



# Securing business transformation with Confidential Computing



# Content

- Executive summary
- Transforming cybersecurity approach
- Business transformation
- Use cases
- Available solutions
- Key takeaways





## Executive summary

To fulfill the promise of digital transformation there is an urgency to adopt cloud capabilities. New cloud-based technologies offer faster innovation to pursue new business growth and increase efficiency. Yet, accelerated cloud adoption exposes organizations to new business risks.

This shift to the cloud requires cybersecurity practices to adapt.

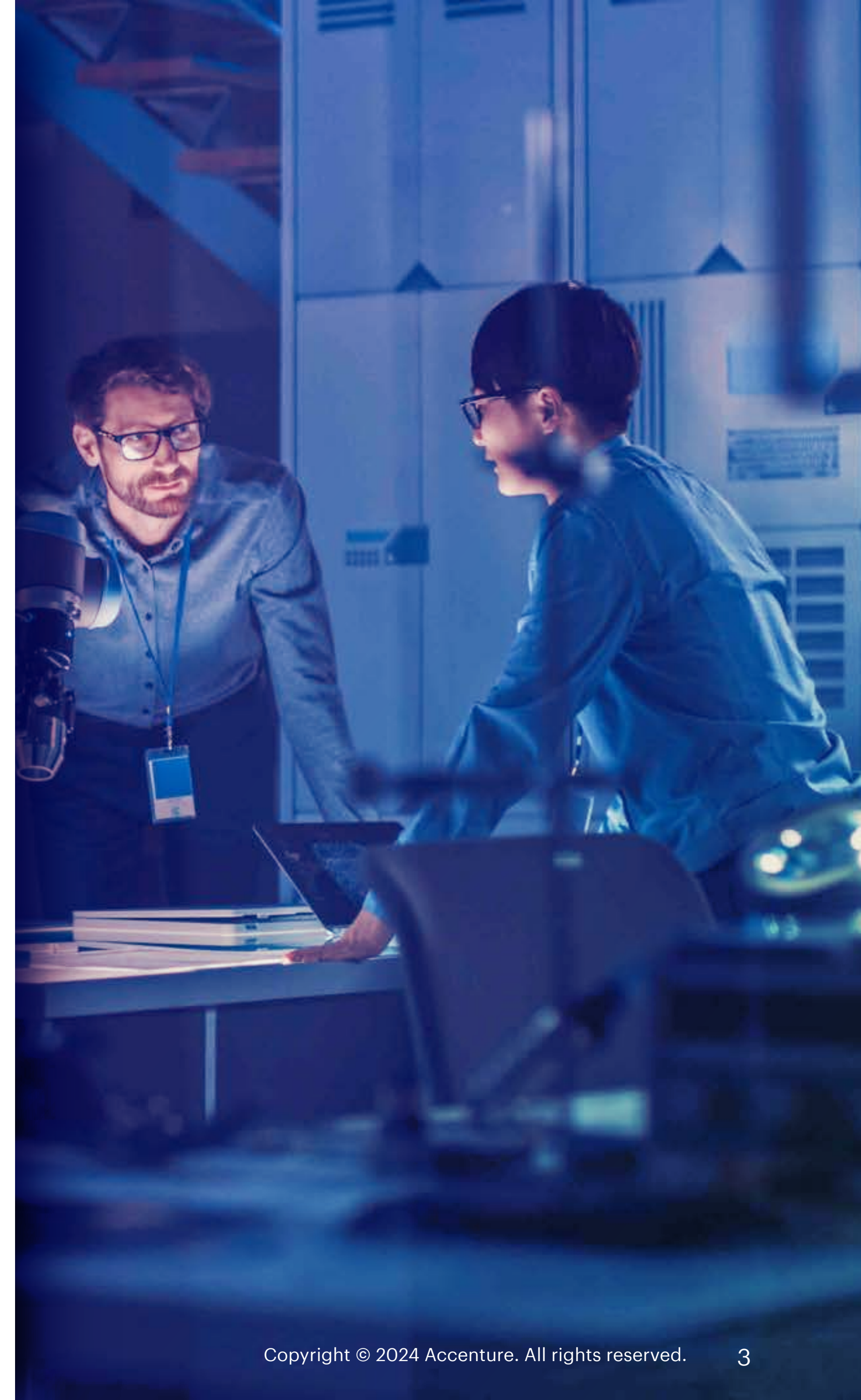
## Introduction

Accenture's research<sup>1</sup> revealed that enterprises that closely align their cybersecurity programs to business objectives are **18%** more likely to increase their ability to **drive revenue growth, increase market share** and **improve customer satisfaction, trust** and **employee productivity**.

Additionally, organizations that embed key cybersecurity actions into their digital transformation efforts and apply strong cybersecurity practices across the organization—we call them cyber transformers—are nearly **6-times** more likely to experience more effective digital transformations than those that don't do both.

However, many organizations **are not engaging in cybersecurity soon enough**. Instead of adopting security practices as part of their transformation journey, they wait until vulnerabilities are detected.

1. <https://www.accenture.com/us-en/insights/security/state-cybersecurity>





# Transforming cybersecurity approach

While most cyber transformers have started to adopt a zero-trust security approach, **many still lag behind in securing the workloads** – application, database, containers, data and enterprise platforms – with a "Secure by Design" method.

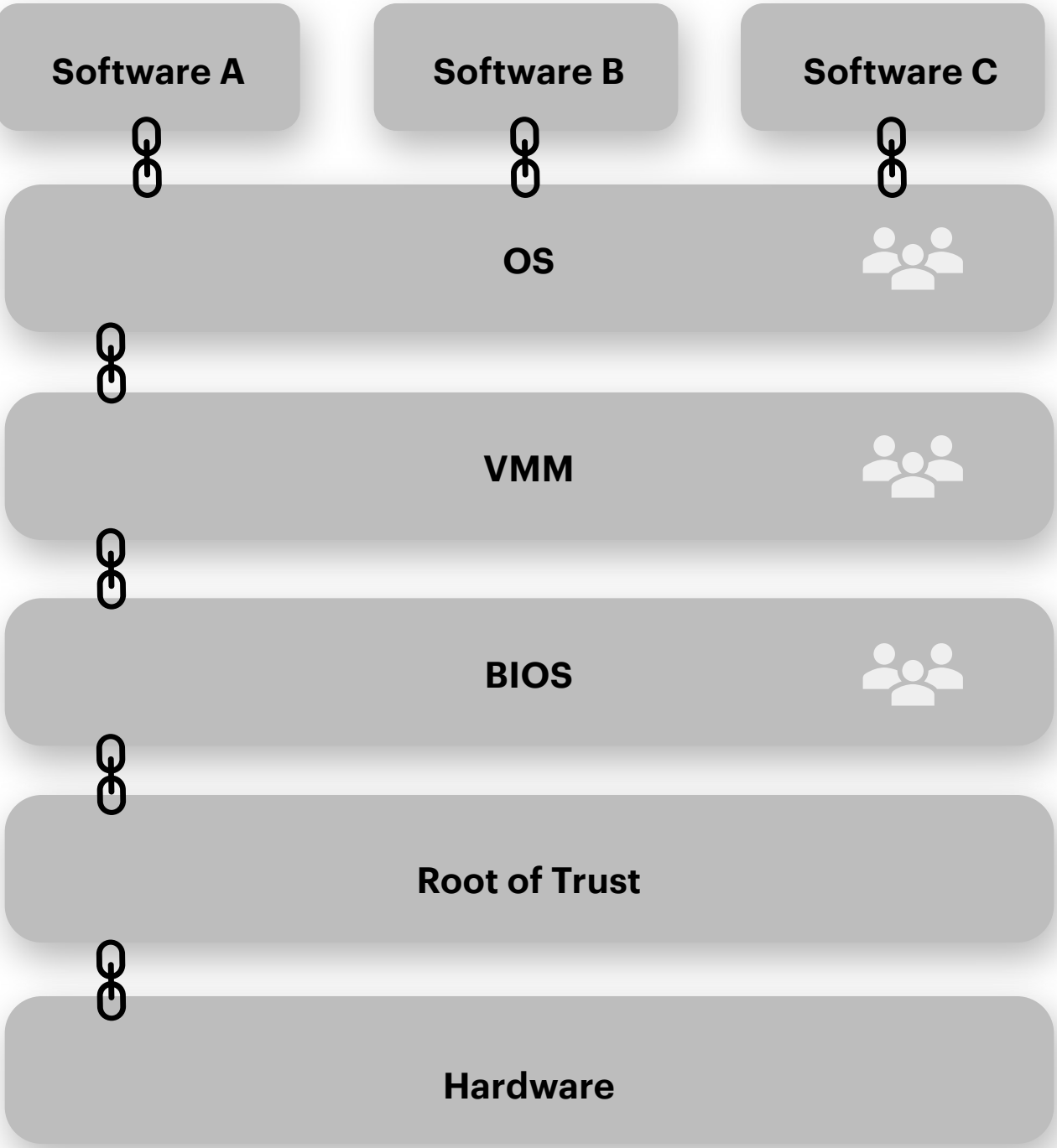
Confidential Computing is one such novel technique that **provides privacy-preserving capability** for existing workloads and enables data to be jointly analyzed without sharing the proprietary data.



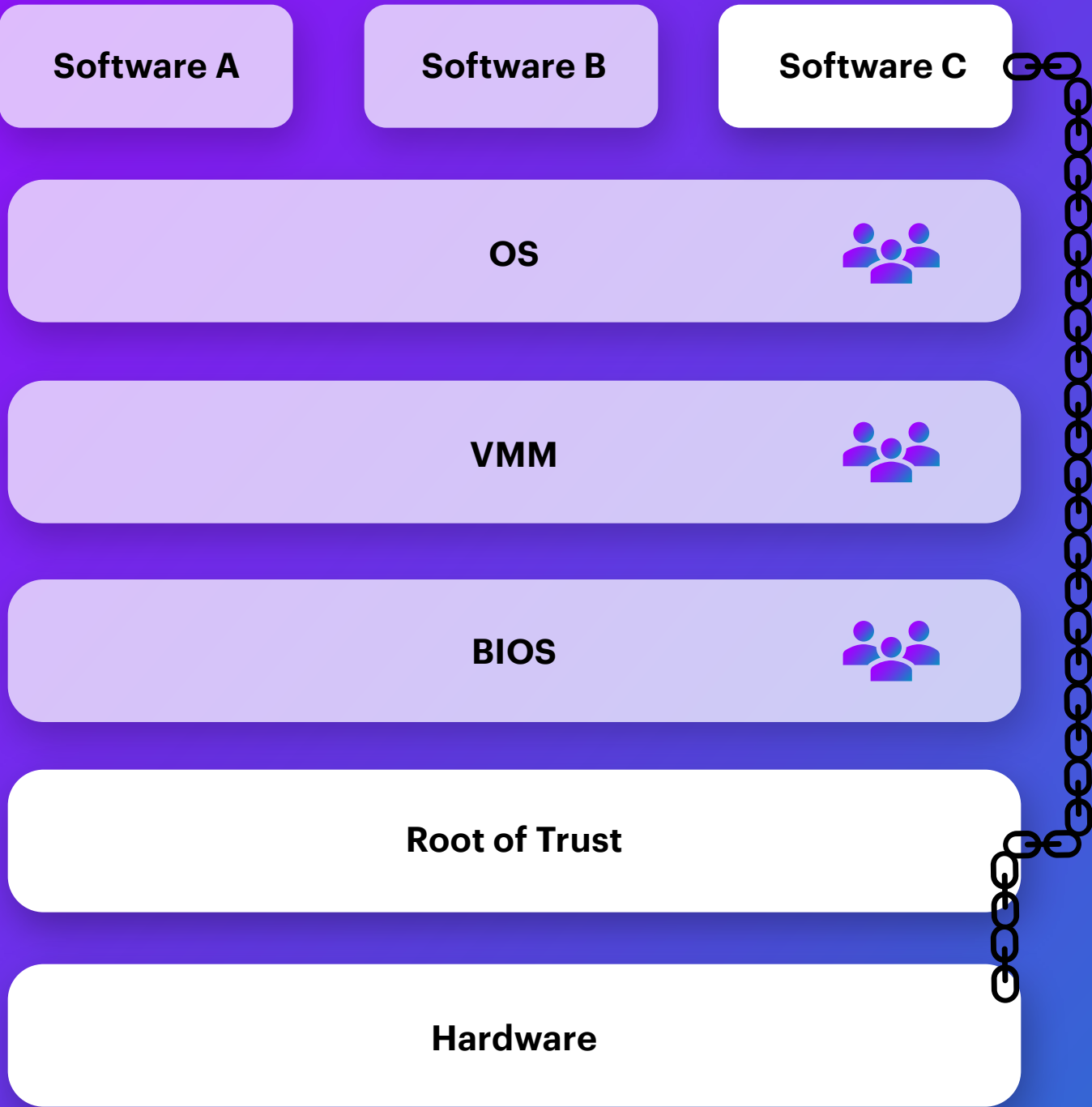
Enterprises can now also **protect data in-use** in addition to **data in-transit** and **data at-rest**. They can also enable multi-party sharing of data **without the risk of exposing it** and provide governance controls through attestation of secure enclaves.



# Traditional chain of trust



# Confidential Computing chain of trust



Confidential Computing reduces trust dependencies on each layer of the stack, thereby minimizing the footprint.





# Confidential Computing – Business transformation, not just mitigation

Confidential Computing is one of the pillars of data protection. It provides data confidentiality while in-use, data integrity, code integrity, and code confidentiality. It also ensures the integrity of a computational environment. Through this underlying technology, Confidential Computing provides additional safeguards against malicious insiders, hacker attacks and third parties accessing data without owner’s consent.

These features of Confidential Computing not only mitigate the risk of existing known risks but also provide **new opportunities for cyber transformers** to build new use cases and business models for additional revenue growth.



### Data and AI security

Closing data security gaps end to end


> **Example:** Running secure workloads and applications in a cloud environment.



### Cloud migration

Protecting confidentiality and integrity in the public cloud

> **Example:** Migrating existing workloads to the cloud using containers.



### Trustworthy AI and ML

Sharing and analyzing sensitive data sets

> **Examples:** Privacy-preserving inferencing or training using 3rd party environment. // Multiparty federated learning.



### Trusted secure environments

Highest level of confidentiality and assurance for business-critical applications

> **Example:** Sovereign cloud environment deployed on bare metal using containers.



# Confidential computing industry use cases



**Mobility**

With confidential computing, sensor data from networked vehicles can be aggregated and processed in an end-to-end encrypted and end-to-end verifiable way. It can be mathematically ensured that no relevant conclusions can be drawn from the output data about individual drivers.



**Financial services**

Through confidential computing, a retailer and a credit card company can cross-check their customer and transaction data for potential fraud while neither of them gets access to the original data. The privacy of their customers’ sensitive data is ensured by Confidential Computing alongside the whole process.



**Healthcare and Life Sciences**

Confidential computing can enable secure multi-party training of AI for different purposes. For example, multiple hospitals can combine their data to train AI for detecting diseases. The patients’ data remains confidential during each step of the process.



**Industry 4.0 – Manufacturing and Industrial**

New approaches to manufacturing try to increase productivity through massive use of sensors and corresponding data analytics. Confidential computing can encourage companies to share their data and processes securely in the cloud or amongst themselves.



**Compliance**

Confidential Computing strengthens compliance by providing secure enclaves to meet various regulatory requirements such as GDPR for sovereign cloud, HIPAA to protect patient data while still able to collaborate on AI models and other industry specific regulatory requirements.



## Available solutions<sup>2</sup>

### **Intel® SGX**

Intel's Software Guard Extensions (SGX) architecture is a hardware-enforced security mechanism that requires Trusted Computing Base (TCB), Hardware Secrets, Remote Attestation, Sealed Storage and Memory Encryption.

### **Intel® TDX**

Trust Domain Extensions (TDX) are designed to isolate VMs from the virtual-machine manager (VMM)/hypervisor to protect TDs from a broad range of software. TD offers more control over the software stack, improving the management of CPU resources, and ability to run legacy applications.

### **Intel® Trust Authority**

Intel Trust Authority attests to the validity of Confidential Computing environments. ITA verifies the trustworthiness of compute assets at the network, edge, and in the Cloud – independent of the Cloud Service Providers.

<sup>2</sup><https://www.intel.com/content/www/us/en/security/confidential-computing.html>



## Key takeaways

**Confidential Computing provides additional resiliency for the cyber transformers to help secure and isolate your most sensitive data, AI, or model assets with hardware-enhanced memory encryption.**

- **Mitigate data breach threats** – By providing security at the lowest layer of the hardware, exposure to potential attackers is reduced throughout the data lifecycle.
- **Move/run sensitive data in the cloud** – Take advantage of cloud computing benefits while keeping in mind that only data owners have access to the data.
- **Protect intellectual property** – You can preserve confidentiality of machine learning algorithms and analytical functions by running them in a protected environment. Confidential Computing makes it possible to combine and analyze sensitive data across organizations and 3rd party entities, without disclosing company secrets.
- **Compartmentalize business applications** – Confidential Computing also supports compartmentalization of workloads such that a compromise in one area (e.g., a poorly written 3rd party event registration app) cannot compromise neighboring VMs on the network.







## **Inderpreet Singh**

Cloud Security Lead

Accenture and Intel Partnership

[inderpreet.singh@accenture.com](mailto:inderpreet.singh@accenture.com)