5 REASONS TO USE AMD SEV *FOR CONFIDENTIAL COMPUTING*

AMD Secure Encrypted Virtualization (SEV) is a field-tested, proven approach for confidential computing that uses hardware to help virtual machines (VMs) protect workloads and data in use, on demand. A component of AMD Infinity Guard,[1] AMD SEV is built into AMD EPYC™ 7000, 8000, and 9000-series Server CPU-based platforms.

1 PROTECT DATA IN USE TODAY — AND SUPPORT YOUR ZERO-TRUST SECURITY GOALS

In the cloud or on premises, AMD SEV is ready to run whenever you need it. It's based on the "never trust, always verify" principles of zero-trust security and is designed to help protect the VM tenant's data from other VMs, applications, hypervisors, and administrators.

- **AMD SEV extends zero-trust principles to the hypervisor so that guests no longer have to trust the hypervisor by default.**

2 ENHANCE VM AND CONTAINER SECURITY, WITH NO CODE CHANGES

It's easy to deploy workloads with AMD SEV. Simply spin up a VM or container on a supported cloud instance or OEM platform to establish a Trusted Execution Environment (TEE). The TEE isolates the VM's guest OS, applications, and data from the host OS, hardware, and hypervisors — no coding, tuning, or tweaking required.

- **AMD SEV supports up to 1006 individual keys.[2]**
- **SEV memory encryption can cover the whole host memory, including CXL® memory expansion.**

3 BUILD A SECURE FOUNDATION FOR CONFIDENTIAL AI

With confidential VMs that enable entirely encrypted AI workflows, even industries with highly sensitive and regulated data, like healthcare and finance, can take advantage of AI and drive innovation.

- **With AMD SEV, multiple parties can share information without exposing their source data, better enabling collaborative AI.**

AMD

4 LEAN ON OPEN STANDARDS AND VALUABLE TRANSPARENCY

AMD SEV is interoperable by design. It aligns with industry APIs and protocols, such as the TEE Device Interface Security Protocol (TDISP), to deliver confidential VMs and trusted I/O.

- **To strengthen transparency and community collaboration, AMD published the SEV firmware source in 2023. Developers can find it on GitHub.**

5 RUN ON PREMISES OR IN THE CLOUD WITH THE INDUSTRY'S GO-TO ECOSYSTEM FOR CONFIDENTIAL COMPUTING

AMD SEV is supported by Alibaba, AWS, Azure, Google Cloud Platform, and Oracle Cloud Infrastructure plus a host of operating systems including Canonical, Fedora, Microsoft, Red Hat, and SUSE, plus virtualization platforms from VMware, Nutanix, OpenStack, and HPE VME.

- **AMD SEV is the most mature and broad confidential computing technology available for cloud and on-premises deployments.[3]**

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

AMD SEV is built into AMD EPYC™ 7000, 8000, and 9000-series Server CPUs,[4] so you can protect data in use everywhere, from on-premises data centers to the world's leading cloud providers.

For more information, visit
amd.com/confidentialcomputing

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)
2. 4th Generation AMD EPYC 8004, 9004, and 9005 processors support up to 1006 keys.
3. 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 CSP; 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)
4. AMD SEV is not available in 4004 and 4005 series AMD EPYC Server CPUs.

AMD
together we advance_