ADDRESSING CLOUD SECURITY THREATS BY ENCRYPTING DATA IN USE

AMD

together we advance_

How **AMD INFINITY GUARD** helps address security threats in the cloud and virtualized environments

TABLE OF CONTENTS

WHY SECURITY MATTERS

Businesses face ever evolving risks as business models shift to cloud service providers and cloud computing to handle everyday business needs, with every successful closure of a gap in protection often followed by the discovery and exploitation of new ones. The result today is a shifting paradigm for data security, focused not on point solutions or "end-to-end" coverage, but multilayered protection instead.

Consider data, the main target of most cyber-attacks. Until fairly recently the objective of most bad actors was to steal data. But as encryption has improved and become more widespread, their focus has turned instead to disrupting access to data. This is a similarly concerning risk for any organization, and the criminals' hope is that target companies will pay a ransom to have their data restored or to stave off the threat of an attack in the first place.

To help guard against attacks on company data, there are ***three levels*** at which it should be protected. Two of these layers benefit from tried-and-true technologies that are widely adopted. First, there's ***data at rest,*** when it's stored on your hard drives, and hard drive encryption is ubiquitous today. Then there's ***encryption in flight,*** through company networks and VPNs.

However, the third layer, ***data in use*** – active data stored in a non-persistent state (i.e. RAM) – has gotten less attention. But because it's a significant potential security gap – particularly in virtualized environments and the cloud – it is important to address.

VULNERABILITIES IN CLOUD AND VIRTUALIZED ENVIRONMENTS

It has become routine to assume that a cloud provider's physical locations and its hyperconverged infrastructure (HCI) are secure – and therefore the data in use in those environments is also secure.

CSPs can spend a fortune on physical security and world-class digital security of their hyperconverged infrastructure (HCI). While, much of the discussion around cloud security focuses on threats coming from outside of their environment and those of their customers, CSPs cannot always control threats coming from inside their environment including a disgruntled employee with administrative of physical access to systems.

As the stakes of data breaches continue to rise, both reputationally and financially, and with the spectrum of bad actors ranging from rogue individuals to well-resourced groups sponsored by nation states, the risks to leaving these virtual environments unprotected are already unacceptable.

Simply put, data in use is uniquely vulnerable to attack vectors that encryption at rest and in transit do not protect against.

Some of these are physical and occur from inside the environment. For example, DIMMs can be physically frozen, with cans of compressed air, and then removed by bad actors with access to the servers with the data extracted later. Virtually, data that is unencrypted when in use can open the door for bad actors to peer into a VM and view or extract the data within.

There can also be small but significant security gaps that could allow hackers to access the servers themselves, by hacking the BIOS during the booting process and changing settings or grabbing boot data. This boot data may not be valuable for all companies, or even most. But for some – particularly in government or financial services – it is certainly sensitive and must be protected as a result.

Finally, while being processed in a CSP's HCI or other virtualized environments, data in use has for a long time remained undefended. The result of this being that compromised hypervisors can reach into guest VMs and expose or extract data that should be private to the VM.

CONFIDENTIAL COMPUTING WITH AMD EPYC™ PROCESSORS

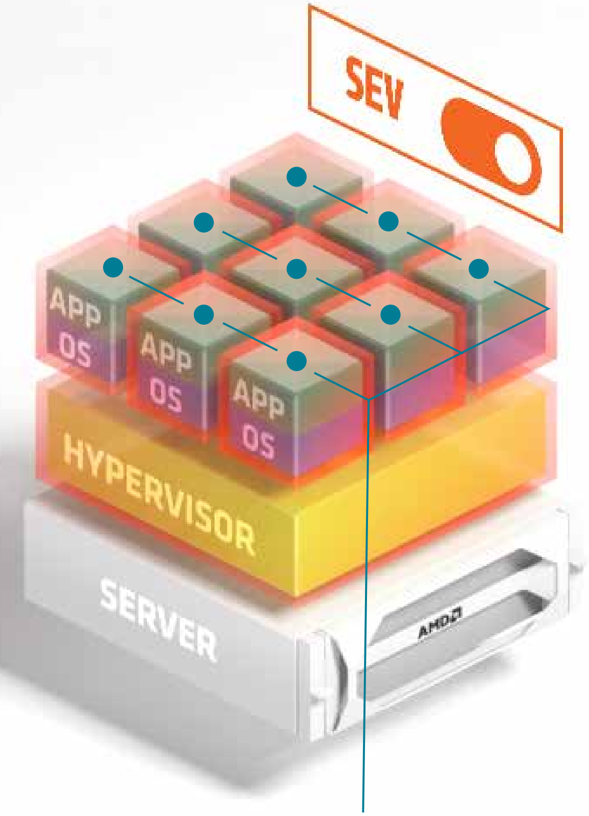
Encrypting data while it's being processed in virtual environments can help to isolate it from malicious users, the hypervisor, and even administrators. This approach, known as confidential computing, can help mitigate the risks of physical DIMMs attacks or virtual attacks in potential HCI environments.

Confidential computing using AMD EPYC™ processors uses built-in security features such as Secure Encrypted Virtualization (SEV). Part of the AMD Infinity Guard suite of advanced security features, SEV helps protect data in use by encrypting VMs using 128-bit encryption technology, with a unique encryption key known only to the AMD Secure Processor.[i]

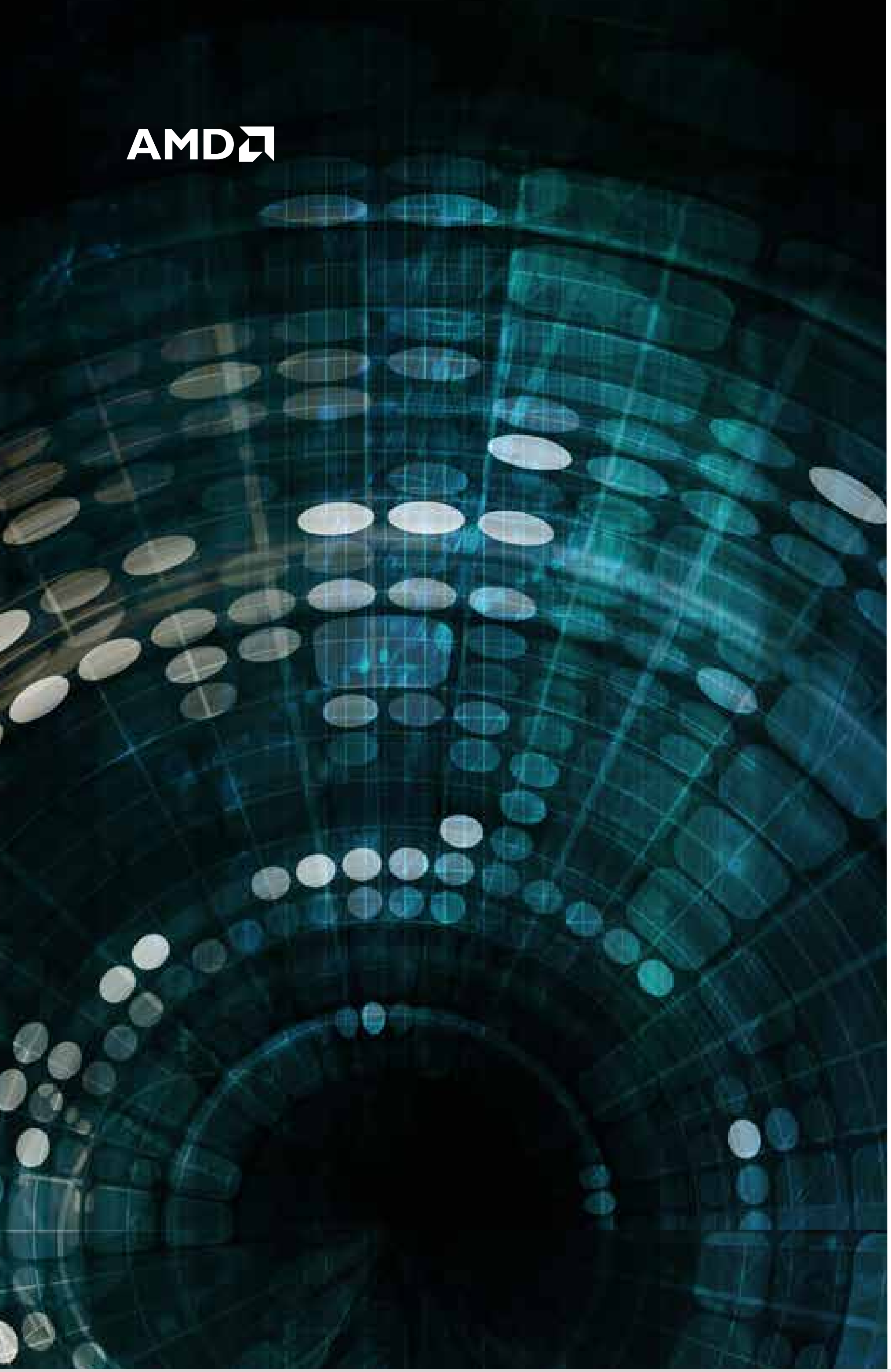
This aids in protecting confidentiality of your data even if a malicious VM finds a way into your VM's memory, or a compromised hypervisor reaches into a guest VM.

Further related features combine with SEV to create strong, multilayer protection for data in use. When enabled, SEV-Encrypted State (SEV-ES), helps prevent the hypervisor from seeing data actively being used by a VM. Meanwhile SEV-Secure Nested Paging (SEV-SNP) adds strong memory integrity protection capabilities to help prevent malicious hypervisor-based attacks, such as data replay and memory re-mapping, to create an isolated execution environment. It achieves this through attestation, providing proof that a particular VM has write access to the memory – an important protection feature in virtual environments where multiple "guests" have access to the shared system memory.

SECURE ENCRYPTED VIRTUALIZATION



Each VM has its own encryption key



AMD INFINITY GUARD

The hardware-based encryption provided by AMD Infinity Guard enables enhanced confidential computing with little compromise on performance.

Competitor CPUs often rely on an offload engine to execute encryption and so can incur a "performance penalty" on application workloads. However, AMD Infinity Guard's 128-bit AES (Advanced Encryption Standard) engine is integrated into each of the eight memory controllers found in AMD EPYC™ processors. In an independent testing example with Principled Technologies, the online transaction processing performance of an AMD EPYC™ 7543 processor-powered server was compared with and without AMD Secure Memory Encryption and Secure Encrypted Virtualization-Encrypted State enabled. Using these security features resulted in just a 1.7 percent reduction in the server's average order-processing rate.[ii]

Help your data remain private - even in the cloud

Secure Memory Encryption (SME) 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. All of this is accomplished without modifications to your application software.

In addition, competitor solutions can force built in security features to operate in enclaves of memory within the encryption engine – potentially only up to 1TB for 2P systems – which often necessitates software rewrites. But AMD Infinity Guard's SEV is not limited to the memory on the CPU and instead has access to the entire processor memory: that's up to 8TB for 2P systems. With eight memory channels and a 128-bit Advanced Encryption Standard (AES) encryption engine on top of each of those channels, the AMD solution offers a large scope for performance acceleration within a robust enclave of memory.

In addition, that enables SEV to provide advanced security features with no application rewrites. This is an important consideration in cloud environments, saving organizations the cost and complexity associated with dedicating precious resources to rewrite code to make it fit into a vendor limited memory enclave. *(Or having to find the money to convince an application provider to do the same.)*

In short, adopting AMD Infinity Guard and employing comprehensive data security features, requires little to no extra considerations, either from an application architecture or environment and performance point of view.

BEYOND CONFIDENTIAL COMPUTING AND BEYOND CLOUD

AMD Infinity Guard, a powerful set of security features, enabled in turn by a multilayered set of technologies accessible by all major HCI vendors' hypervisors. It is an industry-leading set of modern security features that help decrease potential attack surfaces as software is booted, executed, and processes your data.

Built-in at the silicon level, AMD Infinity Guard offers state-of-the-art capabilities to help defend against internal and external threats. It is suitable for use by SMB and enterprise organizations alike, whether they're looking to enable confidential computing in the cloud or enhancing the security of on-premise data centers; and whether they're working with Linux® or Microsoft environments.

As well as SEV, SEV-ES, and SEV-SNP, AMD Infinity Guard also features:

SECURE MEMORY ENCRYPTION

Secure Memory Encryption (SME) 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. All of this is accomplished without modifications to your application software.

AMD PLATFORM SECURE BOOT[iii]

The AMD Platform Secure Boot feature (extends the AMD silicon root of trust to help protect the system BIOS. This helps the system establish an unbroken chain of trust from the AMD silicon root of trust to the BIOS using AMD Platform Secure Boot, and then from the system BIOS to the OS Bootloader using UEFI secure boot. This feature helps defend against remote attackers seeking to embed malware into firmware. AMD believes that the enabling AMD Platform Secure Boot provides a powerful additional layer of security to platforms.

PARTNERS USING CONFIDENTIAL COMPUTING POWERED BY AMD EPYC™ PROCESSORS

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.

WHY AMD

The hardware-based encryption provided by AMD Infinity Guard enables enhanced confidential computing with little compromise on performance.

AMD Infinity Guard is designed to help protect your data to avoid the costs and downtime associated with a data breach.

It uses a unique multifaceted approach to data protection, offering real-world virtualization security features that have minimal impact on performance and are accessible without modifications to your application software. AMD Infinity Guard also offers security measures in many software and hardware solutions for layered defenses at the hardware, system and application levels.

It's this kind of layered approach that can help businesses stay a step ahead of ever evolving security threats.

LEARN MORE

i. 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

i. https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/enabling-sev-es-on-amd-eypc-3rd-generation-processors.pdf

iii. An OEM who has enabled the AMD Secure Boot feature grants permission for their cryptographically signed BIOS code to run only on their platforms using an AMD secure boot enabled motherboard. One-time-programmable fuses in the processor bind the processor to the OEM's firmware code signing key. From that point on, that processor can only be used with motherboards that use the same code signing key

AMD
together we advance_