Enabling two security features on 3rd Gen AMD EPYC processors minimally affected OLTP performance on a Dell EMC PowerEdge R6525 system

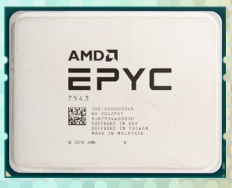
A Dell EMC PowerEdge R6525 server with AMD EPYC 7543 processors delivered similar online transaction processing performance with and without AMD Secure Encrypted Virtualization - Encrypted State and AMD Secure Memory Encryption enabled

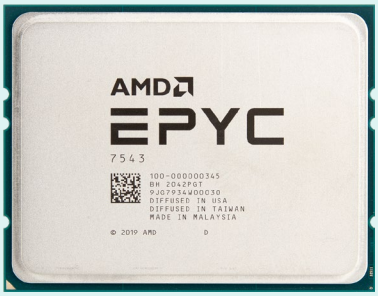
Hardware-level security is important if you want to ensure the continued health of your business and protect sensitive data. But it often comes with a price: Historically, measures to enhance CPU security have at times negatively affected CPU performance. Two security features from AMD have the potential to buck the trend by encrypting system memory, host memory, and guest CPU register with little effect on OLTP performance.

At Principled Technologies, we measured the performance impact of AMD Secure Memory Encryption (SME) and Secure Encrypted Virtualization-Encrypted State (SEV-ES) on a Dell EMC PowerEdge R6525 server powered by AMD EPYC 7543 processors. The server ran a virtualized environment consisting of Microsoft SQL Server 2019 on SUSE Enterprise Linux with VMware vSphere 7.0 Update 1 as the hypervisor. We ran an industry-standard database benchmark, first while using these security features, and then again without them. We found that the server with security features enabled had comparable OLTP performance to the same server with features disabled.

Secure and encrypt virtual machines with minimal performance impact

Enabling AMD Secure Memory Encryption (SME) and AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) resulted in **just a 1.7 percent difference** in online transaction processing (OLTP) performance.





About AMD EPYC 7543 processors

Part of the AMD EPYC 7003 Series, these 32-core processors use AMD Infinity Architecture. The latest offering from AMD, 3rd Gen EPYC processors offer increased I/O with up to 32MB L3 cache per core, 7nm x86 hybrid die core, and new security features such as Secure Encrypted Virtualization - Secure Nested Paging (SEV-SNP), Secure Memory Encryption (SME), and Secure Encrypted Virtualization - Encrypted State (SEV-ES).[1]

Why is security important?

In a 2013 article for WIRED Magazine, then-CTO of PrivateCore Stephen Weis wrote that the processor was quickly becoming the "new security boundary" in IT.[2] While disk encryption was a widely adopted practice and remains so to this day, there were few security options that could shield sensitive information when in use—in other words, when data moves from disk to system memory and is accessed by the CPU. Weis and others noted that a knowledgeable attacker could exploit this security gap, gain access to all of the data in an organization's servers, and compromise online accounts. This is an especially sinister security flaw for non-volatile memory technology, as an attacker could physically remove memory from a system while preserving the data in its unencrypted state. Security features such as AMD SME and SEV-ES aim to prevent these kinds of exploits by leveraging confidential computing.

Confidential computing

Confidential computing is a tenet of modern IT security meant to prevent disclosure or manipulation of sensitive data when it is held within system memory or processors (in other words, "data in use"). According to IBM, confidential computing technology isolates data in use, making it accessible "only to authorized programming code, and invisible and unknowable to anything or anyone else."[3]

Confidential computing limits the number of trusted hardware, firmware, and software components with authorized access to data being processed by the CPU or awaiting processing. The AMD approach for implementing confidential computing uses a dedicated security processor that handles encryption keys and offers several features to meet a variety of IT security needs. These features include AMD Secure Memory Encryption (SME), which encrypts system RAM, and AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES), which encrypts the VM CPU register. In the following sections, we'll take a closer look at these two features, how they work, and how they can help your organization to secure its sensitive information.

AMD Secure Memory Encryption (SME)

SME shields sensitive data in memory, providing protection while the data is in use.

Each time an SME-enabled system boots up, an encryption engine located on the AMD processor will randomly generate an encryption key. These keys are not visible to any software running on the CPU cores themselves. The system can then encrypt all information present in memory, while the CPU's memory controller uses the encryption key to access the information securely.

SME allows for both full and partial memory encryption. With full memory encryption, all information in memory is encrypted using a random key. AMD notes that this would provide protection from attacks such as cold booting and DRAM interface snooping. Full memory encryption would also protect against the scenario of an attacker extracting the contents of a non-volatile memory module. With partial memory encryption, the operating system and hypervisor can choose to encrypt only a subset of memory, providing protection while improving performance for non-sensitive data.[4]

Secure Encrypted Virtualization – Encrypted State (SEV-ES)

SEV-ES is an extension of AMD Secure Encrypted Virtualization (SEV), a technology that provides support for encrypted virtual machines. The original SEV feature creates unique encryption keys for each VM in a system, protecting information stored in virtual memory while everything is running smoothly. However, if a VM stops running or is interrupted for any reason, the data that was previously in-use will be saved to the hypervisor's memory. If the system hypervisor was compromised when the VM stopped working, an attacker would be able to access and read sensitive, unencrypted information on the hypervisor. They would even be able to make unauthorized changes and modifications to the system. By itself, SEV cannot protect from this kind of threat.

The SEV-ES extension, however, encrypts all CPU register contents when a VM stops running, thus preventing this kind of data leak and providing another layer of security beyond the memory encryption from SME and SEV. According to AMD, SEV-ES can also "detect malicious modifications to a CPU register state."[5]

Establishing a root of trust

Both SME and SEV-ES work by establishing a root of trust with incoming data. Within a cryptographic system, a root of trust is a source that can always be trusted because it has passed some verification check.

Imagine you're a spy who needs to hand off sensitive information to a contact in a crowded marketplace. You've never met this person in real life before, so how can you make sure to give your information to the right person? One solution would be to establish a root-of-trust-like verification: You can ask a nonsense question that only your contact knows the response to. When you hear the correct phrase, you know you can trust the person with your sensitive information.

AMD SME and SEV-ES security features work in a similar fashion. When the system boots up, an isolated encryption engine on the AMD processor randomly generates an encryption key that serves as the pass-phrase the system will use to establish root of trust that ensures only authorized system components can access sensitive data.[6,7]

Cyber Resilient Architecture on the Dell EMC PowerEdge R6525 server

The Dell EMC PowerEdge R6525, together with iDRAC9, delivers tools that aim to provide layers of security across hardware and firmware and integrate security "throughout the entire server lifecycle."[8] Dell EMC calls this layered approach to IT security Cyber Resilient Architecture, and it applies to all 14G and 15G Dell EMC PowerEdge servers. According to Dell, Cyber Resilient Architecture includes features such as:

- Silicon-based Root of Trust
- Cryptographically trusted booting
- Digitally signed firmware packages
- Hard drive encryption and enterprise key management
- Drift detection
- Dynamic System Lockdown
- Persistent event-logging
- Audit-logging and alerts
- Chassis Intrusion Detection
- Automated BIOS recovery
- Rapid OS recovery
- Firmware Rollback
- Ability to wipe all data from storage media with Rapid System Erase

To learn more, visit https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf

Our test results

Despite the numerous benefits of a secured and encrypted system, some IT administrators are reluctant to enable optional security features because they fear it will negatively affect workload performance. Our tests aimed to determine whether that is the case with AMD SME and SEV-ES in an online transaction processing (OLTP) database environment.

To quantify the effect of AMD security features on OLTP performance, we ran a DVD Store 3 workload on a Dell EMC PowerEdge R6525 server powered by AMD EPYC 7543 processors, and compared the average rate of orders per minute the server could process with and without the security features enabled. (For a detailed testing methodology as well as instructions for enabling AMD SME and SEV-ES in a VMware vSphere 7.0 U1 environment, see the Science behind this report.)

We found that enabling AMD security features resulted in just a 1.7 percent decrease from baseline performance, which we believe to be a negligible difference. The secured servers processed an average of 72,417 orders per minute compared to an average of 73,636 orders per minute without the security features. In each case, the server achieved around 80 percent average CPU utilization during this test, which we believe is in line with the upper limit of typical real-world usage for this type of work.

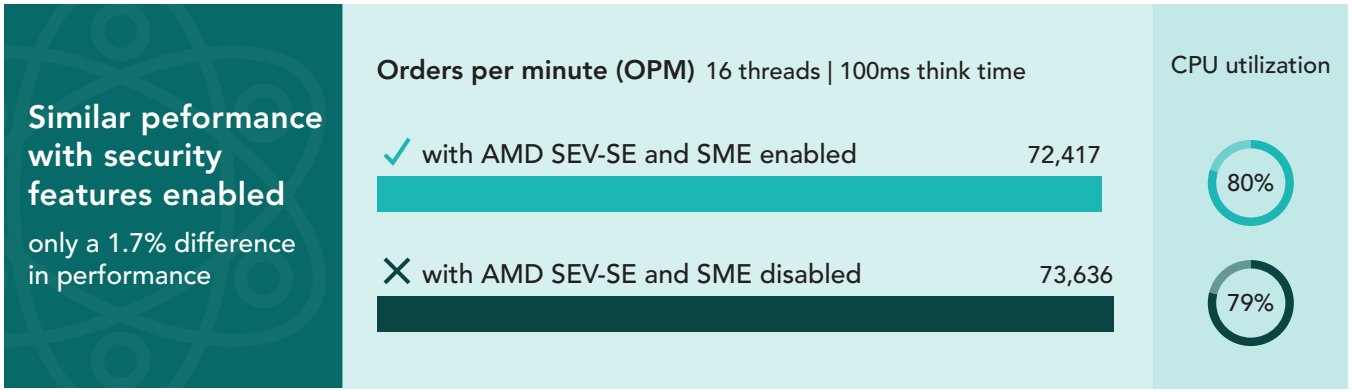


Figure 1: **Center:** Average number of orders per minute (OPM) the environment processed during the DVD Store 3 benchmark workload, using settings of 16 threads and 100ms think time. Higher is better. **Right:** Average CPU utilization of the environment during the DVD Store 3 workload. Our virtualized environment consisted of a Dell EMC PowerEdge R6525 server powered by AMD EPYC 7543 processors. The server ran Microsoft SQL Server 2019 on SUSE Enterprise Linux, with VMware vSphere 7.0 Update 1 as the hypervisor. Source: Principled Technologies.

Real-world benefits

AMD SME and SEV-ES security features have benefits for cloud service providers, for businesses using a private cloud network, and for anyone in charge of a multi-tenant environment where multiple customers have virtualized resources on the same host. You may already have measures such as role-based access control and two-step verification to prevent customers and users from simply logging into each other's virtual machines. However, these measures would not prevent an attacker from gaining access to other users' data via guest OS vulnerabilities or hardware exploits. With SME and SEV-ES, you could rest assured knowing that memory and CPU register data are encrypted and that all sensitive information will be shielded from the hypervisor during VM interruptions and failures.

Conclusion

Failing to properly secure your servers could result in catastrophic damages and a loss of customer trust should attackers gain improper access. Still, no one wants to implement security features that are a detriment to business performance in the short term.

At Principled Technologies, we compared the online transaction processing performance of an AMD EPYC 7543 processor-powered server with and without AMD Secure Memory Encryption and Secure Encrypted Virtualization-Encrypted State enabled. We found that using these security features resulted in just a 1.7 percent reduction in the server's average order-processing rate, meaning that performance was barely affected.

If your business is seeking to shore up its server security without paying a large performance tax, consider using AMD SEV-ES and Secure Memory Encryption on Dell EMC PowerEdge R6525 servers with AMD EPYC 7543 processors.

---

1 "AMD EPYC 7003 processors," accessed March 16, 2021, https://www.amd.com/en/processors/epyc-7003-series

2 Stephen Weiss, "CPU: The New Security Perimeter," accessed March 7, 2021, https://www.wired.com/insights/2013/12/cpu-the-new-security-perimeter/

3 "What is Confidential Computing? | IBM," accessed March 7, 2021, https://www.ibm.com/cloud/learn/confidential-computing

4 David Kaplan, Jeremy Powell, and Tom Woller, " AMD Memory Encryption," accessed March 7, 2021, https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

5 David Kaplan, "Protecting VM Register State with SEV-ES," accessed March 7, 2021, https://www.amd.com/system/files/TechDocs/Protecting%20VM%20Register%20State%20with%20SEV-ES.pdf

6 "What is Root of Trust?" accessed March 7, 2021, https://cpl.thalesgroup.com/faq/hardware-security-modules/what-root-trust

7 Jason Landry, "What is Hardware Root of Trust?" accessed March 7, 2021, https://www.delltechnologies.com/en-us/blog/hardware-root-trust/

8 "Technical White Paper: Cyber Resilient Security in Dell EMC PowerEdge Servers," accessed March 16, 2021, https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf

Read the science behind this report at http://facts.pt/Gpmoizs ►

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.
For additional information, review the science behind this report.

This project was commissioned by Dell EMC.