Besser zusammen: Azure Confidential Computing und Intel® Technik

Herausforderungen in Bezug auf die Sicherheit von Kunden aus regulierten Branchen:

Nutzenmaximierung und Risikominimierung

Wie kann man von den Vorteilen einer digital vernetzten Welt profitieren – universeller Zugang, gebündelte Ressourcen, verbesserte Effizienz und Flexibilität – und gleichzeitig für Privatsphäre und Vertrauen sorgen?

Datensicherheit während der Nutzung

Wenn Daten im Speicher verwendet werden, sind sie oft nicht geschützt, da sie nicht verschlüsselt sind. Zu den Risiken gehören böswillige Insider, Hacker und Malware.

Beibehaltung der Kontrolle über die Daten

Wie kann die Überwachung der Daten während ihrer gesamten Lebensdauer gewährleistet werden? Tragen Sie dazu bei, dass Daten und Code nicht vom Anbieter Ihrer Cloud-Plattform angezeigt werden können.

Gesetzliche Bestimmungen und ihre Einhaltung

Die steigenden Anforderungen an Datenschutz, Sicherheit und Privatsphäre sowie Souveränität und Transparenz verschärfen die Sicherheitsherausforderungen. Besonders streng sind diese Anforderungen bei Finanzdienstleistungen und Behörden sowie im Gesundheitswesen. Weitere Informationen erhalten Sie in der Fallstudie von MobileCoin.

Kundennutzen von Confidential Computing von Microsoft Azure und Intel:

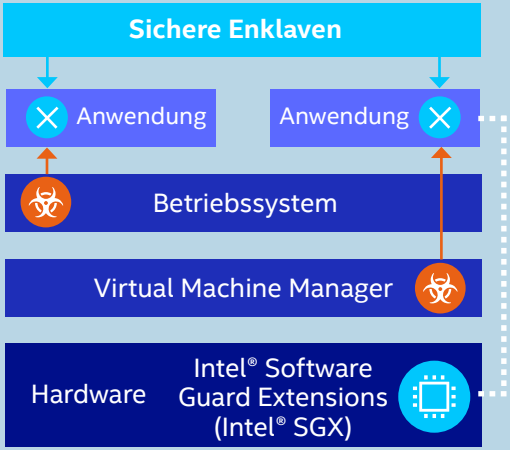
Erhöhte Datensicherheit

- Confidential Computing schützt die Vertraulichkeit und Integrität der verwendeten Daten.
- Intel® SGX war eine der ersten hardwarebasierten TEEs, die für den Schutz von Cloud- und Rechenzentrums-Workloads entwickelt wurde.
- TEEs bieten einen geschützten Container, indem sie einen Teil des Prozessors und des Speichers der Hardware sichern.
- Unternehmen können Software auf der geschützten Umgebung ausführen, um Teile ihres Codes und ihrer Daten vor Einblicken oder Änderungen von außerhalb der TEE zu schützen.
- Selbst Cloud-Administratoren und Rechenzentrumsbetreiber können nicht auf TEE-geschützte Daten zugreifen.

Erfüllung strenger gesetzlicher Anforderungen

- Mit Confidential Computing können Kunden in die Cloud migrieren und gleichzeitig die Kontrolle über ihre Daten behalten, um die gesetzlichen Vorschriften zu erfüllen.
- Dazu gehören der Schutz personenbezogener Daten und der Schutz von geistigem Eigentum des Unternehmens.
- Kunden können auch neue Produkte anbieten, bei denen die Haftung für private Daten durch Blindverarbeitung aufgehoben wird, sodass die Nutzerdaten nicht vom Dienstleister abgerufen werden können.

Intel® Software Guard Extensions (Intel® SGX)



- **Unterstützt den Schutz vor** Angriffen, die aus der Ferne erfolgen, und Softwareattacken, selbst wenn Betriebssystem/Treiber/BIOS/VMM/SMM kompromittiert sind.
- **Erhöht den Schutz sensibler Informationen** (Daten/Schlüssel/etc.), selbst wenn der Angreifer die volle Kontrolle über die Plattform hat.
- **Hilft, Hardwareangriffe**, wie z. B. Speicherbus-Snooping, Speichermanipulationen und Kaltstartangriffe, gegen Speicherinhalte im RAM zu verhindern.
- **Bietet Funktionen zur** hardwarebasierten Attestierung von Messungen und Prüfungen gültiger Code- und Datensignaturen.

Skaleneffekte durch Datenfreigabe

- Durch die Kombination der Skalierbarkeit der Cloud mit der Möglichkeit, Daten während der Nutzung zu verschlüsseln, ermöglicht Azure Confidential Computing neue Szenarien für die Freigabe von Daten.
- Neue Szenarien könnten beispielsweise eine sichere Blockchain oder maschinelles Lernen mit mehreren Parteien sein.
- Mit sicheren Enklaven hat keine Partei Zugriff auf die Daten der anderen.
- Das bedeutet, dass Kunden branchenweite Probleme, die das ganze Unternehmen betreffen, in Angriff nehmen können, um umfassendere Datenanalysen und tiefere Einblicke zu gewinnen.

Eine bewährte Lösung auf dem Markt

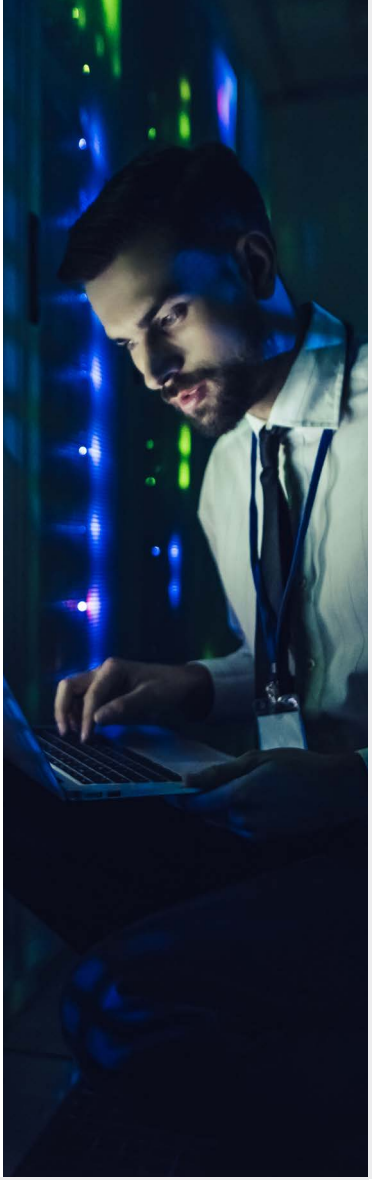
- In den letzten zwei Jahren hat Intel zusammen mit Microsoft Azure immer mehr Kunden gesehen, die Lösungen für Confidential Computing in Cloud-Infrastrukturen entwickeln und einsetzen.

Offenes SDK für Entwickler

- Die Zusammenarbeit zwischen Azure und Intel konzentriert sich auf die Nutzung der neuesten Technologien, um eine Lösung zu entwickeln, die es Unternehmen ermöglicht, die Entwicklung und Verwaltung ihrer Confidential-Computing-Anwendungen zu vereinfachen.
- Entwickler können mit dem Open Enclave SDK oder dem Intel® SDK für Intel® Software Guard Extensions (Intel® SGX) Plattformen für Azure Confidential Computing erstellen.
- Microsoft und Intel sind beide Mitglieder des Confidential Computing Consortium, das sich auf die Entwicklung von Open-Source-Technologien zum Schutz von Daten während der Nutzung konzentriert.

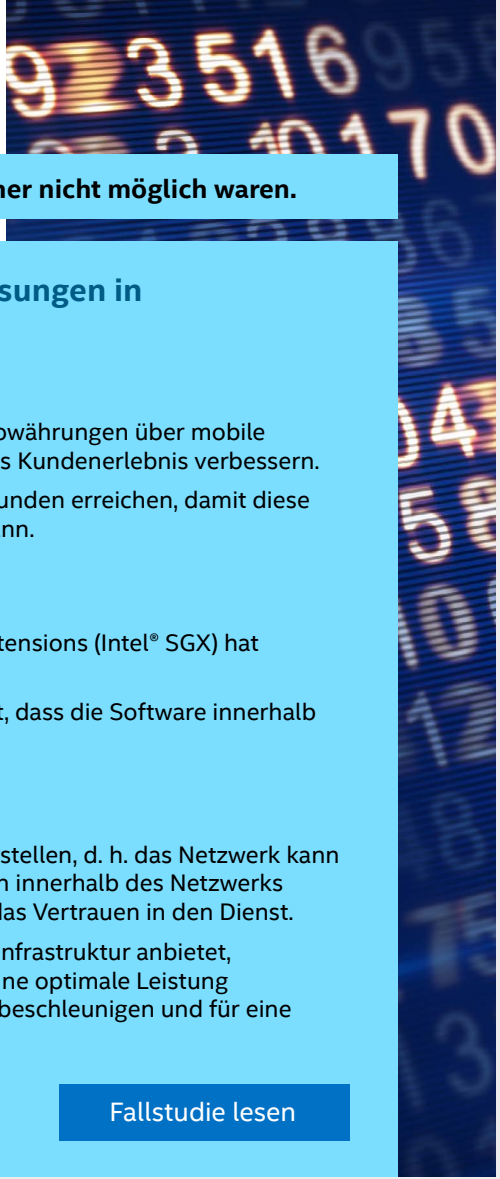
So bieten Azure und Intel ihren Kunden Confidential Computing an

- Skalierbare Intel® Xeon® Prozessoren der 3. Generation mit 1 TB Intel® SGX Enklaven unterstützen die rechenintensivsten vertraulichen Workloads.
- Intel® SGX liefert eine hardwarebasierte Speicherverschlüsselung, die spezifischen Anwendungscode und Daten im Speicher isoliert.
- Mithilfe von Intel® SGX kann Code auf Benutzerebene, private Speicherbereiche, so genannte Enklaven, zuzuweisen, die vor Prozessen mit höheren Berechtigungsstufen geschützt sind.
- Blockiert den Zugriff des Betriebssystems, des Hypervisors und derjenigen, die Zugriff auf den physischen Server haben, einschließlich des Anbieters des Cloud-Dienstes.
- Kunden kontrollieren die Nutzung ihrer Daten und den Ort, an dem sie gespeichert sind, und beschleunigen die Nutzung mehrerer Clouds.
- Intel setzt seine Expansion auf eine breitere Palette von datenzentrierten Plattformen fort und erwartet, dass der Schutz in Zukunft ausgeweitet wird, um Beschleuniger-Workloads auszugleichen und die Leistung zu verbessern.



Kundenfallstudie 1

Confidential Computing bietet Lösungen, die in regulierten Branchen bisher nicht möglich waren.



MobileCoin ermöglicht schnelle, vertrauenswürdige Überweisungen in Kryptowährungen

Das Was:

- MobileCoin, ein Anbieter von schnellen, benutzerfreundlichen Zahlungen in Kryptowährungen über mobile Messaging-Apps, wollte den Datenschutz, die Transaktionsgeschwindigkeit und das Kundenerlebnis verbessern.
- Das Unternehmen wollte dies durch die Anonymisierung der Finanzdaten seiner Kunden erreichen, damit diese Überweisungen tätigen können, ohne dass jemand ihre Transaktionen anzeigen kann.

Das Wie:

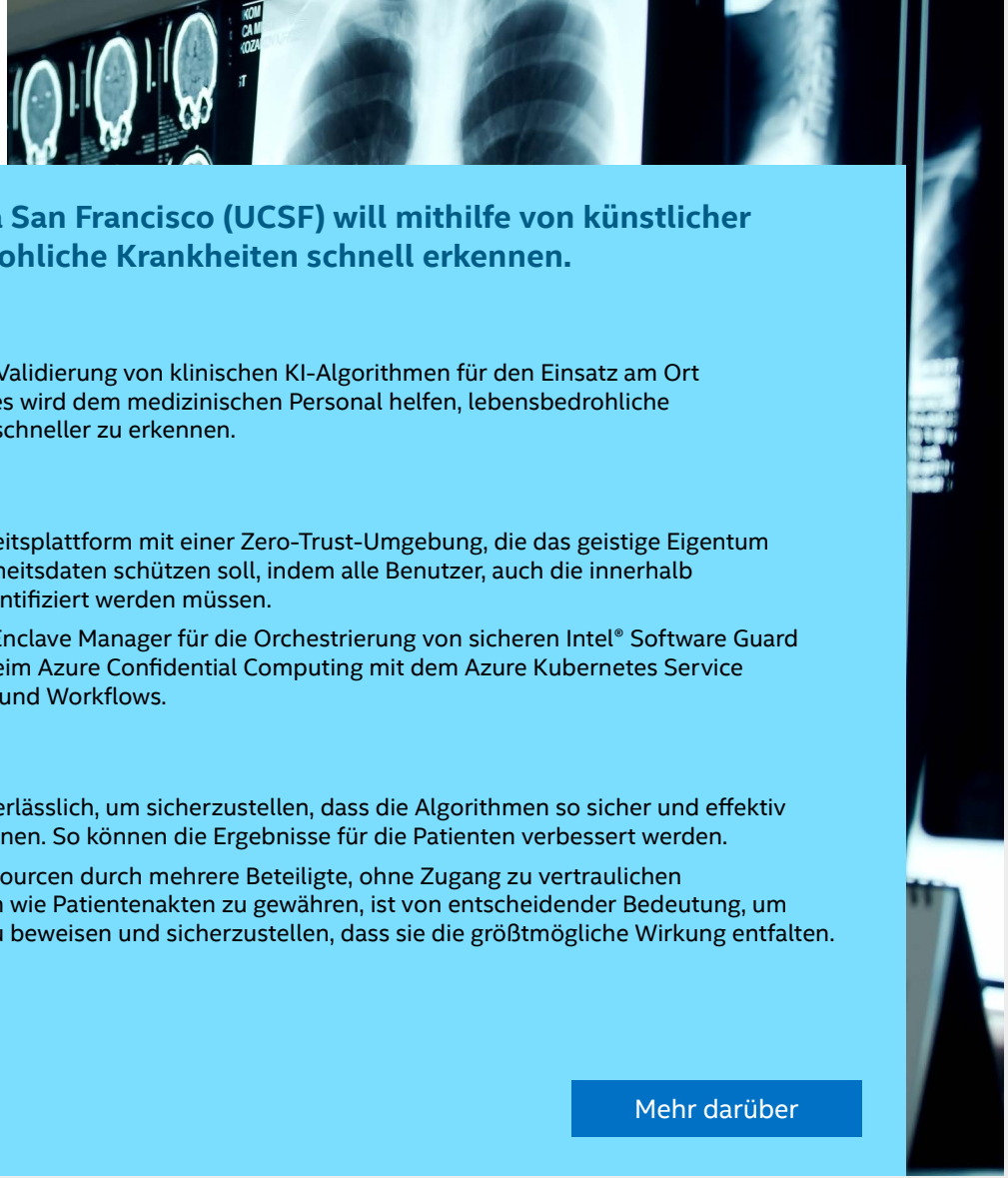
- Durch den Einsatz von Azure Confidential Computing mit Intel® Software Guard Extensions (Intel® SGX) hat MobileCoin eine hardwarebasierte Trusted Execution Environment (TEE) erstellt.
- Intel® SGX fungiert als Speichercontainer für die verwendeten Daten, was bedeutet, dass die Software innerhalb der TEE nicht von außerhalb der TEE geändert werden kann.

Das Warum:

- Dank Azure Confidential Computing konnte MobileCoin eine „blinde“ Blockchain erstellen, d. h. das Netzwerk kann überprüfen, ob alles korrekt ist, ohne die Details der Transaktionen den Validatoren innerhalb des Netzwerks offenzulegen. Dies trägt zum Schutz der Privatsphäre der Kunden bei und erhöht das Vertrauen in den Dienst.
- Die verschiedenen Maschinengrößen, die Azure in seiner Confidential-Computing-Infrastruktur anbietet, ermöglichten es MobileCoin, mit den Spezifikationen zu experimentieren, die für eine optimale Leistung erforderlich sind. Dadurch konnte MobileCoin Transaktionen in Kryptowährungen beschleunigen und für eine optimierte Benutzererfahrung sorgen.

Fallstudie lesen

Kundenfallstudie 2



Die University of California San Francisco (UCSF) will mithilfe von künstlicher Intelligenz (KI) lebensbedrohliche Krankheiten schnell erkennen.

Das Was:

- Die UCSF will die Entwicklung und Validierung von klinischen KI-Algorithmen für den Einsatz am Ort der Behandlung beschleunigen. Dies wird dem medizinischen Personal helfen, lebensbedrohliche Erkrankungen auf Röntgenbildern schneller zu erkennen.

Das Wie:

- Die UCSF entwickelt eine Gesundheitsplattform mit einer Zero-Trust-Umgebung, die das geistige Eigentum eines Algorithmus und die Gesundheitsdaten schützen soll, indem alle Benutzer, auch die innerhalb der Organisation, vollständig authentifiziert werden müssen.
- Die Universität nutzt den Fortanix Enclave Manager für die Orchestrierung von sicheren Intel® Software Guard Extensions (Intel® SGX) Enklaven beim Azure Confidential Computing mit dem Azure Kubernetes Service zusammen mit proprietären Daten und Workflows.

Das Warum:

- Detaillierte klinische Daten sind unerlässlich, um sicherzustellen, dass die Algorithmen so sicher und effektiv wie möglich eingesetzt werden können. So können die Ergebnisse für die Patienten verbessert werden.
- Die gemeinsame Nutzung von Ressourcen durch mehrere Beteiligte, ohne Zugang zu vertraulichen personenbezogenen Informationen wie Patientenakten zu gewähren, ist von entscheidender Bedeutung, um die Nutzbarkeit von Algorithmen zu beweisen und sicherzustellen, dass sie die größtmögliche Wirkung entfalten.

Mehr darüber

Intel® Technik kann entsprechend geeignete Hardware, Software oder die Aktivierung von Diensten erfordern.

Kein Produkt und keine Komponente bietet absolute Sicherheit.

Intel hat keinen Einfluss auf und keine Aufsicht über die Daten Dritter. Sie sollten andere Quellen heranziehen, um die Richtigkeit zu beurteilen.

Kosten und Ergebnisse können variieren.

© Intel Corporation. Intel, das Intel Logo und andere Intel Markenbezeichnungen sind Marken der Intel Corporation oder ihrer Tochtergesellschaften.
*Andere Marken oder Produktnamen sind Eigentum der jeweiligen Inhaber. 0421/JS/CAT/PDF 344587-001EN