Better Together: Azure Confidential Computing & Intel® Technologies

Security customer challenges in regulated industries:

Maximize benefits, minimize risk

How to benefit from the best aspects of a cloud to edge digitally-connected world—universal access, pooled resources, improved efficiency and agility—while still maintaining privacy and trust.

In-use data security

When data is in use, in memory, it is often open to attack because it is unencrypted. Risks include malicious insiders, hackers and malware.

Maintaining control of data

How to ensure oversight of data throughout its lifetime. Help to keep data and code outside of the view of the cloud platform provider.

Regulation and compliance

Increasing regulatory and compliance requirements for data protection, security and privacy, sovereignty, and transparency compound the security challenge. These requirements are particularly stringent in financial services, healthcare and government. Find out more: MobileCoin case study.

Customer value - confidential computing on Microsoft Azure & Intel:

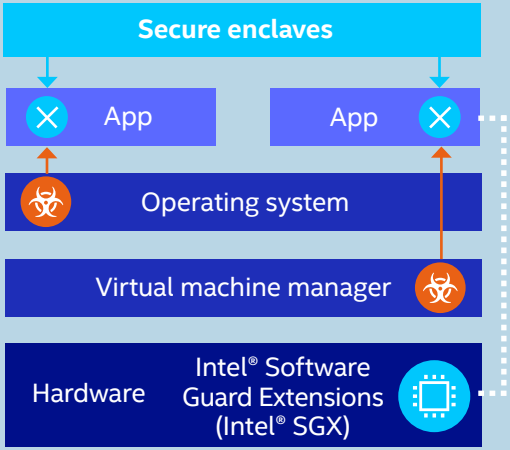
Added data security

- Confidential computing protects the confidentiality and integrity of data in use
- Intel SGX was one of the first hardware-based TEEs designed to protect cloud and data center workloads
- TEEs provide a protected container by securing a portion of the hardware's processor and memory
- Enterprises can run software on top of the protected environment to shield portions of their code and data from view or modification from outside of the TEE
- Even cloud administrators and data center operators cannot access TEE-protected data

Meet strict regulatory requirements

- With confidential computing, customers can migrate to the cloud while retaining control of data to satisfy government regulations
- This includes protecting personal information and securing organizational intellectual property (IP)
- Customers can also offer new products that remove liability on private data with blind-processing, so user data cannot be retrieved by the service provider

Intel® Software Guard Extensions (Intel® SGX)



- **Helps protect against remote/software attacks** even if OS/drivers/BIOS/VMM/SMM are compromised
- **Helps increase protections for sensitive information** (data/keys/et al.) even when attacker has full control of platform
- **Helps prevent in-person hardware attacks**, such as memory bus snooping, memory tampering, and "cold boot" attacks, against memory contents in RAM
- **Provides an option for hardware-based attestation** capabilities to measure and verify valid code and data signatures

Economies of scale with data-sharing

- By combining the scalability of the cloud and ability to encrypt data while in use, Azure confidential computing enables new data sharing scenarios
- For example, secure blockchain or multi-party machine learning
- Neither party has access to the other's data with secure enclaves
- This means customers can tackle industry-wide, world-scale problems across organizations to unlock broader data analytics and deeper insights

A proven solution in the market

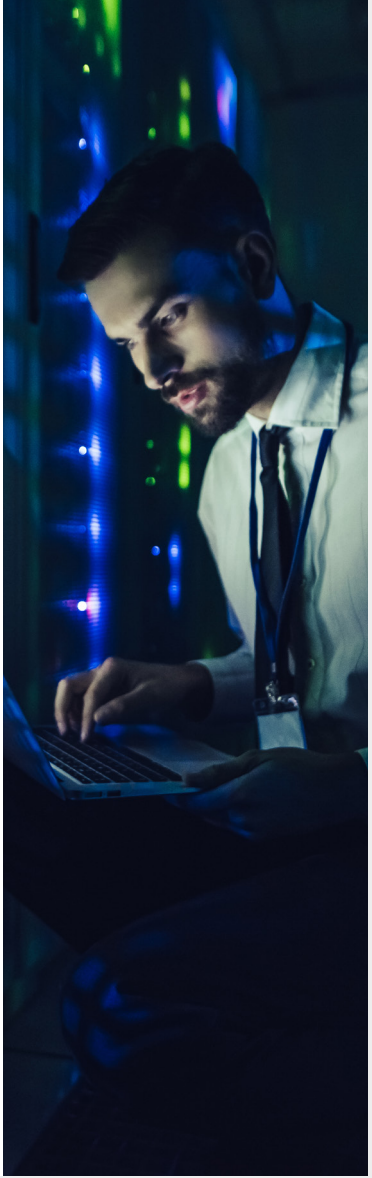
- Over the past two years with Microsoft Azure, Intel has seen even more customers building and deploying confidential computing solutions utilizing cloud infrastructure

Open SDK for developers

- The Azure/Intel collaboration is focused on harnessing the latest technologies to develop a solution that enables organizations to simplify the development and management of their confidential computing applications
- Developers can build platforms for Azure confidential computing using the Open Enclave SDK or Intel SDK for Intel® Software Guard Extensions (Intel® SGX)
- Microsoft and Intel are both Confidential Computing Consortium members focused on developing open-source tech to protect data in use

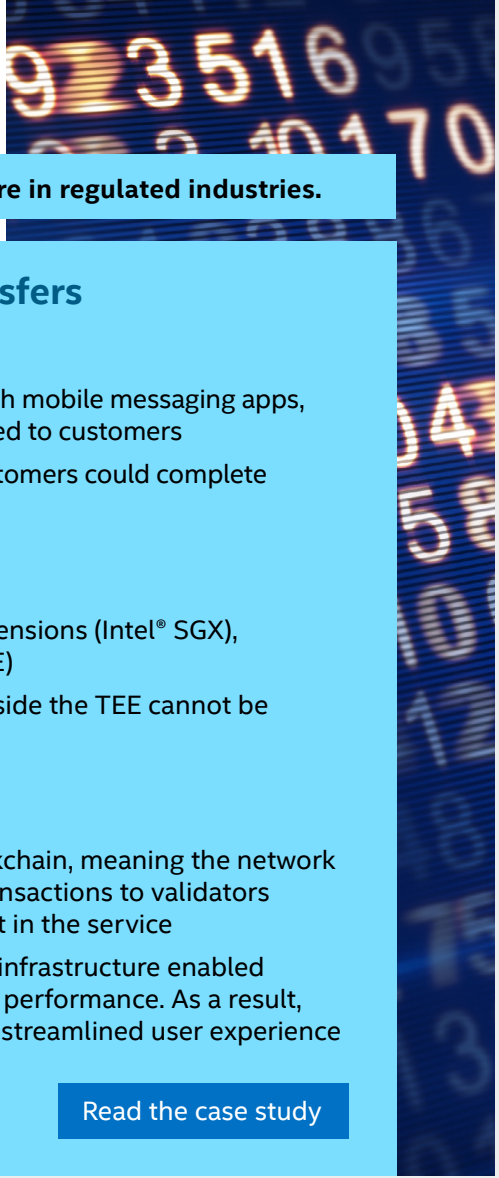
How Azure and Intel enable customers to compute confidentially

- 3rd generation Intel® Xeon® Scalable processors with 1TB Intel SGX enclaves can support the most compute-intensive confidential workloads
- Intel SGX offers hardware-based memory encryption that isolates specific application code and data in memory
- Intel SGX allows user-level code to allocate private regions of memory, called enclaves, protected from processes running at higher privilege levels
- Blocks access from the operating system (OS), hypervisor, and those with physical server access including the cloud service provider (CSP)
- Customers control the use of their data and where it resides, accelerating multi-cloud usages
- Intel continues to expand to a broader range of mainstream data-centric platforms and expects to extend future security protections to balance accelerator workloads and help improve performance



Customer case study 1

Confidential computing is enabling solutions that weren't possible before in regulated industries.



MobileCoin creates fast, trusted cryptocurrency transfers

The what:

- MobileCoin, a provider of fast, easy-to-use cryptocurrency payments through mobile messaging apps, wanted to improve the privacy, transaction speeds and experience it provided to customers
- It was looking to do this by anonymizing its customers' financial data so customers could complete transfers without anyone having insight into their transactions

The how:

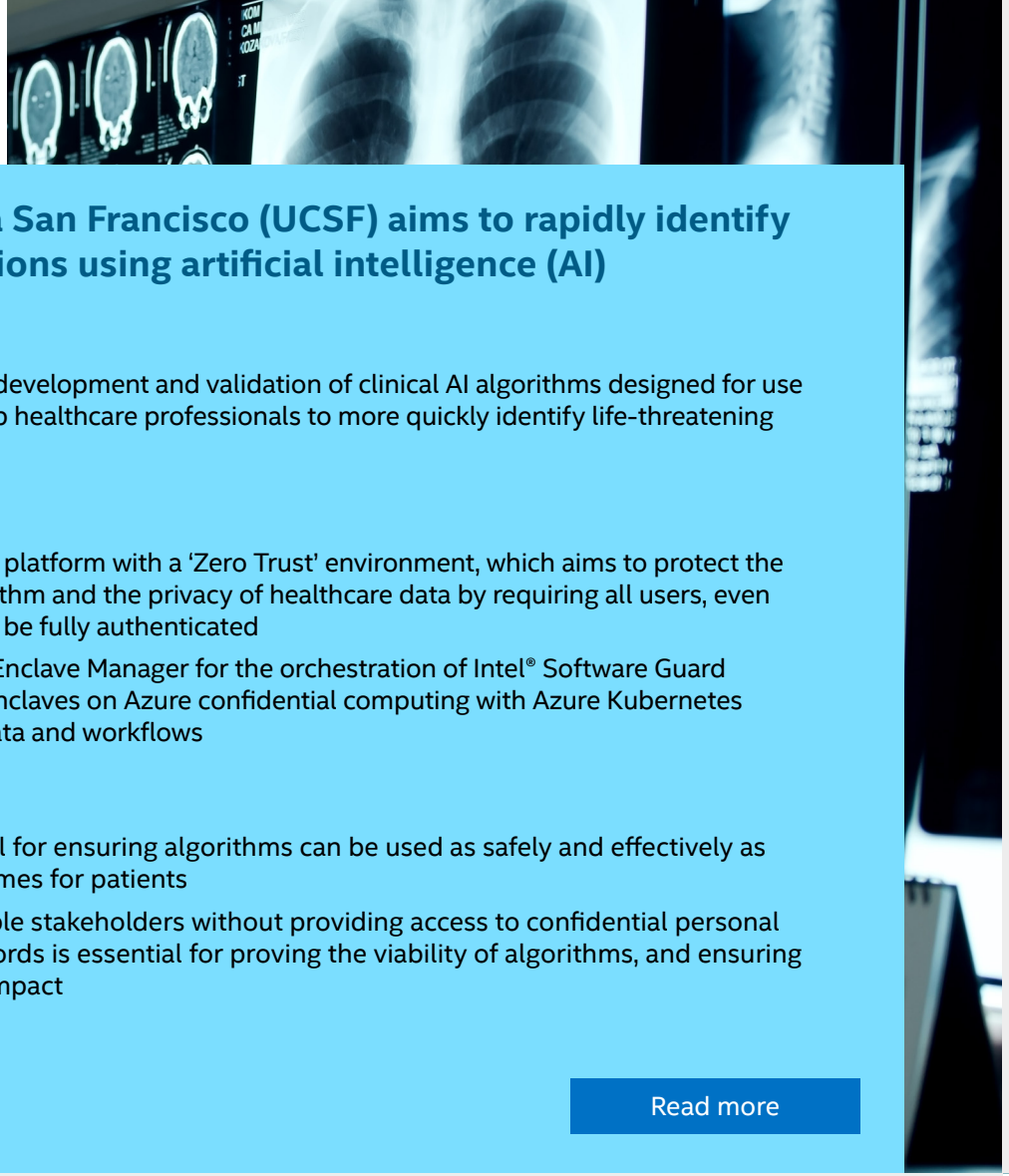
- By deploying Azure confidential computing with Intel® Software Guard Extensions (Intel® SGX), MobileCoin created a hardware-based trusted execution environment (TEE)
- Intel SGX acts as a memory container for data in use, meaning software inside the TEE cannot be modified from outside the TEE

The why:

- Azure confidential computing enabled MobileCoin to create a "blind" blockchain, meaning the network can verify that everything is correct without exposing the details of the transactions to validators within the network. This helps to protect customer privacy, increasing trust in the service
- The multiple machine sizes offered by Azure in its confidential computing infrastructure enabled MobileCoin to experiment with the specifications it needed to get the best performance. As a result, MobileCoin was able to accelerate cryptocurrency transactions to create a streamlined user experience

Read the case study

Customer case study 2



University of California San Francisco (UCSF) aims to rapidly identify life-threatening conditions using artificial intelligence (AI)

The what:

- UCSF is aiming to speed up the development and validation of clinical AI algorithms designed for use at the point of care. This will help healthcare professionals to more quickly identify life-threatening conditions on x-ray

The how:

- UCSF is developing a healthcare platform with a 'Zero Trust' environment, which aims to protect the intellectual property of an algorithm and the privacy of healthcare data by requiring all users, even those inside the organization, to be fully authenticated
- The university is using Fortanix Enclave Manager for the orchestration of Intel® Software Guard Extensions (Intel® SGX) secure enclaves on Azure confidential computing with Azure Kubernetes Service alongside proprietary data and workflows

The why:

- Detailed clinical data is essential for ensuring algorithms can be used as safely and effectively as possible to help improve outcomes for patients
- Sharing resources across multiple stakeholders without providing access to confidential personal information such as patient records is essential for proving the viability of algorithms, and ensuring they have the widest possible impact

Read more

0421/JS/CAT/PDF 344587-001EN