enclaive

Whitepaper

# Confidential Computing Requirement Guidelines for Data Center and Cloud Service Providers

## Summary

This document describes the technical requirements to set up a confidential computing execution environment on bare metal machines in any of your environments.

# Copyrights

## Acknowledgement

Table of Contents

# 1 Introduction

The rapid expansion of cloud-native workloads, cross-border data flows, and increasingly sophisticated cyber-threats has pushed traditional security architectures to their limits. Data center and cloud service providers are now expected to deliver uncompromising security guarantees, even as infrastructure becomes more distributed, automated, and heterogeneous. In this environment, **Confidential Computing** is emerging as the new industry standard for building, managing, and maintaining compute infrastructure with the highest levels of security and workload isolation.

Confidential Computing introduces a paradigm shift by protecting data not only at rest and in transit—capabilities that have long been standard—but also **during active use**. This third dimension, the encryption of data in use, closes the last major gap in the security model of modern compute platforms. enclaive refers to this unified protection model as **3D Encryption** ("enclaved computation"), ensuring that sensitive data remains cryptographically shielded throughout its full lifecycle.

For the first time, workloads remain encrypted throughout execution in memory, even from privileged system software and infrastructure operators. This capability fundamentally elevates the threat model that data center and cloud providers can defend against. It enables robust protection even in scenarios of infrastructure compromise, malicious insiders, or supply-chain vulnerabilities—risks that traditional methods cannot sufficiently mitigate.

## 1.1 Benefits for Data Center and Cloud Providers

Confidential Computing delivers strategic and operational advantages for hyperscalers, colocation operators, and cloud service providers:

- **Stronger Infrastructure Security Posture**
  Providers can harden their compute stack against insider threats, firmware-level attacks, and hypervisor-level exploits, strengthening trust in multi-tenant environments.
- **Operational Cost Reductions**
  By isolating workloads cryptographically at the hardware level, providers can reduce the tooling, auditing, and manual security processes required to maintain compliance and availability.
- **New High-Assurance Service Offerings**
  Providers can differentiate with confidential VMs, confidential Kubernetes, secure enclaves, and regulated-data hosting services—opening up new revenue streams in sectors like healthcare, finance, and public administration.
- **Simplified Compliance**
  Built-in hardware attestation and verifiable workload isolation ease adherence to regulatory frameworks such as NIS2, C5, BSI Grundschutz, and reduce certification overhead.

## 1.2 Benefits for the Provider's Customers

End customers—ranging from SaaS vendors to enterprises running sensitive workloads—gain equally transformative advantages:

- **Maximal Data Protection Across the Full Lifecycle**
  Workloads remain protected at rest, in transit, and in use, drastically limiting the impact of breaches or infrastructure compromise.

- **Secure Multi-Cloud and Edge Deployments**
  Enclaved computation allows applications to run safely across distributed or untrusted environments without changing application logic.
- **Faster Onboarding of Sensitive Workloads**
  Customers can migrate regulated or business-critical workloads to the cloud faster, backed by verifiable attestation and hardware-rooted trust.
- **Reduced Vendor Lock-In**
  Standardized confidential computing primitives across major hardware vendors and cloud providers allow customers to maintain flexibility in where and how they run workloads.
- **Built-In Compliance and Auditability**
  Cryptographically verifiable execution environments simplify audits and accelerate compliance with frameworks like GDPR, NIS2, HIPAA, and financial-sector regulations.

## 1.3 New Business Opportunities Through Confidential-Computing-Augmented Services

Confidential Computing enables providers to offer entirely new classes of high-assurance, high-margin services that were previously not feasible or not certifiable:

- **Confidential Virtual Machines**
  Provide per-tenant or per-workload runtime encryption with hardware-rooted attestation—now a requirement or strong expectation in regulated sectors.
- **Confidential Kubernetes**
  Deliver end-to-end encrypted container execution, enabling secure multi-tenant cluster designs and zero-trust orchestration.
- **Data-in-Use Encrypted Databases**
  Support high-value customers who must ensure query processing and analytics happen inside attested enclaves.
- **Confidential AI / Confidential Inference**
  Enclaved CPU/GPU execution ensures that training data, models, and inference results remain encrypted throughout the entire AI pipeline. This is particularly valuable for **SMEs**, which increasingly rely on AI but cannot expose business-critical data—such as customer records, financial projections, pricing models, or proprietary algorithms—to third-party operators or shared infrastructure. Confidential AI provides the privacy guarantees SMEs need to adopt advanced analytics and AI without risking data leakage, intellectual-property exposure, or compliance violations.

By offering confidential-computing-augmented services, data center providers position themselves as compliant-by-design infrastructure partners, unlocking access to high-value workloads that were historically prohibited from moving to the cloud.

# 2 Hardware Requirements

## 2.1 Intel CPU

All CPUs with support of Security Guard Extension (SGX). Intel introduced the extension into XEON 1st-4th gen processors (release: July 2017; code name: Skylake).

All Intel CPUs with support of Trusted Domain Extension (TDX). Intel introduced the extension into XEON 5th gen processors (release: December 14, 2023; code name: emeralds rapids) and XEON 6th gen processors (release: June 14, 2024; code name: sierra forest and granite rapids).

Please check on this site or Intel homepage.

> **Hint**
>
> A quick check is to look at the 2nd digit in the CPU encoding xXxx ($X \geq 5$: TDX, $X < 5$ SGX). Intel TDX CPUs include support for SGX. TDX remote integrity protection is based on the Intel DCAP framework build upon SGX.

> **Important Note**
>
> Intel CPUs require at least 8 memory DIMMs. This is needed, as TDX requires that the Integrated Memory Controller (IMC) has all his slots populated.

| Intel (5th gen) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Name** | **Codename** | **Cores** | **Clock** | **Socket** | **Process** | **L3 Cache** | **TDP** | **Released** |
| Xeon Bronze 3508U | Emerald Rapids | 8 (8) | 2.1 to 2.2 GHz | Socket 4677 | Intel 7 | 22.5 MB | 125 W | Q4'23 |
| Xeon Silver 4509Y | Emerald Rapids | 8 (16) | 2.6 to 4.1 GHz | Socket 4677 | Intel 7 | 22.5 MB | 125 W | Q4'23 |
| Xeon Silver 4510 | Emerald Rapids | 12 (24) | 2.4 to 4.1 GHz | Socket 4677 | Intel 7 | 30 MB | 150 W | Q4'23 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon Silver 4510T | Emerald Rapids | 12 (24) | 2 to 3.7 GHz | Socket 4677 | Intel 7 | 30 MB | 115 W | Q4'23 |
| Xeon Silver 4514Y | Emerald Rapids | 16 (32) | 2 to 3.4 GHz | Socket 4677 | Intel 7 | 30 MB | 150 W | Q4'23 |
| Xeon Silver 4516Y+ | Emerald Rapids | 24 (48) | 2.2 to 3.7 GHz | Socket 4677 | Intel 7 | 45 MB | 185 W | Q4'23 |
| Xeon Gold 5512U | Emerald Rapids | 28 (56) | 2.1 to 3.7 GHz | Socket 4677 | Intel 7 | 52.5 MB | 185 W | Q4'23 |
| Xeon Gold 5515+ | Emerald Rapids | 8 (16) | 3.2 to 4.1 GHz | Socket 4677 | Intel 7 | 22.5 MB | 165 W | Q4'23 |
| Xeon Gold 5520+ | Emerald Rapids | 28 (56) | 2.2 to 4 GHz | Socket 4677 | Intel 7 | 52.5 MB | 205 W | Q4'23 |
| Xeon Gold 6526Y | Emerald Rapids | 16 (32) | 2.8 to 3.9 GHz | Socket 4677 | Intel 7 | 37.5 MB | 195 W | Q4'23 |
| Xeon Gold 6530 | Emerald Rapids | 32 (64) | 2.1 to 4 GHz | Socket 4677 | Intel 7 | 160 MB | 270 W | Q4'23 |
| Xeon Gold 6534 | Emerald Rapids | 8 (16) | 3.9 to 4.2 GHz | Socket 4677 | Intel 7 | 22.5 MB | 195 W | Q4'23 |
| Xeon Gold 6538N | Emerald Rapids | 32 (64) | 2.1 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 205 W | Q4'23 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon Gold 6538Y+ | Emerald Rapids | 32 (64) | 2.2 to 4 GHz | Socket 4677 | Intel 7 | 60 MB | 225 W | Q4'23 |
| Xeon Gold 6542Y | Emerald Rapids | 24 (48) | 2.9 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 250 W | Q4'23 |
| Xeon Gold 6544Y | Emerald Rapids | 16 (32) | 3.6 to 4.1 GHz | Socket 4677 | Intel 7 | 45 MB | 270 W | Q4'23 |
| Xeon Gold 6548N | Emerald Rapids | 32 (64) | 2.8 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 250 W | Q4'23 |
| Xeon Gold 6548Y+ | Emerald Rapids | 32 (64) | 2.5 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 250 W | Q4'23 |
| Xeon Gold 6554S | Emerald Rapids | 36 (72) | 2.2 to 4 GHz | Socket 4677 | Intel 7 | 180 MB | 270 W | Q4'23 |
| Xeon Gold 6558Q | Emerald Rapids | 32 (64) | 3.2 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 350 W | Q4'23 |
| Xeon Platinum 8558 | Emerald Rapids | 48 (96) | 2.1 to 4 GHz | Socket 4677 | Intel 7 | 260 MB | 330 W | Q4'23 |
| Xeon Platinum 8558P | Emerald Rapids | 48 (96) | 2.7 to 4 GHz | Socket 4677 | Intel 7 | 260 MB | 350 W | Q4'23 |
| Xeon Platinum 8558U | Emerald Rapids | 48 (96) | 2 to 4 GHz | Socket 4677 | Intel 7 | 260 MB | 300 W | Q4'23 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon Platinum 8562Y+ | Emerald Rapids | 32 (64) | 2.8 to 4.1 GHz | Socket 4677 | Intel 7 | 60 MB | 300 W | Q4'23 |
| Xeon Platinum 8568Y+ | Emerald Rapids | 48 (96) | 2.3 to 4 GHz | Socket 4677 | Intel 7 | 300 MB | 350 W | Q4'23 |
| Xeon Platinum 8570 | Emerald Rapids | 56 (112) | 2.1 to 4 GHz | Socket 4677 | Intel 7 | 300 MB | 350 W | Q4'23 |
| Xeon Platinum 8571N | Emerald Rapids | 52 (104) | 2.4 to 4 GHz | Socket 4677 | Intel 7 | 300 MB | 300 W | Q4'23 |
| Xeon Platinum 8580 | Emerald Rapids | 60 (120) | 2 to 4 GHz | Socket 4677 | Intel 7 | 300 MB | 350 W | Q4'23 |
| Xeon Platinum 8581V | Emerald Rapids | 60 (120) | 2 to 3.9 GHz | Socket 4677 | Intel 7 | 300 MB | 270 W | Q4'23 |
| Xeon Platinum 8592+ | Emerald Rapids | 64 (128) | 1.9 to 3.9 GHz | Socket 4677 | Intel 7 | 320 MB | 350 W | Q4'23 |
| Xeon Platinum 8592V | Emerald Rapids | 64 (128) | 2 to 3.9 GHz | Socket 4677 | Intel 7 | 320 MB | 330 W | Q4'23 |
| Xeon Platinum 8593Q | Emerald Rapids | 64 (128) | 2.2 to 3.9 GHz | Socket 4677 | Intel 7 | 320 MB | 385 W | Q4'23 |

| Intel (6th gen) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Name** | **Codename** | **Cores** | **Clock** | **Socket** | **Process** | **L3 Cache** | **TDP** | **Released** |
| Xeon 6740E | Sierra Forest | 96 (96) | 2.4 to 3.2 GHz | Socket 4710 | 3 | 96.0 MB | 250.0 W | Q2'24 |
| Xeon 6756E | Sierra Forest | 128 (128) | 1.8 to 2.6 GHz | Socket 4710 | 3 | 96.0 MB | 225.0 W | Q2'24 |
| Xeon 6780E | Sierra Forest | 144 (144) | 2.2 to 3 GHz | Socket 4710 | 3 | 108.0 MB | 330.0 W | Q2'24 |
| Xeon 6710E | Sierra Forest | 64 (64) | 2.4 to 3.2 GHz | Socket 4710 | 3 | 96.0 MB | 205.0 W | Q2'24 |
| Xeon 6766E | Sierra Forest | 144 (144) | 1.9 to 2.7 GHz | Socket 4710 | 3 | 108.0 MB | 250.0 W | Q2'24 |
| Xeon 6731E | Sierra Forest | 96 (96) | 2.2 to 3.1 GHz | Socket 4710 | 3 | 96.0 MB | 250.0 W | Q2'24 |
| Xeon 6746E | Sierra Forest | 112 (112) | 2 to 2.7 GHz | Socket 4710 | 3 | 96.0 MB | 250.0 W | Q2'24 |
| Xeon 6960P | Granite Rapids | 72 (144) | 2.7 to 3.9 GHz | Socket 7529 | 3 | 432.0 MB | 500.0 W | Q3'24 |
| Xeon 6980P | Granite Rapids | 128 (256) | 2 to 3.9 GHz | Socket 7529 | 3 | 504.0 MB | 500.0 W | Q3'24 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6979P | Granite Rapids | 120 (240) | 2.1 to 3.9 GHz | Socket 7529 | 3 | 504.0 MB | 500.0 W | Q3'24 |
| Xeon 6966P-C | Granite Rapids | 96 (192) | 3.1 to 3.9 GHz | Socket 7529 | 3 | 432.0 MB | 550.0 W | Q2'25 |
| Xeon 6972P | Granite Rapids | 96 (192) | 2.4 to 3.9 GHz | Socket 7529 | 3 | 480.0 MB | 500.0 W | Q3'24 |
| Xeon 6357P | Granite Rapids | 8 (16) | 3 to 5.4 GHz | Socket 1700 | 3 | 24.0 MB | 80.0 W | Q1'25 |
| Xeon 6952P | Granite Rapids | 96 (192) | 2.1 to 3.9 GHz | Socket 7529 | 3 | 480.0 MB | 400.0 W | Q3'24 |
| Xeon 6747P | Granite Rapids | 48 (96) | 2.7 to 3.9 GHz | Socket 4710 | 3 | 288.0 MB | 330.0 W | Q1'25 |
| Xeon 6741P | Granite Rapids | 48 (96) | 2.5 to 3.8 GHz | Socket 4710 | 3 | 288.0 MB | 300.0 W | Q1'25 |
| Xeon 6730P | Granite Rapids | 32 (64) | 2.5 to 3.8 GHz | Socket 4710 | 3 | 288.0 MB | 250.0 W | Q1'25 |
| Xeon 6781P | Granite Rapids | 80 (160) | 2 to 3.8 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q1'25 |
| Xeon 6760P | Granite Rapids | 64 (128) | 2.2 to 3.8 GHz | Socket 4710 | 3 | 320.0 MB | 330.0 W | Q1'25 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6788P | Granite Rapids | 86 (172) | 2 to 3.8 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q1'25 |
| Xeon 6740P | Granite Rapids | 48 (96) | 2.1 to 3.8 GHz | Socket 4710 | 3 | 288.0 MB | 270.0 W | Q1'25 |
| Xeon 6768P | Granite Rapids | 64 (128) | 2.4 to 3.9 GHz | Socket 4710 | 3 | 336.0 MB | 330.0 W | Q1'25 |
| Xeon 6761P | Granite Rapids | 64 (128) | 2.5 to 3.9 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q1'25 |
| Xeon 6787P | Granite Rapids | 86 (172) | 2 to 3.8 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q1'25 |
| Xeon 6767P | Granite Rapids | 64 (128) | 2.4 to 3.9 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q1'25 |
| Xeon 6737P | Granite Rapids | 32 (64) | 2.9 to 4 GHz | Socket 4710 | 3 | 144.0 MB | 270.0 W | Q1'25 |
| Xeon 6738P | Granite Rapids | 32 (64) | 2.9 to 4.2 GHz | Socket 4710 | 3 | 144.0 MB | 270.0 W | Q1'25 |
| Xeon 6521P | Granite Rapids | 24 (48) | 2.6 to 4.1 GHz | Socket 4710 | 3 | 144.0 MB | 225.0 W | Q1'25 |
| Xeon 6731P | Granite Rapids | 32 (64) | 2.5 to 4.1 GHz | Socket 4710 | 3 | 144.0 MB | 245.0 W | Q1'25 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6530P | Granite Rapids | 32 (64) | 2.3 to 4.1 GHz | Socket 4710 | 3 | 144.0 MB | 225.0 W | Q1'25 |
| Xeon 6748P | Granite Rapids | 48 (96) | 2.5 to 4.1 GHz | Socket 4710 | 3 | 192.0 MB | 300.0 W | Q1'25 |
| Xeon 6736P | Granite Rapids | 36 (72) | 2 to 4.1 GHz | Socket 4710 | 3 | 144.0 MB | 205.0 W | Q1'25 |
| Xeon 6520P | Granite Rapids | 24 (48) | 2.4 to 4 GHz | Socket 4710 | 3 | 144.0 MB | 210.0 W | Q1'25 |
| Xeon 6732P | Granite Rapids | 32 (64) | 3.8 to 4.3 GHz | Socket 4710 | 3 | 144.0 MB | 350.0 W | Q2'25 |
| Xeon 6527P | Granite Rapids | 24 (48) | 3 to 4.2 GHz | Socket 4710 | 3 | 144.0 MB | 255.0 W | Q1'25 |
| Xeon 6728P | Granite Rapids | 24 (48) | 2.7 to 4.1 GHz | Socket 4710 | 3 | 144.0 MB | 210.0 W | Q1'25 |
| Xeon 6517P | Granite Rapids | 16 (32) | 3.2 to 4.2 GHz | Socket 4710 | 3 | 72.0 MB | 190.0 W | Q1'25 |
| Xeon 6511P | Granite Rapids | 16 (32) | 2.3 to 4.2 GHz | Socket 4710 | 3 | 72.0 MB | 150.0 W | Q1'25 |
| Xeon 6505P | Granite Rapids | 12 (24) | 2.2 to 4.1 GHz | Socket 4710 | 3 | 48.0 MB | 150.0 W | Q1'25 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6507P | Granite Rapids | 8 (16) | 3.5 to 4.3 GHz | Socket 4710 | 3 | 48.0 MB | 150.0 W | Q1'25 |
| Xeon 6515P | Granite Rapids | 16 (32) | 2.3 to 3.8 GHz | Socket 4710 | 3 | 72.0 MB | 150.0 W | Q1'25 |
| Xeon 6724P | Granite Rapids | 16 (32) | 3.6 to 4.3 GHz | Socket 4710 | 3 | 72.0 MB | 210.0 W | Q1'25 |
| Xeon 6714P | Granite Rapids | 8 (16) | 4 to 4.3 GHz | Socket 4710 | 3 | 48.0 MB | 165.0 W | Q1'25 |
| Xeon 6944P | Granite Rapids | 72 (144) | 1.8 to 3.9 GHz | Socket 7529 | 3 | 432.0 MB | 350.0 W | Q1'25 |
| Xeon 6726P-B | Granite Rapids | 42 (84) | 2.3 to 3.5 GHz | Socket 4368 | 3 | 168.0 MB | 235.0 W | Q1'25 |
| Xeon 6503P-B | Granite Rapids | 12 (24) | 2 to 3.5 GHz | Socket 4368 | 3 | 48.0 MB | 110.0 W | Q1'25 |
| Xeon 6516P-B | Granite Rapids | 20 (40) | 2.3 to 3.5 GHz | Socket 4368 | 3 | 80.0 MB | 145.0 W | Q1'25 |
| Xeon 6533P-B | Granite Rapids | 32 (64) | 2.2 to 3.9 GHz | Socket 4368 | 3 | 128.0 MB | 205.0 W | Q1'25 |
| Xeon 6523P-B | Granite Rapids | 24 (48) | 2.5 to 3.9 GHz | Socket 4368 | 3 | 96.0 MB | 175.0 W | Q1'25 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6546P-B | Granite Rapids | 32 (64) | 2.3 to 3.5 GHz | Socket 4368 | 3 | 128.0 MB | 195.0 W | Q1'25 |
| Xeon 6543P-B | Granite Rapids | 32 (64) | 2 to 3.3 GHz | Socket 4368 | 3 | 128.0 MB | 160.0 W | Q1'25 |
| Xeon 6553P-B | Granite Rapids | 36 (72) | 2.6 to 4 GHz | Socket 4368 | 3 | 144.0 MB | 235.0 W | Q1'25 |
| Xeon 6706P-B | Granite Rapids | 40 (80) | 2.5 to 3.5 GHz | Socket 4368 | 3 | 160.0 MB | 235.0 W | Q1'25 |
| Xeon 6563P-B | Granite Rapids | 38 (76) | 2.4 to 4 GHz | Socket 4368 | 3 | 152.0 MB | 235.0 W | Q1'25 |
| Xeon 6556P-B | Granite Rapids | 36 (72) | 2.3 to 3.5 GHz | Socket 4368 | 3 | 144.0 MB | 215.0 W | Q1'25 |
| Xeon 6716P-B | Granite Rapids | 40 (80) | 2.5 to 3.5 GHz | Socket 4368 | 3 | 160.0 MB | 235.0 W | Q2'25 |
| Xeon 6513P-B | Granite Rapids | 20 (40) | 2 to 3.3 GHz | Socket 4368 | 3 | 80.0 MB | 130.0 W | Q1'25 |
| Xeon 6745P | Granite Rapids | 32 (64) | 3.1 to 4.3 GHz | Socket 4710 | 3 | 336.0 MB | 300.0 W | Q1'25 |
| Xeon 6776P | Granite Rapids | 64 (128) | 2.3 to 3.9 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q2'25 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| Xeon 6774P | Granite Rapids | 64 (128) | 2.5 to 3.9 GHz | Socket 4710 | 3 | 336.0 MB | 350.0 W | Q2'25 |
| Xeon 6532P-B | Granite Rapids | 32 (64) | 2.2 to 3.9 GHz | Socket 4368 | 3 | 128.0 MB | 205.0 W | Q3'25 |
| Xeon 6962P | Granite Rapids | 72 (144) | 2.7 to 3.9 GHz | Socket 7529 | 3 | 432.0 MB | 500.0 W | Q3'25 |
| Xeon 6978P | Granite Rapids | 120 (240) | 2.1 to 3.9 GHz | Socket 7529 | 3 | 504.0 MB | 500.0 W | Q3'25 |
| Xeon 6725P | Granite Rapids | 16 (32) | 3.7 to 4.8 GHz | Socket 4710 | 3 | 192.0 MB | 235.0 W | Q3'25 |
| Xeon 6776P-B | Granite Rapids | 72 (144) | 2.3 to 3.5 GHz |  | 3 | 288.0 MB | 325.0 W | Q4'25 |
| Xeon 6766P-B | Granite Rapids | 64 (128) | 2.3 to 3.5 GHz |  | 3 | 256.0 MB | 305.0 W | Q4'25 |
| Xeon 6756P-B | Granite Rapids | 64 (128) | 2.2 to 3.5 GHz |  | 3 | 256.0 MB | 325.0 W | Q4'25 |
| Xeon 6762P | Granite Rapids | 64 (128) | 2.9 to 3.9 GHz | Socket 4710 | 3 | 320.0 MB | 350.0 W | Q3'25 |
| Xeon 6768P-B | Granite Rapids | 64 (128) | 2.2 to 3.5 GHz |  | 3 | 256.0 MB | 325.0 W | Q4'25 |

## 2.2 AMD CPU

All AMD CPUs with support of Secure Encrypted Virtualization (SEV). AMD introduced the extension into EPYC processors. While SEV is generally available from EPYC 1st gen, we recommend our clients the 4th gen (release: May 16, 2023; codename: Genoa) or later, the 3rd gen (release: March 15, 2021; codename: Rome), and the 2nd gen (release: August 7, 2019, codename: Rome).

Please check on this site, if your CPU supports SEV.

> **Hint**
>
> A quick check is to look at the 4th digit in the CPU encoding xxxX (X ≥ 2). AMD CPUs with a 4 at the first digit Xxxx generally do not support SEV even though the 4th digit encoding might hint at it.

| AMD (5th gen) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Name** | **Codename** | **Cores** | **Clock** | **Socket** | **Process** | **L3 Cache** | **TDP** | **Released** |
| EPYC 9015 | Turin | 8 / 16 | 3.6 to 4.1 GHz | Socket SP5 | 4 nm | 64 MB | 125 W | Oct 2024 |
| EPYC 9115 | Turin | 16 / 32 | 2.6 to 4.1 GHz | Socket SP5 | 4 nm | 64 MB | 125 W | Oct 2024 |
| EPYC 9135 | Turin | 16 / 32 | 3.65 to 4.3 GHz | Socket SP5 | 4 nm | 64 MB | 200 W | Oct 2024 |
| EPYC 9175F | Turin | 16 / 32 | 4.2 to 5 GHz | Socket SP5 | 4 nm | 512 MB | 320 W | Oct 2024 |
| EPYC 9255 | Turin | 24 / 48 | 3.25 to 4.8 GHz | Socket SP5 | 4 nm | 128 MB | 200 W | Oct 2024 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 9275F | Turin | 24 / 48 | 4.1 to 4.8 GHz | Socket SP5 | 4 nm | 256 MB | 320 W | Oct 2024 |
| EPYC 9335 | Turin | 32 / 64 | 3 to 4.4 GHz | Socket SP5 | 4 nm | 128 MB | 210 W | Oct 2024 |
| EPYC 9355 | Turin | 32 / 64 | 3.55 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 280 W | Oct 2024 |
| EPYC 9355P | Turin | 32 / 64 | 3.55 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 280 W | Oct 2024 |
| EPYC 9365 | Turin | 36 / 72 | 3.4 to 4.3 GHz | Socket SP5 | 4 nm | 192 MB | 300 W | Oct 2024 |
| EPYC 9375F | Turin | 32 / 64 | 3.85 to 4.8 GHz | Socket SP5 | 4 nm | 256 MB | 320 W | Oct 2024 |
| EPYC 9455 | Turin | 48 / 96 | 3.15 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 300 W | Oct 2024 |
| EPYC 9455P | Turin | 48 / 96 | 3.15 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 300 W | Oct 2024 |
| EPYC 9475F | Turin | 48 / 96 | 3.65 to 4.8 GHz | Socket SP5 | 4 nm | 256 MB | 400 W | Oct 2024 |
| EPYC 9535 | Turin | 64 / 128 | 2.4 to 4.3 GHz | Socket SP5 | 4 nm | 256 MB | 300 W | Oct 2024 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 9555 | Turin | 64 / 128 | 3.2 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 360 W | Oct 2024 |
| EPYC 9555P | Turin | 64 / 128 | 3.2 to 4.4 GHz | Socket SP5 | 4 nm | 256 MB | 360 W | Oct 2024 |
| EPYC 9565 | Turin | 72 / 144 | 3.15 to 4.3 GHz | Socket SP5 | 4 nm | 384 MB | 400 W | Oct 2024 |
| EPYC 9575F | Turin | 64 / 128 | 3.3 to 5 GHz | Socket SP5 | 4 nm | 256 MB | 400 W | Oct 2024 |
| EPYC 9645 | Turin | 96 / 192 | 2.3 to 3.7 GHz | Socket SP5 | 3 nm | 256 MB | 320 W | Oct 2024 |
| EPYC 9655 | Turin | 96 / 192 | 2.6 to 4.5 GHz | Socket SP5 | 4 nm | 384 MB | 400 W | Oct 2024 |
| EPYC 9655P | Turin | 96 / 192 | 2.6 to 4.5 GHz | Socket SP5 | 4 nm | 384 MB | 400 W | Oct 2024 |
| EPYC 9745 | Turin | 128 / 256 | 2.4 to 3.7 GHz | Socket SP5 | 3 nm | 256 MB | 400 W | Oct 2024 |
| EPYC 9755 | Turin | 128 / 256 | 2.7 to 4.1 GHz | Socket SP5 | 4 nm | 512 MB | 500 W | Oct 2024 |
| EPYC 9825 | Turin | 144 / 288 | 2.2 to 3.7 GHz | Socket SP5 | 3 nm | 384 MB | 390 W | Oct 2024 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 9845 | Turin | 160 / 320 | 2.1 to 3.7 GHz | Socket SP5 | 3 nm | 320 MB | 390 W | Oct 2024 |
| EPYC 9965 | Turin | 192 / 384 | 2.25 to 3.7 GHz | Socket SP5 | 3 nm | 384 MB | 500 W | Oct 2024 |

| AMD (4th gen) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Name** | **Codename** | **Cores** | **Clock** | **Socket** | **Process** | **L3 Cache** | **TDP** | **Released** |
| EPYC 9124 | Genoa | 16 / 32 | 3 to 3.7 GHz | Socket SP5 | 5 nm | 64 MB | 200 W | Nov 10th, 2022 |
| EPYC 9174F | Genoa | 16 / 32 | 4.1 to 4.4 GHz | Socket SP5 | 5 nm | 256 MB | 320 W | Nov 10th, 2022 |
| EPYC 9224 | Genoa | 24 / 48 | 2.5 to 3.7 GHz | Socket SP5 | 5 nm | 64 MB | 200 W | Nov 10th, 2022 |
| EPYC 9254 | Genoa | 24 / 48 | 2.9 to 4.15 GHz | Socket SP5 | 5 nm | 128 MB | 200 W | Nov 10th, 2022 |
| EPYC 9274F | Genoa | 24 / 48 | 4.05 to 4.3 GHz | Socket SP5 | 5 nm | 256 MB | 320 W | Nov 10th, 2022 |
| EPYC 9334 | Genoa | 32 / 64 | 2.7 to 3.9 GHz | Socket SP5 | 5 nm | 128 MB | 210 W | Nov 10th, 2022 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 9354 | Genoa | 32 / 64 | 3.25 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 280 W | Nov 10th, 2022 |
| EPYC 9354P | Genoa | 32 / 64 | 3.25 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 280 W | Nov 10th, 2022 |
| EPYC 9374F | Genoa | 32 / 64 | 3.85 to 4.3 GHz | Socket SP5 | 5 nm | 256 MB | 320 W | Nov 10th, 2022 |
| EPYC 9454 | Genoa | 48 / 96 | 2.75 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 290 W | Nov 10th, 2022 |
| EPYC 9454P | Genoa | 48 / 96 | 2.75 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 290 W | Nov 10th, 2022 |
| EPYC 9474F | Genoa | 48 / 96 | 3.6 to 4.1 GHz | Socket SP5 | 5 nm | 256 MB | 360 W | Nov 10th, 2022 |
| EPYC 9534 | Genoa | 64 / 128 | 2.45 to 3.7 GHz | Socket SP5 | 5 nm | 256 MB | 280 W | Nov 10th, 2022 |
| EPYC 9554 | Genoa | 64 / 128 | 3.1 to 3.75 GHz | Socket SP5 | 5 nm | 256 MB | 360 W | Nov 10th, 2022 |
| EPYC 9554P | Genoa | 64 / 128 | 3.1 to 3.75 GHz | Socket SP5 | 5 nm | 256 MB | 360 W | Nov 10th, 2022 |
| EPYC 9634 | Genoa | 84 / 168 | 2.25 to 3.7 GHz | Socket SP5 | 5 nm | 384 MB | 290 W | Nov 10th, 2022 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 9654 | Genoa | 96 / 192 | 2.4 to 3.7 GHz | Socket SP5 | 5 nm | 384 MB | 360 W | Nov 10th, 2022 |
| EPYC 9654P | Genoa | 96 / 192 | 2.4 to 3.7 GHz | Socket SP5 | 5 nm | 384 MB | 360 W | Nov 10th, 2022 |
| EPYC Embedded 9124 | Genoa | 16 / 32 | 3 to 3.7 GHz | Socket SP5 | 5 nm | 64 MB | 200 W | Mar 14th, 2023 |
| EPYC Embedded 9254 | Genoa | 24 / 48 | 2.9 to 4.15 GHz | Socket SP5 | 5 nm | 128 MB | 200 W | Mar 14th, 2023 |
| EPYC Embedded 9354 | Genoa | 32 / 64 | 3.25 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 280 W | Mar 14th, 2023 |
| EPYC Embedded 9354P | Genoa | 32 / 64 | 3.25 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 280 W | Mar 14th, 2023 |
| EPYC Embedded 9454 | Genoa | 48 / 96 | 2.75 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 290 W | Mar 14th, 2023 |
| EPYC Embedded 9454P | Genoa | 48 / 96 | 2.75 to 3.8 GHz | Socket SP5 | 5 nm | 256 MB | 290 W | Mar 14th, 2023 |
| EPYC Embedded 9554 | Genoa | 64 / 128 | 3.1 to 3.75 GHz | Socket SP5 | 5 nm | 256 MB | 360 W | Mar 14th, 2023 |
| EPYC Embedded 9554P | Genoa | 64 / 128 | 3.1 to 3.75 GHz | Socket SP5 | 5 nm | 256 MB | 360 W | Mar 14th, 2023 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC Embedded 9654 | Genoa | 96 / 192 | 2.4 to 3.7 GHz | Socket SP5 | 5 nm | 384 MB | 360 W | Mar 14th, 2023 |
| EPYC Embedded 9654P | Genoa | 96 / 192 | 2.4 to 3.7 GHz | Socket SP5 | 5 nm | 384 MB | 360 W | Mar 14th, 2023 |

## AMD (3rd gen)

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 7203 | Milan | 8 / 16 | 2.8 to 3.4 GHz | Socket SP3 | 7 nm | 64 MB | 120 W | Sep 5th, 2023 |
| EPYC 7203P | Milan | 8 / 16 | 2.8 to 3.4 GHz | Socket SP3 | 7 nm | 64 MB | 120 W | Sep 5th, 2023 |
| EPYC 72F3 | Milan | 8 / 16 | 3.7 to 4.1 GHz | Socket SP3 | 7 nm | 256 MB | 180 W | Mar 15th, 2021 |
| EPYC 7303 | Milan | 16 / 32 | 2.4 to 3.4 GHz | Socket SP3 | 7 nm | 64 MB | 130 W | Sep 5th, 2023 |
| EPYC 7303P | Milan | 16 / 32 | 2.4 to 3.4 GHz | Socket SP3 | 7 nm | 64 MB | 130 W | Sep 5th, 2023 |
| EPYC 7313 | Milan | 16 / 32 | 3 to 3.7 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Mar 15th, 2021 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 7313P | Milan | 16 / 32 | 3 to 3.7 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Mar 15th, 2021 |
| EPYC 7343 | Milan | 16 / 32 | 3.2 to 3.9 GHz | Socket SP3 | 7 nm | 128 MB | 190 W | Mar 15th, 2021 |
| EPYC 73F3 | Milan | 16 / 32 | 3.5 to 4 GHz | Socket SP3 | 7 nm | 256 MB | 240 W | Mar 15th, 2021 |
| EPYC 7413 | Milan | 24 / 48 | 2.65 to 3.6 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Mar 15th, 2021 |
| EPYC 7443 | Milan | 24 / 48 | 2.85 to 4 GHz | Socket SP3 | 7 nm | 128 MB | 200 W | Mar 15th, 2021 |
| EPYC 7443P | Milan | 24 / 48 | 2.85 to 4 GHz | Socket SP3 | 7 nm | 128 MB | 200 W | Mar 15th, 2021 |
| EPYC 7453 | Milan | 28 / 56 | 2.75 to 3.45 GHz | Socket SP3 | 7 nm | 64 MB | 225 W | Mar 15th, 2021 |
| EPYC 74F3 | Milan | 24 / 48 | 2.8 to 4 GHz | Socket SP3 | 7 nm | 256 MB | 240 W | Mar 15th, 2021 |
| EPYC 7513 | Milan | 32 / 64 | 2.6 to 3.65 GHz | Socket SP3 | 7 nm | 128 MB | 200 W | Mar 15th, 2021 |
| EPYC 7543 | Milan | 32 / 64 | 2.8 to 3.7 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Mar 15th, 2021 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 7543P | Milan | 32 / 64 | 2.8 to 3.7 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Mar 15th, 2021 |
| EPYC 75F3 | Milan | 32 / 64 | 2.95 to 4 GHz | Socket SP3 | 7 nm | 256 MB | 280 W | Mar 15th, 2021 |
| EPYC 7643 | Milan | 48 / 96 | 2.3 to 3.6 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Mar 15th, 2021 |
| EPYC 7643P | Milan | 48 / 96 | 2.3 to 3.6 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Sep 5th, 2023 |
| EPYC 7663 | Milan | 56 / 112 | 2 to 3.5 GHz | Socket SP3 | 7 nm | 256 MB | 240 W | Mar 15th, 2021 |
| EPYC 7663P | Milan | 56 / 112 | 2 to 3.5 GHz | Socket SP3 | 7 nm | 256 MB | 240 W | Sep 5th, 2023 |
| EPYC 7713 | Milan | 64 / 128 | 2 to 3.675 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Mar 15th, 2021 |
| EPYC 7713P | Milan | 64 / 128 | 2 to 3.675 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Mar 15th, 2021 |
| EPYC 7763 | Milan | 64 / 128 | 2.45 to 3.5 GHz | Socket SP3 | 7 nm | 256 MB | 280 W | Mar 15th, 2021 |

| AMD (2nd gen) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Name** | **Codename** | **Cores** | **Clock** | **Socket** | **Process** | **L3 Cache** | **TDP** | **Released** |
| EPYC 7232P | Rome | 8 / 16 | 3.1 to 3.2 GHz | Socket SP3 | 7 nm | 32 MB | 120 W | Aug 7th, 2019 |
| EPYC 7252 | Rome | 8 / 16 | 2.8 to 3.2 GHz | Socket SP3 | 7 nm | 64 MB | 120 W | Aug 7th, 2019 |
| EPYC 7262 | Rome | 8 / 16 | 3.1 to 3.3 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Aug 7th, 2019 |
| EPYC 7272 | Rome | 12 / 24 | 2.6 to 3.2 GHz | Socket SP3 | 7 nm | 64 MB | 120 W | Aug 7th, 2019 |
| EPYC 7282 | Rome | 16 / 32 | 2.8 to 3.2 GHz | Socket SP3 | 7 nm | 64 MB | 120 W | Aug 7th, 2019 |
| EPYC 7302 | Rome | 16 / 32 | 3 to 3.3 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Aug 7th, 2019 |
| EPYC 7302P | Rome | 16 / 32 | 3 to 3.3 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Aug 7th, 2019 |
| EPYC 7352 | Rome | 24 / 48 | 2.4 to 3.3 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Aug 7th, 2019 |
| EPYC 7402 | Rome | 24 / 48 | 2.8 to 3.35 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Aug 7th, 2019 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 7402P | Rome | 24 / 48 | 2.8 to 3.35 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Aug 7th, 2019 |
| EPYC 7452 | Rome | 32 / 64 | 2.2 to 3.35 GHz | Socket SP3 | 7 nm | 128 MB | 155 W | Aug 7th, 2019 |
| EPYC 7502 | Rome | 32 / 64 | 2.5 to 3.35 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Aug 7th, 2019 |
| EPYC 7502P | Rome | 32 / 64 | 2.5 to 3.35 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Aug 7th, 2019 |
| EPYC 7542 | Rome | 32 / 64 | 2.9 to 3.4 GHz | Socket SP3 | 7 nm | 128 MB | 225 W | Aug 7th, 2019 |
| EPYC 7552 | Rome | 48 / 96 | 2.2 to 3.35 GHz | Socket SP3 | 7 nm | 192 MB | 200 W | Aug 7th, 2019 |
| EPYC 7642 | Rome | 48 / 96 | 2.4 to 3.4 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Aug 7th, 2019 |
| EPYC 7702 | Rome | 64 / 128 | 2 to 3.35 GHz | Socket SP3 | 7 nm | 256 MB | 200 W | Aug 7th, 2019 |
| EPYC 7702P | Rome | 64 / 128 | 2 to 3.35 GHz | Socket SP3 | 7 nm | 256 MB | 200 W | Aug 7th, 2019 |
| EPYC 7742 | Rome | 64 / 128 | 2.25 to 3.4 GHz | Socket SP3 | 7 nm | 256 MB | 225 W | Aug 7th, 2019 |

| Name | Codename | Cores | Clock | Socket | Process | L3 Cache | TDP | Released |
|---|---|---|---|---|---|---|---|---|
| EPYC 7F32 | Rome | 8 / 16 | 3.7 to 3.9 GHz | Socket SP3 | 7 nm | 128 MB | 180 W | Apr 14th, 2020 |
| EPYC 7F52 | Rome | 16 / 32 | 3.5 to 3.9 GHz | Socket SP3 | 7 nm | 256 MB | 155 W | Apr 14th, 2020 |
| EPYC 7F72 | Rome | 24 / 48 | 3.2 to 3.7 GHz | Socket SP3 | 7 nm | 192 MB | 240 W | Apr 14th, 2020 |
| EPYC 7H12 | Rome | 64 / 128 | 2.6 to 3.3 GHz | Socket SP3 | 7 nm | 256 MB | 280 W | Sep 18th, 2019 |

## 2.3 ARM CPU

All ARM CPUs with support of Confidential Computing Architecture (CCA). ARM is going to introduce the extension into Cortex A9 processors. While CCA is generally specified, first CPUs are expected in Q1/26.

## 2.4 NVIDIA

All NVIDIA processors with support of Confidential Computing (CC). This extension is available in GPUs with Hopper architecture. As of June 21, 2024, there's only one NVIDIA GPU that supports the Hopper architecture: the NVIDIA H100 Tensor Core GPU.

# 3 Software Requirements

## 3.1 Linux

Any Linux distribution with a mainline kernel. The kernel includes the necessary modifications to support the security extensions.

| | SEV-ES | SEV-SNP | Intel TDX |
|---|---|---|---|
| **Kernel Version** | 5.19 | 6.11 | 6.16 |

> ⓘ **Remark**
>
> In the case of Intel TDX, it is necessary to install additional software, including Intel TDX module, SEAM firmware files and DCAP tooling for remote attestation. See Intel guidelines for additional information.

As of **19th November 2025**, the following enterprise distributions with Linux long-term support exist. Please contact your Linux distribution partner for updated information and/or backports.

| Distribution | Latest/Upcoming Stable Version/ Release | Default Kernel Series | Support for Kernel 6.11 | Support for Kernel 6.16 |
|---|---|---|---|---|
| **Debian** | **Debian 13 (Trixie)** | **6.12** (Fixed LTS kernel) | **Yes** (Very close to the 6.12 LTS base) | **No** (Will not be the default in stable. Was available in Debian Unstable before 6.12 was chosen.) |
| **SUSE Enterprise (SLES)** | **SLES 16** | **6.12** (Fixed LTS kernel) | **Yes** (Very close to the 6.12 LTS base) | **No** (The fixed SLES kernel will be the 6.12 LTS branch.) |
| **Ubuntu** | **Ubuntu 26.04 LTS** (Resolute Raccoon) | **6.17** or **6.18** (Newest LTS kernel) | **Yes, via HWE** | **Yes** |

| Distribution | Latest/Upcoming Stable Version/ Release | Default Kernel Series | Support for Kernel 6.11 | Support for Kernel 6.16 |
|---|---|---|---|---|
| **Fedora** | **Fedora 43** | Latest mainline **(e.g., 6.17+)** | **Yes** | **Yes** (Often the default or immediately succeeded by the current mainline kernel.) |
| **RHEL** | RHEL 10 | **6.12** (Fixed LTS kernel) | **Yes** (Close to the fixed 6.12 LTS base) | No |
| **Oracle Linux** | Oracle Linux 10 | **UEK 8.1** (Based on **6.12** LTS) & **RHCK** | **Yes** (Close to the fixed 6.12 LTS base) | No |

## 3.2 Hypervisor/VirtualMachine Managers

### 3.2.1 KVM/QEMU and LibVirt/Proxmox/Openstack support

KVM/QEMU require the right kernel or the patches to be installed (see Section 3.1).

This enables the support of VMMs listed in the table below.

| | SEV-ES | SEV-SNP | Intel TDX |
|---|---|---|---|
| **Qemu** | 6.0 | 9.1 | 10.1 |
| **LibVirt** | 8.10.0 | 10.5.0 | Under Development |
| **Proxmox** | 8.3 | 8.4 | None |
| **Cloud Hypervisor** | N/A | Under Development | Under Development |
| **Kubevirt** | N/A | 1.7.0 | Under Development |
| **Openstack** | Nova 32.0.0 | Under Development | Under Development |

### 3.2.2 VMware

VMware supports AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) technology starting from vSphere 7.0 Update 1. This technology helps enhance the security of virtual machines running on AMD EPYC 2nd gem (Rome) processors.

vSphere supports SEV-SNP (Milan or newer) and TDX (Emeralds Rapids or newer) with VMware Cloud Foundation 9.0.

| | SEV-ES | SEV-SNP | Intel TDX |
|---|---|---|---|
| **VMware** | 7.0 Update 1 | 9.0 | 9.0 |

### 3.2.3 Hyper-V

Microsoft continues improving the Hyper-V support within the Linux kernel for benefiting Linux guest VMs running within this hypervisor on Windows. With Linux 6.6 the Hyper-V code adds support for SEV-SNP secure guests on the AMD EPYC side while over on the Intel Xeon Scalable Sapphire Rapids side is initial support for Trust Domain Extensions (TDX) protected guests. Running guests with Hyper-V as the hypervisor however remains limited to Azure, as the binaries for Hyper-V are not freely distributed. Under the paravisor model Windows 11 24H2 supports running confidential guests using the OpenHCL paravisor.

# Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) may represent or impact current enclaive product offerings and practices, which are subject to change without notice, and © does not create any commitments or assurances from enclaive and its affiliates, suppliers, or licensors. enclaive products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of enclaive to its customers are governed by enclaive agreements, and this document is not part of, nor does it modify, any agreement between enclaive and its customers.