Product Brief

Security Accelerated
Intel® Xeon® Scalable Processors

Accelerate innovation and enhance data protection with Intel® Security Engines

Maintain performance while helping preserve data confidentiality and code integrity with Intel® Security Engines on Intel® Xeon CPUs

Confidential Computing with the Intel Xeon® Scalable platform — put data into action while helping to keep it private

Today, it's standard procedure to encrypt data while it's in storage and in transit. However, the weak point companies face in data protection is when the data is actively in use by the processor and memory. At that point, sensitive data such as personally identifiable information, medical records and financial transactions can be vulnerable to potential exploits, accidental exposure or compliance violations.

Confidential Computing allows for the extraction of insights or training of AI models using sensitive data without exposing that data to other software, collaborators or your cloud provider. This opens wide possibilities for businesses to harness data that was previously too sensitive or regulated to activate for analytics and other purposes.

With a dual-socket Intel Xeon Scalable processor-based server, up to 1 terabyte of data can be processed inside Intel® Software Guard Extensions (Intel® SGX) enclaves, creating opportunities for applications requiring large data sets. When the training or processing is complete, private information can be deleted or re-encrypted before leaving the enclave.

Activate your data and move forward faster with Intel Xeon Scalable processor-based security technologies

Data is the fuel of innovation and progress. Businesses can put their data to work to accomplish everything from detecting fraud and developing more responsive supply chains to training breakthrough AI models. Those who can turn data into business insights will go faster and further.

Security technologies built into Intel Xeon Scalable processors are designed to accelerate the pace of innovation by making data available for analysis even if it's sensitive, confidential or regulated. Intel SGX is a unique technology that helps protect data while it's actively in use. Rather than excluding sensitive data from analytics or AI models, businesses using Intel Xeon Scalable processors can create access-restricted data enclaves with Intel SGX. These isolated environments can help businesses extract value from their most sensitive data while helping to keep it confidential.

Embrace Confidential Computing with Intel SGX and Intel® TDX

Confidential Computing powered by Intel SGX enables application-level, VM, container or function-level isolation. Whether you're in the cloud, at the edge, or on-prem, you can be confident that your sensitive computations and data are kept more private and secure from the cloud service provider, unauthorized administrators , the OS and even other privileged applications.

Intel SGX is the most deployed, researched and trusted execution environment (TEE) for the data center, and it provides the smallest attack surface within the system.[1] This feature of Intel Xeon Scalable processors provides the ingredients for Confidential Computing solutions across multiple clouds and edges.

Intel SGX offers a hardware-based security solution that helps protect data in use via unique application-isolation technology. By protecting selected code and data from inspection or modification, developers can run sensitive data operations inside enclaves to help increase application security and protect data confidentiality.

Intel will provide further protection with Intel® Trust Domain Extensions (Intel® TDX). Available through select cloud providers starting in 2023, this new tool offers isolation and confidentiality at the virtual machine (VM) level. Intel TDX isolates the guest OS and VM applications from the cloud host, hypervisor and other VMs on the platform. The trust boundary for Intel TDX is larger than the application-level isolation of Intel SGX, but Intel TDX is designed so that confidential VMs are easier to deploy and manage at scale than application enclaves.

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 needs and regulatory requirements.

Customer success: Security is driving innovation with Intel Xeon Scalable processors

Intel SGX and Intel Xeon Scalable processors helped **Nationwide Building Society** streamline compliance with evolving Know Your Customer (KYC) regulations.

Get the details ›

UPenn leveraged Intel Xeon processors and Intel SGX for its 3DResUnet tumor segmentation model. The result: a marked improvement in accuracy in its detection of tumor boundaries.

Read the story ›

Choice for Confidential Computing

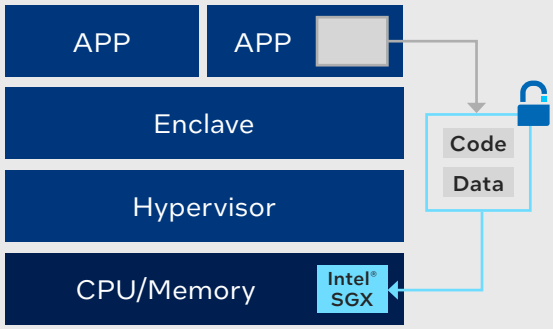

Figure 1. Intel® SGX helps protect the most sensitive data by isolating it into enclaves up to 1 TB in size.

Intel® SGX use cases

Artificial intelligence (AI)/machine learning (ML)

Process sensitive or regulated data using AI and ML while improving compliance with privacy regulations.

Cloud infrastructure

Restrict access to your data by the service provider or other public cloud tenants.

Trusted multiparty compute/ multiparty analytics

Enable multiple parties to collaborate on shared data in the cloud while keeping sensitive data confidential.

Secure key management

Use enclaves to help protect cryptographic keys and provide hardware security module (HSM)–like functionality.

Blockchain

Increase privacy and security for transaction processing, consensus, smart contracts and key storage.

Network function virtualization (NFV)

Establish trust for virtualized network functions.

Enhance security, better protect performance by tapping into Intel® Crypto Acceleration

Data centers today rely on cryptography for processes spanning networking, storage and data compression, in addition to traditional perimeter defense. With the growth of cryptography comes an explosion in the number of encryption cycles that need to be performed by the CPUs. This, in turn, can lead to potential impacts on performance and user experience.

The advanced crypto-acceleration technologies embedded in 4th Gen Intel Xeon Scalable processors enable greater levels of cryptographic security, enhance performance and enable a more seamless user experience — and without having to add more cores and more processors to the data center.

Intel® Quick Assist Technology (Intel® QAT), a mature data compression and encryption accelerator, is a new built-in accelerator on 4th Gen Intel Xeon Scalable processors for on-the-fly data compression/decompression and cryptographic workloads. By offloading compute-intensive workloads, Intel QAT can free up core capacity for other workloads while significantly reducing costs and compressed data footprints.[2]

Intel Crypto Acceleration instructions use stronger encryption protocols, like larger key sizes, stronger algorithms and more types of data encrypted[3] — with minimal impact upon UX. By utilizing faster cryptographic algorithms, users can see improved performance, support for better service-level agreements (SLAs) and a reduction in compute cycles typically spent on cryptography processing.

Crypto acceleration benefits performance on three main areas of cryptographic computing at the algorithm level:

Public key encryption: Up to six times faster public key encryption and decryption for uses like Secure Sockets Layer (SSL), front-end web and public key infrastructure (PKI).[4]

Bulk cryptography: Up to four times faster and stronger encryption[5] with Intel® Advanced Vector Extensions (Intel® AVX-512) for uses like secure data transmission, disk encryption and streaming video encryption.[6]

Hashing: Up to two times faster secure[7] hash performance for uses like digital signatures, authentication and integrity checking like Secure Hash Algorithm 1 (SHA-1) and Secure Hash Algorithm 2 (SHA-2, also known as SHA-256), which is used by SSL.

Many commercial software packages from companies like Microsoft, SAP and Oracle have been optimized to take advantage of Intel Crypto Acceleration. Open-source software — numerous Linux distributions, NGINX, the Java OpenJDK runtime and OpenSSL library — has been optimized by Intel to support Intel Crypto Acceleration.

Developer tools like the Crypto API toolkit can run cryptographic operations more securely inside an Intel SGX enclave. Additionally, the Intel Integrated Performance Primitives (Intel IPP) cryptography library automatically takes advantage of available CPU capabilities, while Intel QAT engine for OpenSSL lets network security software solutions transparently take advantage of Intel Crypto Acceleration.

By tapping into the built-in cryptographic acceleration technologies of Intel Xeon processors, you can reduce the compute cycles spent on cryptography processing, increase developer agility, gain DevOps efficiency and improve the UX in the enterprise.

Improve regulatory compliance while speeding data analysis

Data that holds value for businesses regularly falls under stringent privacy regulations, such as GDPR in Europe, HIPAA in the United States and PIPL in China. Violating these regulations can result in stiff fines and other penalties, which can make it risky for organizations to fully harness sensitive data. Workarounds for using personally identifiable information are available, such as painstakingly anonymizing it, but they significantly slow down the processes of analysis and may even reduce accuracy. With Intel Xeon Scalable processors and built-in Intel SGX technology, businesses can create encrypted enclaves that help keep data and applications confidential, improving both compliance and data availability.

"By 2023, 65 percent of the world's population will have its personal information covered under modern privacy regulations, up from 10% today."

—Gartner[8]

Overcoming barriers to sharing sensitive data

Sharing data between entities can greatly increase accuracy and speed processes, such as training neural networks. Intel Xeon Scalable processors, make sharing confidential data possible by enabling trusted multiparty compute models such as federated learning. Employing Intel Xeon Scalable processors with Intel SGX enclaves allows multiple parties to pool sensitive data and share the benefits of a common analysis without exposing their private data to the other parties. The attestation capabilities of Intel SGX provide greater confidence that the software running in the enclave is exactly what is expected and previously agreed upon by all parties.

Helping Bosch move past security obstacles

Intel collaborated with engineering leader Bosch and software innovator Edgeless Systems to speed development of Bosch's autonomous driver assistance project. To train the computer vision models, Bosch uses real-world video and imagery from the streets and locations where the vehicles will operate. This footage

contains regulated, personally identifiable information such as faces and license plate numbers and therefore needs to be anonymized to be accessed by Bosch personnel. However, anonymizing the data would typically make it less accurate for AI training. With Intel SGX, Bosch can leverage the unaltered real-world footage inside an Intel SGX data enclave to train the model, improving the speed of their process and the quality of their results while staying in compliance with data privacy laws.

Expansive, scalable trust in the cloud and data center

Intel® security technologies are helping businesses take advantage of the flexibility and scalability of the cloud while reducing the risk of exposing sensitive data. Confidential Computing using Intel Xeon Scalable processors isolates your sensitive data from the cloud provider's software, administrators and other tenants. Remote attestation allows the owner of the data to verify that their enclave is genuine, up-to-date and running only the software they expect.

Do more with your data today by choosing Intel Xeon Scalable processors

Intel Xeon Scalable processors with built-in security features like Intel SGX are available through cloud providers and system manufacturers across the globe. They can be used to help power new services, amplify the value of transactions, guard against financial crime, shorten R&D cycles and drive the progress of applications where sensitive, valuable or regulated data is in play. The future belongs to those with data, and Intel® Accelerator Engines can get you there sooner.

Learn more about how Intel Security Engines can help achieve peak performance and security for workloads that matter most to your business.

Intel – Confidential Computing

intel® xeon®

[1] Intel® Software Guard Extensions Protects Data

[2] https://www.intel.com/content/www/us/en/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html

[3] Intel Solution Brief, "Tapping into Cryptographic Acceleration," https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[4] Intel Solution Brief, "Tapping into Cryptographic Acceleration," https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[5] Intel Solution Brief, "Tapping into Cryptographic Acceleration," https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[6] Intel Solution Brief, "Tapping into Cryptographic Acceleration," https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[7] Intel Solution Brief, "Tapping into Cryptographic Acceleration," https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf

[8] "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations," Gartner, September 2020, gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w.