YOUR DATA SHOULD BE FOR YOUR EYES ONLY

Confidential computing powered by AMD EPYC™ processors

AT A GLANCE

Shrink a potential security gap in virtualized environments and the cloud, with confidential computing. It helps protect data in use.

Confidential computing can be enabled by AMD Infinity Guard, a suite of advanced security features built into AMD EPYC™ processors.[1]

AMD Infinity Guard includes Secure Encrypted Virtualization (SEV), which encrypts virtual machines (VMs) using an encryption key known only to the processor.

Challenge

DATA IN USE CAN BE VULNERABLE TO SNOOPING

Unencrypted data in use can open the door for bad actors to peer into a VM. This point of exposure is especially risky when your business depends on a high level of privacy.

Financial Services
Must mitigate the risk of disclosure or alteration of financial data.

Healthcare
Required to defend patient records against unauthorized access.

Retail
Expected to secure customer data, including transactions.

Manufacturing
Needs to automate confidently across on-premises and cloud infrastructures.

Solution

SHRINK THE PRIVACY GAP WITH CONFIDENTIAL COMPUTING

Confidential computing helps keep data private while it's in use. In the past, data remained undefended while it was being processed virtually or in the cloud. Confidential computing on AMD EPYC™ processors can be enabled using built-in security features like Secure Encrypted Virtualization (SEV), which helps protect data in use.[1]

- **SEV** helps ensure data privacy from bare metal to the cloud. It encrypts VMs with a unique encryption key known only to the processor.
- **SEV-Encrypted State (SEV-ES)** helps prevent the hypervisor from seeing data actively being used by a VM.
- **SEV-Secure Nested Paging (SEV-SNP)** adds strong memory integrity protection capabilities to help prevent attack by a malicious hypervisor.

Encrypt data in use
Encrypt data while its being processed. Help isolate it from malicious users, the hypervisor, even admins.

Migrate easily
Efficiently move current x86 instances to AMD EPYC™ powered instances. Little to no code rewrites required.

Don't compromise performance
Enjoy advanced security features with virtually zero impact to performance.

Partners

CONFIDENTIAL COMPUTING SOLUTIONS

Take advantage of confidential computing in the cloud and virtualized environments when you select VM instances powered by AMD EPYC™ processors with SEV enabled.

Google Cloud

Cloud Platform and Kubernetes Engine

vmware

VMware® vSphere 7.0U1

Microsoft Azure

Azure Confidential VMs

There are also a variety of independent software vendors (ISVs) supporting SEV to help secure bare metal public cloud providers and hosts utilizing AMD EPYC™ processors.

LEARN MORE ABOUT AMD INFINITY GUARD

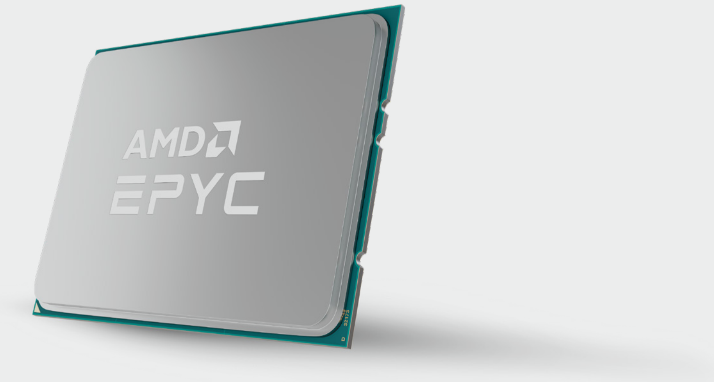
LEARN MORE ABOUT AMD EPYC™ FOR CLOUD

AMD Data Center Solutions

We are the market leader in CPU technology at a time when many businesses are modernizing their data centers.

That's a responsibility we take seriously. It's why AMD is strengthening its commitment to drive data center innovation now and into the future. Our solutions are backed by long-term roadmaps for continuous technological advancement and ongoing optimization of your IT investment.

AMD is the ideal partner today and tomorrow. We deliver more choice and outstanding value with future-ready solutions that offer high performance, easy scalability, and advanced security features.



[1] AMD Infinity Guard features vary by EPYC™ Processor generations. 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.co1m/en/technologies/infinity-guard. GD-183