

# Intel Core i9-12900KS processor

---



<b>Artikel</b>	125831
<b>Herstellernummer</b>	BX8071512900KS
<b>EAN</b>	0735858513289
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.<sup>1</sup> Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

## **Intel® Clear-Video-HD-Technik**

Intel® Clear-Video-HD-Technik ist wie die Vorgängerversion Intel® Clear-Video-Technik eine Suite von Bilddecodierungs- und Bildverarbeitungstechnologien in der integrierten Prozessorgrafik, die die Videowiedergabe verbessert und bessere, schärfere Bilder und natürlichere, realitätsgetreuere und lebendigere Farben sowie ein klares und stabiles Videobild bietet. Die Intel® Clear-Video-HD-Technik bietet Qualitätsverbesserungen für Videos und somit sattere Farben und realistischere Hauttöne.

## **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.

## **Ruhezustände**

Ruhezustände (C-Zustände) werden genutzt, um Energie zu sparen, wenn der Prozessor sich im Leerlauf befindet. C0 ist der Betriebszustand, d. h. die CPU führt sinnvolle Aufgaben aus. C1 ist der erste Leerlaufzustand, C2 der zweite usw., wobei für höhere Nummern des C-Zustands mehr Energiesparmaßnahmen durchgeführt werden.

## **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 maximale Turbo-Taktfrequenz ist die maximale Einzelkern-Taktfrequenz, zu der der Prozessor mit der Intel® Turbo-Boost-Technik und, falls vorhanden, mit Intel® Thermal Velocity Boost betrieben werden kann. Die Frequenz wird in Gigahertz (GHz) gemessen bzw. in Milliarden Takten 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.

## **Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

## **Intel® Quick-Sync-Video**

Intel® Quick-Sync-Video bietet schnelle Videoumwandlung für tragbare Medienplayer, Online-Veröffentlichung sowie Videobearbeitung und -entwicklung.

## **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.

## **Intel® Optane™ Speicher unterstützt**

Intel® Optane™ Speicher ist eine revolutionäre neue Klasse von nichtflüchtigem Speicher, der zwischen dem Systemspeicher und dem Datenspeicher angesiedelt ist, um die Leistung und Reaktionsgeschwindigkeit des Systems zu beschleunigen. In Kombination mit dem Intel® Rapid-Storage-Technik-Treiber verwaltet er nahtlos mehrere Speicherstufen, bei Bereitstellung eines virtuellen Laufwerks für das Betriebssystem. Dadurch wird sichergestellt, dass sich häufig verwendete Daten auf der schnellsten Speicherstufe befinden. Intel® Optane™ Speicher erfordert eine spezifische Hardware- und Softwarekonfiguration. Die Konfigurationsvoraussetzungen finden Sie unter .

## **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.

## **Secure Key**

Intel® Secure Key basiert auf einem digitalen Zufallszahlengenerator, der vollkommen zufällige Zahlen generiert und so Verschlüsselungsalgorithmen stärkt.

## **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.

### **Taktfrequenzen mit Intel® Thermal Velocity Boost**

Intel® Thermal Velocity Boost (Intel® TVB) ist eine Funktion, die die Taktfrequenz opportunistisch und automatisch über die Einzelkern- und Multicore-Taktfrequenzen der Intel® Turbo-Boost-Technik hinaus erhöht, und zwar basierend darauf, wie stark der Prozessor unter der Maximaltemperatur betrieben wird und ob ein Turboantriebbudget vorhanden ist. Die Frequenzsteigerung und ihre Dauer hängen von der Last, der Prozessorfunktionalität und der Kühlösung ab.

### **Intel® Turbo Boost Max-Technik 3.0 Frequenz**

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 Temperaturreerven verwendet. Intel® Turbo Boost Max-Technik 3.0 Frequenz ist die Taktfrequenz der CPU, wenn sie in diesem Modus läuft.

### **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 Temperaturreerven verwendet.

### **Intel® Total Memory Encryption**

TME – Total Memory Encryption (TME) schützt Daten vor dem Risiko physischer Angriffe auf den Speicher, wie Kaltstartattacken.

### **Thermal-Monitoring-Technologien**

Thermal-Monitoring-Technologien schützen das Prozessorkpaket und das System über Temperaturverwaltungsfunktionen vor temperaturbedingten Ausfällen. Ein digitaler Temperatursensor auf dem Chip erkennt die Temperatur des Kerns, und die Temperaturverwaltungsfunktionen senken bei Bedarf den Energieverbrauch des Pakets und damit die Temperatur, um die Grenzwerte für den normalen Betrieb einzuhalten.

### **Intel® Thermal Velocity Boost - Temperatur**

Bei der Temperatur des Intel® Thermal Velocity Boost (Intel® TVB) handelt es sich um den Grenzwert der Betriebstemperatur, die eine Intel® TVB Taktfrequenz zulässt; höhere Temperaturen können opportunistisch die Intel® TVB Taktfrequenz zulassen.

### **Intel® Thermal Velocity Boost**

Intel® Thermal Velocity Boost (Intel® TVB) ist eine Funktion, die die Taktfrequenz opportunistisch und automatisch über die Einzelkern- und Multicore-Taktfrequenzen der Intel® Turbo-Boost-Technik hinaus erhöht, und zwar basierend darauf, wie stark der Prozessor unter der Maximaltemperatur betrieben wird und ob ein Turboantriebbudget vorhanden ist. Die Frequenzsteigerung und ihre Dauer hängen von der Last, der Prozessorfunktionalität und der Kühlösung ab.

### **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.

### **Intel® Gauß- und neuraler Beschleuniger**

Der Intel® Gauß- und neuraler Beschleuniger (GNA) ist ein bei äußerst niedrigem Stromverbrauch laufender Beschleunigerblock, der für Audio- und geschwindigkeitszentrierte KI-Workloads entwickelt wurde. Intel® GNA wurde entwickelt, um audiobasierte neurale Netzwerke bei äußerst niedrigem Stromverbrauch auszuführen und gleichzeitig der CPU diese Arbeitslast abzunehmen.

### **MBE (Mode-based Execute Control, modusbasierte Ausführungssteuerung)**

Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

### **Intel® Boot Guard**

Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und böartigen Softwareangriffen vor der Aktivierung des Betriebssystems bei.

### **Intel® Control-Flow Enforcement Technology**

CET – Intel Control-Flow Enforcement Technology (CET) schützt vor dem Missbrauch legitimer Code-Ausschnitte durch ROP-Angriffe (return-oriented programming) zur Übernahme der Kontrollstruktur.

## **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 Rechengvorgänge 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.<sup>1</sup> Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

### **Intel® Clear-Video-HD-Technik**

Intel® Clear-Video-HD-Technik ist wie die Vorgängerversion Intel® Clear-Video-Technik eine Suite von Bildecodierungs- und Bildverarbeitungstechnologien in der integrierten Prozessorgrafik, die die Videowiedergabe verbessert und bessere, schärfere Bilder und natürlichere, realitätsgetreuere und lebendigere Farben sowie ein klares und stabiles Videobild bietet. Die Intel® Clear-Video-HD-Technik bietet Qualitätsverbesserungen für Videos und somit sattere Farben und realistischere Hauttöne.

### **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.

### **Ruhezustände**

Ruhezustände (C-Zustände) werden genutzt, um Energie zu sparen, wenn der Prozessor sich im Leerlauf befindet. C0 ist der Betriebszustand, d. h. die CPU führt sinnvolle Aufgaben aus. C1 ist der erste Leerlaufzustand, C2 der zweite usw., wobei für höhere Nummern des C-Zustands mehr Energiesparmaßnahmen durchgeführt werden.

### **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 maximale Turbo-Taktfrequenz ist die maximale Einzelkern-Taktfrequenz, zu der der Prozessor mit der Intel® Turbo-Boost-Technik und, falls vorhanden, mit Intel® Thermal Velocity Boost betrieben werden kann. Die Frequenz wird in Gigahertz (GHz) gemessen bzw. in Milliarden Takten 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.

### **Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

### **Intel® Quick-Sync-Video**

Intel® Quick-Sync-Video bietet schnelle Videoumwandlung für tragbare Medienplayer, Online-Veröffentlichung sowie Videobearbeitung und -entwicklung.

### **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.

### **Intel® Optane™ Speicher unterstützt**

Intel® Optane™ Speicher ist eine revolutionäre neue Klasse von nichtflüchtigem Speicher, der zwischen dem Systemspeicher und dem Datenspeicher angesiedelt ist, um die Leistung und Reaktionsgeschwindigkeit des Systems zu beschleunigen. In Kombination mit dem Intel® Rapid-Storage-Technik-Treiber verwaltet er nahtlos mehrere Speicherstufen, bei Bereitstellung eines virtuellen Laufwerks für das Betriebssystem. Dadurch wird sichergestellt, dass sich häufig verwendete Daten auf der schnellsten Speicherstufe befinden. Intel® Optane™ Speicher erfordert eine spezifische Hardware- und Softwarekonfiguration. Die Konfigurationsvoraussetzungen finden Sie unter .

### **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.

### **Secure Key**

Intel® Secure Key basiert auf einem digitalen Zufallszahlengenerator, der vollkommen zufällige Zahlen generiert und so Verschlüsselungsalgorithmen stärkt.

### **Intel® Speed Shift Technology**

Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-States, 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.

### **Taktfrequenzen mit Intel® Thermal Velocity Boost**

Intel® Thermal Velocity Boost (Intel® TVB) ist eine Funktion, die die Taktfrequenz opportunistisch und automatisch über die Einzelkern- und Multicore-Taktfrequenzen der Intel® Turbo-Boost-Technik hinaus erhöht, und zwar basierend darauf, wie stark der Prozessor unter der Maximaltemperatur betrieben wird und ob ein Turboantriebbudget vorhanden ist. Die Frequenzsteigerung und ihre Dauer hängen von der Last, der Prozessorfunktionalität und der Kühlung ab.

### **Intel® Turbo Boost Max-Technik 3.0 Frequenz**

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 Temperaturreerven verwendet. Intel® Turbo Boost Max-Technik 3.0 Frequenz ist die Taktfrequenz der CPU, wenn sie in diesem Modus läuft.

### **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 Temperaturreerven verwendet.

### **Intel® Total Memory Encryption**

TME – Total Memory Encryption (TME) schützt Daten vor dem Risiko physischer Angriffe auf den Speicher, wie Kaltstartattacken.

## Thermal-Monitoring-Technologien

Thermal-Monitoring-Technologien schützen das Prozessorpaket und das System über Temperaturverwaltungsfunktionen vor temperaturbedingten Ausfällen. Ein digitaler Temperatursensor auf dem Chip erkennt die Temperatur des Kerns, und die Temperaturverwaltungsfunktionen senken bei Bedarf den Energieverbrauch des Pakets und damit die Temperatur, um die Grenzwerte für den normalen Betrieb einzuhalten.

### Intel® Thermal Velocity Boost - Temperatur

Bei der Temperatur des Intel® Thermal Velocity Boost (Intel® TVB) handelt es sich um den Grenzwert der Betriebstemperatur, die eine Intel® TVB Taktfrequenz zulässt; höhere Temperaturen können opportunistisch die Intel® TVB Taktfrequenz zulassen.

### Intel® Thermal Velocity Boost

Intel® Thermal Velocity Boost (Intel® TVB) ist eine Funktion, die die Taktfrequenz opportunistisch und automatisch über die Einzelkern- und Multicore-Taktfrequenzen der Intel® Turbo-Boost-Technik hinaus erhöht, und zwar basierend darauf, wie stark der Prozessor unter der Maximaltemperatur betrieben wird und ob ein Turboantriebbudget vorhanden ist. Die Frequenzsteigerung und ihre Dauer hängen von der Last, der Prozessorfunktionalität und der Kühllösung ab.

### 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.

### Intel® Gauß- und neuraler Beschleuniger

Der Intel® Gauß- und neuraler Beschleuniger (GNA) ist ein bei äußerst niedrigem Stromverbrauch laufender Beschleunigerblock, der für Audio- und geschwindigkeitszentrierte KI-Workloads entwickelt wurde. Intel® GNA wurde entwickelt, um audiobasierte neuronale Netzwerke bei äußerst niedrigem Stromverbrauch auszuführen und gleichzeitig der CPU diese Arbeitslast abzunehmen.

### MBE (Mode-based Execute Control, modusbasierte Ausführungssteuerung)

Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

### Intel® Boot Guard

Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und bösartigen Softwareangriffen vor der Aktivierung des Betriebssystems bei.

### Intel® Control-Flow Enforcement Technology

CET – Intel Control-Flow Enforcement Technology (CET) schützt vor dem Missbrauch legitimer Code-Ausschnitte durch ROP-Angriffe (return-oriented programming) zur Übernahme der Kontrollstruktur.

Intel Core i9-12900KS, Intel® Core™ i9, LGA 1700, Intel, i9-12900KS, 64-Bit, Intel® Core™ i9 Prozessoren der 12. Generation

Intel Core i9-12900KS. Prozessorfamilie: Intel® Core™ i9, Prozessorsockel: LGA 1700, Prozessorhersteller: Intel. Speicherkanäle: Zweikanalig, Maximaler interner Speicher, vom Prozessor unterstützt: 128 GB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM, DDR5-SDRAM. On-Board Grafikkartenmodell: Intel UHD Graphics 770, On-Board Grafikkarten unterstützte Ausgänge: Embedded DisplayPort (eDP) 1.4b, DisplayPort 1.4a, HDMI 2.1, On-Board Grafikkarten Basisfrequenz: 300 MHz. Marktsegment: Desktop, Nutzungsbedingungen: PC/Client/Tablet, PCI-Express-Slots-Version: 4.0, 5.0. Intel® Turbo Boost Max Technology 3.0 frequency: 5,3 GHz, Intel® Thermal Velocity Boost Temperature: 50 °C, Intel® Thermal Velocity Boost Frequency: 5,5 GHz

## Merkmale

### Betriebsbedingungen

Tjunction 90 °C

### Gewicht und Abmessungen

Prozessor-Paketgröße 45 x 37.5 mm

### Logistikdaten

Warentarifnummer (HS) 85423119

### Speicher

Maximaler interner Speicher, vom128 GB  
Prozessor unterstützt  
Speichertypen, vom Prozessor unterstützt DDR4-SDRAM, DDR5-SDRAM  
Speicherkanäle Zweikanalig  
ECC Ja  
Speicherbandbreite (max.) 76,8 GB/s

### Merkmale

Execute Disable Bit Ja  
Leerlauf Zustände Ja

## Verpackungsdaten

Verpackungsart	Einzelhandels-Box
----------------	-------------------

## Sonstige Funktionen

RAM-Speicher maximal	128 GB
Grafischer Ausgang	eDP 1.4b, DP 1.4a, HDMI 2.1

## Technische Details

Zielmarkt	Gaming, Content Creation
OpenCL-Version	2.1
Startdatum	Q1'22
Status	Launched

Thermal-Überwachungstechnologien	Ja
Marktsegment	Desktop
Nutzungsbedingungen	PC/Client/Tablet
Maximale Anzahl der PCI-Express-Lanes	20
PCI-Express-Slots-Version	4.0, 5.0
PCI Express Konfigurationen	1x16+1x4, 2x8+1x4
Unterstützte Befehlssätze	SSE4.1, SSE4.2, AVX 2.0
Skalierbarkeit	1S
CPU Konfiguration (max)	1
Eingebettete Optionen verfügbar	Nein
Direkte Medienschnittstelle (DMI)	4.0
Revision	
Exportkontroll-Klassifizierungsnummer (ECCN)	5A992CN3
Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS)	G167599

## Grafik

Eingebaute Grafikkadaper	Ja
Separater Grafikkadaper	Nein
On-Board Grafikkadapermodell	Intel UHD Graphics 770
On-Board Grafikkadaper unterstützte Ausgänge	Embedded DisplayPort (eDP) 1.4b, DisplayPort 1.4a, HDMI 2.1
On-Board Grafikkadaper Basisfrequenz	300 MHz
Maximale dynamische Frequenz der On-Board Grafikkadaper	1550 MHz
Anzahl an unterstützten Displays (On-Board-Grafik)	4
On-Board Grafikkadaper DirectX Version	12.0
On-Board Grafikkadaper OpenGL Version	4.5
Maximale Auflösung des On-Board Grafikkadapers (DisplayPort)	7680 x 4320 Pixel
Maximale Auflösung des On-Board Grafikkadapers (eDP - integrierter Flachbildschirm)	5120 x 3200 Pixel
Integrierter Grafik-Adapter maximale Auflösung (HDMI)	4096 x 2160 Pixel
Bildwiederholffrequenz des On-Board Grafikkadapers bei maximaler Auflösung (DisplayPort)	60 Hz
Bildwiederholffrequenz des On-Board Grafikkadapers bei maximaler Auflösung (eDP - integrierter Flachbildschirm)	120 Hz
Bildwiederholffrequenz des On-Board Grafikkadapers bei maximaler Auflösung (HDMI)	60 Hz
On-Board Grafikkadaper Geräte-ID	0x4680
Dediziertes Grafikkadapermodell	Nicht verfügbar
Anzahl der Rechenwerke	32
Multi-Format-Codec-Engines	2

## Prozessor

Prozessorhersteller	Intel
Prozessorgeneration	Intel® Core™ i9 Prozessoren der 12. Generation
Prozessor	i9-12900KS
Prozessorfamilie	Intel® Core™ i9
Anzahl Prozessorkerne	16
Prozessorsockel	LGA 1700
Prozessor-Threads	24
Prozessorbetriebsmodi	64-Bit
Leistungskerne	8
Effiziente Kerne	8
Prozessor Boost-Frequenz	5,5 GHz
Leistung Kern-Boost-Frequenz	5,2 GHz
Leistung Basisfrequenz des Kerns	3,4 GHz
Effiziente Kern-Boost-Frequenz	4 GHz
Effiziente Basisfrequenz des Kerns	2,5 GHz
Prozessor-Cache	30 MB
Prozessor Cache Typ	Smart Cache
Box	Ja
Grundleistung des Prozessors	150 W
Maximale Turboleistung	241 W
Bus Typ	DMI4
Maximale Anzahl DMI-Spuren	8
Durch den Prozessor (max) unterstützte Speicherbandbreite	76,8 GB/s
Prozessor Codename	Alder Lake
ARK Prozessorerkennung	225916

## Prozessor Besonderheiten

Intel® Hyper-Threading-Technik (Intel® HT Technology)	Ja
Intel® Turbo-Boost-Technologie	2.0
Intel® Quick-Sync-Video-Technik	Ja
Intel® Clear Video HD Technology für (Intel® CVT HD)	Ja
Intel® AES New Instructions (Intel® AES-NI)	Ja
Verbesserte Intel SpeedStep Technologie	Ja
Intel® Trusted-Execution-Technik	Ja
Intel®-Speed-Shift-Technologie	Ja
Intel® Thermal Velocity Boost (Thermischer Geschwindigkeitsanstieg)	Ja
Intel® Adaptive Boost Technology	Ja
Intel® Turbo Boost Max Technology 3.0 frequency	5,3 GHz
Intel® Total Memory Encryption	Ja
Intel® Gaussian & Neural Accelerator (Intel® GNA) 3.0	Ja
Intel® Thermal Velocity Boost Temperature	50 °C
Intel® Thermal Velocity Boost Frequency	5,5 GHz
Intel® Control-flow Enforcement Technology (CET)	Ja
Intel® Thread Director	Ja
Intel® VT-x mit Extended Page Tables (EPT)	Ja
Intel® Sicherer Schlüssel	Ja

Intel® Active Management Technologie (Intel® AMT)	Ja
Intel® OS Guard	Ja
Intel® 64	Ja
Intel® Virtualization Technologie (VT-X)	Ja
Intel® Virtualisierungstechnik für direkte I/O (VT-d)	Ja
Intel Turbo Boost Max Technology 3.0	Ja
Intel® Optane™ Memory-bereit	Ja
Intel® Boot Guard	Ja
Intel® Deep Learning Boost (Intel® DL Boost)	Ja
Intel® Volume Management Device (VMD)	Ja
Modusbasierte Execute Control (MBE)	Ja
Intel® vPro™ Platform Eligibility	Ja
Intel® Standard Manageability (ISM)	Ja
Intel® One-Click Recovery	Ja
Intel® Virtualisierungstechnik mit Umleitungsschutz (VT-rp)	Ja
Intel vPro® Enterprise Plattform-Berechtigung	Ja
Intel® Threat Detection Technology (TDT)	Ja
Intel® Hardware Shield Eligibility	Ja
Intel® Total Memory Encryption - Multi Key	Ja

Preisänderungen und Irrtümer vorbehalten. Alle Produkte solange der Vorrat reicht.