

FLEXIBLE, POWERFUL, SECURE

3rd Generation Intel® Xeon®



Modern infrastructures are highly distributed, and organisations want to run cloud-native workloads everywhere across the distributed infrastructure. These include the data centre, public cloud, the edge and on telco provider network infrastructure. 3rd generation Intel® Xeon® Scalable processor-based servers from CDW provide extraordinary cloud performance, flexibility and security.

Performance meets flexibility and security

3rd generation Intel® Xeon® processors have up to 40 cores with outstanding per-core performance, optimised for popular cloud databases, high-performance computing (HPC), virtualisation and artificial intelligence (AI) workloads. Performance and security enhancements, as well as AI acceleration, are built in.

Extended memory

Adding to this power and flexibility is the capability to extend system memory up to 12 TB on a two-socket server—delivering 32% higher bandwidth on average when compared with 1st generation.¹

Fast, flexible storage

3rd generation Intel® Xeon®-based servers offer breakthrough storage performance with support for the new Intel® Optane™ SSD P5800X. They also support the ultra-dense Intel® SSD D5-P5316, which enables an incredible 1-petabyte of storage capacity per 1U server.

Silicon-enhanced security

3rd Gen Intel® Xeon® Scalable processors integrate many of the silicon-hardened security innovations that Intel has designed over the years, but also include a number of important new or enhanced features that help better protect your data, applications and platforms. These include:

- Intel® Crypto Acceleration—greatly accelerates a variety of cryptography tasks to speed data encryption and decryption
- Intel® Software Guard Extensions (Intel® SGX)—processor-created, secured and isolated enclaves for sensitive apps and data that provide true confidential computing capabilities, helping protect data and code even if the system's software stack has been compromised
- Intel® Total Memory Encryption (Intel® TME)—delivers full physical memory encryption support to enhance data and virtualised workload protection
- Intel® Platform Firmware Resilience (Intel® PFR)—an Intel FPGA-based solution that can help protect platform firmware, detect corruptions and restore back to a known-good state

¹ Source: Based on testing by Intel as of April 27, 2020 (Baseline) and March 23, 2021 (New). Baseline configuration: 1-node, 1x Intel Xeon Platinum 8280L processor (28 cores at 2.7 GHz) on Neon City with a single Intel Optane PMem module configuration (6 x 32 GB DRAM; 1x {128 GB, 256 GB, 512GB} Intel Optane PMem module), ucode rev: 04002F00 running Fedora 29 kernel 5.1.18-200.fc29.x86_64 and Intel Memory Latency Checker (Intel MLC) version 3.8 with App Direct Mode. New Configuration: 1-node, 1x Intel Xeon pre-production ICX-XCC processor (38 cores at 2.0 GHz) on Wilson City with a single Intel Optane PMem module configuration (8 x 32 GB DRAM; 1x {128 GB, 256 GB, 512 GB} Intel Optane PMem module), ucode rev: 8d000270 running RHEL 8.1 kernel 4.18.0-147.el8.x86_64 and Intel MLC version 3.9 with App Direct Mode.

Outstanding cloud performance and innovation

1.58x

higher web microservices performance vs. prior generation

Up to **1.72x**

higher virtualisation performance vs. prior generation

1.74x

higher AI batch inference throughput vs. prior generation²

Up to **1.63x**

CDN Live Linear throughput vs. prior generation

Intel® Optane™ persistent memory 200 series

Up to **6TB**

total memory per processor

Intel® Optane™ SSD P5800X

Up to **4x**

Greater IOPS performance vs. prior generation

² ibid

Next steps

Have more questions?
Get in touch with one of our consultants



Follow us to stay updated on all our latest announcements, product developments, and relevant industry news.



Intel Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.