5 REASONS WHY AMD INFINITY GUARD MATTERS FOR SECURITY

AT A GLANCE

AMD EPYC™ processors are designed with a sophisticated suite of security technologies called AMD Infinity Guard.[1] Built-in at the silicon level, AMD Infinity Guard helps your organization take control of security and decrease risks to your most important assets.

1

MODERN APPROACH

Modernize with a multilayered approach to security

Implement security features designed to be highly resistant to complex attacks, from BIOS manipulation to in-memory return-oriented programming (ROP) and virtualized malicious hypervisor attacks. AMD Infinity Guard also complements many ecosystem software and hardware solutions.

2

SECURITY FOUNDATION

Establish a strong foundation for platform security

Help mitigate malware with the AMD EPYC™ hardware "root of trust," an embedded security checkpoint designed to validate the initial BIOS software boot without corruption

3

HARDWARE-BASED ENCRYPTION

Achieve full memory encryption

Help protect against internal and physical attacks, such as certain cold boot attacks. With full memory encryption, data is encrypted even if memory is physically removed from the server.

4

CONFIDENTIAL COMPUTING

Help ensure privacy in virtualized environments

Encrypt memory data for each virtual machine. This aids in protecting confidentiality of your data even if a malicious virtual machine finds a way into your virtual machine's memory.

5

QUICK DEPLOYMENT

Seamless x86 application support

Take advantage of security features fast. AMD Infinity Guard is designed to work seamlessly with your x86 applications – without having to modify code.

Continue reading for more technical detail

TECHNICAL DEEP DIVE

#1 AMD SECURE PROCESSOR

- Authenticates the initial BIOS software boot without corruption.
- Provides cryptographic functionality for secure key generation and management in virtualized environments.

#2 SECURE MEMORY ENCRYPTION

- Helps protect against attacks on the integrity of main memory (such as certain cold-boot attacks) because it encrypts the data.
- High-performance encryption engines integrated into the memory channels help speed performance.

#3 AMD SHADOW STACK

- Maintains a record of return addresses, so a comparison can be made to ensure integrity.
- Helps guard against threat vectors such as ROP attacks.
- Enables Microsoft® hardware enforced stack protection.

#4 SECURE ENCRYPTED VIRTUALIZATION (SEV)

- Only x86 server processor with full Secure Encrypted Virtualization.
- Encrypts each VM with one of up to 509 unique encryption keys known only to the AMD Secure Processor.
- Aids in protecting data confidentiality even if a malicious virtual machine (VM) accesses your VM's memory or a compromised hypervisor reaches into a guest VM.
- SEV-ES (Encrypted State) provides additional confidentiality and integrity layers for data in use.

#5 SEV-SECURE NESTED PAGING (SEV-SNP)

- Adds strong memory integrity protection capabilities to help prevent malicious hypervisor-based attacks like data replay, memory re-mapping, and more in order to create an isolated execution environment.

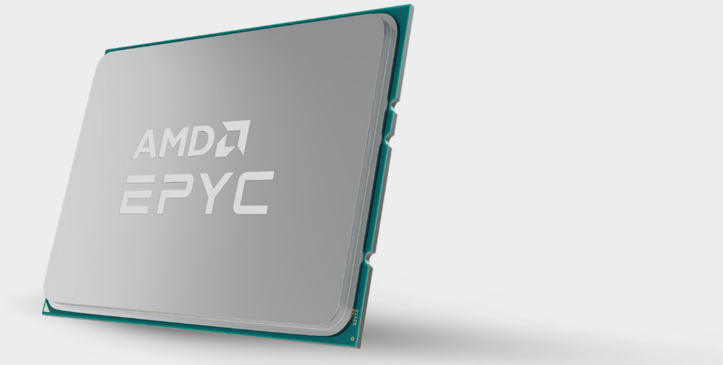
LEARN MORE AT AMD.COM/EPYC

AMD DATA CENTER SOLUTIONS

We are the undisputed 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 far 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 reinforced security features. Learn more about AMD EPYC™ for your data center.



[1] AMD Infinity Guard features vary by EPYC processor generations. Infinity Guard 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-183