PRODUCT BRIEF
AUGUST 2019

HIGHLIGHTS

- HELP PROTECT YOUR BUSINESS CRITICAL DATA
- RESTRICT INTERNAL VULNERABILITIES
- SAFEGUARD VIRTUAL AND CLOUD INFRASTRUCTURE
- SCRUTINIZE SOFTWARE BOOTS FOR CORRUPTION

'Hardened at the Core:'

Security Leadership to Help Protect Your Data

The AMD EPYC™ Family of Processors help protect your most important asset—your data. From performance-optimized countermeasures that help prevent certain side-channel vulnerabilities, to proactive encryption in memory, AMD EPYC provides advanced protection at scale for modern datacenter computing.

HELP PROTECT YOUR BUSINESS-CRITICAL DATA

The loss of critical data across many industries, and heightened data security regulations, has raised awareness that you should consider encrypting your data to help secure it from a range of prying eyes including customers, employees, service providers, domestic and foreign hackers, and even government agencies. You also need to consider how to protect your processor from a new class of attacks that can exploit speculative execution functions to infer the contents of memory that would not otherwise be authorized. Finally, you need to consider protecting the integrity of the boot process to so that both bare-metal and virtual machine boot processes do not load corrupted software.

First Gen AMD EPYC Processors pioneered a new approach with an architecture designed to help defend against certain side-channel attacks, encrypt main memory and virtual machine memory, and cryptographically help secure the boot process. With the industry's first x86-architecture silicon-embedded security subsystem, 2nd Gen AMD EPYC Processors bring increased depth and optimization to these features with growing support in the software ecosystem.

Hardened at the Core: Security Leadership to Help Protect Your Data

SILICON-EMBEDDED SECURITY SUBSYSTEM

- EMBEDDED SECURITY PROCESSOR IN THE I/O DIE
- SECURE MEMORY ENCRYPTION WITH NO CHANGES IN SOFTWARE THROUGH A SIMPLE BIOS SETTING
- 509 ENCRYPTION KEYS AVAILABLE FOR SECURE ENCRYPTED VIRTUALIZATION
- AES-128 ENCRYPTION ENGINES BUILT INTO THE MEMORY CONTROLLERS
- CPU CORES ISOLATE DIFFERENT MEMORY SOURCES
- SUPPORTS SECURE GUEST MIGRATION
- HANDLES ATTESTATION FEATURE
- HELPS SECURE THE BOOT PROCESS WITH PROTECTION AGAINST BOOTING DOWNLEVEL SOFTWARE

HELP RESIST EXTERNAL ATTACKS

Spectre, Meltdown, Foreshadow—all of these attacks have increased awareness that processor design choices are important to security. Side-channel attacks based on subtle differences in processor state now can be exploited to expose customer software and data. AMD pioneered a new approach that makes design choices with security in mind.

SAFE MULTITHREADING

Our CPU microarchitecture is designed with data isolation in mind. Data from different sources (or different threads) are designed to be isolated from different threads within the CPU. In addition to this architectural level of protection, 2nd Gen EPYC Processors further increase security capabilities with performance-optimized countermeasures against known attacks.

RESTRICT INTERNAL SOURCES OF ATTACK

The AMD EPYC Family of Processors sets a new standard for secure memory encryption (SME) by making it possible to encrypt the contents of main memory with only a change in BIOS settings. With encrypted memory, integrity attacks (such as cold-boot attacks) are unlikely to divulge memory contents because any data obtained is encrypted. High-performance encryption engines integrated into the memory channels minimize performance overhead. All of this is accomplished with no modifications to your software.

SAFEGUARD VIRTUAL AND CLOUD INFRASTRUCTURE

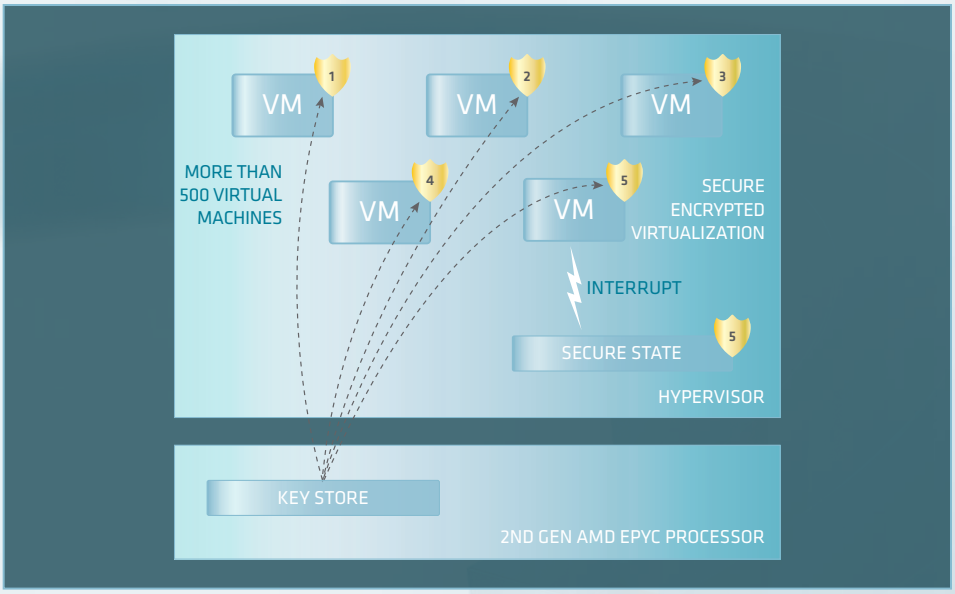
The promise of virtualization is to isolate virtual machines as if each one were running on its own server. This isolation is threatened by processor-based attacks that attempt to leak memory between virtual machines and by attempts to breach the walls between the hypervisor and other virtual machines. These are risks that you need to consider.

SECURE ENCRYPTED VIRTUALIZATION (SEV)

To help maintain the promise of virtualization, 2nd Gen EPYC Processors help protect confidentiality by encrypting each virtual machine with a unique key that is known only to the processor, with up to 509 contexts. This helps protect confidentiality of your data even if a malicious virtual machine finds a way into your virtual machine's memory, or a compromised hypervisor reaches into a guest virtual machine. Why so many more security contexts than even threads on our fastest CPUs? Because we envision a future in which containers are similarly protected and we are helping to prepare for the future by supporting abundance of security resources.

Hardened at the Core: Security Leadership to Help Protect Your Data

AMD processors isolate memory within the CPU so that the active thread can access memory only assigned to that thread.



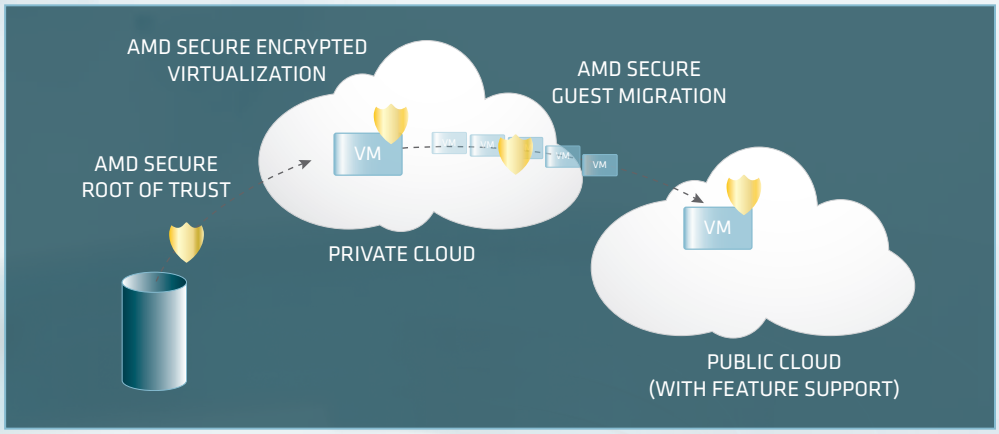
Encryption alone cannot fully lock down a virtual machine, and our processor designs are evolving to support a future in which clients do not have to trust the hypervisor:

- ENCRYPTED STATE helps secure virtual machine execution context when interrupts cause register and execution state to be stored in hypervisor memory. These buffers are now encrypted, helping deter a hypervisor or a successful intruder from obtaining a glimpse into a virtual machine's memory.
- SECURE GUEST MIGRATION helps protect confidentiality as virtual machines migrate from server to server. The source and destination AMD EPYC processors negotiate a transit key known only to the CPUs and the virtual machine contents are transferred over a secure connection, shielding software and data from exposure.

SCRUTINIZE SOFTWARE BOOTS FOR CORRUPTION

A secure root of trust monitors whether the initial BIOS software is booted without corruption. In virtualized environments, you can cryptographically validate that your entire software stack is booted without corruption on the cloud server or services you choose (attestation feature). This feature can be used to help you comply with various sovereignty regulations by helping ensure that your software runs where it is intended to run.

PRODUCT BRIEF
AUGUST 2019



WHY AMD

Security vulnerabilities have become more of a concern to the industry. AMD EPYC Processors feature an architecture that helps isolate data between threads, secure memory encryption, secure encrypted virtualization with encrypted state and secure guest migration, and a secure root of trust. With these features finding support today in a growing ecosystem of open-source and commercial products, we are committed to developing security features that help protect your business-critical data

LE-70005-00 08/19