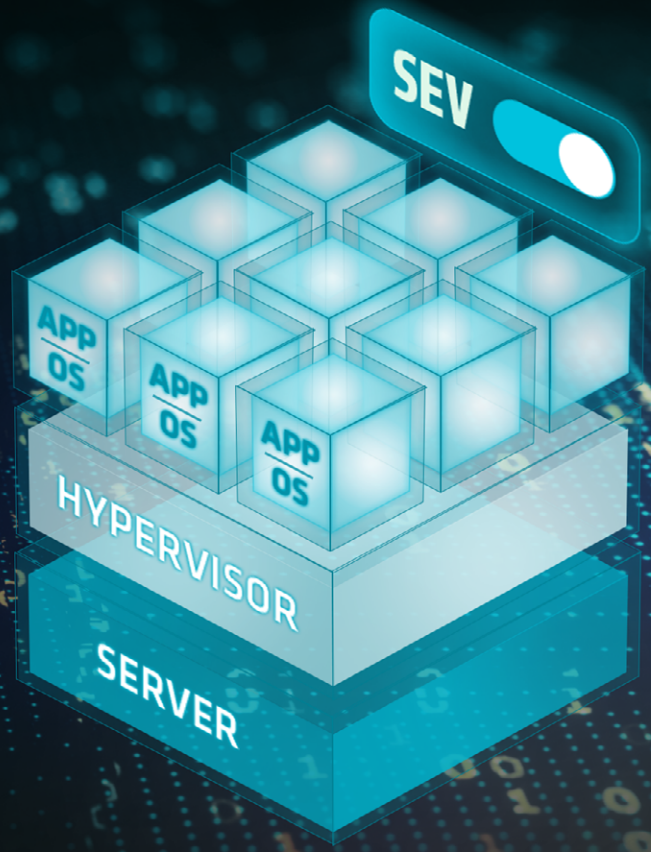
AMD
together we advance_



THE *CONFIDENTIAL COMPUTING* REVOLUTION

SEE HOW AMD EPYC™ SERVER CPU-POWERED CONFIDENTIAL COMPUTING IS TRANSFORMING COLLABORATION AND UNLOCKING INNOVATION

CONFIDENTIAL COMPUTING *ON DEMAND* CHANGES EVERYTHING

We usually think of security as a cost of doing business – restrictions and guardrails that limit what we can do with data. But the truth is far different. Advances in confidential computing are transforming security into an engine for innovation – while still mitigating risks.

The AMD ecosystem is making this sea change possible with confidential computing solutions that are as easy to deploy as launching a virtual machine (VM) or spinning up a container.

Built on AMD Secure Encrypted Virtualization (SEV), these solutions help address a persistent gap in data protection – protecting data while it is in use by system memory and the CPU. By closing this gap, confidential computing helps establish new levels of privacy, erases barriers to collaboration, and creates entirely new ways of working.

WHAT IS CONFIDENTIAL COMPUTING?

Secure encryption solutions have protected data at rest in storage and data in motion on networks for decades. Confidential computing technologies extend security measures to data and applications as they run, helping to protect data in use as it is computed.

Confidential computing begins with trusted execution environments (TEEs). TEEs isolate data and application code inside an encrypted space. The host system, hypervisors, and other workloads can't access the protected data inside a TEE. Workloads and data inside a TEE are protected even if the system around it is compromised.

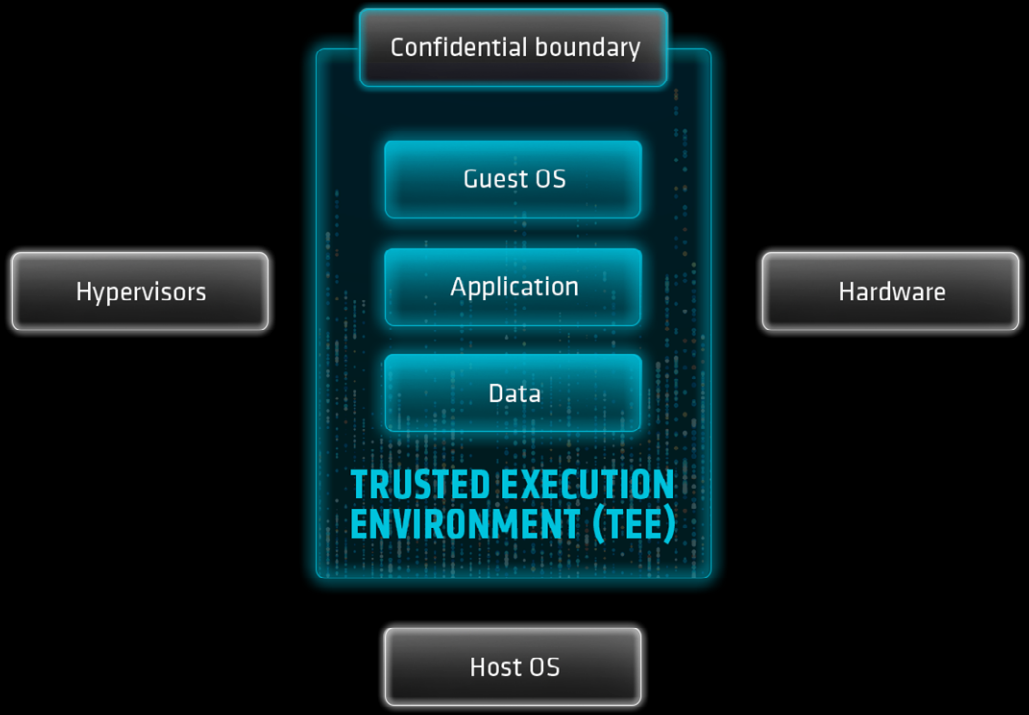
ZERO TRUST AND CONFIDENTIAL COMPUTING: ARE THEY THE SAME?

Zero trust is a security framework that assumes nothing should be trusted by default — not users, devices, applications, or data. With zero trust, any and every request for access must be verified.

Confidential computing adheres to the principles of zero trust by isolating workloads and data inside TEEs, reducing the attack surface and enforcing strong security boundaries. Communications in and out of TEEs are handled by security protocols that verify each request.

Zero trust and confidential computing are complementary but not the same. Confidential computing enhances zero trust by addressing the critical concern of data privacy and security while in use.

Confidential computing uses TEEs to isolate workloads and data at runtime



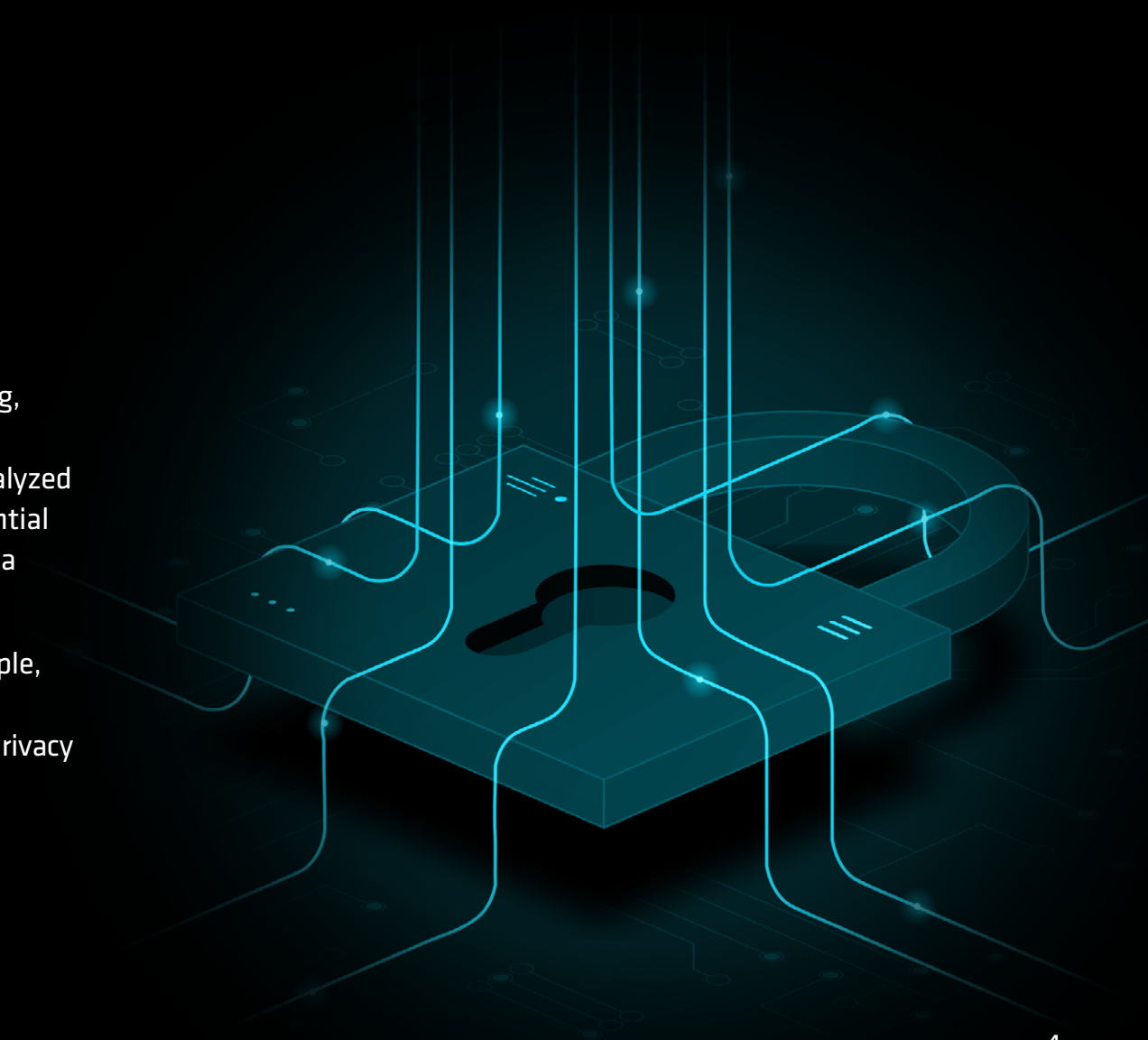
WORK TOGETHER. KEEP YOUR DATA PRIVATE.

COLLABORATION IS THE ULTIMATE CONFIDENTIAL COMPUTING USE CASE

For businesses with sensitive and/or regulated information, privacy concerns can make sharing data difficult if not impossible.

By isolating data and workloads while they are running, confidential computing creates environments where private information can be shared, processed, and analyzed securely with memory encryption — including confidential AI environments that keep models, pipelines, and data isolated in the encrypted environment.

With confidential computing and confidential AI, people, applications, and AI models can work with sensitive information in an isolated state, helping to preserve privacy and security.



CONFIDENTIAL COMPUTING FUELS INNOVATION AND COLLABORATION

Confidential computing and confidential AI help enable secure information sharing and privacy-compliant cooperative workflows that can transform practically any digital toolset, unlocking immense value and breakthrough services.

SaaS and cloud computing

SaaS providers, hyperscalers, and hosted service providers use confidential computing to enable protected services, help maintain data privacy, and engineer multi-tenant clouds with strong protection measures.

AI platforms and services

Confidential AI allows AI developers to protect their IP, train and fine tune models without exposing source data, and provide AI services that process client data stored in encrypted memory, helping ensure end-to-end privacy and data security.

Healthcare

Providers, insurers, and researchers can migrate regulated workloads to the cloud, share protected health data securely, train AI models on encrypted patient data, and extend confidential AI services to patient settings.

Finance

Financial services firms can perform analytics on encrypted data, use confidential cloud instances, and detect fraud and criminal activity without decrypting private transaction data.

Public sector

Public agencies can process and analyze sensitive data in an encrypted state, bake privacy policies into how data is accessed and shared, and provide confidential, private services for personnel and citizens.

Product design

Developers and designers can run computer-aided design (CAD), finite element analysis, and computational fluid dynamics (CFD) in the cloud and collaborate with partners and suppliers — all while keeping their data and designs encrypted.

Pharmaceuticals

Pharmaceutical companies can use high-performance computing and AI for drug discovery, share information for analysis and auditing, and help comply with data privacy and sovereignty rules programmatically — without decrypting sensitive data.

Retail

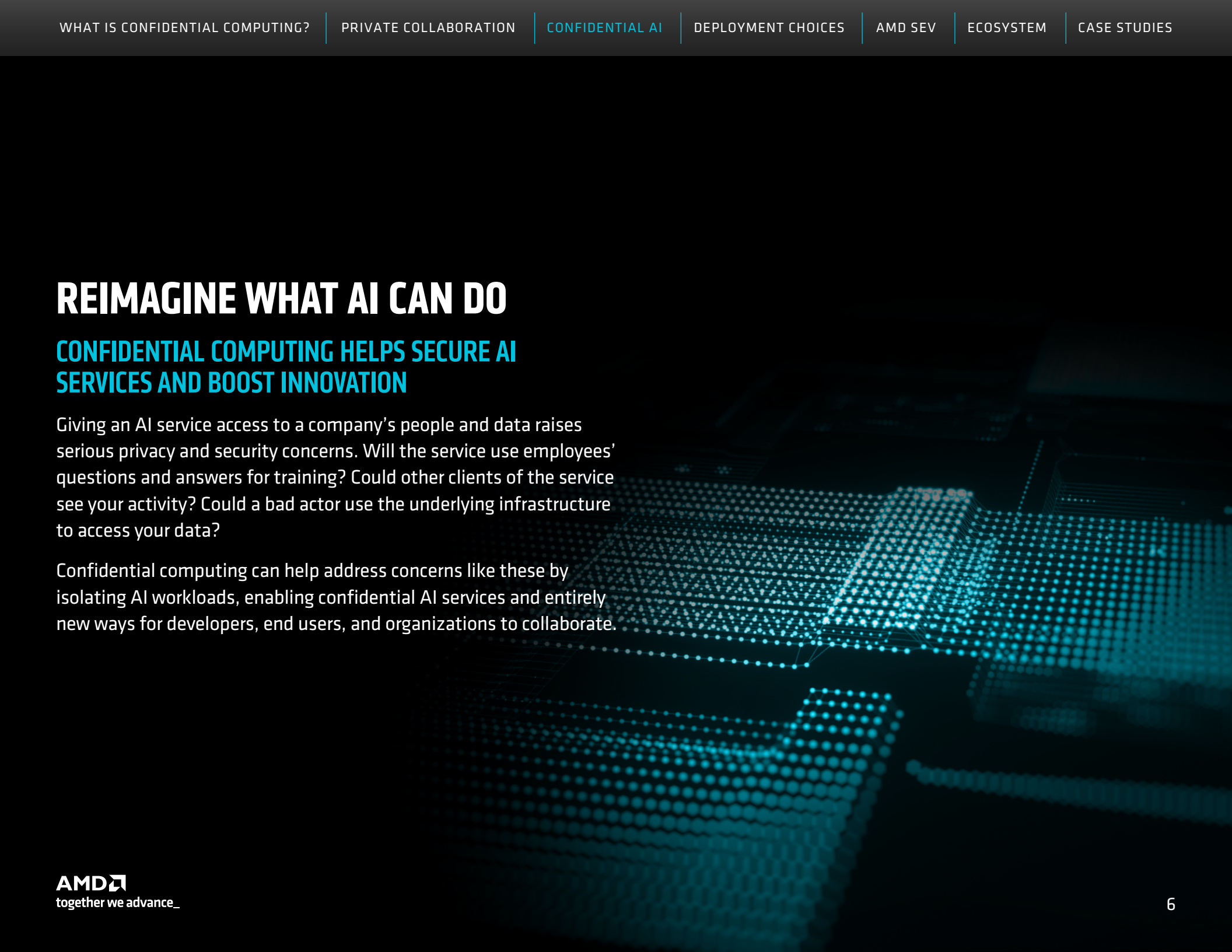
Retailers can use confidential computing to extract insights from encrypted data, integrate with vendors and third-party services without revealing private data, and share pooled data with partners and AI services confidentially.

REIMAGINE WHAT AI CAN DO

CONFIDENTIAL COMPUTING HELPS SECURE AI SERVICES AND BOOST INNOVATION

Giving an AI service access to a company's people and data raises serious privacy and security concerns. Will the service use employees' questions and answers for training? Could other clients of the service see your activity? Could a bad actor use the underlying infrastructure to access your data?

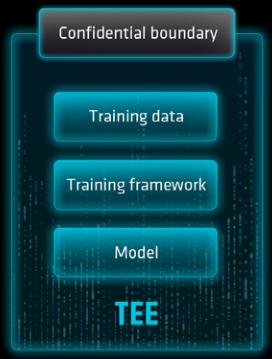
Confidential computing can help address concerns like these by isolating AI workloads, enabling confidential AI services and entirely new ways for developers, end users, and organizations to collaborate.



DELIVERING DATA PRIVACY WITH CONFIDENTIAL AI CREATES NEW WAYS OF WORKING

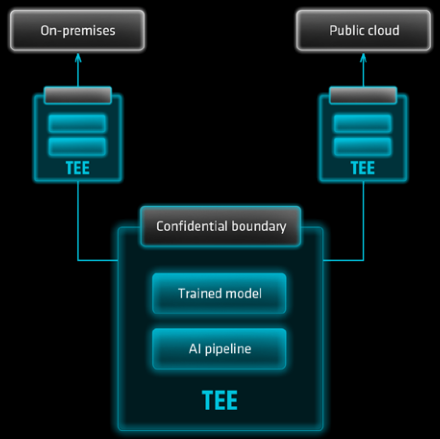
BY ENCRYPTING WORKLOADS AND DATA IN TRUSTED EXECUTION ENVIRONMENTS (TEEs), CONFIDENTIAL AI HELPS PROTECT THE ENTIRE AI LIFECYCLE FROM MODEL TRAINING TO END-USER SERVICES

AI developers can manage data and train models securely



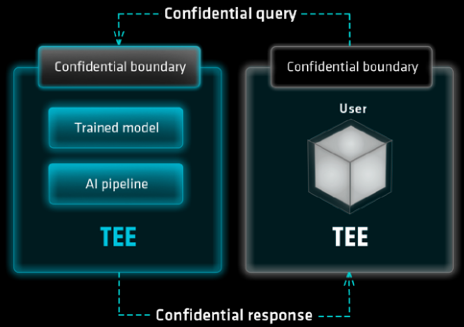
By protecting valuable IP as it runs, confidential AI allows developers to use public cloud computing or other shared IT resources and innovate faster.

Models and pipelines can be deployed with versatility



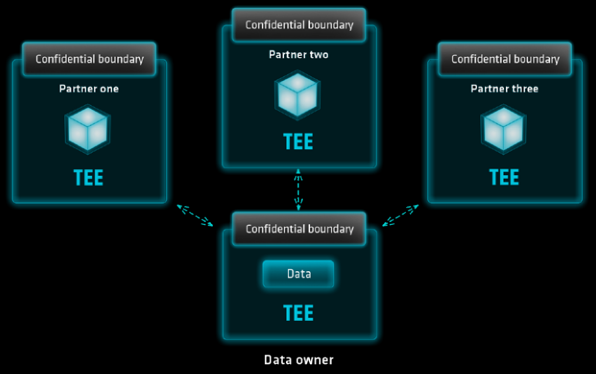
With confidential AI, models and pipelines can deploy across environments without sacrificing privacy or security.

AI can deliver confidential services



Confidential AI helps ensure only end users see queries and results. Nothing outside the TEE can see user data, including service providers, other AI pipelines, and AI models.

Organizations can share data and collaborate confidentially for AI and analytics



Confidential AI helps protect sensitive training and inference data while being shared across different businesses, which boosts AI innovation and analytics.

CODE OR NO CODE?

THERE ARE TWO MAIN WAYS TO DEPLOY CONFIDENTIAL COMPUTING: ONE COMPLICATED, ONE VERY SIMPLE

There are two basic approaches to confidential computing: confidential application enclaves and confidential VMs. Each technology uses hardware-based encryption and verification, integrated on modern CPUs.

Confidential application enclaves create trusted execution environments (TEEs) at the application level, often around the portion of the workload that is most sensitive. Enclaves can provide granular protection, but creating them requires development resources, code changes, and workload partitioning, which slows time to market.

The confidential VM approach is truly simple. With this approach, a virtual machine uses the CPU functionality to establish and enforce the TEE. Operating systems, applications, and data inside the confidential VM are protected with no code changes. Unlike application enclaves, confidential VMs can spin up on demand and be used in public cloud instances, on-premises, and as containers in cloud-native environments.

Confidential VM solutions are widely available through public cloud services thanks to AMD Secure Encrypted Virtualization (SEV). AMD SEV is a hardware-based technology built into AMD EPYC server CPUs that has become the de facto confidential computing solution for the industry.[1]

TWO PATHS TO CONFIDENTIAL COMPUTING

Establishing a confidential computing environment can be a challenging engineering task or as easy as spinning up a VM.

WRITE NEW CODE	NO CODE CHANGES
CONFIDENTIAL APPLICATION ENCLAVES	**CONFIDENTIAL VIRTUAL MACHINES**
Needs development time to engineer enclave-aware applications	Spin up on demand No code changes Helps secure any workload that can run in a VM or container
TEE protects a portion of the workload, requiring partitioning	TEE includes application, data, and OS
Runs on specifically configured systems	Runs across cloud and on-premises
Limited adoption	Mature, adopted industry-wide
IDEAL FOR Fine-grained security for cryptography, extremely sensitive code, and high-value IP	**IDEAL FOR** Confidential AI, sensitive and regulated workloads and data, protecting legacy applications

CONFIDENTIAL COMPUTING STARTS WITH AMD SEV ON AMD EPYC™ SERVER CPUs

PROTECT DATA IN USE ON-PREM AND IN THE CLOUD

Introduced on AMD EPYC server CPUs in 2017, AMD SEV pioneered the virtual machine-based approach to confidential computing. Today, AMD SEV is the go-to foundation for confidential computing in the cloud.

A built-in feature of AMD EPYC server CPUs, AMD SEV helps secure data in use on demand simply by spinning up a confidential VM. No code changes required.

AMD SEV KEY FEATURES AND BENEFITS

Built into AMD EPYC server CPUs

Delivers confidential computing via confidential VMs

Protects guest OS, applications, and data

No code changes required

Attests secure status through third-party verifier services

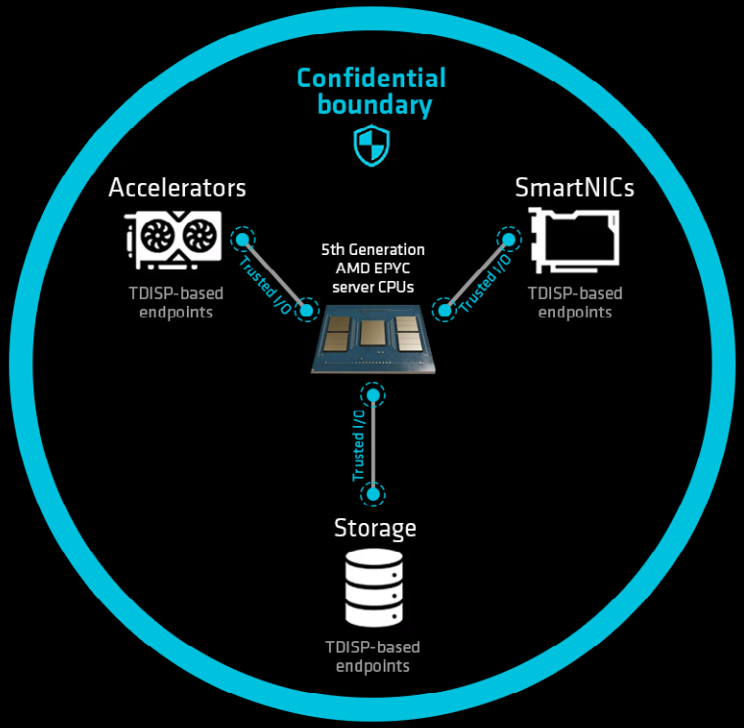
Supports TEE Device Interface Security Protocol (TDISP), a new protocol for trusted I/Os

Note: AMD SEV is not available on AMD EPYC 4004 and 4005 small business server CPUs

THE FUTURE OF CONFIDENTIAL COMPUTING IS BUILT INTO AMD EPYC SERVER CPUs

5th Generation AMD EPYC server CPUs are the first AMD CPUs to support TEE Device Interface Security Protocol (TDISP). This new protocol uses PCIe® technology to establish secure communications between confidential VMs and compatible devices, extending confidential computing to GPUs, NICs, and storage devices.

As more workloads run on dedicated accelerators, protecting data in use on PCIe-connected processors becomes critical. By incorporating TDISP, AMD SEV provides a ready-to-deploy foundation for confidential computing wherever the computing happens.



TDISP-based confidential computing for PCIe devices is built into the latest AMD EPYC server CPUs and ready for deployment.

BUILD ON THE INDUSTRY'S MOST MATURE ECOSYSTEM[1]

AMD SEV POWERS CONFIDENTIAL COMPUTING SOLUTIONS FOR CLOUDS, OPERATING SYSTEMS, AND MANUFACTURERS

To strengthen collaboration with standards organizations and industry partners, AMD publishes AMD SEV Firmware on GitHub and grants a fee-free license for its use. This has helped AMD SEV garner the support of the most mature and broad ecosystem for confidential computing in the industry.[1]

The AMD SEV confidential computing ecosystem is constantly evolving to meet emerging threats, expand capabilities, and make confidential computing easier to deploy and manage.

IF YOU RUN CONFIDENTIAL COMPUTING TODAY, YOU'RE PROBABLY RUNNING ON AMD SEV

From confidential cloud services and containers to on-premises security, AMD SEV is the foundation for confidential computing throughout the industry.

CLOUD & HYPERSCALE PARTNERS

- Alibaba
- AWS
- Google Cloud
- IBM Hybrid Cloud
- Meta
- Microsoft Azure
- Oracle Cloud Infrastructure

HYPERVISORS & VIRTUALIZATION PLATFORMS

- HPE VME
- Nutanix
- OpenStack
- VMware

OPERATING SYSTEMS

- Canonical
- Fedora
- Microsoft
- Red Hat
- SUSE

CONTAINERS

- Confidential Containers
- Docker
- Kata Containers
- Kubernetes
- Red Hat OpenShift

DEVICE MANUFACTURERS

- Dell
- HPE
- IBM
- Lenovo
- Supermicro

BMW GROUP MODERNIZES IDENTITY MANAGEMENT WITH THE HELP OF AMD SEV

For a global business like the BMW Group, secure, reliable access to computing systems and services is critical. If employees, contract workers, and industrial IoT systems can't log in securely, operations come to a halt.

To improve reliability, performance, and security, BMW Group migrated its on-site Active Directory environment and domain controllers to Microsoft Azure. To ensure this sensitive data remains secure in the public cloud, the team migrated their Active Directory to Azure DCasv5 confidential VMs running on AMD EPYC server CPUs with AMD SEV.

The results: a seamless migration, improved reliability, and zero-trust security with no code changes. Future upgrades include support for biometric log ins and transitioning to Azure DCasv6 VMs.

For details, read BMW Group Boosts Security with AMD and Azure.

"It was key not to have any downtime or business impacts. Company staff successfully and seamlessly deployed services for customers without those customers noticing."

—RAKESH GINJUPALLI, SENIOR PROGRAM MANAGER, Microsoft

ZONAR ENHANCES GDPR AND SCHREMS II COMPLIANCE WITH AMD SEV

Zonar is a smart fleet management provider that serves a global customer base. As Zonar began expanding its services to Europe, the company had to comply with the EU's General Data Protection Regulations (GDPR) and meet U.S.-Europe data transfer rules mandated by the Schrems II ruling.

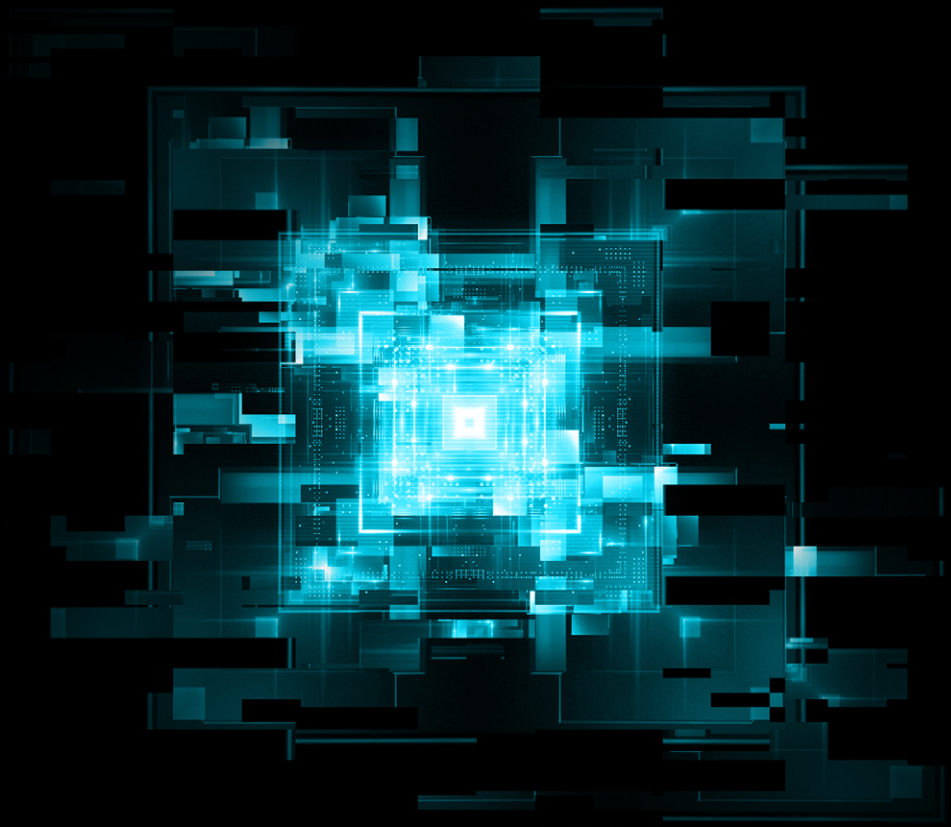
To meet these data privacy requirements, Zonar migrated EU workloads to cloud-native confidential computing solutions on the Google Cloud Platform. The Google solution uses AMD SEV to establish confidential VMs at the click of a button.

Confidential Google Kubernetes Engine (GKE) nodes and clusters deploy within the confidential VMs, providing GDPR and Schrems II compliant computing for Zonar's European workloads.

For complete details, read Zonar Enhances Privacy and Data Protection.

"Confidential Computing provided the security and compliance we wanted and was the clear choice to secure our customers' data and ensure GDPR and Schrems II compliance for European needs."

—GORDON WADDELL, SENIOR VICE PRESIDENT OF SOFTWARE DEVELOPMENT, Zonar



BEEKEEPERAI USES AMD SEV TO HELP TEAMS COLLABORATE WITHOUT EXPOSING SENSITIVE DATA

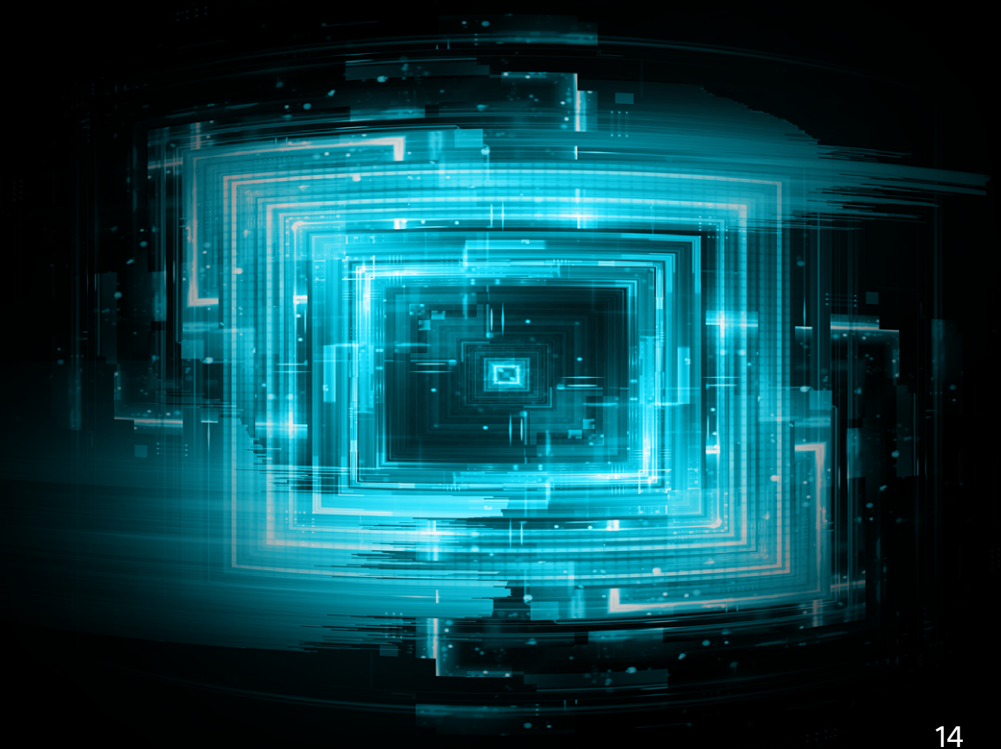
BeeKeeperAI is a zero-trust platform that secures AI models and processes in trusted execution environments (TEEs). The platform extends confidentiality to third-party cloud storage, so that data never leaves infrastructure outside of the owner's control and nothing — including the AI model — can see the data.

Built on Microsoft Azure Confidential Computing powered by AMD SEV, the BeeKeeperAI platform uses confidential VMs and containers to provide lift-and-shift solutions for AI developers that run across operating systems.

For more, read BeeKeeperAI & AMD Infinity Guard: Enabling innovation, collaboration through confidential computing.

"Using confidential containers or confidential virtual machines based on the EPYC processor is a huge benefit. Because now you have this lift-and-shift solution for algorithm developers who don't need to conform to any specific type of OS."

— ALAN CZESZYNSKI, VICE PRESIDENT, PRODUCT,
BeeKeeperAI



CONCLUSION

DEPLOY CONFIDENTIAL COMPUTING WITH ZERO CODE CHANGES

AMD SEV IS BUILT INTO AMD EPYC SERVER CPUS

AMD SEV is part of AMD Infinity Guard,[2] a robust set of modern, hardware-enabled features built into AMD EPYC server CPUs. The most mature confidential computing ecosystem in the industry,[1] AMD SEV is backed by open standards and trusted by major companies to help future-proof security strategies, reduce supply-chain risks, and keep platform options open.

Learn more at amd.com/confidential-computing

1. Confidential Computing on EPYC is enabled by the SEV security feature, which was introduced with 1st Generation EPYC in 2017. 2nd Gen EPYC powered the first confidential computing cloud instance in Google Cloud in 2020. EPYC: Powers the highest number of confidential VM options available on all major CSPs; Supports both host and guest in the Linux Kernel; Is available on all major Linux Distributions; Has support on VMware; Supports confidential containers. (EPYC-056)
2. AMD Infinity Guard features vary by EPYC™ Processor generations and/or series. Infinity Guard security features must be enabled by server OEMs and/or Cloud Service Providers to operate. Check with your OEM or provider to confirm support of these features. Learn more about Infinity Guard at https://www.amd.com/en/technologies/infinity-guard. (GD-183A)