Product Brief

Security Accelerated
Intel® Xeon® Scalable Processors

Accelerate Innovation and Enhance Data Protection with Built-In Intel® Security Engines

Maintain performance while helping preserve data confidentiality and code integrity with Intel® Security Engines and 5th Gen Intel® Xeon® Scalable processors

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

Today it's standard practice to encrypt data while it's in storage and in transit. However, the challenge 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 — is vulnerable to potential exploits, accidental exposure or compliance violations.

In an increasingly data-driven world, businesses need to protect their data from unauthorized access. Intel Xeon Scalable processors with Intel Security Engines provide a hardware-based solution for Confidential Computing, allowing businesses to extract insights or deploy AI models and harness the power of data while helping keep it private.

With 5th Gen Intel Xeon processors, businesses can create secure enclaves within their processors where sensitive data can be processed and analyzed without being exposed to other software, collaborators or cloud providers. This opens new possibilities for using data that was previously too sensitive or regulated to analyze. By protecting data in use, 5th Gen Intel Xeon Scalable processors can also help organizations meet privacy and compliance obligations.

With these secure enclaves, data is protected from unauthorized access while it's actively in use. With the availability of both Intel® Software Guard Extensions (Intel® SGX) and Intel® Trust Domain Extensions (Intel® TDX), Intel Xeon scalable processors allow customers to choose the Confidential Computing technologies that best meet their business and regulatory requirements.

Embrace Confidential Computing with Intel SGX and Intel TDX

Confidential Computing powered by Intel SGX enables application- or function-level isolation. Whether you're in the cloud, at the edge, or on premises, 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 other privileged applications.

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

Intel Xeon Scalable processors are helping BeeKeeperAI develop machine learning algorithms for health care while safeguarding sensitive data. Data stewards can verify the integrity of the consuming AI application using Intel SGX.

Get the details ›

Zscaler's cloud-native Zero Trust Exchange platform securely connects users, devices and applications in any location. Zscaler isolates its Zero Trust Exchange and App Connectors in Intel TDX TEEs and uses Intel® Trust Authority to verify their authenticity and integrity across multiple cloud infrastructures.

Read the story ›

Opportunities for transformation abound

- AI-powered analysis and services
- Cloud economics and scale
- Distributed and edge applications
- Service innovation enabled by new data sources
- Privacy-preserving technology
- Blockchain-based services
- Multiparty collaboration around data

Intel SGX is the most researched and updated 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.

In addition, 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.

While Intel SGX is for application and function isolation, Intel TDX offers isolation and confidentiality at the virtual machine (VM) level. This tool 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. Intel TDX also offers a simpler migration path for existing applications to move to a TEE. Customers can see up to an 11% higher virtual machine performance on 5th Gen Intel Xeon Scalable platforms with TDX versus 4th Gen Intel Xeon Scalable platforms without TDX on integer, floating point and BERT-large.[2]

Improve regulatory compliance while speeding data analysis

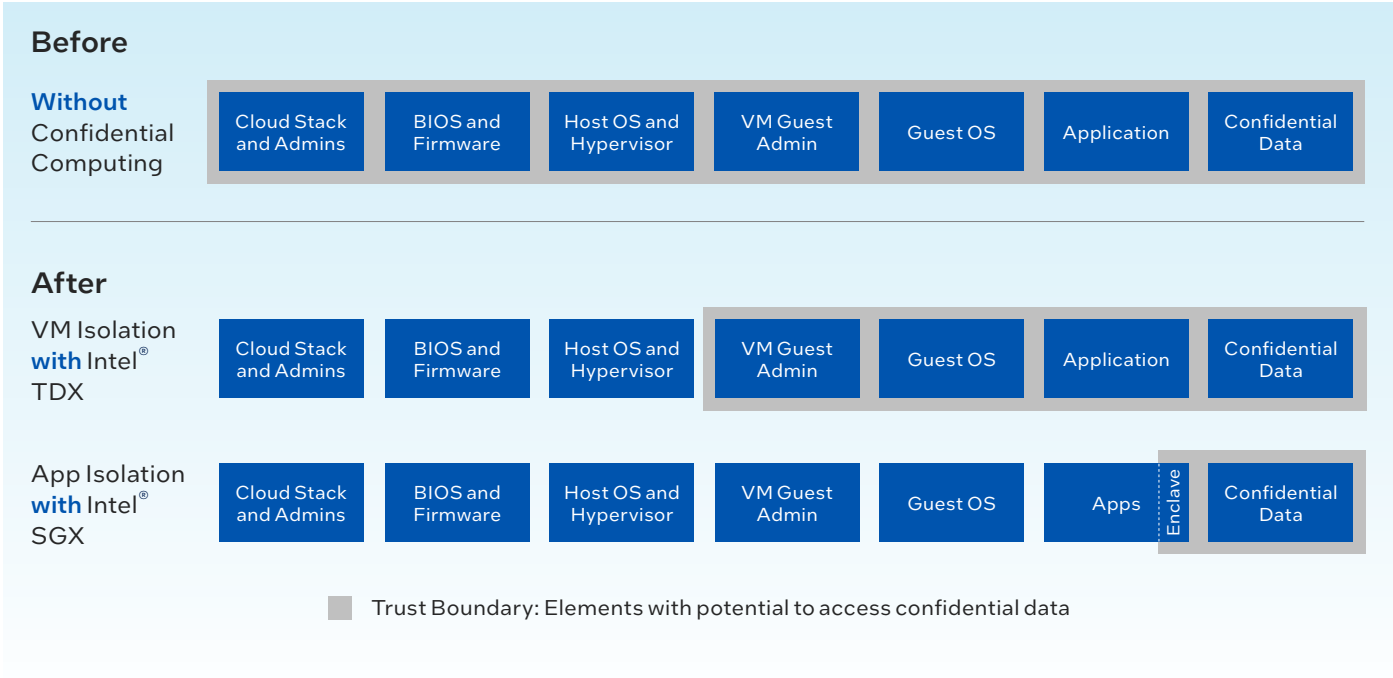
Data that holds value for businesses regularly falls under stringent privacy regulations. Violating these regulations can result in stiff fines and other penalties, making it risky for organizations to fully harness sensitive data. Workarounds for using personally identifiable information are available, but they often significantly slow down the processes of analysis and may even reduce accuracy. With 5th Gen Intel Xeon Scalable processors and Intel's Confidential Computing portfolio, businesses can create encrypted enclaves that help keep data and applications confidential, improving both compliance and data availability.

"As the cost of a data breach under the GDPR may be as high as 4% of gross annual revenue, data custodians are strongly incentivized to protect potential surface areas against attack, including data-in-use."

— Confidential Computing Consortium, November 2022[3]

Overcoming barriers to sharing sensitive data

Sharing data between entities can greatly increase the accuracy and speed of business processes such as training neural networks. 5th Gen Intel Xeon Scalable processors make sharing confidential data possible by enabling trusted multiparty compute models like federated learning. Employing 5th Gen Xeon Scalable processors with Intel Confidential Computing technologies allows multiple parties to pool sensitive data and share the benefits of a common analysis without exposing their private data to unauthorized users.



Enhance security—protect performance by tapping into Intel® Crypto Acceleration and Intel® QuickAssist Technology (Intel® QAT)

While working to protect their data, 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 5th Gen Intel Xeon Scalable processors enable greater levels of cryptographic security, enhance performance and enable a more seamless user experience — without having to add more cores and more processors to the data center.

Intel QAT a mature data compression and encryption accelerator, is integrated into the built-in accelerator on 5th 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 helping to significantly reduce costs and compressed data footprints.[4] Customers can see up to a 1.85x higher NGINX TLS Handshake performance per core with 5th Gen Intel Xeon Platinum 8592+ with integrated QAT versus 4th Gen AMD EPYC 9554 OOB.[5]

Intel Crypto Acceleration instructions use stronger encryption protocols like larger key sizes, stronger algorithms and more types of data encrypted and 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 in three main areas of cryptographic computing at the algorithm level:

Public key encryption: For uses like Secure Sockets Layer (SSL), front-end web, and public key infrastructure (PKI).

Bulk cryptography: For uses like secure data transmission, disk encryption, and streaming video encryption.

Hashing: 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 — Intel has optimized 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) library automatically takes advantage of available CPU capabilities, while the Intel QAT engine for OpenSSL enables network security software solutions to 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 and improve the UX in the enterprise.

Enabling end-to-end data protection for Thales

Thales and Intel are collaborating to make Confidential Computing commonplace, and to add data protection capabilities for data in use by its CipherTrust Data Security Platform. Together, Intel and Thales create a trusted harmonized ecosystem that offers comprehensive end-to-end data protection solutions for both cloud and on-premises environments, attesting to the environment's authenticity before decrypting the customer-sensitive workloads.

By using trusted attestation provided by Intel® Trust Authority, Thales' CipherTrust Data Security Platform sensitive workloads are never decrypted outside of an Intel TDX or Intel SGX TEE. Thales' CipherTrust Data Security Platform is FIPS 140-2 Level 3 compliant.

There are many industry use cases for this technology. In health care, for example, enabling the use of patient datasets to train machine-learning models can facilitate the diagnosis of diseases and the development of pharmaceutical drugs. In banking, multiple banks can share data without exposing personal information, which helps to detect money laundering or other transactional irregularities.

Expansive, scalable trust in the cloud and data center

Intel Security Engines on 5th Gen Intel Xeon Scalable processors help 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 Intel Security Engines 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® Security 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.

Confidential Conmputing ›

Intel Security Engines ›

1. https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html
2. See [S1] at intel.com/processorclaims: 5th Gen Intel Xeon Scalable processors. Results may vary.
3. Confidential Computing: Hardware-Based Trusted Execution for Applications and Data," The Confidential Computing Consortium November 2022, V1.3.
4. https://www.intel.com/content/www/us/en/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html
5. See [N202] at intel.com/processorclaims: 5th Gen Intel Xeon Scalable processors. Results may vary.