den Prozessor an drei spezifischen Betriebspunkten zu konfigurieren.

Intel® Speed Select Technology – Grundtaktfrequenz
Diese Technik ermöglicht es Nutzern, die garantierte Grundtaktfrequenz auf bestimmten Kernen (Kerne mit hoher Priorität) zu erhöhen, indem die restlichen Kerne (Kerne mit niedriger Priorität) eine niedrigere Grundtaktfrequenz erhalten. Dadurch wird die Gesamtleistung erhöht, indem die Frequenz auf den kritischen Kernen erhöht wird.

Intel® Volume Management Device (VMD)
Intel® Volume Management Device (VMD) bietet eine allgemeine, robuste Hot-Plug- und LED-Management-Methode für NVME-Solid-State-Laufwerke.

Persistenter Intel® Optane™ DC Speicher unterstützt
Der persistente Intel® Optane™ DC Speicher stellt eine revolutionäre Ebene von nichtflüchtigem Speicher dar, der zwischen dem Arbeits- und Datenspeicher angesiedelt ist, um eine große und kostengünstige Speicherkapazität zu liefern, die mit DRAM-Leistung vergleichbar ist. Dank der großen Speicherkapazität auf Systemebene bei Kombinierung mit traditionellem DRAM unterstützt der persistente Intel Optane DC Speicher die Wandlung von Workloads mit beschränktem Speicher: Cloud, Datenbanken, In-Memory-Analysen, Virtualisierung und CDN-Anwendungen (Netzwerke zur Inhaltsbereitstellung).

Mode-based Execute Control (modusbasierte Ausführungssteuerung, MBEC)
Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

Intel® TSX-NI
Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

Intel Xeon 6248, Intel® Xeon® Gold, LGA 3647 (Socket P), 14 nm, Box, Intel, 2,5 GHz

Intel Xeon 6248. Prozessorfamilie: Intel® Xeon® Gold, Prozessorsockel: LGA 3647 (Socket P), Prozessor Lithografie: 14 nm. Speicherkanäle: Hexa-Kanal, Maximaler interner Speicher, vom Prozessor unterstützt: 1,02 TB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM. Marktsegment: Server, Unterstützte Befehlssätze: SSE4.2, AVX, AVX 2.0, AVX-512, Skalierbarkeit: 4S. Prozessor-Paketgröße: 76mm x 56.5mm. RAM-Speicher maximal: 1 TB

Merkmale

Betriebsbedingungen

Tcase	86 °C

Gewicht und Abmessungen

Prozessor-Paketgröße	76mm x 56.5mm

Logistikdaten

Warentarifnummer (HS)	85423119

Sonstige Funktionen

RAM-Speicher maximal	1 TB

Speicher

Maximaler interner Speicher, vom Prozessor unterstützt	1,02 TB
Speichertypen, vom Prozessor unterstützt	DDR4-SDRAM
Speichertaktraten, vom Prozessor unterstützt	2933 MHz
Speicherkanäle	Hexa-Kanal
ECC	Ja

Technische Details

Startdatum	Q2'19
Produkttyp	Processor
Status	Launched
Unterstützte Arbeitsspeicher	DDR4-SDRAM
Speichergeschwindigkeit (max.)	2933 MHz
Anzahl der UPI-Links	3
Instandhaltungsstatus	Baseline Servicing

Grafik

Eingebaute Grafikadapter	Nein
Separater Grafikadapter	Nein
Eingebautes Grafikkartenmodell	Nicht verfügbar
Separates Grafikkartenmodell	Nicht verfügbar

Merkmale

Execute Disable Bit	Ja
Marktsegment	Server
Maximale Anzahl der PCI-Express-Lanes	48
PCI-Express-Slots-Version	3.0
Unterstützte Befehlssätze	SSE4.2, AVX, AVX 2.0, AVX-512
Skalierbarkeit	4S
Eingebettete Optionen verfügbar	Nein
PCI Express CEM Revision	3.0
Exportkontroll-Klassifizierungsnummer (ECCN)	5A992C
Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS)	G077159

Prozessor

Prozessorhersteller	Intel
Prozessorgeneration	Skalierbare Intel® Xeon® der 2. Generation
Prozessor	6248
Grundfrequenz des Prozessors	2,5 GHz
Prozessorfamilie	Intel® Xeon® Gold
Anzahl Prozessorkerne	20
Prozessorsockel	LGA 3647 (Socket P)
Komponente für	Server/Arbeitsstation
Prozessor Lithografie	14 nm
Prozessor-Threads	40
Prozessorbetriebsmodi	64-Bit
Prozessor Boost-Frequenz	3,9 GHz
Prozessor-Cache	27,5 MB
Thermal Design Power (TDP)	150 W
Verpackungsart	Box
Kühler enthalten	Ja
Prozessor Codename	Cascade Lake
ARK Prozessorerkennung	192446

Prozessor Besonderheiten

Intel® Hyper-Threading-Technik (Intel® HT Technology)	Ja
Intel® Turbo-Boost-Technologie	2.0
Intel® AES New Instructions (Intel® AES-NI)	Ja
Verbesserte Intel SpeedStep Technologie	Ja
Intel® Trusted-Execution-Technik	Ja
Intel®-Speed-Shift-Technologie	Ja
Intel® Transactional Synchronization Extensions	Ja
Intel® VT-x mit Extended Page Tables (EPT)	Ja
Intel® TSX-NI	Ja
Intel® 64	Ja
Intel® Virtualization Technologie (VT-X)	Ja
Intel® Virtualisierungstechnik für direkte I/O (VT-d)	Ja
Intel Turbo Boost Max	Nein

Technology 3.0	
AVX-512 Abgesicherte Multiply-Add (FMA) Einheiten	2
Intel® Deep Learning Boost (Intel® DL Boost) on CPU	Ja
Intel® Speed Select-Technologie - Leistungsprofil (Intel® SST-PP)	Nein
Intel® Resource Director Technology (Intel® RDT)	Ja
Intel® Volume Management Device (VMD)	Ja
Intel® Run Sure Technology	Ja
Modusbasierte Execute Control (MBE)	Ja
Intel® Optane™ DC Persistent Memory unterstützt	Ja
Intel® vPro™ Platform Eligibility	Ja
Intel Speed Select Technology (SST)	Nein
Intel® Speed Select Technology - Base Frequency (Intel® SST-BF)	Nein
Intel® Optane™ DC Persistent Memory-Technologie	Ja