# Enable security features with no impact to OLTP performance with Dell PowerEdge R7625 servers powered by 4th Gen AMD EPYC 9274F processors

Get comparable online transaction processing (OLTP) performance with or without enabling AMD Secure Memory Encryption and AMD Secure Encrypted Virtualization - Encrypted State

Security is a critical concern for any business with sensitive data to protect—which is pretty much every business. And, the larger the business and more sensitive the data, the greater the importance. Each security breach carries a tremendous cost in time, reputation, and dollars, with the average cost of a data breach in the US amounting to over $9.4M in 2023.[1] Hardware-level security is a key piece of the puzzle for those securing data centers, but IT teams may worry that enhancing CPU security will diminish CPU performance. That doesn't have to be the case.

To look at how well security and performance can coexist, we assessed the impact of two security features—AMD Secure Memory Encryption (SME) and Secure Encrypted Virtualization-Encrypted State (SEV-ES)—on the online transaction processing (OLTP) performance of an AMD EPYC® 9274F processor-powered Dell™ PowerEdge™ R7625 server. We ran an industry-standard database benchmark twice, first with the security features enabled and then with the features disabled. We found that enabling AMD SME and AMD SEV-ES did not negatively impact OLTP performance, resulting in a less than one percent difference in orders per minute—well within acceptable variance. Our results show that with this Dell and AMD solution, you can boost security without reducing the performance of your OLTP database workloads.

## Boost security with no performance loss

Enabling SME and SEV-ES had less than 1% impact on OLTP performance

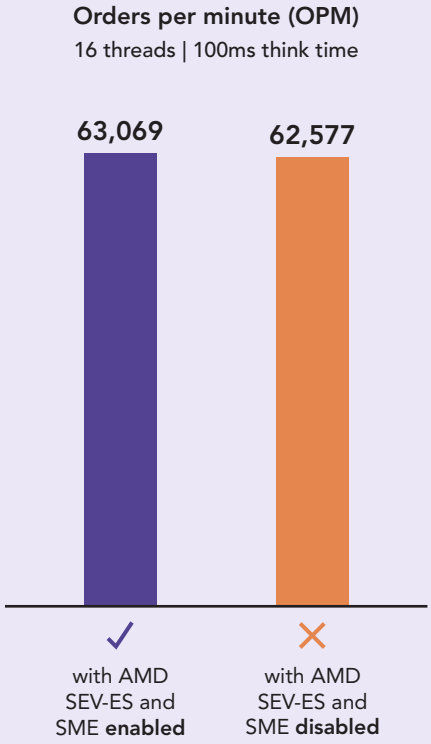


Figure 1: Average number of orders per minute (OPM) the environment processed during the DVD Store 3 benchmark workload, using settings of 16 threads and 100ms think time. Higher is better.

## What we found

The more sensitive the data your organization handles, the more vital security becomes. Because strong performance is also critical, some IT teams may worry that enabling optional security features will cause a hit to performance. We investigated this concern by assessing a an AMD EPYC 9274F processor-powered Dell PowerEdge R7625 server's OLTP performance with and without AMD SME and SEV-ES enabled.

For our test workload, we used DVD Store 3, an industry-standard online transactional database benchmark that simulates the activities of an online store. We compared how many orders per minute (OPM), on average, the PowerEdge R7625 server could process with and without the AMD processor-level security features enabled. (For a detailed methodology and hardware and software disclosures, see the science behind the report.)

When we ran the workload with the AMD SME and SEV-ES features enabled, the server's OLTP performance was actually very slightly higher than it was with the features disabled. The servers with the added encryption processed 63,069 OPM on average, while those without the extra security processed an average of 62,577 OPM— a less than one percent difference in OPM and well within acceptable variance. Average CPU utilization hovered around 75 percent in both cases, a level of utilization that we believe is in line with the upper range of typical OLTP usage in the real world.

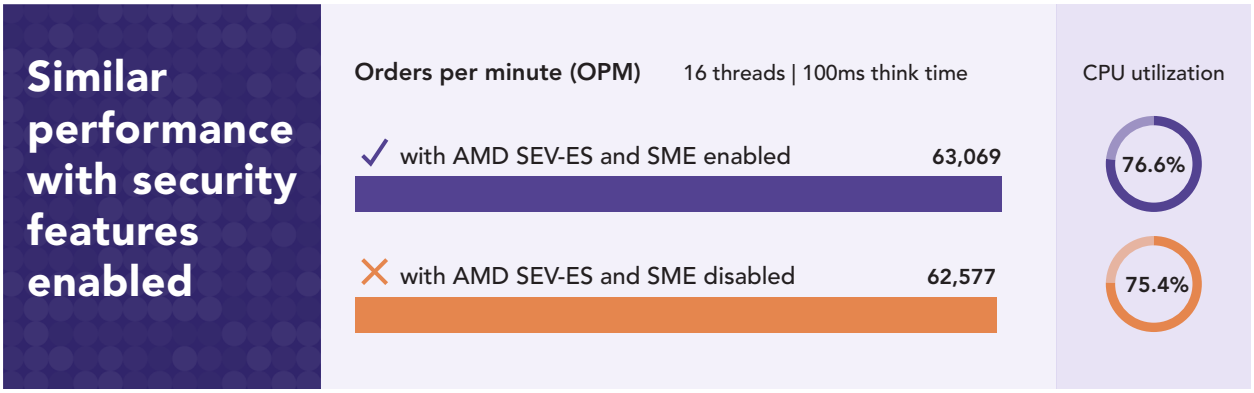


Figure 2: **Center:** Average number of orders per minute (OPM) the environment processed during the DVD Store 3 benchmark workload, using settings of 16 threads and 100ms think time. Higher is better. **Right:** Average CPU utilization of the environment during the DVD Store 3 workload. Our virtualized environment consisted of a Dell PowerEdge R7625 server powered by AMD EPYC 9274F processors. The server ran Red Hat Enterprise Linux 8. Source: Principled Technologies.

### About AMD EPYC 9274F processors

4th Gen AMD EPYC 9274F processors, part of the AMD EPYC 9004 series with AMD Infinity Architecture, offer 24 cores, 48 threads, and 256MB L3 cache.[2] The F in the processor name means that it's a high-frequency processor. They support AMD Infinity Guard, which can "help minimize potential attack surfaces as software is booted, executed, and processes your critical data," and, according to AMD, are ideal for high-performance and VDI workloads, among others.[3]

With no impact to performance, AMD SME and AMD SEV-ES can add an extra layer of security for data in memory, even in cases when the VM fails or experiences an interruption. This is particularly critical if your data center hosts data from multiple groups or organizations, each with its own sensitive data that must remain confidential from the others. In conjunction with standard security measures such as role-based access control and two-step verification, enabling these two AMD features can help prevent bad actors from accessing sensitive data.

### About the Dell PowerEdge R7625 server

The Dell PowerEdge R7625, powered by 4th Generation AMD EPYC processors, is "designed to be the backbone of your data center," per Dell.[14] This 2U server incorporates PCIe Gen5, optional GPUs, and more memory than previous generations; it also comes in air or liquid-cooled configurations. In a recent Principled Technologies study, which you can view at https://infohub.delltechnologies.com/en-us/p/the-case-for-upgrading-your-servers-to-dell-poweredge-r7625-servers-powered-by-4th-gen-amd-epyc-processors-2/, we saw the PowerEdge R7625 deliver significantly higher throughput on Bayes and k-means workloads compared to an older PowerEdge R7525 server.

To learn more about the Dell PowerEdge R7625, visit https://i.dell.com/sites/csdocuments/Product_Docs/en/poweredge-r7625-spec-sheet.pdf.

## The importance of hardware security

There were 72 percent more data breaches in 2023 than in 2021, representing a surge in cyberattacks.[4] Savvy organizations must prioritize security at all levels, including hardware. Both AMD and Dell offer a host of hardware-level security features, including AMD Platform Secure Boot, AMD Platform Secure Processor, and UEFI Secure Boot through iDRAC, among other features.[5] AMD SME and SEV-ES add a layer of protection for data in use, taking a confidential computing approach.

### Confidential computing

The National Institute of Standards and Technology (NIST) defines confidential computing as a set of "hardware-enabled features that isolate and process encrypted data in memory so that the data is at less risk of exposure and compromise from concurrent workloads or the underlying system and platform."[6] These aspects of confidential computing aim to provide an additional layer on top of encryption or other security measures to protect data in transit or data in storage, so other applications or actors on the same system cannot compromise it.

AMD incorporates several confidential computing features into their processors, including AMD Secure Memory Encryption, which offers in-memory data encryption, and AMD Secure Encrypted Virtualization-Encrypted State, which encrypts each virtual machine (VM) separately and prevents neighboring VMs or hypervisors from accessing the data on that VM. In the following pages, we examine how these two features work and how your organization can benefit from enabling them on your Dell PowerEdge servers.

## AMD Secure Memory Encryption (SME)

AMD SME protects data in memory, meaning that it shields sensitive data while the server is using that data.

Every time you boot up an SME-enabled system, such as the Dell PowerEdge R7625 we tested, an encryption engine on the AMD processor randomly generates an encryption key. Applications running on the CPU cores cannot "see" these keys, adding an extra layer of security. The system then encrypts all the data present in memory, while the processor's memory controller uses the encryption key to securely access the information. SME offers two encryption models: full memory encryption and partial memory encryption.

Full memory encryption, as you might expect from the name, encrypts all of the data in memory using the random encryption key we discussed above. According to AMD, full memory encryption is ideal "when physical attacks on the system are of concern, including government data centers and/or smaller or remote enterprise data centers that have more limited physical security."[7]

Partial memory encryption allows you to encrypt just some of the memory, protecting sensitive data more comprehensively while leaving less-sensitive data unencrypted. This offers the potential to help "provide a layer of isolation for critical workloads" while removing any performance impact—even a modest one—for your non-sensitive data.[8]

## Secure Encrypted Virtualization – Encrypted State (SEV-ES)

AMD SEV-ES is an extension of AMD Secure Encrypted Virtualization (SEV), which allows IT teams to encrypt virtual machines with unique encryption keys for each VM, thus protecting them from hypervisor corruption or threats from other VMs on the system.[9] If a VM stops running for any reason, however, the system saves the data that VM was using to the hypervisor's memory. If the hypervisor is compromised, a bad actor could access the data from that VM via the hypervisor.

The SEV-ES extension eliminates this potential attack vector by encrypting a VM's data as soon as the VM stops running. According to Dell, "Each VM, upon creation, receives a unique key, ensuring that any unauthorized attempt to access its memory results in incomprehensible data," and per AMD, SEV-ES "can even detect malicious modifications to a CPU register state."[10,11]

## Establishing a root of trust

A root of trust is a source of data that is always trustworthy because it has passed a verification check. Both of the AMD security features we looked at work by establishing a root of trust with incoming data. When a system boots up, an isolated encryption engine on the AMD processor randomly generates an encryption key that serves as the passphrase the system will use to establish root of trust. This root of trust ensures that only authorized system components can access sensitive data.

### About cyber-resilient security in Dell PowerEdge servers

Dell PowerEdge servers include a range of Cyber Resilient Architecture features, anchored in a silicon-based root of trust and spanning the entire server life cycle.[12] These start with a Secure Development Lifecycle that prioritizes security and incorporates security best practices. Dell also weaves security into the physical server and its components, its firmware and software, and its management tools, including iDRAC and OpenManage.[13]

To learn more, visit https://www.delltechnologies.com/asset/sv-se/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

## Conclusion

You've likely already implemented many security measures for your servers, which may include physical security for the data center, hardware-level security, and software-level security. With the cost of data breaches high and still growing, however, wise IT teams will consider what additional security measures they may be able to implement.

AMD SME and SEV-ES are technologies that are already available within your AMD processor-powered 16th Generation Dell PowerEdge servers—and in our testing, we saw that they can offer extra layers of security without affecting performance. We compared the online transaction processing performance of a Dell PowerEdge R7625 server, powered by AMD EPYC 9274F processors, with and without these two security features enabled. We found that enabling AMD Secure Memory Encryption and Secure Encrypted Virtualization-Encrypted State did not impact performance at all.

If your team is assessing areas where you might be able to enhance security—without paying a large performance cost—consider enabling AME SME and AMD SEV-ES in your Dell PowerEdge servers.

1. Statista, "Average cost of a data breach in the United States from 2006 to 2023," accessed April 10, 2024, https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/.
2. AMD, "AMD EPYC 9274F," accessed April 16, 2024, https://www.amd.com/en/products/cpu/amd-epyc-9274F.
3. AMD, "AMD EPYC 9274F."
4. Mariah St. John, "Cybersecurity Stats: Facts And Figures You Should Know," accessed April 10, 2024, https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/.
5. Dell, "Securing the Digital Frontier: Inside Dell and AMD's Zero Trust Approach," accessed April 10, 2024, https://infohub.delltechnologies.com/en-US/p/securing-the-digital-frontier-inside-dell-and-amd-s-zero-trust-approach/.
6. Information Technology Laboratory Computer Security Resource Center, "Confidential Computing," accessed April 10, 2024, https://csrc.nist.gov/glossary/term/confidential_computing.
7. David Kaplan, Jeremy Powell, and Tom Woller, "AMD Memory Encryption," accessed April 10, 2024, https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
8. David Kaplan, Jeremy Powell, and Tom Woller, "AMD Memory Encryption."
9. David Kaplan, Jeremy Powell, and Tom Woller, AMD Memory Encryption."
10. Dell, "Securing the Digital Frontier: Inside Dell and AMD's Zero Trust Approach," accessed April 10, 2024, https://infohub.delltechnologies.com/en-US/p/securing-the-digital-frontier-inside-dell-and-amd-s-zero-trust-approach/.
11. AMD, "AMD Secure Encrypted Virtualization (SEV)," accessed April 10, 2024, https://www.amd.com/pt/developer/sev.html.
12. Dell, "Cyber Resilient Security in Dell PowerEdge Servers," accessed April 10, 2024, https://www.delltechnologies.com/asset/sv-se/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.
13. Dell, "Cyber Resilient Security in Dell PowerEdge Servers."
14. Dell, "PowerEdge R7625," accessed April 10, 2024, https://i.dell.com/sites/csdocuments/Product_Docs/en/poweredge-r7625-spec-sheet.pdf.

**Read the science behind this report at https://facts.pt/gpFCYF4 ►**

Principled Technologies®

Facts matter.®



This project was commissioned by Dell.