intel xeon

4 Facts: Intel at the Foundation of Confidential Computing

Confidential Computing—the ability to keep data-in-use secure by isolating it in a hardware-based enclave—is an opportunity for businesses to realize more value from private, sensitive, or regulated data while remaining protected and compliant.

But not all Confidential Computing solutions are alike.

You need hardware-enabled security and a robust ecosystem. Intel offers the most comprehensive Confidential Computing portfolio in the industry.

Let's break this down with four figures.

2018

Intel® Software Guard Extensions (Intel® SGX) on Intel® Xeon® processors is the first Confidential Computing solution introduced into the data center.

2016 2017 2018 2019 2020 2021 2022 2023

Intel SGX is the most tested, researched, and deployed hardware-based data center Trusted Execution Environment (TEE), with the smallest attack surface within the system. If you have strict data privacy and security requirements, Intel SGX offers a clear strategic advantage.

Intel SGX protects against thousands[1] of known industry-reported threats, many still lacking mitigations, as well as threats yet to be discovered. Your code and data remain significantly more protected with Intel SGX than without it.

300+

Organizations have engaged with Intel to develop and deploy Confidential Computing services.

« Intel® SGX »

Over 80 software and service vendors offer Intel SGX solutions. Today, dozens of enterprises actively protect production workloads with Intel SGX.

$300M

Is the estimated value of infrastructure deployed with Intel SGX on Intel Xeon processors.

››› Intel® SGX

4

Global cloud providers have committed to offer Intel® Trust Domain Extensions (Intel® TDX) on 4th Gen Intel Xeon processors in 2023.[2]

Alibaba Azure IBM Cloud Google Cloud

Intel TDX offers confidentiality at the virtual machine (VM) level, isolating the guest OS and all VM applications from the cloud host, hypervisor, and other VMs on the platform. Intel TDX is designed so that confidential VMs are easier to deploy and manage at scale than application enclaves.

Choose the proven leader in Confidential Computing

Powered by 4th Gen Intel Xeon Scalable processors, Intel offers the most comprehensive Confidential Computing portfolio in the industry.

With Intel SGX and Intel TDX, Intel's portfolio of Confidential Computing technologies allows businesses to choose the level of security they need to help meet their business and regulatory requirements.

Intel Confidential Computing:
https://intel.com/confidentialcomputing

[1] - Intel SGX is not vulnerable to most OS layer threats, and there are over 140,000 such threats in the Common Vulnerabilities & Exposure database today. https://cve.mitre.org.

[2] - Intel TDX will be available on select 4th Gen Intel Xeon Scalable processors instances through four leading cloud providers. Previews have begun with select providers. Check with your provider for availability. Intel TDX becomes generally available with 5th Gen Intel Xeon Scalable processors.

Intel technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. All product plans and roadmaps are subject to change without notice.

intel.