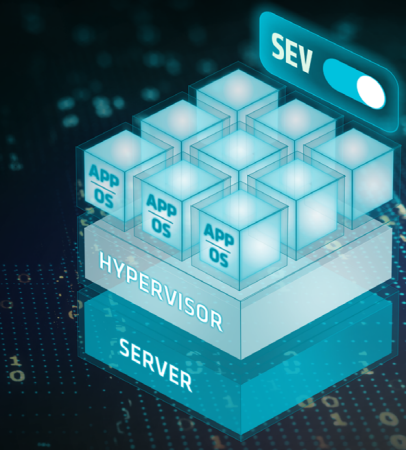
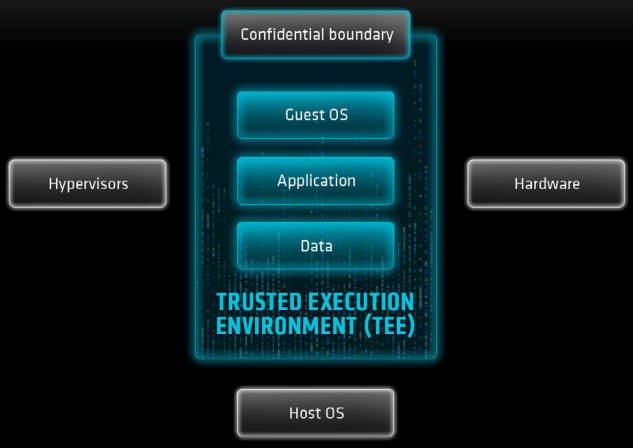
HELP PROTECT DATA IN USE ON DEMAND WITH AMD SEV

Deliver confidential computing with no code changes

Traditionally, applications and data are vulnerable when they are actively in use by system memory, CPUs, and attached devices like GPUs and network controllers. AMD Secure Encrypted Virtualization (SEV) helps protect workloads at runtime by isolating them in encrypted virtual machines (VMs) and containers that can spin up on demand — no code changes required. Because each VM is in control of its own encrypted space, data is protected from host systems, hypervisors, other users, and malicious actors.





AMD SEV enables confidential VMs that isolate workloads and data at runtime.

CONFIDENTIAL COMPUTING REINVENTS COLLABORATION

Collaboration and innovation have historically been limited by data security and privacy concerns related to sensitive information. But sensitive data has the potential to create major value when safely used for broader business purposes. By making confidential computing as simple as spinning up a VM, AMD SEV helps organizations put their most valuable data to work in new ways and collaborate with partners, all without sacrificing security.

Run sensitive workloads on public cloud instances

Running in public cloud environments provides immense scale and performance, but it can also risk exposing workloads to other tenants, host CPUs, and hypervisors. AMD SEV confidential VMs and containers help defend against threats, so cloud users don't have to trade security for scale.

Share highly sensitive data confidentially

With AMD SEV, organizations can share datasets confidentially, so that private information is protected. Teams can collaborate freely, extract insights, and even train AI models while source data stays protected — so unauthorized people, processes, and pipelines don't see it.

Document security compliance programmatically

AMD SEV verifies confidentiality at run time and provides reports for third-party attestation services. This is a critical capability for every confidential VM guest, especially in highly regulated industries such as healthcare and banking that must prove compliance.

AMD SEV MAKES CONFIDENTIAL AI POSSIBLE

By protecting workloads and data in confidential VMs, AMD SEV helps secure the AI lifecycle from training to inference.

Simplify AI training and development
By keeping source data private, confidential computing can help AI developers sidestep anonymizing training data.

Deliver confidential AI services
With AMD SEV, AI platforms can isolate user workspaces from models and AI pipelines, keeping end user queries and results private.

AMD SEV FOUNDATION

How AMD SEV delivers confidential computing

AMD SEV is a component of AMD Infinity Guard[1] that uses hardware-based security technologies built into enterprise-class AMD EPYC™ server CPUs. Encryption, acceleration, and management for virtualized confidential computing solutions are ready to run.

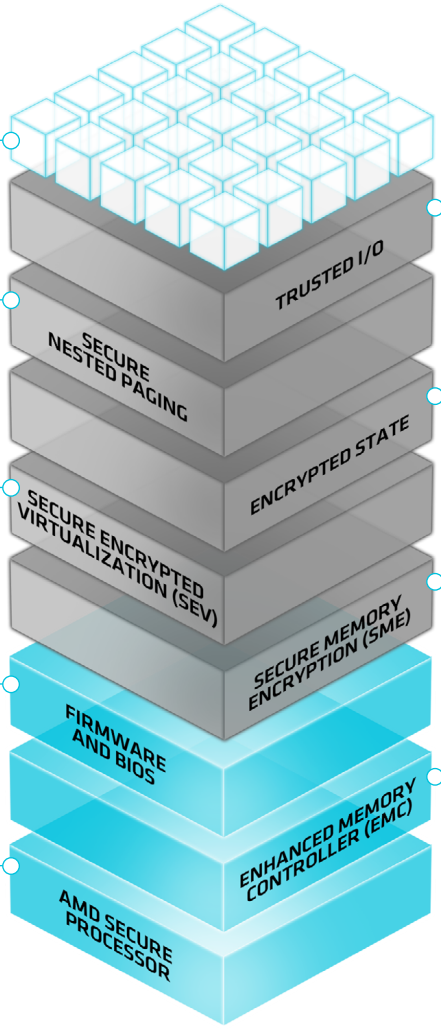
SEV-POWERED CONFIDENTIAL VMs
Establish trusted execution environments (TEEs) for guest operating systems, applications, and data

Provides VM integrity against malicious hypervisors with optional defenses against certain interrupt injections, side-channel, and rollback attacks

Encrypts VM memory with a unique key for each VM; supports encrypting all available DRAM memory with support for CXL™ memory expansion

Enable and manage AMD SEV technologies for operating systems, hypervisors, and APIs

Provides hardware root of trust, handles cryptographic operations, establishes and manages TEEs



Extends SEV to external trusted devices, such as GPUs, accelerators, NICs, and storage that support TEE Device Interface Security Protocol (TDISP)

Protects the contents of CPU registers when the virtual machine is offline

Encrypts system memory, enabling AMD SEV

Includes hardware-accelerated encryption/decryption for memory read/writes when activated

AMD SEV is a built-in feature that can be enabled on AMD EPYC 7000, 8000, and 9000 Series server CPUs. AMD SEV capabilities vary by CPU generation. AMD SEV is not available on AMD EPYC 4004 and 4005 Series server CPUs or AMD Ryzen™ CPUs.

AMD SEV ADVANCES SECURITY WITH EACH GENERATION

AMD SEV has continuously improved through the work of AMD, ecosystem partners, and industry organizations such as PCI-SIG, the Confidential Computing Consortium, and Caliptra. Each advance creates new technologies and protocols that extend the capabilities of confidential computing for all.

AMD EPYC server CPU generation	New features	New capabilities
AMD EPYC 7001	Encrypted State via confidential VMs	128-bit AES XEX encryption 128 Threads 15 Keys
AMD EPYC 7002	Encrypted CPU registers via Encrypted State (ES)	256 Threads 509 Keys Enhanced scalability
AMD EPYC 7003	Hypervisor isolation and guest attestation support via Secure Nested Paging (SNP)	–
AMD EPYC 8004 and 9004	Memory Encryption for CXL attached memory	Stronger 256-bit AES-XTS encryption 512 Threads 1006 Keys Support for up to 63 Multi Host Keys
AMD EPYC 9005	Trusted I/O	Segmented RMP Secure AVIC Performance Counter (PMC) Virtualization Guest Intercept Controls Ciphertext Hiding

LEARN MORE ABOUT CONFIDENTIAL COMPUTING WITH AMD SEV

Find confidential computing solutions built on AMD SEV and explore case studies, technical resources, and FAQs.

Visit amd.com/confidential-computing

1. 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)