Product Brief

Security Accelerated
Intel® Xeon® Scalable Processors

Speed Innovation while Helping Ensure Privacy and Compliance Using Intel® Xeon® Scalable Processors

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

—Gartner[1]

Accelerate your pace of innovation while working toward your data privacy and compliance goals. With built-in, robust security technologies on Intel® Xeon® Scalable processors, you can put more of your data into action.

Free 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 have access to more data will go faster and further.

Security technologies built into Intel Xeon Scalable processors accelerate the pace of innovation by making data available for analysis even if it's sensitive, confidential, or regulated. Intel® Software Guard Extensions (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 protected data enclaves with Intel SGX. These isolated environments can enable businesses to extract value from their most sensitive data while helping to keep it confidential.

Confidential computing with the Intel Xeon Scalable platform—put data to use 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 in data protection is when the data is actively in use in the processor and memory. At that point, sensitive data such as personally identifiable information, medical records, and financial transactions becomes vulnerable to exploits, accidental exposure, or compliance violations.

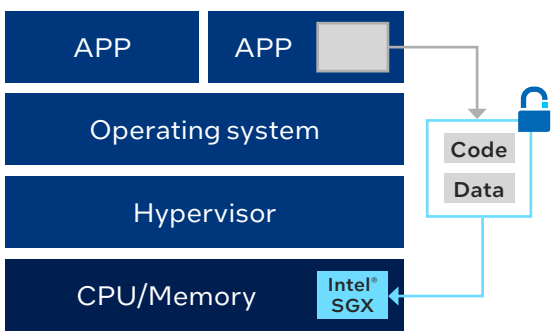

Figure 1. Intel® SGX helps protect the most sensitive data by isolating it into enclaves up to 1 TB in size.

Confidential computing using Intel Xeon Scalable processors with Intel SGX helps close this gap by better protecting data in use. Intel SGX is the most deployed, researched and battle-tested confidential computing technology for data centers on the market today. Intel SGX is the most deployed, researched and battle-tested Confidential Computing technology in data centers on the market today. Intel SGX allows you to create encrypted enclaves within the CPU and memory that help protect data from access by anything other than authorized, verified application code. The hypervisor, OS, and even administrators with root access can't see the data inside the Intel SGX enclave. Confidential computing allows the extraction of insights or training of models from sensitive data without exposing it 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 TB of data can be processed inside Intel SGX enclaves, creating opportunities for applications requiring large data sets. When the training or processing is complete, any private information can be deleted or re-encrypted before leaving the enclave.

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 ever-evolving Know Your Customer (KYC) regulations.

Get the details ›

Nasdaq technologists leveraged Intel Xeon Scalable processors to significantly speed up their advanced homomorphic encryption (HE) applications.

Read the story ›

Improve regulatory compliance while speeding up 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.

Overcoming the barriers to sharing sensitive data

Sharing data between entities can greatly increase accuracy and speed up 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.

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
Minimize 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.

Helping Bosch move past security obstacles

Intel collaborated with engineering leader Bosch and software innovator Edgeless Systems to speed up the 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.

Intel SGX is available today and will be joined in a future Intel Xeon Scalable processor by Intel® Trust Domain Extensions (Intel® TDX), a new tool that offers confidentiality at the virtual machine (VM) level. Within an Intel TDX confidential VM, the guest OS and all the VM's applications are isolated from the cloud host, hypervisor, and other VMs on the platform. With Intel TDX, the trust boundary will be larger than the application-level isolation of Intel SGX, but confidential VMs will be easier to deploy and manage at scale than application enclaves. With Intel SGX and Intel TDX, the Intel® portfolio of confidential computing technologies will allow businesses to choose the level of security they need to meet their business needs and regulatory requirements.

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 to drive the progress of applications where sensitive, valuable, or regulated data is in play. The future belongs to those with the data, and Intel Xeon Scalable processors can get you there sooner.

Learn more

Explore Intel SGX ›

Download Intel SGX technical documents ›

Start using Intel SGX ›

Get an overview of Intel TDX ›

intel XEON

1. "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.

0922/MP/CMD/PDF