Product Brief

Security Accelerated
Intel® Security Engines

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 Intel® Xeon® processors.

The Intel® Xeon® platform puts data into action while helping to keep it private and protected with confidential computing

It's standard practice to encrypt data in storage and 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 must protect their data from unauthorized access. Intel Xeon 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 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 regulated or too sensitive to analyze. By protecting data in use, Intel Xeon 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 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 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 cloud service providers, unauthorized administrators, the OS, and other privileged applications.

Customer successes: Enhanced security drives innovation with Intel® Xeon® processors

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

Get the details ›

Azure Cloud Services is using Intel SGX to help Microsoft protect US$25B in annual customer payments. Deploying confidential computing enables Microsoft to exceed the current Payment Card Industry Data Security Standard (PCI-DSS) and meet its scalability, uptime, and cost-effectiveness requirements.

Read more ›

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 confidential computing technology on the market today and provides the smallest trust boundary in the data center when compared to other confidential computing technologies. It helps protect data actively being used in the processor and memory by creating a trusted execution environment (TEE) called an enclave. Only the code or functions inside protected enclaves can access confidential data. 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. Additionally, 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 technology 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. However, Intel TDX is designed so that confidential VMs are easier to deploy and manage at scale than application enclaves. Intel TDX offers a simpler migration path for existing applications to move to a TEE.

Customers can see up to 11 percent higher VM performance on 5th Gen Intel® Xeon® Scalable platforms with Intel TDX vs. 4th Gen Intel® Xeon® Scalable platforms without Intel TDX on integer, floating point, and BERT large.[1]

Intel® Xeon® 6 processors help push confidential computing capabilities further by incorporating an AES-256 encryption engine to both Intel SGX and Intel TDX. AES-256 is a quantum-resistant algorithm that adds an additional layer of security to confidential computing. Intel Xeon 6 processors also support up to 2,048 Intel TDX encryption keys,[2] allowing a larger number of VMs to enable trust domains on high-core-count systems.

Improve regulatory compliance while speeding data analysis

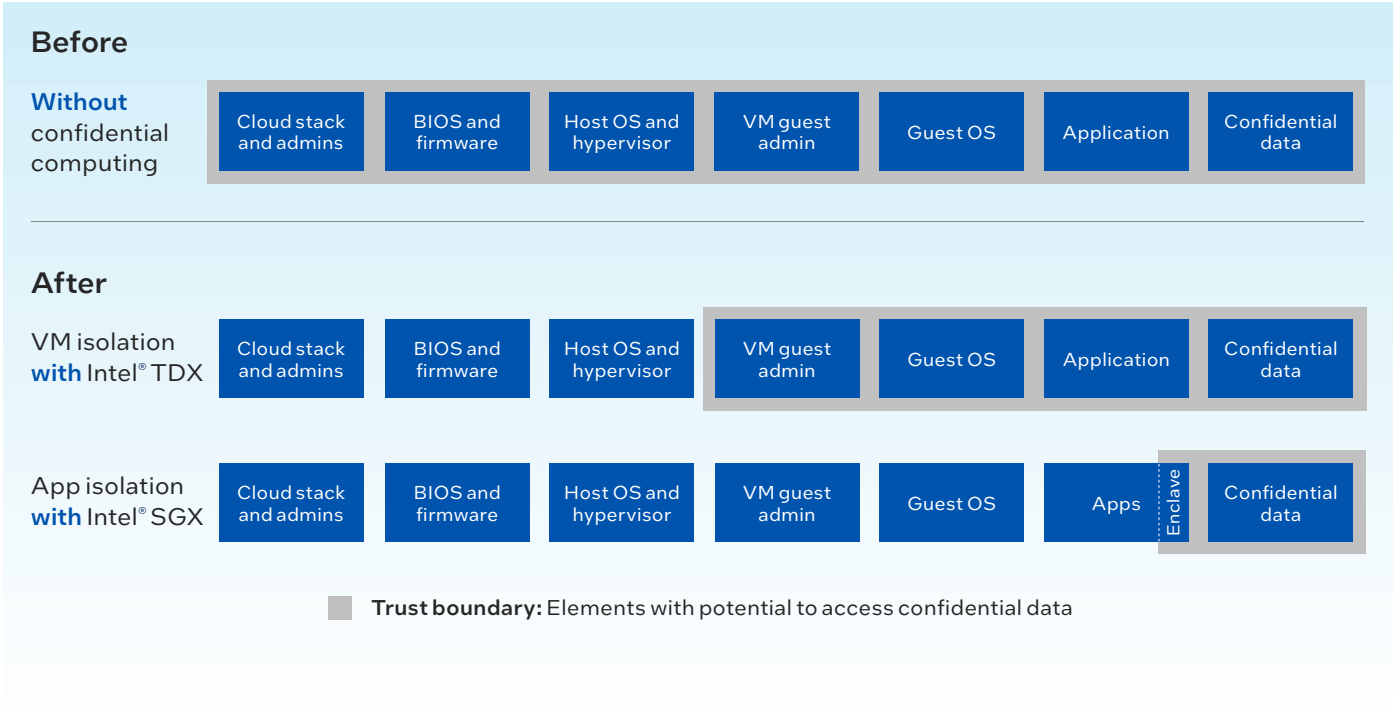
Data that holds value for businesses regularly falls under stringent privacy regulations. Violating these regulations can result in stiff fines and other penalties. Alternatives to using personal data are available, but they often significantly slow down the processes of analysis and may even reduce accuracy. With Intel Xeon processors and Intel® confidential computing solutions, businesses can create encrypted enclaves that help keep data and applications confidential, aligning to regulatory compliance and improving 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]

Overcome barriers to sharing sensitive data

Sharing data between entities can greatly increase the accuracy and speed of business processes such as training neural networks. Intel Xeon processors make sharing confidential data possible by enabling trusted multiparty compute models like federated learning. Employing Intel Xeon 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 Intel Xeon processors enable greater levels of cryptographic security, enhance performance, and allow for a more seamless user experience—without adding more cores and processors to the data center.

Intel QAT, a mature data compression and encryption accelerator, is integrated into the built-in accelerator on Intel Xeon 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 vs. 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 with minimal impact on 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 are used by SSL.

Many commercial software packages from companies like Microsoft, SAP, and Oracle have been optimized to take advantage of Intel Crypto Acceleration. Examples of open source software programs that are optimized to support Intel Crypto Acceleration include NGINX, the Java OpenJDK runtime, OpenSSL library, and several Linux distributions.

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. At the same time, 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 designed to be decrypted only inside of an Intel TDX or Intel SGX TEE, and Thales' CipherTrust Data Security Platform is FIPS 140-2 Level 3 compliant.

There are many industry use cases for this technology. In healthcare, for example, using 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 the Intel Xeon platform 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 processors isolates your sensitive data from the cloud provider's software, administrators, and other tenants. Remote attestation allows the data owner 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 processors

The Intel Xeon platform with built-in Intel Security Engines is available through cloud providers and system manufacturers across the globe. It can be used to help power new services, amplify the value of transactions, help 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 enhanced security for workloads that matter most to your business.

Intel confidential computing solutions ›

Intel Security Engines ›

intel® xeon®

1. See [S1] at intel.com/processorclaims: 5th Gen Intel® Xeon® Scalable processors. Results may vary.
2. Maximum number of keys based on SKU.
3. "Confidential Computing: Hardware-Based Trusted Execution for Applications and Data," The Confidential Computing Consortium, November 2022, confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf.
4. Hualong Feng, "Offloading Compression and Encryption in Ceph using Intel® QuickAssist Technology," Intel, October 2022, 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.

0624/BR/CMD/PDF