



Performance and Cost Advantages When Running Latest-Generation VMs

Key performance indicators (KPIs) show how Microsoft Azure® virtual machines (VMs) powered by 4th Generation AMD EPYC™ processors can exceed the performance of VMs powered by previous-generation processors and run confidential compute with minimal performance overhead.

Executive Summary

Enterprises must now protect sensitive data not just at rest or in transit, but also during active processing. Confidential computing steps in as a strategic solution, enabling data-in-use protection through hardware-based trusted execution environments. Microsoft Azure® and AMD have taken the lead in operationalizing this capability, with AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) technology offering advanced memory encryption and Azure delivering production-ready confidential virtual machine (VM) types. Together, these solutions provide a critical option for organizations evaluating secure-cloud adoption.

In this study, commissioned by Microsoft, Prowess Consulting tested Azure confidential VMs powered by 4th Generation AMD EPYC™ processors, comparing these VMs against confidential VMs powered by 3rd Gen AMD EPYC processors and against general-purpose VMs powered by 4th Gen AMD EPYC processors. The results show clear generation-over-generation gains: up to 30% higher CPU throughput, up to 77% stronger memory bandwidth, and up to 34% better Redis® performance. At the same time, AMD SEV-SNP protections introduced only modest overheads, both at the system level (2% in memory, 8% in CPU) and at the application level (8% in Redis).

For IT leaders, the message is clear: confidential computing with Azure VMs powered by 4th Gen AMD EPYC processors can deliver stronger safeguards and real performance gains—without steep trade-offs. With measurable gains across diverse workloads and minimal overhead from AMD SEV-SNP, Azure confidential VMs are now a practical, mainstream option for enterprises balancing security, performance, and value in their cloud strategies.

Generation-on-generation
performance gain of

30–77%

for Microsoft Azure®
confidential VMs with AMD
SEV-SNP technology

Performance overhead of

2–8%

for Microsoft Azure
confidential VMs with AMD
SEV-SNP technology

Study Overview

For this study, Prowess Consulting set out to answer a simple but pressing question: can enterprises gain stronger security without giving up the performance they rely on? We tested Azure confidential VMs powered by AMD EPYC processors to find out, measuring both generation-over-generation progress and the real impact of enabling AMD SEV-SNP protections. The result is a data-driven view of confidential computing performance that cuts through speculation and provides IT leaders with clear, actionable insights.

Study Motivation

Data security no longer stops at rest or in transit. Attackers now target data from the moment it's actively processed, and regulators demand enterprises prove they can protect their data during this critical time. Regulations like the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States raise the stakes for zero-trust architectures, pushing organizations to secure workloads not just from outside threats but also from risks inside the infrastructure itself.

Confidential computing is a powerful option. Enterprises can safeguard sensitive transactions, analytics, intellectual property (IP), and personally identifiable information (PII) against exposure—even in the cloud—by isolating data-in-use within hardware-based trusted execution environments. Leading providers such as Azure now deliver confidential VM families that combine strong protections with cloud agility, making this capability a strategic imperative rather than a niche option.

Performance Concerns Impeding Adoption

For all its promise, confidential computing still comes with a shadow of uncertainty. IT leaders worry that enabling features like AMD SEV-SNP could erode performance for CPU- and memory-intensive workloads.

AMD SEV-SNP is a hardware-based confidential computing technology that uses memory access firmware to protect VM memory by ensuring that only the processes within the VM can write and read the VM's memory. This technology even excludes the cloud provider's host operating system or hypervisor from accessing this memory. An understandable concern this raises is that compute overhead for this security could undermine the agility that cloud adoption is meant to deliver. Others question whether the added security is worth the potential increase in cost, complexity, or operational risk—especially when budgets are under scrutiny and performance expectations are non-negotiable.

Generation-to-Generation Progress Requires Empirical Validation

Each new processor generation brings bold claims of faster performance, tighter security, and greater efficiency. With 4th Gen AMD EPYC processors, those claims center on both raw architectural improvements and more efficient handling of AMD SEV-SNP-enabled confidential computing. Azure has already acted on this promise by rolling out new VM families, such as the DCas_v6 VM types, that make use of these processors to deliver stronger confidentiality guarantees without sacrificing speed or scalability.

But with enterprise decisions, claims alone don't suffice. What IT leaders need is clear, empirical validation: evidence that confidential VMs powered by 4th Gen AMD EPYC processors truly outperform their 3rd Gen AMD EPYC processor-based counterparts. Only through transparent, generation-over-generation comparisons can organizations assess whether these advances translate into measurable value in real-world workloads.

Why AMD EPYC Processor-Powered Azure Instances?

AMD SEV-SNP technology stands out as one of the most advanced, hardware-enforced approaches to protecting data in use. It offers strong encryption and integrity safeguards baked directly into the processor. At the same time, Azure has emerged as a leader among cloud service providers (CSPs) in operationalizing this capability, making confidential VM types broadly available for production workloads. Together, these platforms offer a natural testbed to gauge the maturity and readiness of confidential computing for enterprise use.

This study delivers insights that are not just technically rigorous but also highly relevant and actionable by focusing on AMD EPYC processor-powered Azure instances. IT leaders evaluating their next steps in secure-cloud infrastructure can see how the hardware protections offered by the AMD EPYC processors and the Azure platform's service delivery combine in practice, helping users make informed choices grounded in data rather than assumptions.

Study Methodology

This study measured confidential computing performance with transparency, rigor, and relevance for enterprise IT leaders in order to move past speculation. Our objectives were clear and tightly focused:

- 1. **Compare performance across generations:** Measure Azure confidential VM instances powered by 4th Gen AMD EPYC processors against those powered by 3rd Gen AMD EPYC processors.
- 2. **Assess the impact of AMD SEV-SNP:** Evaluate how enabling AMD SEV-SNP affects performance in representative enterprise workloads.
- 3. **Provide validation:** Test Microsoft’s and AMD’s performance claims through benchmarking designed to reflect real-world deployment conditions.

By addressing these objectives, the study provides results based on data that can be used to inform decisions regarding architecture, budgeting, and long-term cloud strategy.

Testbed Configuration and Instance Selection

To ensure representative comparisons, we tested a mix of current and prior-generation Azure VM types under consistent conditions. The configurations we tested included:

- 3rd Gen AMD EPYC processor–based DCas_v5 confidential VMs
- 4th Gen AMD EPYC processor–based DCas_v6 confidential VMs
- 4th Gen AMD EPYC processor–based Das_v6 general-purpose VMs (for a non-confidential baseline)

Table 1. Microsoft Azure® VM sizes and operating systems used in this testing

| VM sizes | Operating systems |
|---|--|
| <ul style="list-style-type: none">• D16/DC16• D96/DC96 | <ul style="list-style-type: none">• Windows Server® 2025• Ubuntu® 24.04 LTS |

For our testing, we ran all workloads locally within each VM to minimize external network dependencies. This setup allowed us to isolate the effects of processor generation and AMD SEV-SNP enablement, providing clean, apples-to-apples results across the test matrix.

Workload and Benchmark Selection

We selected workloads that reflect the mix of compute, memory, and data-intensive demands faced by modern enterprises. To measure raw system performance, we used the SPEC CPU® 2017 suite, with SPECspeed® gauging task latency and SPECrate® capturing throughput across cores.

For memory performance, the AMD STREAM benchmark provided a clear view of bandwidth and latency behavior at the subsystem level. And to capture performance in latency-sensitive and throughput-driven in-memory data store scenarios, we included Redis, evaluated with the redis-benchmark tool. Together, these benchmarks ensured a balanced and representative assessment of confidential VM performance.

Test Execution Approach

We followed a structured execution plan for all benchmarks to ensure the validity and repeatability of our results:

- **Consistency:** We ran each scenario three times, with median results reported to smooth out anomalies.
- **Contextual metrics:** We tracked CPU, memory, and disk utilization throughout to support accurate interpretation of outcomes.
- **Standardization:** We applied identical configurations and deployment patterns across test cases to keep comparisons uniform.
- **Best practices:** All testing followed a Microsoft-approved test plan, aligning with platform guidance for representative results.

Limitations and Scope

This study focuses on single-VM performance. This research excludes multi-node scaling and distributed workloads, even though they are critical in many enterprise scenarios. Our goal was to isolate performance characteristics at the VM level to ensure clear and comparable results.

Performance Findings

The results of our testing highlight both the advancement to AMD’s latest architecture and the practicality of confidential computing in real-world workloads.

Test Results

Across CPU-bound, memory-intensive, and database-driven workloads, the data tells a consistent story: confidential computing on 4th Gen AMD EPYC processors delivers substantial performance improvements over the prior generation. It also narrows the gap with non-confidential instances running on the same generation of processors. The following sections summarize the most telling results, focusing on the metrics that matter most to IT leaders evaluating secure-cloud adoption.

Generation-over-Generation Gains

In CPU- and system-level benchmarks with SPEC CPU 2017, 4th Gen AMD EPYC processor–based confidential VMs such as the DC96as_v6 delivered about a 30% increase in throughput compared to 3rd Gen AMD EPYC processor–based equivalents across both Windows Server® and Ubuntu® environments. Workloads including the GNU® C compiler (SPEC test 502.gcc_r) and H.264/AVC video encoder (525.x264_r) demonstrated faster instruction execution and improved thread efficiency, with latency-focused runs also showing quicker completion times.

Memory performance saw the strongest gains. Using the STREAM benchmark, 4th Gen AMD EPYC processor–based confidential VMs achieved roughly a 77% improvement in memory bandwidth, particularly in copy and scale operations. These results validate AMD’s architectural enhancements, such as the transition to DDR5 and a redesigned memory subsystem. Likewise, Redis testing showed a 34% increase, highlighting the real-world benefits for latency-sensitive, in-memory workloads (see Figure 1 and Table 2).

Taken together, these results establish that confidential computing on 4th Gen AMD EPYC processors is not only more secure but also measurably faster across diverse workloads. For enterprises, the shift from 3rd Gen AMD EPYC processor–based confidential VMs to 4th Gen AMD EPYC processor–based confidential VMs offers both stronger protections and tangible performance dividends.

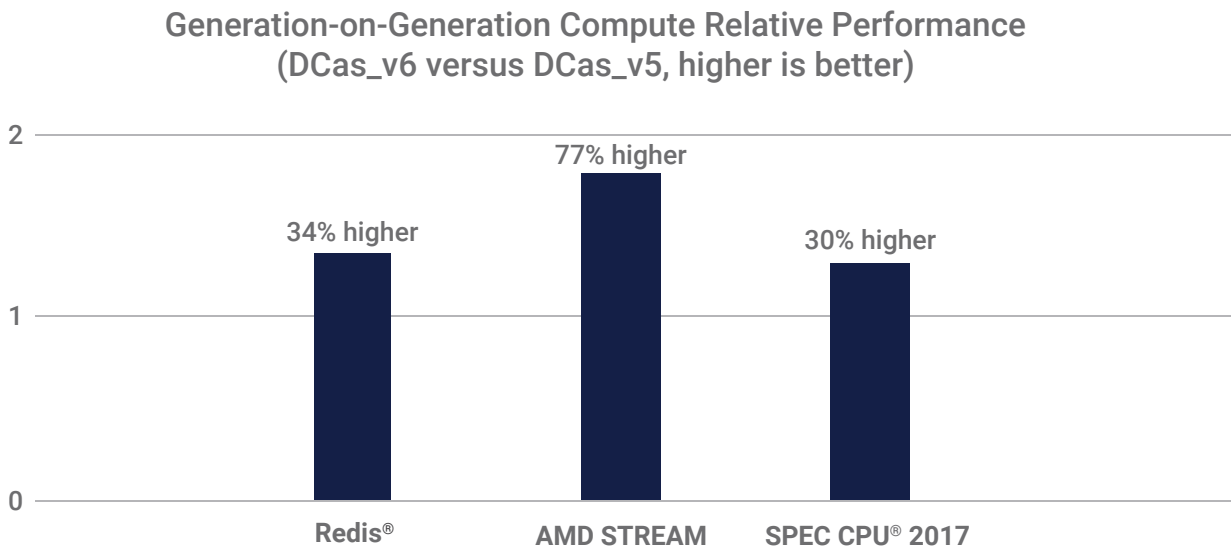


Figure 1. Generation-over-generation performance of Microsoft Azure® confidential VMs: DCas_v6 (with a 4th Gen AMD EPYC™ processor) vs. DCas_v5 (with a 3rd Gen AMD EPYC processor), summarized by benchmark geometric mean

Table 2. Benchmark-by-benchmark relative performance: Microsoft Azure® confidential DCas_v6 VMs (with 4th Gen AMD EPYC™ processors) vs. DCas_v5 VMs (with 3rd Gen AMD EPYC processors), geometric-mean results

| Benchmark | Relative Performance |
|----------------|----------------------|
| Redis® | 1.34x |
| AMD STREAM | 1.77x |
| SPEC CPU® 2017 | 1.30x |

AMD SEV-SNP Impact: Confidential Instances vs. General-Purpose Instances

The key question in examining the performance trade-offs of enabling AMD SEV-SNP protections is how much performance, if any, do organizations give up when moving from a 4th Gen AMD EPYC processor–based general-purpose VM to its confidential counterpart?

The results show that the cost of confidentiality is generally modest and predictable. In CPU-intensive workloads using the SPEC CPU 2017 suite, AMD SEV-SNP–enabled VMs retained about 92% of throughput relative to general-purpose siblings—an 8% overhead. Latency-sensitive, in-memory workloads such as Redis followed the same pattern, with confidential VMs also sustaining 92% of baseline performance.

Memory performance proved stronger still for confidential-compute VMs. AMD STREAM benchmarks showed only a 2% overhead, indicating that AMD SEV-SNP protections introduce virtually no penalty in bandwidth or latency.

Figure 2 and Table 3 show that AMD SEV-SNP protections impose minimal burden in most cases. Even where the impact is more noticeable, it is stable, transparent, and offset by the stronger security posture. For enterprises, this balance makes confidential computing on 4th Gen AMD EPYC processors a practical, dependable option for a wide spectrum of workloads.

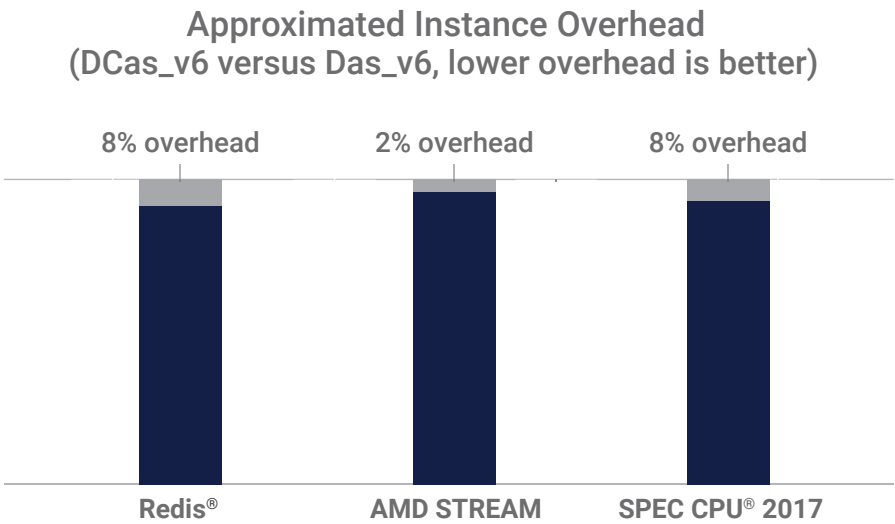


Figure 2. Estimated performance overhead when enabling AMD SEV-SNP on Azure confidential VMs (DCas_v6) compared to same-generation general-purpose VMs (Das_v6), based on benchmark geometric mean

Table 3. Relative performance and estimated overhead of Azure confidential VMs (DCas_v6) vs. general-purpose VMs (Das_v6) on 4th Gen AMD EPYC™ processors, summarized by benchmark geometric mean

| Benchmark | Relative Performance | Approximated Overhead |
|----------------|----------------------|-----------------------|
| Redis® | 92% | 8% overhead |
| AMD STREAM | 98% | 2% overhead |
| SPEC CPU® 2017 | 92% | 8% overhead |

Performance Insights

The benchmark data provides a clear throughline: confidential computing on 4th Gen AMD EPYC processors is not just viable, it is compelling. Confidential VMs consistently delivered stronger results than their predecessors across workloads ranging from raw compute to memory bandwidth. Just as importantly, the performance gap between AMD SEV-SNP-enabled instances and their general-purpose counterparts narrowed to the point where confidentiality no longer feels like a compromise in many cases.

These findings can shift the conversation for IT leaders. Confidential VMs can be evaluated not only on the strength of their security protections, but also on the strength of their performance. While traditional cloud workloads benefit from robust security measures, confidential computing adds an additional layer of protection for data-in-use, addressing emerging threats and regulatory demands. The generational improvements in throughput and latency can place AMD SEV-SNP as a mainstream solution and a special feature reserved for the most sensitive workloads. AMD SEV-SNP can now be a viable option for any enterprise application that requires both performance and advanced security.

4th Gen AMD EPYC Processor–Based Confidential VMs Deliver Clear Generation-Over-Generation Gains

The performance uplift from 3rd Gen to 4th Gen AMD EPYC processors was evident across every category of our testing. At the application level, CPU-bound workloads improved by about 30%, and Redis performance rose by 34%. At the system level, memory throughput also climbed by roughly 77%. These gains reflect both architectural enhancements (such as DDR5 and expanded memory bandwidth) and practical benefits for real-world enterprise workloads. For organizations already invested in Azure confidential VMs, the move to 4th Gen AMD EPYC processors offers stronger security guarantees alongside measurable performance dividends.

AMD SEV-SNP Security Features Can Introduce Minimal Performance Overhead in Many Cases

Perhaps more important than raw uplift is the reassurance that enabling AMD SEV-SNP no longer carries prohibitive performance costs. In our testing, confidential VMs exhibited about an 8% overhead in SPEC CPU workloads and Redis, and only a 2% overhead in AMD STREAM memory tests.

From Security Trade-Offs to Performance Dividends

This study demonstrates that confidential computing on 4th Gen AMD EPYC processors in Azure delivers on its promise: stronger data protection without unacceptable performance trade-offs. Across CPU and memory, confidential VMs showed measurable generation-over-generation gains over 3rd Gen AMD EPYC processor-based counterparts. These same VMs also demonstrated that the overhead of enabling AMD SEV-SNP relative to general-purpose VMs proved modest, predictable, and, in some cases, truly negligible. These findings validate that enterprises no longer need to choose between high performance and data protection in memory—both are achievable on the same platform.

For IT leaders, the implications are clear. Confidential VMs are now a mainstream option for securing highly sensitive workloads in the cloud. By combining AMD's hardware-based protections with the mature service delivery provided by Azure, organizations can modernize their cloud strategies with confidence. The result is a cloud infrastructure that is not only more secure, but also better aligned with the performance and economic demands of today's enterprise IT landscape.

Appendix

Table A1. Benchmarks used for this study

| Benchmark | Description |
|------------------------|---|
| <u>SPEC CPU®</u> | A widely used, vendor-agnostic suite of compute-intensive processor benchmarks (measuring integer and floating-point performance via SPECspeed® and SPECrate® metrics), maintained by the non-profit Standard Performance Evaluation Corporation. |
| <u>STREAM</u> | A simple, synthetic benchmark program that measures sustainable memory bandwidth (MB/s) and computation rate using vector kernels like Copy, Scale, Add, and Triad. |
| <u>redis-benchmark</u> | A command-line utility bundled with Redis® that provides a quick method to estimate the performance and throughput of a Redis instance on given hardware. |

Table A2. Instance sizes, tests, and operating systems

| Instance Type | Operating System | Test |
|--|----------------------|-----------------|
| D16as_v6, DC16as_v6, DC16as_v5, D96as_v6, DC96as_v6, and DC96as_v5 | Windows Server® 2025 | SPEC CPU® |
| D16as_v6, DC16as_v6, and DC16as_v5 | Ubuntu® Linux® 24.04 | SPEC CPU |
| D96as_v6, DC96as_v6, and DC96as_v5 | Windows Server 2025 | AMD STREAM |
| D96as_v6, DC96as_v6, and DC96as_v5 | Ubuntu Linux 24.04 | redis-benchmark |



Legal Notices and Disclaimers

The analysis in this document was done by Prowess Consulting and commissioned by Microsoft. Results have been simulated and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. Prowess Consulting and the Prowess logo are trademarks of Prowess Consulting, LLC. Copyright © 2025 Prowess Consulting, LLC. All rights reserved. Other trademarks are the property of their respective owners.