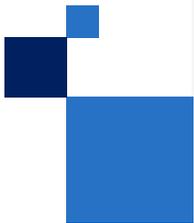
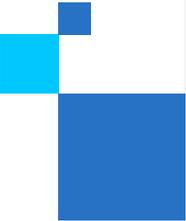


# Confidential Computing:

Bewältigung kritischer geschäftlicher  
Herausforderungen mit Intel-basierten Lösungen





# Was ist Confidential Computing?

# Was ist Confidential Computing?

Confidential Computing ermöglicht die Extraktion von Erkenntnissen oder das Trainieren von KI-Modellen mit sensiblen Daten, ohne diese Daten für andere Software, Mitarbeiter oder Ihren Cloud-Anbieter freizugeben  
Das eröffnet Unternehmen weitreichende Möglichkeiten, Daten für Analysen und andere Zwecke zu nutzen, die dafür bisher zu sensibel oder zu reguliert waren

Das Segment für Confidential Computing Software wird voraussichtlich das größte und am schnellsten wachsende Marktsegment sein, gefolgt von Hardware und Dienstleistungen



In nur wenigen Jahren hat Confidential Computing breite Aufmerksamkeit und Dynamik als leistungsstarke neue Möglichkeit erhalten, einen End-to-End-Schutz von In-Use-Code und Daten zu bieten

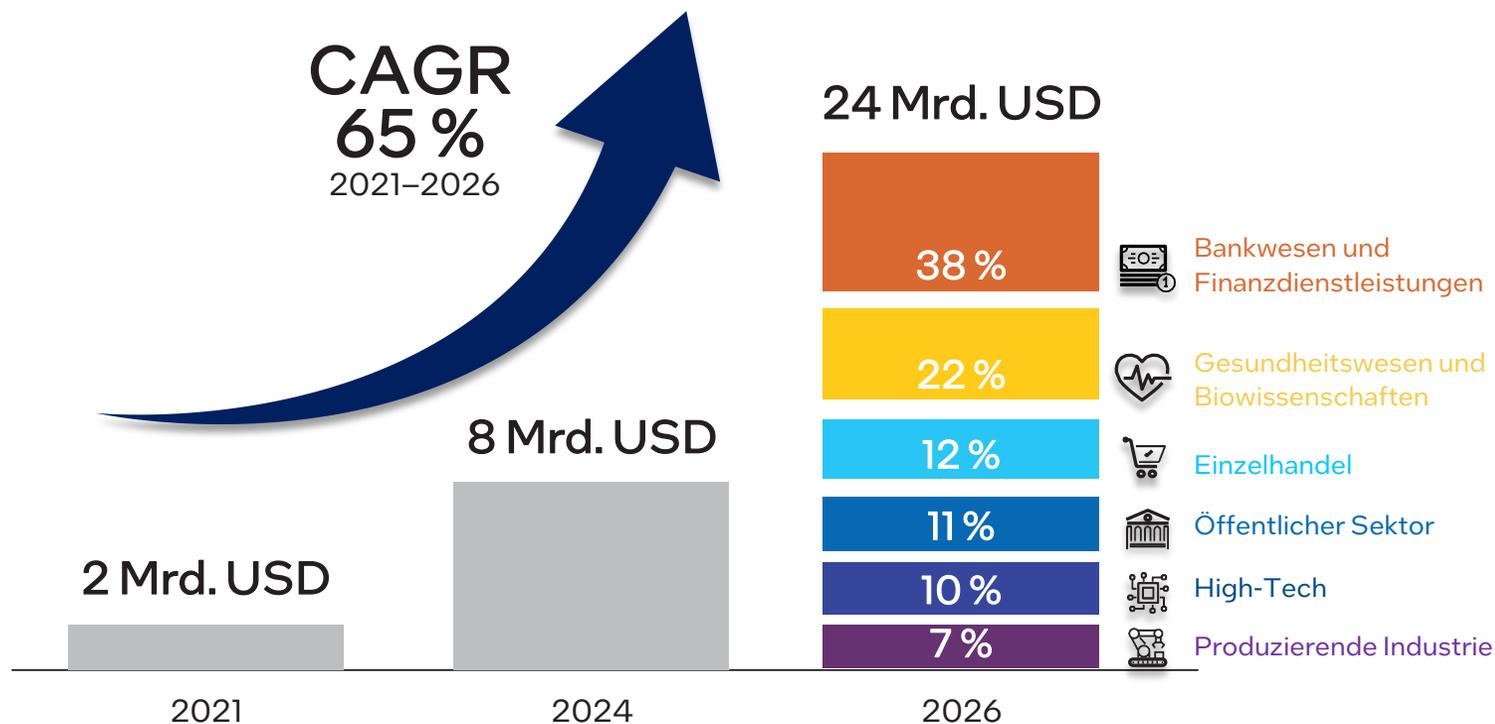
## Die Notwendigkeit für Confidential Computing Schließt eine große Lücke im Datenschutz-Kontinuum



Laut der Everest Group ist diese „nächste Grenze in der Datensicherheit ... für exponentielles Wachstum aufgestellt.“  
Der globale Markt (1,9 Milliarden USD im Jahr 2021) wird bis 2026 voraussichtlich mit einer jährlichen Wachstumsrate von 40 % bis 95 % wachsen, angetrieben durch Cloud- und Sicherheitsprojekte.

# Marktprognose für Confidential Computing

Erwartetes exponentielles Wachstum, angetrieben von Cloud-Sicherheit und datenschutzerhaltender Mehrparteienberechnung

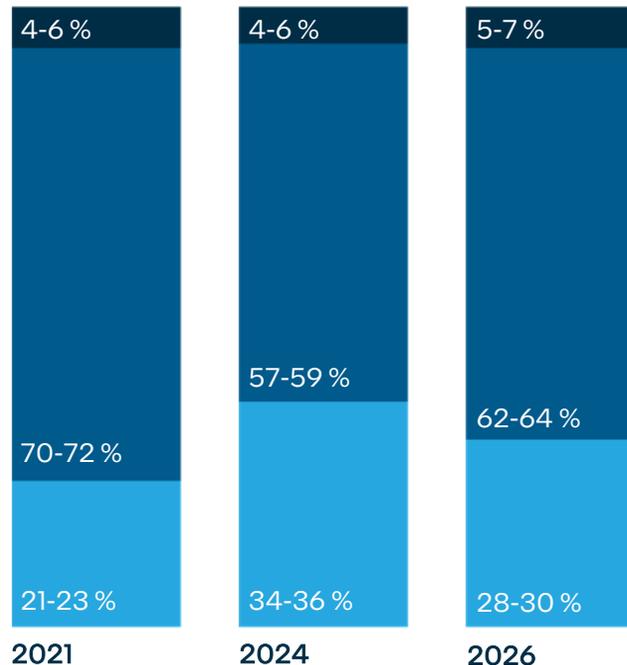


# Markt für Confidential Computing

Das Segment für Confidential Computing Software wird voraussichtlich das größte und am schnellsten wachsende Marktsegment sein, gefolgt von Hardware und Dienstleistungen

**Confidential Computing TAM, nach Technologiesegment**  
Prozentsatz, KJ 2021-26

100 % = 1,9-2 Mrd. USD    16-18 Mrd. USD    52-54 Mrd. USD



Hardware Software Dienst

## DIENSTLEISTUNGS-UNTERSEGMENTE

CAGR = 100-105 %

Globale Systemintegratoren (Anteil in %)	Interne Dienstleistungspraktiken von ISVs (Anteil in %)
8-10 %	90-92 %

- Dienstleistungen bleiben auf frühe Konzeptnachweise mit minimalen Lösungen oder Serviceangeboten beschränkt
- Der Großteil der Dienstleistungsnachfrage wird wahrscheinlich durch interne Dienstleistungspraxis von ISVs erfüllt werden

## SOFTWARE-UNTERSEGMENTE

CAGR = 90-95 %

Cloud-Serviceanbieter (Anteil in %)	Enablement-Software-ISVs (Anteil in %)
83-85 %	15-17 %

- Das Enablement-Softwaresegment besteht aus Technologien, die zur Einführung und Verwaltung von TEEs und TEE-basierten Anwendungen verwendet werden
- Mit zunehmender Marktreife wird der Beitrag von Enablement-Software voraussichtlich steigen
- Nimmt 2021 eine Preisprämie des 1,5-2-fachen normalen Computing für CSPs mit Normalisierung im Laufe der Zeit an

## HARDWARE-UNTERSEGMENTE

CAGR = 100-105 %

Halbleiter-Chipsatz-OEMs (Anteil in %)	Montierte Server-OEMs (Anteil in %)
51-53 %	47-49 %

- Begrenzte bis keine Preisunterschiede bei Computing-Hardware für CC im Vergleich zu regulärer Hardware werden die Nachfrage weiter ankurbeln
- Beitrag von Halbleiter-Chipsätzen, die aufgrund der zunehmenden Einführung in Cloud-Umgebungen den Markt für montierte Server nach 2024 voraussichtlich übertreffen werden

# Warum Confidential Computing?

Migrieren Sie vertrauensvoll in die Cloud mit dem Wissen, dass Sie die Kontrolle haben

Selbst mit vertraulichen oder regulierten Daten

Arbeiten Sie mit mehreren Parteien an vorteilhaften gemeinsamen Analysen

Unter Wahrung von Datenschutz und Compliance

Stärken Sie Compliance- und Datensouveränitätsprogramme

Mit technologischen Kontrollen

Anwendungssicherheit und IP-Schutz härten

Hardware-basierte Isolations- und Zugriffskontrollen

## Warum ist Confidential Computing für Ihr Unternehmen unerlässlich?

**Datensicherheit und IP-Schutz**

Schützen Sie Apps und Daten vor Angriffen, Manipulation oder Diebstahl

**Datenschutz und Compliance**

Stärken Sie Datenvertraulichkeit und Einhaltung gesetzlicher Vorschriften

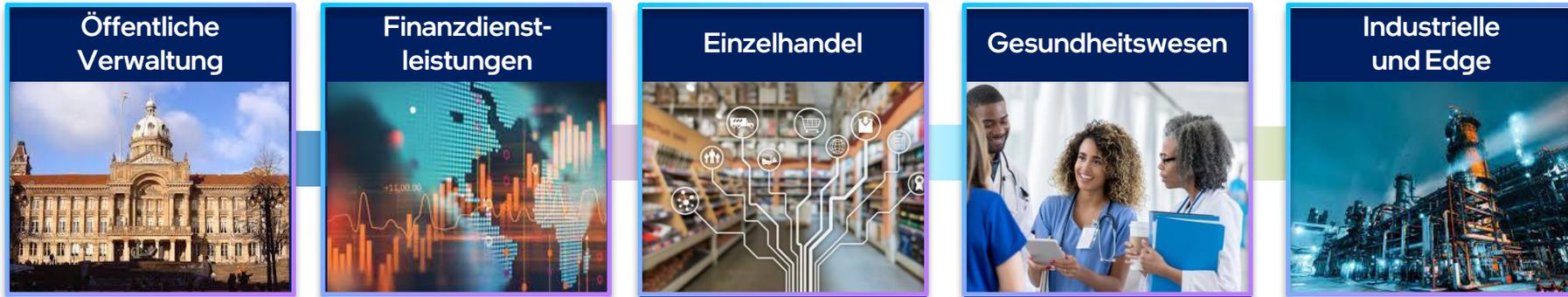
**Datensouveränität und Kontrolle**

Zugriff durch Cloud-Anbieter oder andere Mandanten untersagen; Datensouveränität und Governance um Schutzmechanismen erweitern

# Confidential Computing

## Sektoren & Anwendungsfälle

### Sektoren



### Anwendungsfälle



# Confidential Computing

## Wichtige KI-Anwendungsfälle

### Maschinelles Lernen mit mehreren Parteien

Nutzen Sie das Potenzial maschinellen Lernens ohne die Vertraulichkeit und die Privatsphäre sensibler Kundendaten zu beeinträchtigen



[Beschreibung für Unternehmen](#)



Maschinelles Lernen mit mehreren Parteien mit Confidential Computing kann besonders nützlich sein in:



#### Gesundheitswesen

können die Macht von Daten nutzen, um fortschrittlichere Forschung durchzuführen, ohne vertrauliche Patienteninformationen preiszugeben



#### Finanzdienstleistungen

können potenziell betrügerische Aktivitäten besser vorhersagen und gleichzeitig die Geldwäsche und die Finanzierung des Terrorismus bekämpfen

# Kundenfallstudie

## Gesundheitswesen

Kollaboratives Computing mit regulierten Daten



### Situation

Novartis Biome entwickelt diagnostische Modelle und Therapien für seltene Krankheiten. Informationen über seltene Krankheiten sind spärlich und über mehrere Krankenhäuser und Forschungseinrichtungen verteilt

### Herausforderung

Patienteninformationen sind privat und stark reguliert. Krankenhäuser wollen keine Daten auslagern oder private Datensätze an BeeKeeperAI oder Novartis weitergeben

### Lösung

Ein Intel® Software Guard Extensions (Intel® SGX)-fähiger BeeKeeperAI-Knoten, der lokal in jedem Krankenhaus installiert ist, analysiert private Daten und aktualisiert Mastermodellgewichte in der Cloud. Weder Novartis- noch BeeKeeperAI-Personal sehen oder speichern regulierte Gesundheitsdatensätze



„[Confidential-Computing-Plattformen] ermöglichen uns, die Zykluszeit für die Validierung eines Algorithmus auf die Hälfte zu reduzieren. Außerdem lassen sich so die Kosten beinahe halbieren. Diese Arten von Einsparungen ermöglichen es uns, generalisierbare Algorithmen viel schneller zu trainieren, zu validieren und auf den Markt zu bringen. Und mit der Weiterentwicklung der Technologien und Prozesse, auf denen CCPs basieren, wird das nur noch schneller und kostengünstiger werden.“ MaryBeth Chalk, Mitbegründerin und Chief Commercial Officer, BeeKeeperAI, Inc



Whitepaper

[Beschleunigte Entwicklung von klinischen KI-Algorithmen](#)

# Kundenfallstudie

## Hochsicherheits-Schlüsselschutz



### Situation

Schnell proliferierende Schlüssel und Zertifikate erfordern starken Schutz und zentralisierte Verwaltung. HSM-Lösungen sind teuer und Cloud-Lösungen verlassen sich auf CSP-Sicherheit und -Compliance

### Herausforderung

Entwickeln Sie ein skalierbares, softwarebasiertes Schlüsselmanagementsystem mit HSM-ähnlicher Sicherheit, das technologisch vom Cloud-Host isoliert ist

### Lösung

Fortanix basiert seine Self-Defending KMS-Software auf Intel® SGX, um Schlüssel und Zertifikate vor externen Gegnern und dem Cloud-Anbieter zu schützen und sicherzustellen, dass die Geheimnisse des Besitzers unter ihrer Kontrolle bleiben



Die Leistung bleibt mit aktiviertem Intel® SGX hoch

Die Implementierung einer Mehrfachinstanz-Konfiguration bietet erhebliche Durchsatzgewinne. Diese Leistungsverbesserungen werden durch die Aktivierung von Intel® SGX minimal beeinflusst, was bedeutet, dass Unternehmen gleichzeitig Sicherheit und Leistung erhöhen können.



Lösungs-Snapshot

[Vertrauliche KI-Daten Intel Sicherheitslösung – Fortanix](#)

# PRC-Kundenfallstudie

## Mining-Datenwert



### Chuanglin-Technologie

#### Situation

Wie die Sicherheit von Unternehmensdaten und Datenschutz gewährleistet werden kann, ist ein häufiges Problem, dem Datenbank- und Hardware-Hersteller gegenüberstehen

#### Herausforderung

Traditionelle Datenverschlüsselungstechnologie verschlüsselt nur Festplattenspeicher und Netzwerkübertragung, und ihre Effektivität basiert auf der Prämisse, dass die Kontrollbefugnis des Servers nicht nach außen gelangt ist. Wenn die Kontrolle des Servers abgefangen wird, können die verwendeten Daten von einem Dritten gestohlen oder geändert werden

#### Lösung

Chuanglin Technology und Intel haben gemeinsam eine Grafikdatenverschlüsselungslösung auf den Markt gebracht, die Intel® SGX Speicherverschlüsselung verwendet. Es garantiert die ultimative Leistung von Galaxybase und schafft so ein speichersicheres Graph-Datenbankprodukt

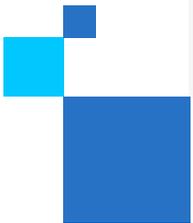


Man glaubt, dass die durch Chuanglin-Technologie entwickelte Graphdatenbank Galaxybase der neuen Generation mit Hilfe der Intel® SGX Speicherverschlüsselungstechnologie Kunden qualitativ hochwertige und sicherere Datendienste bieten, Datenverbindungen effizient realisieren und Unternehmen die Möglichkeit geben kann, den Wert von Datenressourcen in stabiler Weise zu realisieren.



[Pressemitteilung](#)

# Was Intel für Confidential Computing bietet



# 4 Fakten: Intel an der Grundlage von Confidential Computing



2018

Intel® Software Guard Extensions (Intel® SGX) auf Intel® Xeon® Prozessoren ist die erste Confidential Computing-Lösung, die im Rechenzentrum eingeführt wurde



300+

Unternehmen haben sich mit Intel zusammengetan, um Confidential Computing-Dienste zu entwickeln und bereitzustellen



300 Mio USD

Ist der geschätzte Wert der mit Intel® SGX auf Intel® Xeon® Prozessoren bereitgestellten Infrastruktur



4

Globale Cloud-Anbieter haben sich 2023 verpflichtet, Intel® Trust Domain Extensions (Intel® TDX) auf Intel® Xeon® Prozessoren der 4. Generation anzubieten



IBM Cloud



Google Cloud



# Intel bietet das umfassendste Sicherheitsportfolio

Intel® Software Guard Extensions (Intel® SGX)



Anwendungsisolation

Intel® Trust Domain Extensions (Intel® TDX)



Isolierung virtueller Maschinen

Intel® Trust Authority



Unabhängige Vertrauensverifizierungsservices für Multi-Cloud- und Hybrid-Cloud

Softwarelösungen, Cloud, OEM und Systemintegrator – Technologieumfeld

Intel Security-First-Entwicklungs- und Lifecycle-Support

\*Intel® TDX über bestimmte Cloud-Anbieter verfügbar

# Intel® Trust Authority

Bringen Sie Zero Trust in Reichweite und profitieren Sie von Public-Cloud-Flexibilität mit Private-Cloud-Sicherheit.

Intel® Trust Authority ist ein neues Portfolio von Software und Diensten, das verbesserte Sicherheit und Schutz für Confidential Computing mit Zero-Trust-Prinzipien bietet. In seiner ersten Generation bietet Intel® Trust Authority einen unabhängigen Attestierungsdienst, der **Trusted Execution Environments (TEEs)** bestätigt, die auf **(Intel® SGX)** und **(Intel® TDX)** basieren.

Implementieren Sie die Grundsätze von Zero Trust, ohne die Kosten und Komplexität der Entwicklung Ihres eigenen Attestierungsdienstes zu verursachen.



Unabhängig



Skalierbar



Einfache  
Bereitstellung

Weitere Informationen

[Enablement-Paket für Confidential Computing](#)



[Produktbeschreibung](#)



[Noname-Fallstudie](#)

 noname



[Thales-Fallstudie](#)

**THALES**



[Zscaler-Fallstudie](#)





[Was das bedeutet – Video](#)

# Confidential Computing

Software- & und Lösungsumfeld für Intel® SGX

Kommerziell unterstützte Lösungen

Stellen Sie es selbst zusammen

## Commercial Solution Provider

anJUNA

cosmian

decentriq

EDGELESS SYSTEMS

CYBERNETICA

Fortanix®

Mithril Security

Opaque

enclave

SCONTAIN

HUB SECURITY

secretarium

## Kuratierte, Ready-to-Deploy Container (bis Q1 2023)\*

PyTorch

redis

scikit learn

Spark

TensorFlow

## Tools für Entwickler

GRAMINE

SCONE

Mystikos

Occlum

Open Enclave SDK

Teaclave

intel®  
Intel SGX SDK

## Systemintegratoren

accenture

KPMG

Capgemini

IBM

Atos

leidos

avanade

## Hypervisoren (SGX)

KVM  
5.13 &  
spätere

vmware®  
vSphere 8

\* Verfügbar auf [Azure Marketplace](#)

# Intel® TDX Verfügbarkeit

Intel® TDX ist auf skalierbaren Intel® Xeon® Instanzen der 4. Generation in der öffentlichen Vorschau über drei führende Cloud-Anbieter verfügbar.

Klicken Sie auf die Logos unten, um weitere Informationen über das Angebot der einzelnen Cloud-Anbieter zu erhalten.



**IBM Cloud**

\*Öffentliche Vorschau TBA  
(noch nicht bekannt)

Intel® TDX ist für die folgenden Gastbetriebssystemanbieter aktiviert



# Wettbewerbsvergleich

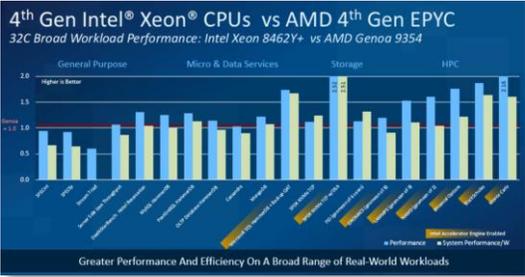
	Intel® SGX	Intel® TDX	AMD SEV-SNP	AWS-Nitro-Enklaven	Conf. Kompilieren auf NVIDIA H100 GPU
Hardware/Firmware, Hypervisor und Cloud-Management-Stack des Cloud-Infrastrukturanbieters von der Vertrauensgrenze ausgeschlossen	●	●	●		●
Verfügbar über mehrere Cloud-Anbieter zur Erleichterung von Multi-Sourcing	●	● <sup>1</sup>	●		●
Entwickelt für ältere Anwendungen mit geringem oder keinem Porting, Neudesign oder Neuverpackung		●	●		○ <sup>2</sup>
Bestätigung der Hardware-Authentizität und korrekter TEE-Start	●	●	●	●	●
Bestätigung der Integrität des in TEE geladenen Softwarebildes	●	○ <sup>3</sup>	○ <sup>3</sup>	●	
Vertrauliche Daten nur über den designierten Anwendungscode zugänglich; VM-Admin, Gast-Betriebssystem, andere Apps und Cloud-Stack vom Zugriff ausgeschlossen	●				
Bereitstellbar auf reinen Hardware-Servern ohne Virtualisierung	●				●
Hardware-basierte Option für kryptografische Speicherintegrität für zusätzlichen Rowhammer-Schutz	●				
Kompatibel mit Intels unabhängigem Vertrauensdienst mit dem Code-Namen Project Amber	●	●			
<i>Wettbewerbsfähige Datenquellen (Stand: März 2023)</i>			<a href="#">Link</a> , <a href="#">Link</a>	<a href="#">Link</a> , <a href="#">Link</a> , <a href="#">Link</a>	<a href="#">Link</a>

<sup>1</sup> Intel® TDX-Instanzen, die 2023 bei ausgewählten Cloud-Anbietern online gehen; das Verfügbarkeits-Timing wird variieren

<sup>2</sup> Keine oder geringe Änderungen für älteren Code. Teile der Workload, die die CPU verwenden, müssten eine CPU-basierte TEE und eine Möglichkeit zum Schutz der PCIe-Kommunikation enthalten.

<sup>3</sup> Keine inhärente Fähigkeit der verfügbaren Hardwaretechnologie, sondern ist als Mehrwertfunktion des Cloud- oder Attestierungsdienstleisters machbar.

# Wettbewerbsanalyse von Intel® Xeon® der 4. Generation



Skalierbare Intel® Xeon® Prozessoren der 4. Generation übertreffen die Konkurrenz bei realen Workloads



im Vergleich



Skalierbare Intel® Xeon® Prozessoren der 4. Generation mit Software optimiert für CPUs sind bis zu 2,5-mal schneller als NVIDIA A100 GPUs



im Vergleich



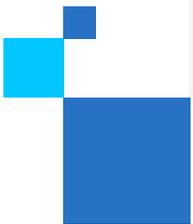
Führende Rechenzentrumsleistung mit skalierbaren Intel® Xeon® Prozessoren der 4. Generation



im Vergleich



# Warum Intel für Confidential Computing wählen?



# Warum Intel für Confidential Computing wählen?

## Technologieoptionen zur Erfüllung verschiedener Sicherheitsanforderungen



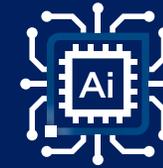
Nur Intel bietet sowohl App-Isolation (Intel® SGX) als auch VM-Isolation (Intel® TDX), damit Kunden die Lösung präzise auf unterschiedliche Sicherheitsstufen abstimmen können

## Breites Lösungsökosystem



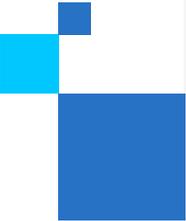
Intel arbeitet mit Dutzenden von ISVs und Cloud-Anbietern zusammen, um Hosting-Dienste und Softwarelösungen anzubieten, einschließlich Vertrauliche KI, Analysen, Blockchain, Datenbanken und mehr

## Zugriff auf Experten bei Intel und unseren Lösungspartnern



Intel-Experten sind bereit, Kunden bei der Lösungsarchitektur, Partner-Matching, POC-Ressourcen und Fehlerbehebung bei der Bereitstellung zu unterstützen

Verbinden Sie sich mit Ihrem PSAM, um weitere Informationen zu erhalten

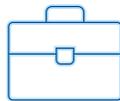


# Wie die Intel<sup>®</sup> Partner Alliance helfen kann

# Erste Schritte mit der Intel® Partner Alliance

Eine Mitgliedschaft in der Intel® Partner Alliance bietet Ihnen exklusive Möglichkeiten zur Geschäftsentwicklung, zum Beispiel Zugang zu unserem globalen Markt, erweiterte Schulungsangebote und Marketingunterstützung – stets zugeschnitten auf Ihre individuellen Bedürfnisse.

## Schulungen und Kompetenzen



Zugang zur Intel® Partner University bietet Ihnen spezielle Schulungen zu fortschrittlichen Techniken, Zertifizierungsprogramme und Prämien für das Lernen.

## Marketingressourcen



Zugang zum Intel® Solutions Marketplace und Intel® Partner-Marketing-Studio hilft Ihnen dabei, zusätzliche Nachfrage nach Ihren Produkten und Dienstleistungen zu schaffen.

## Wertvolle Prämien



Sammeln Sie Prämienpunkte für Ihre qualifizierten Aktivitäten, verbessern Sie Ihren Mitgliedschaftsstatus und erhalten Sie Zugriff auf zusätzliche Ressourcen, um Ihre Geschäfte auszubauen.

**Wenn Sie noch kein Mitglied sind**  
**[Jetzt teilnehmen](#)**

# Leistungen für Mitglieder

## Punkte sammeln



Eine der beliebtesten und differenziertesten Leistungen innerhalb der Intel® Partner Alliance sind Prämienpunkte, die wir Partnern vergeben, um ihre Geschäftsergebnisse mit Intel und ihr Engagement für Aktivitäten mit hoher Priorität anzuerkennen.

Es gibt über 1000 Möglichkeiten, innerhalb der Intel® Partner Alliance Prämienpunkte zu sammeln und mehr als 100 Einlösemöglichkeiten.

## Cloud Insider Community



Die Intel® Cloud Insider Community bietet ständig aktualisierte, erstklassige Cloud-Inhalte und -Tools. Mitglieder haben die Möglichkeit, sich mit Gleichgesinnten und dem Ökosystem zu vernetzen, um innovative, gemeinsame Cloud-Lösungen auf den Markt zu bringen

[Weitere Informationen](#)

## Brancheneinblicke



Gold- und Titanium-Mitglieder können auf speziell kuratierte vierteljährliche Brancheneinblicke zugreifen, um ihr Wachstum zu fördern

[Weitere Informationen](#)

## Finanzielle Anreize



Die Mitgliedschaft bietet starke Marketingentwicklungsfonds und Anreizprogramme, die Ihren Erfolg im Produktmarketing beschleunigen. Sprechen Sie mit Ihrem PSAM, um mehr über Beschleunigerinitiativen der Intel® Partner Alliance und weitere finanzielle Anreize zu erfahren.

## Zugriff auf Kundensupport

### Intel Virtual Assistant

Dieser Chat-Bot befindet sich in der unteren rechten Ecke jeder Partner Alliance-Webseite und bietet Selbsthilfe bei den meisten Fragen oder einen schnellen Link zu einem Live-Support-Mitarbeiter.



### Hilfe erhalten – „Blade“

Senden Sie eine [Online-Support-Anfrage](#).

Dieser Link befindet sich in der Fußzeile der meisten Seiten auf dem Partner Alliance-Portal.

#### Get Help

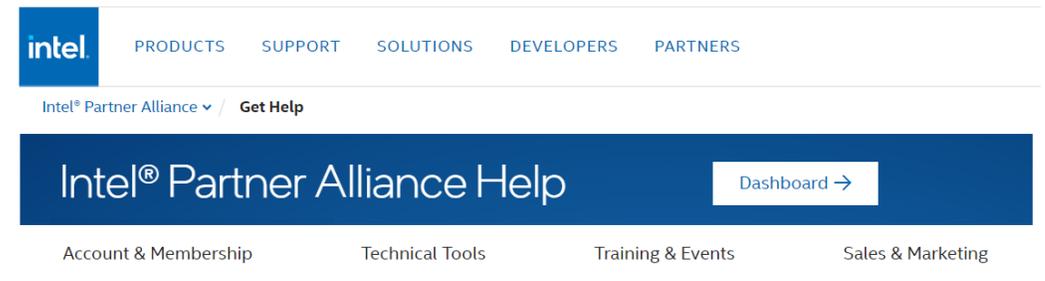
##### Request Support

Contact us anytime to create a support request.

[Submit request >](#)

### Partner Alliance-Seite „Hilfe erhalten“

Die Seite [Hilfe erhalten](#) bietet detaillierte Selbsthilfe-Leitfäden zu den meisten Tools und Leistungen, die Mitgliedern der Partner Alliance zur Verfügung stehen.





# Ressourcen

# Cloud TV

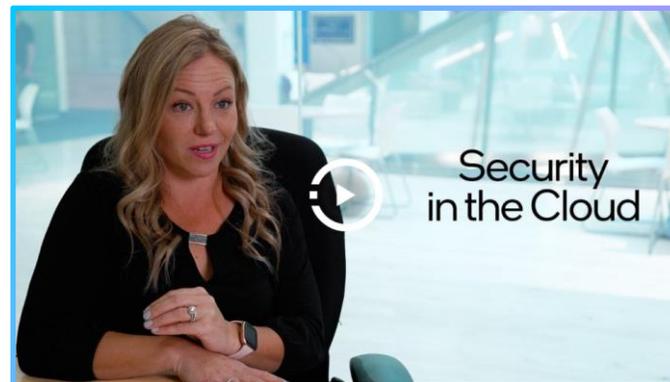
Intel® Cloud TV berichtet über Cloud-Computing Nachrichten, Trends und Strategien, um Ihren Erfolg zu fördern



Sapphire Rapids in der Cloud



Erfahren Sie, wie Sie Ihre Cloud-Assets schützen können



Sicherheit in der Cloud



Sicherheitsherausforderungen in der Cloud

# Confidential Computing Informationen und Ressourcen



## 30-3-30

[Confidential Computing 30-3-30](#)



## Videos

[Confidential Computing – Überblick](#)

[Sicherheit ist eine Herausforderung](#)



## Infografik

[Wie man Cloud-Sicherheitsbedrohungen abwehrt](#)



## Forschungsbericht

[Schutz von Daten und Modellen innerhalb neuer KI-Workflows](#)



## Tech-Artikel

[Entwicklungsstand des Confidential Computing](#)

[Eine Einführung in Cloud-Sicherheit](#)



## Blogs

[Ein neues Paradigma für Leistung und Cybersicherheit](#)

[Sicherheit beginnt mit Intel](#)



# Weitere Ressourcen



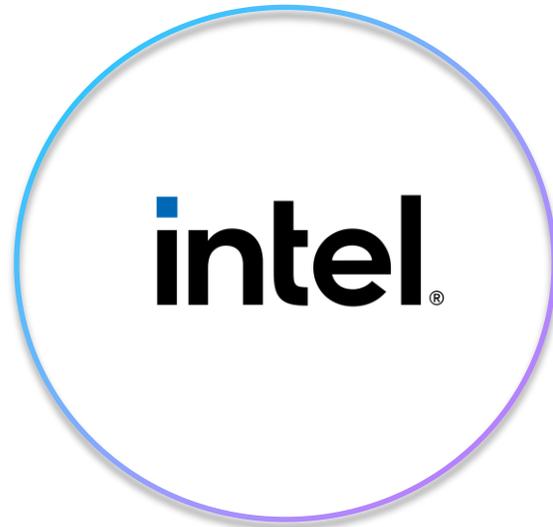
## Leistungsindex

Skalierbare Intel® Xeon®  
Prozessoren der 4. Generation



## Live-Webinare

Cloud Solution Architect (CSA)  
Tech-Talk: Reduzieren Sie die  
Gesamtbetriebskosten und verbessern  
Sie die Effizienz mit skalierbaren  
Intel® Xeon® Prozessoren  
der 4. Generation



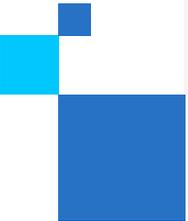
## Aufgezeichnete Webinars

Cloud Solution Architect (CSA)  
Tech-Talk: Beschleunigung kritischer  
Workloads mit skalierbaren Intel® Xeon®  
Prozessoren der 4. Generation



## Zusätzliche Schulung

Kompetenzen und Zertifizierungen



# Confidential Computing- Schulungslinks

# Links zu Sicherheitsschulungen

## Kurse / Schulung

Thema - Zielgruppe
<a href="#">3 Schlüsseltechnologien zur Steigerung Ihrer Cybersicherheits-Resilienz</a> DevOps, Cloud-Architekten – Confidential Computing
<a href="#">End-to-End-Sicherheit für IOT-Lösungen</a> DevOps
<a href="#">Edge-to-Cloud-Sicherheit</a> DevOps, Cloud-Architekten
<a href="#">Virtuelle Private Cloud, Cloud-Netzwerk und Cloud-Sicherheit</a> DevOps
<a href="#">Sicherheitsvorteile von Intel® Produkten und Lösungen</a> ALL
<a href="#">Sicherung von Anwendungen in der Cloud</a> DevOps
<a href="#">Sicherheit beim Cloud-Computing</a> DevOps, Cloud-Architekten

Thema - Zielgruppe
<a href="#">Virtuelle Private Cloud, Cloud-Netzwerk und Cloud-Sicherheit</a> DevOps, Cloud-Architekten
<a href="#">Sicherheit im geschäftlichen Umfeld</a> Cloud-Architekten, C-Suite
<a href="#">Eine Einführung in die Verschlüsselung für die Intel Architektur</a> DevOps
<a href="#">Sicherheitsvorteile von Intel® Produkten und Lösungen</a> DevOps, Cloud-Architekten

intel®

# Backup



# Intels Security-First-Pledge

„Die Sicherheit unserer Produkte ist eine unserer wichtigsten Prioritäten. Wir sind bestrebt, die sichersten Technologieprodukte der Welt zu entwickeln, herzustellen und zu verkaufen, und wir arbeiten ständig daran, die Sicherheitsfunktionen unseres Produkts zu erneuern und zu verbessern.“

Pat Gelsinger, CEO



**93 %**

der 2022 behobenen Schwachstellen resultierten direkt aus Intels Investitionen in die Sicherung der Produktsicherheit

**56 %**

der im Jahre 2022 veröffentlichten 243 CVEs wurden intern von Intel-Mitarbeitern entdeckt

**93 %**

Seit dem ersten Produktsicherheitsbericht für das Kalenderjahr 2019 waren durchschnittlich 93 % aller veröffentlichten CVEs das direkte Ergebnis von Intels Investitionen in die Sicherung der Produktsicherheit

**85 %**

Von den 85 % der 106 Schwachstellen, die 2022 von externen Forschern gemeldet wurden, wurden 90 Schwachstellen oder 85 % über das Bug Bounty Program von Intel gemeldet

Vollständigen Bericht anzeigen: [Hier](#)

# Wettbewerbsanalyse der skalierbaren Intel® Xeon® Prozessoren der 4. Generation

## Mainstream-Compute-Leadership

75 %

Höhere Leistung

50 %

Höhere Leistung/Watt

20 %

Kg Co2-Einsparungen und  
Gesamtbetriebsmitteleinsparungen

## KI-Führung

80 %

Höherer  
Inferenzdurchsatz

## HPC-Führung

40 %

Höhere Leistung über  
verschiedene Workloads

[Klicken Sie für Cloud-Fakten](#)