AMD

4 WAYS

AMD Infinity Guard Helps Protect Your Data

AMD EPYC™ processors are designed with a sophisticated suite of security features called AMD Infinity Guard.[1] Built-in at the silicon level, it offers the advanced capabilities required to help defend against internal and external threats — all with minimal impact to system performance.

1 YOUR DATA SHOULD BE FOR YOUR EYES ONLY

TIP

Ask your cloud provider if your instance enables confidential computing.

BENEFIT

AMD Secure Encrypted Virtualization (SEV) helps safeguard privacy and integrity by encrypting each virtual machine. 3rd Gen AMD EPYC™ processors feature SEV-Secure Nested Paging (SEV-SNP) which adds strong memory integrity protection capabilities to help prevent malicious hypervisor-based attacks.

AMD Secure Encrypted Virtualization

2 HELP YOUR DATA REMAIN PRIVATE, EVEN IN THE CLOUD

TIP

Shield system memory from snooping in the cloud.

BENEFIT

Help protect against attacks on the integrity of main memory from bare metal to the cloud.

AMD Secure Memory Encryption

3 DESIGNED TO BOOT ONLY WHAT YOU WANT TO BOOT

TIP

Help protect against bad actors.

BENEFIT

A secure root of trust made to boot only authorized firmware authenticated by the AMD Secure Processor.

AMD Secure Boot

4 DON'T LET YOUR OWN SOFTWARE WORK AGAINST YOU

TIP

Help protect against Return Oriented Programming (ROP) attacks.

BENEFIT

Keeps a record of return addresses so a comparison can be made to help ensure software code integrity is not compromised.

AMD Shadow Stack

HELP SECURE YOUR DATA WITH AMD INFINITY GUARD

LEARN MORE

AMD EPYC

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.com/en/technologies/infinity-guard. GD-181