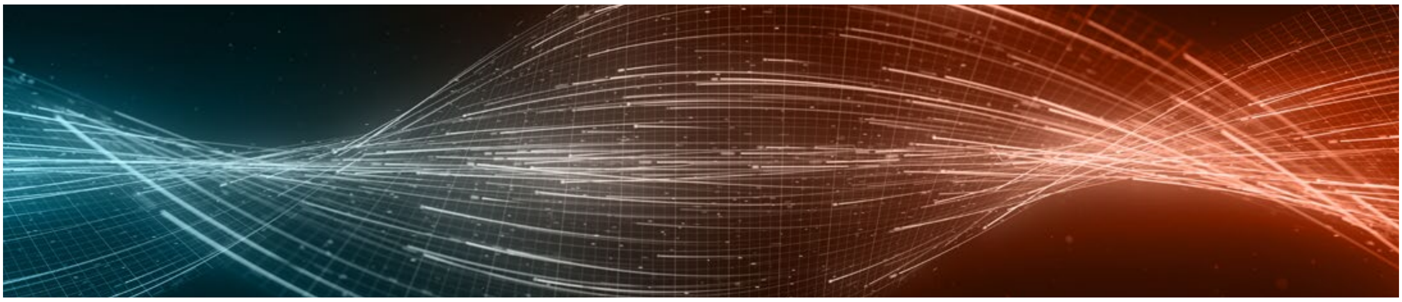
PROWESS



Technical Brief

Seamless Virtual Machine Migration Depends on Processor Consistency

In testing by Prowess Consulting, Intel-to-Intel migrations supported live workload mobility with no downtime, whereas mixed-vendor CPU environments required cold migration, increasing service interruption risk and management complexity.

Executive Summary

Organizations can migrate live virtual machines (VMs) between Intel® processor–based servers, but migration in a mixed CPU environment still requires downtime and extra administrative work.

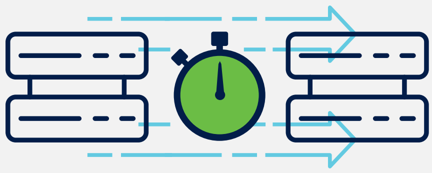
In testing conducted by Prowess Consulting, VMware® vMotion® remained an available option when the source and destination servers used Intel® Xeon® processors, even when the source and destination systems came from different Intel Xeon CPU generations. The inclusion of VMware Enhanced vMotion Compatibility (EVC) allowed a legacy Intel Xeon processor–based server and a current Intel Xeon processor–based server to execute live migration without interrupting the application running inside the VM.[1]

By contrast, moving a VM from an Intel Xeon processor–based server to a server powered by an AMD EPYC™ processor required a cold migration. That process introduced measurable downtime in both shared-storage and direct-attached-storage (DAS) configurations.

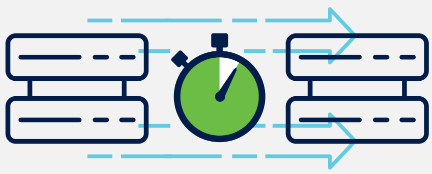
Why the Migration Decision Matters

Teams that run hybrid or multi-cloud environments expect to move workloads when conditions change. A maintenance window can force the issue, such as with a data center expansion, hardware refresh cycles, consolidation efforts, or a policy decision to shift capacity between environments. In each case, the question is not only whether a workload can move, but whether it can do so without service interruption.

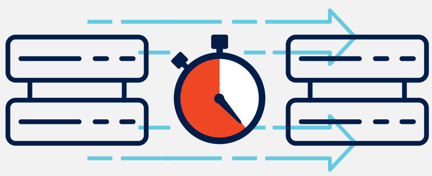
Key Findings



NO DOWNTIME during live migration in a homogeneous processor environment



MINIMAL PERFORMANCE IMPACT for VM migration with Intel® QuickAssist Technology (Intel® QAT) encryption



2 MINUTES 31 SECONDS OF DOWNTIME for a cold migration (with shared storage) in a heterogeneous processor environment

That distinction often drives the real business cost. Live migration lets an IT team move a running VM while the application continues to answer requests. Users stay connected, admins don't need to negotiate the same level of downtime planning, and the work can happen during business hours if policy allows. Cold migration changes that equation. The VM must stop before the move begins, which means the application pauses until the destination host brings it back online.

Even a short outage can create ripple effects. Application owners might need to approve outage windows. Operations staff might need to monitor the move after hours. Support teams might have to prepare for user questions, roll back plans, or make temporary service exceptions. For a single migration, that overhead could look manageable. But across a fleet of business-critical VMs, it can become a material, persistent operational tax.

Architecture consistency plays a direct role here. VMware vSphere® vMotion remains the standard tool for live migration in enterprise VMware environments and depends on compatible processor architecture. VMware EVC extends that support across Intel processor generations with a common CPU feature baseline inside the cluster. That capability protects prior investments because it helps older and newer Intel-based systems work together in the same mobility strategy.

A mixed Intel and AMD environment changes the boundary conditions. AMD documentation has long stated that vMotion isn't supported across vendor architectures.[2] While AMD's Virtual Automated Migration Tool (VAMT) can improve parts of the migration workflow, it still requires the shutdown, service interruption, and downtime of a cold migration.

Test Environment Overview

For this evaluation, we examined migration behavior in a four-server environment that represents a realistic expansion path for a virtualized data center:

- Two current-generation servers powered by Intel Xeon 6767P processors
- One legacy server powered by Intel Xeon Platinum 8380 processors
- One current-generation server powered by AMD EPYC 9555 processors

This mix let us test same-generation Intel migration, cross-generation Intel migration with VMware EVC, and cross-vendor migration from Intel to AMD.

For this testing, we used VMware ESXi™ 9.1 as the hypervisor. The workload ran in a 64 GB VM based on Windows Server® 2025 with Microsoft® SQL Server® 2022 and the DS3.5 benchmark workload. That setup gave us an active application context during migration and let us focus on the user-facing effect of each move, rather than relying solely on migration-task completion status in VMware vCenter®. We tested compute-only migration with shared Network File System (NFS) storage and compute-and-storage migration with host-local DAS; VMware vSAN™ was not used in either scenario. These configurations represent two common approaches to VM storage management.

About VMware® vMotion®

VMware vMotion supports several migration patterns, but two matter most in this comparison. The first is compute-only migration, where the source and destination hosts share access to the VM's storage. In this pattern, only the active compute state moves between hosts. The second is compute-and-storage migration, where vMotion moves both the compute state and the VM files because the hosts do not share storage.

The distinction matters because storage movement changes how long a migration takes and, in a cold migration scenario, how long users wait for the application to return. A compute-only move tends to be the fastest path when shared storage is already in place. A compute-and-storage move reflects a more demanding situation, such as local storage on discrete hosts or staged moves during hardware replacement.

Migration Testing Results

We measured downtime during the following migration scenarios:

- Using VMware vMotion to move an active VM between two current-generation servers powered by Intel Xeon 6767P processors.
- Using VMware vMotion to move an active VM from a legacy server powered by Intel Xeon Platinum 8380 processors to a current-generation server powered by Intel Xeon 6767P processors.
- Using cold migration to move a VM from a server powered by Intel Xeon 6767P processors to a server powered by AMD EPYC 9555 processors.

We also examined the effects of encryption on migration times in follow-on testing, described in the **Encryption in Flight and Intel® QuickAssist Technology (Intel® QAT)** section.

Scenario 1: Current Intel Xeon Processor–Based Server to Current Intel Xeon Processor–Based Server with VMware® EVC

In the first scenario, we migrated an active VM between two current-generation servers powered by Intel Xeon 6767P processors. We tested both compute-only migration and compute-and-storage migration. **In both cases, because the migration was in a homogeneous, Intel-to-Intel environment, the migration remained live. The application running inside the VM stayed available throughout the move with no downtime.**

This result reinforces a familiar but still important point. When an organization expands with servers that share the same processor architecture, it preserves freedom of movement inside the virtualization cluster. Teams can place workloads on the host that makes the most sense at that moment and adjust later without accepting service interruption as a normal part of lifecycle management.

Scenario 2: Legacy Intel Xeon Processor–Based Server to Current Intel Xeon Processor–Based Server with VMware EVC

In the second scenario, we migrated an active VM from a legacy server powered by an Intel Xeon Platinum 8380 processor to a current-generation server powered by an Intel Xeon 6767P processor. We used VMware EVC to normalize processor features across the hosts, and we tested both compute-only migration and compute-and-storage migration.

The VM remained online during both tests with no downtime, which means users wouldn't have seen an outage. Most data centers carry multiple server generations for years. VMware EVC helps bridge that reality by letting organizations add newer Intel-based systems without giving up vMotion across the installed base.

Staying consistent also has practical benefits. It protects current operations while a team rolls in new servers with built-in accelerators like Intel QAT and confidential computing with Intel® Trust Domain Extensions (Intel® TDX), retires older ones, or redistributes workloads across clusters. It also lowers the risk that a refresh project will create two isolated islands of computing with different operational rules.

Scenario 3: Cold Migration from Intel to AMD

In the third scenario, we attempted to move a VM from a current-generation Intel Xeon processor–based server to a server powered by an AMD EPYC 9555 processor. We tested both compute-only migration and compute-and-storage migration. Due to the underlying platform differences, vMotion wasn't an option.

To complete the move, we used a cold-migration workflow. AMD VAMT helped automate the process, but the VM still had to shut down before the transfer:

- In the compute-only test with shared storage, the application experienced 2 minutes 31 seconds of downtime before service resumed.
- In the compute-and-storage test with DAS, downtime increased to 7 minutes 37 seconds.

Table 1 | Downtime during Intel-to-AMD cold migration tests

Storage Configuration	Total Downtime
Shared storage	2 minutes 31 seconds
DAS	7 minutes 37 seconds

Cross-vendor migration breaks the vMotion model. If an organization adds AMD-based servers to an existing Intel-based estate and expects to move VMs between them, the environment effectively splits into two migration domains. Workloads can still move, but they do so under a different ruleset that includes outage planning.

That distinction becomes more important as VM counts rise. A single maintenance event can require multiple migrations, each one with a dependency chain behind it. Application owners might need notification. Change managers might require formal approvals. Teams might have to queue migrations for nights or weekends to reduce user impact. When service levels are tight, some organizations might decide to avoid the move entirely and leave capacity stranded where it sits.

Encryption in Flight and Intel® QuickAssist Technology (Intel® QAT)

Many organizations now require encryption for data in transit, including VM migration traffic. VMware vMotion supports encrypted migration, but encryption can add processing overhead unless supported by hardware acceleration. For that reason, we also tested encryption-focused VM migration in a homogeneous, Intel-to-Intel environment. For this testing, we measured VM migration time between current-generation Intel Xeon processor–based servers under three conditions:

1. Software encryption in flight
2. Intel QAT encryption in flight
3. Migration with no encryption

Note: VMware vMotion encryption was enabled using the “Required” setting for encrypted migration testing. The VMs themselves were not encrypted.

VMware® vMotion® Time Comparison (lower is better)

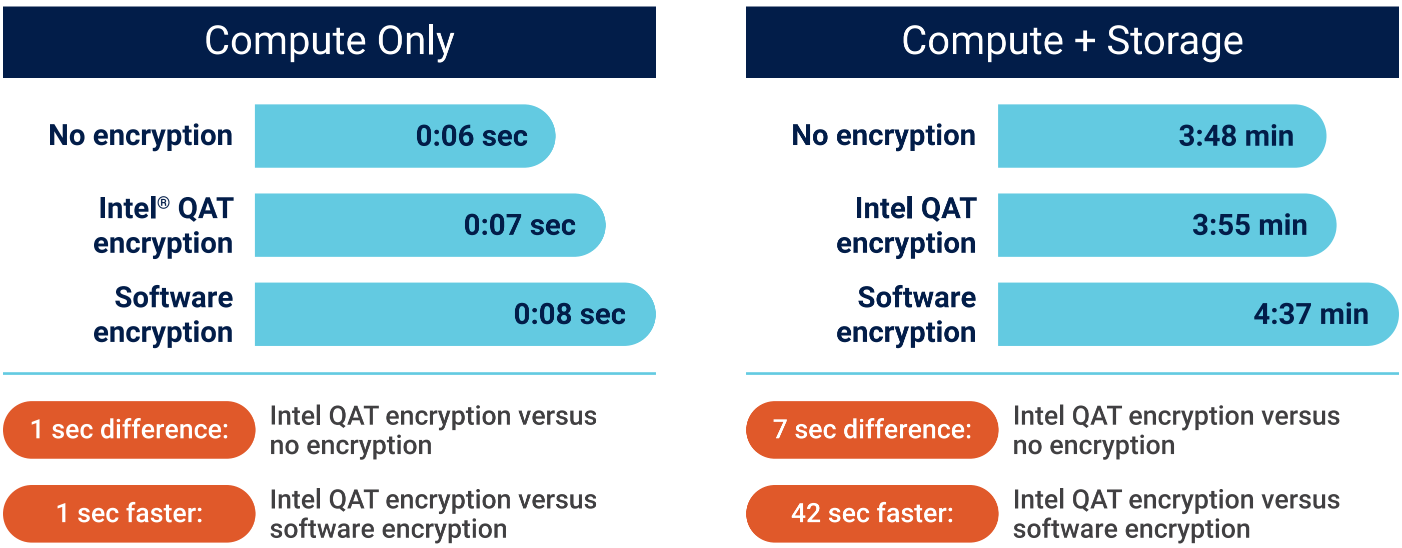


Figure 1 | Intel-to-Intel scenarios tested at varying levels of encryption and with migration times for each

In the compute-only test, encrypted vMotion with software encryption took 8 seconds. With Intel QAT encryption, it took 7 seconds, or 12% less time (see Table 2). Migration with no encryption took 6 seconds. That means the gap between encrypted migration with Intel QAT encryption and migration with no encryption was only 1 second (see Table 3), resulting in a negligible amount of additional time for encrypted migration.

In the compute-and-storage test, encrypted vMotion with software encryption took 4 minutes 37 seconds. With Intel QAT encryption, it took 3 minutes 55 seconds, or 15% less time (see Table 2). Migration with no encryption took 3 minutes 48 seconds. Here, Intel QAT encryption reduced encrypted migration time by 42 seconds versus software encryption, and the remaining gap between migration with Intel QAT encryption and migration with no encryption was 7 seconds (see Table 3).

Table 2 | Comparison of migration times with software encryption versus Intel® QuickAssist Technology (Intel® QAT) encryption for VMware® vMotion®

Scenario	Time with Software Encryption	Time with Intel® QAT Encryption	Time Difference with Intel QAT Encryption
Current-generation Intel-to-Intel (compute only)	0:00:08	0:00:07	1 second
Current-generation Intel-to-Intel (compute and storage)	0:04:37	0:03:55	42 seconds

Table 3 | Comparison of migration times for VMware® vMotion® with Intel® QuickAssist Technology (Intel® QAT) encryption versus with no encryption

Scenario	Time with Intel® QAT Encryption	Time with No Encryption	Time Difference with Intel QAT Encryption
Current-generation Intel-to-Intel (compute only)	0:00:07	0:00:06	1 second
Current-generation Intel-to-Intel (compute and storage)	0:03:55	0:03:48	7 seconds

Security requirements increasingly push organizations toward encrypted vMotion. In many environments, that raises concerns about additional processing overhead and longer migration times. Intel QAT, integrated into Intel Xeon processors, helps address that concern by offloading encryption tasks to dedicated hardware. As a result, organizations can enable encrypted migration with minimal operational impact and at no additional cost while maintaining the mobility benefits that make vMotion valuable in the first place. This approach helps reduce the CPU burden associated with encrypted migration, which allows organizations to enable encrypted vMotion while preserving compute resources for other workloads.

What the Results Mean for Your Organization

The current-Intel-to-current-Intel and legacy-Intel-to-current-Intel scenarios show the mobility advantage of a homogeneous Intel processor architecture. Current-generation Intel Xeon processor–based servers can participate in vMotion with each other, and they can also use vMotion with older Intel platforms when VMware EVC is configured appropriately. That gives organizations a smoother path for capacity growth and hardware refresh, and it keeps routine migration work from turning into a planned outage.

The heterogeneous-architecture scenario shows where that live-migration model breaks. AMD insertion into an Intel estate creates a second migration domain. A mixed Intel and AMD CPU environment does not support vMotion across vendor lines. The extra downtime might look small on paper for a shared-storage move, but it can create planning overhead that far exceeds the clock-time required for the migration itself. Someone has to schedule the change, communicate the interruption, watch for application recovery, and handle the exception path if something drifts off script.

For some organizations, the issue will not be raw migration duration, but the burden of operating two pools of infrastructure with different mobility characteristics. That burden can influence refresh timing, cluster design, and even which workloads teams feel comfortable moving. Once mobility becomes conditional, administrators lose one of the cleanest tools they have for reducing maintenance friction.

The encryption results add a second point of planning guidance. Security requirements don't have to erase the benefits of live migration. In our testing, Intel QAT kept the added time for encrypted migration low, especially in the compute-only case. For teams that need encrypted vMotion as part of a compliance, governance, or zero-trust posture, that support strengthens the argument for a platform design that combines mobility with practical security overhead.

Conclusion

Workload mobility depends on processor architecture. In this test set, live migration remained available between current and legacy Intel processor–based servers, including cross-generation movement enabled by VMware EVC. Moving from Intel to AMD required cold migration, and that requirement introduced measurable downtime in both storage configurations.

For infrastructure teams, the takeaway is straightforward. Homogeneous processor architecture preserves the simplest and least disruptive migration path across the life of the environment. It helps teams maintain service during routine change, and it limits the scheduling and coordination burden that comes with planned outages. This brief also shows that Intel platform capabilities can extend beyond architecture consistency alone. With Intel QAT encryption, encrypted migration stays close to the timing of migration with no encryption, which can help organizations support both workload mobility and security requirements at the same time.

As data centers continue to blend refresh cycles, cloud connections, and stricter security expectations, those details become strategic rather than incidental. A migration plan isn't only about moving a VM from one host to another, it's about deciding how much disruption your operating model will have to absorb every time the business asks IT to change something.

To learn more about Intel QAT, visit the **product page**.

Endnotes

[1] For more information about processors supported by VMware® EVC live migration and about CPU compatibility, see the following references:
- Broadcom. "**Enhanced vMotion Compatibility Requirements for Hosts**." Accessed July 2026.
- Broadcom. "**Enhanced vMotion Compatibility**." Accessed July 2026.
- Broadcom. "**CPU Compatibility and vSphere Enhanced vMotion Compatibility**." Accessed July 2026.
- Broadcom. "**VMware EVC and CPU Compatibility FAQ**." Accessed July 2026.

[2] AMD. "**Virtual Machine (VM) Migration Guide for AMD EPYC™ 9000, 8000, & 7000 Series Processors**." Accessed August 2026.

PROWESS