Solution Brief

Intel® Software Guard Extensions (Intel SGX)
Intel® Xeon® Scalable Processors

Help Protect and Isolate Confidential Data—Even While You Share and Process It

Intel Software Guard Extensions (Intel SGX) on Intel Xeon Scalable processors helps secure data for confidential computing solutions.

Companies and organizations are leaning more on IT to help them innovate and design new products and services, increase efficiency, and make new discoveries. This means drawing insights from enormous amounts of data that must be protected. But how do organizations use data to support their goals, while also protecting that data and keeping it private?

For example, highly regulated industries such as healthcare and financial services operate under strict compliance requirements for data. Hospitals need to protect the confidentiality of private data, such as health records, from third parties that might be using multi-party computing and confidential blockchains. Clinicians and administrators might want to collaborate with those at other hospitals on research, but they must comply with the Health Insurance Portability and Accountability Act (HIPAA) and other requirements. Enterprises operating in the cloud need to control or protect the sovereignty of data by technologically removing cloud service providers (CSPs) or hosts from the trust boundary. Many companies in general also need to increase the security of services by limiting which software can access data or protect business or customer data and software intellectual property (IP) from theft or tampering.

Intel Software Guard Extensions (Intel SGX) on 3rd Gen Intel Xeon Scalable processors provides a confidential computing solution that can help organizations overcome this challenge. Intel SGX does this by creating trusted execution environments (TEEs), or encrypted enclaves, that help protect data and applications while in use. Intel SGX enables confidential computing solutions that allow users to unlock insights and collaborate with partners while maintaining control of the data and keeping it private, regardless of where the data sits.

Data must be protected everywhere it is exposed

At rest
Keep data encrypted when stored

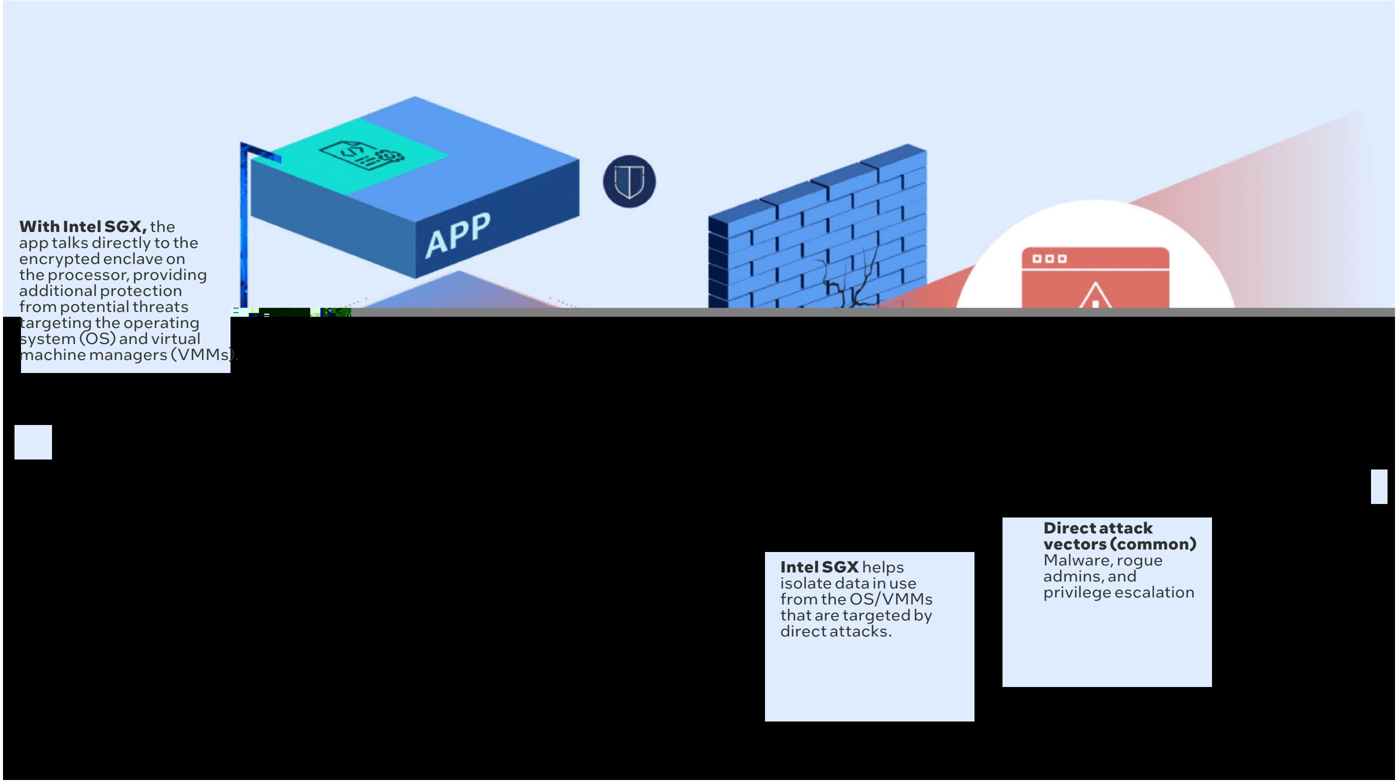
In flight
Encrypt data when transmitted

In use
Guard against software threats when data is being actively processed

How Intel SGX works

Traditionally, when a system's BIOS, hypervisor, or operating system is compromised by a malicious attack, the attacker's code can gain visibility and access to everything higher in the system stack, such as applications and data. Intel SGX utilizes memory encryption and hardware-enforced access controls to change how data is accessed, providing enclaves of protected memory in which to run applications and data.

Intel SGX currently provides the smallest trust boundary in data center confidential computing, compared to other confidential computing technologies. With Intel SGX, only the code or functions inside the protected enclave can access confidential data. Up to 1 TB of enclave capacity for code and data is available to Intel SGX on dual-socket 3rd Gen Intel Xeon Scalable processor–based servers.



With Intel SGX, the app talks directly to the encrypted enclave on the processor, providing additional protection from potential threats targeting the operating system (OS) and virtual machine managers (VMMs).

Intel SGX helps isolate data in use from the OS/VMMs that are targeted by direct attacks.

Direct attack vectors (common) Malware, rogue admins, and privilege escalation

Figure 1. How Intel SGX helps protect data from attacks

Use cases for Intel SGX

With Intel SGX, enterprises can unlock the value of data through increased collaboration with partners, and they can also provide attestation that their systems are patched and uncompromised. Intel SGX provides a layer of defense by helping to reduce the attack surface, allowing users to break down data silos in multiple use cases.

Confidential artificial intelligence (AI) and analytics: AI is one of the fastest-growing workloads in the world. When AI models must train or inference using sensitive, confidential, or regulated data, that data must be protected. Intel SGX not only enables confidential computing solutions that help keep data confidential, it also helps shield proprietary models and software IP from theft or modification.

For example, the BeeKeeperAI program at the University of California at San Francisco (UCSF) required validation of AI algorithms using private datasets that are protected under patient privacy laws. UCSF utilized Intel SGX to accelerate the validation of data and algorithms on innovative medical devices to improve both patient care and privacy. The confidential computing platform enables life-saving clinical AI algorithms to be validated in days instead of years, while helping to secure private patient data and AI algorithms.

Sovereign data/compliance: Companies with a global presence are affected by each country's data privacy, sovereignty, and geolocation regulations. Compliance might require the best available technology and practices to ensure data is not readable by foreign companies or cloud providers. Intel SGX on 3rd Gen Intel Xeon Scalable processors can help companies comply with strict regulations requiring privacy for personal data with security-enabled data enclaves that are inaccessible by software or CSPs.

AOK, a network of 11 regional health insurers in Germany, chose Intel SGX to meet stringent integrity and confidentiality requirements for patients' electronic health records (EHRs). As the German government moves toward a centralized digital health system, compliance with data-privacy laws is a foundational design requirement. Intel SGX was the security technology used to help protect patient EHRs while they were being accessed. Today, centralized AOK e-health and insurance platforms all run on Intel SGX–enabled hardware with a centralized e-prescription platform.

Confidential blockchain: Blockchain technology has many unique properties that make it attractive beyond cryptocurrency uses, such as ownership records of digital assets and supply chain tracking. Some use cases require that records in a ledger be kept private and accessible only by authorized parties. Intel SGX helps protect the confidentiality of blockchain records and limits access to authorized parties, providing the basis for attestation that only authorized, trusted software is allowed to inspect blockchain records.

Blockchain can increase liquidity in the energy trading market and speed up and simplify transactions. But companies don't want to publish private data. Intel SGX technology addresses this problem by creating a privacy-preserving environment that provides underlying proof of funds while maintaining the commercial privacy of the parties involved. Applied Blockchain's platform uses Intel SGX to restrict how data is accessed, and it shrouds transactions behind a privacy curtain. It also provides financial proof and attestation that the data and code are protected.

Leading the way in confidential computing

Intel SGX helps enterprises move confidently into the future and collect, analyze, and store data anywhere. Intel SGX has been deployed in data centers since 2018, with thousands of global deployments. Unlike other confidential computing technologies, Intel SGX can be deployed in virtualized or bare-metal environments using virtual machines (VMs) or cloud-native containers, among other advantages. And the robust Intel SGX software ecosystem offers a variety of ready-to-deploy solutions and developer tools.

Learn more about Intel SGX

Get started with a confidential computing solution today: intel.com/sgx

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Printed in USA 0922/MG/PRW/PDF Please Recycle 352729-001US