Confidential computing with Intel SGX

Deploy zero trust applications and services on virtual machines with Intel SGX support.

What is the SGX type of instance?

The SGX type is a Gcore Cloud virtual machine supporting Intel Software Guard Extensions (SGX) technology. Intel SGX is a set of security-related instruction codes that are built into some Intel CPUs. SGX involves encryption by the CPU of a portion of memory (the enclave).

Data and code originating in the enclave are decrypted on the fly within the CPU, protecting them from being examined or read by other code, including code running at higher privilege levels such as the operating system and any underlying hypervisors.

Why use Intel SGX?

Gcore Cloud Intel SGX provides consistency and confidentiality of computation with extra security requirements that take place on the systems where privileged processes are considered unreliable.

Neither the cloud service provider, nor anyone else from the outside can get into the encrypted area and gain access to the data stored there. Even if, let's say, the servers were hacked.

Cloud features

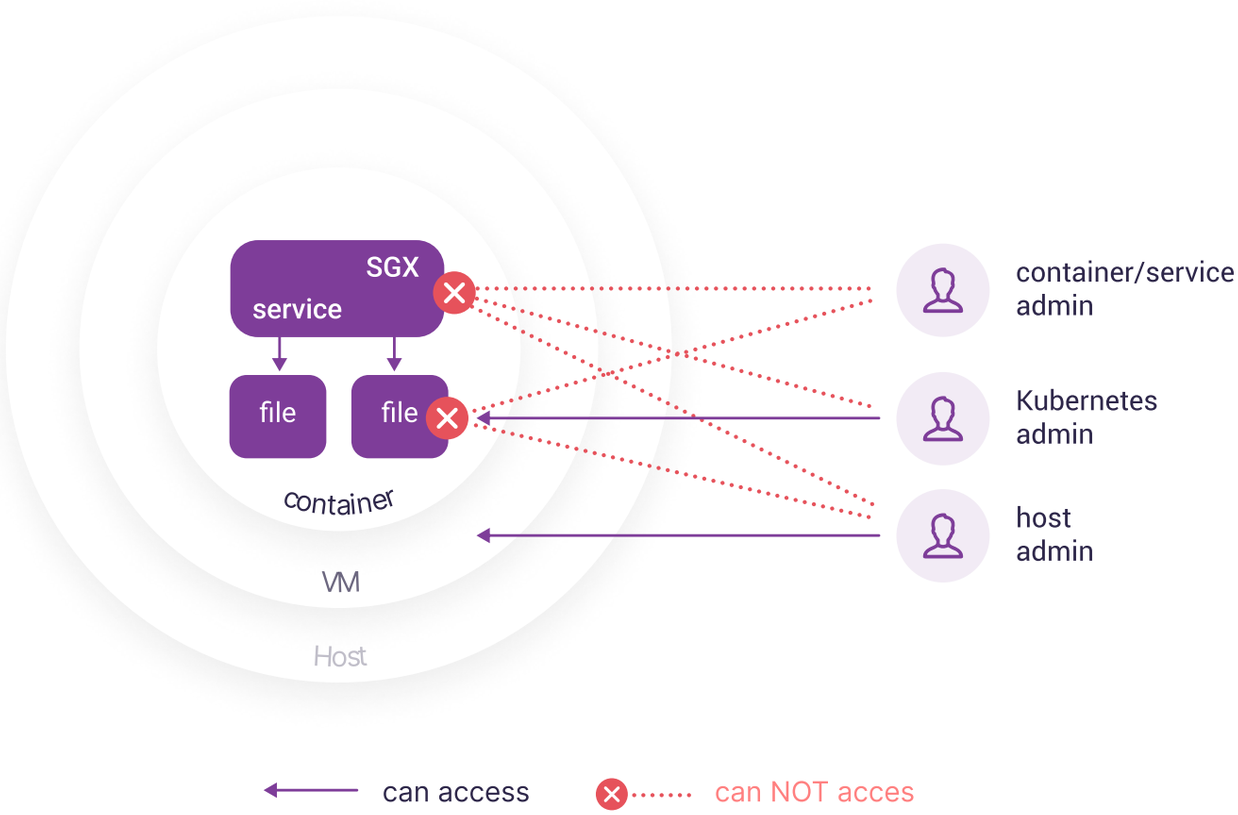
Tier IV data centers
Luxembourg, Amsterdam, Manassas, Frankfurt

L2 connectivity
between bare metal and virtual machines with Intel SGX

High-skilled technical support 24/7

Up to 40 Gbps channels

API, Terraform
management via control panel



Benefits for the key industries

Confidential computing enables organizations to better protect data in use, when it is being actively processed, by placing it in a secure, hardware-enforced area of memory. This is primarily relevant for financial services, healthcare, government, defense, and retail.

Financial crimes detection and prevention

Criminals who commit financial crimes often spread their activity across multiple banks, knowing it is very difficult to detect malicious and anomalous activities that are “one offs” at that institution. If banks could aggregate their data, and analyze an individual’s activity across all banks, malicious anomalies can quickly become more apparent.

Confidential computing with Intel SGX can enable banks to analyze activity data collectively enabling them to comply with strict industry regulations and avoid revealing customer data to competitors. The sensitive underlying data remains private, and only the insights indicating this individual’s activity are highly suspicious because of their overall pattern of activities.

Personalized care and medical outcomes improvement

Patient data is highly confidential, typically requiring healthcare, pharmaceutical, and life sciences organizations to maintain their data in a single, protected location. These smaller, siloed data pools limit their ability to discover optimized treatments for patients.

Confidential computing enables you to aggregate and analyze data across organizations while maintaining data privacy. And that can be key to identifying better treatments and care for individual patients to help improve outcomes.

More use cases

Artificial Intelligence & Machine Learning

Protect your AI and ML workloads and applications while they are running.

Cloud infrastructure

Ensure the confidentiality of customer applications and workloads in public cloud infrastructures.

Trusted multi-party compute/multi-party analytics

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

Secure key management

Use enclaves to help protect cryptographic keys and provide HSM-like functionality.

Blockchain

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

Network function virtualization

Establish trust for virtualized network functions.

Trusted by

WARGAMING.NET · BANDAI NAMCO · RedFox Games · WARPCACHE · SynEdge · avast · NANOBIT · SANDBOX INTERACTIVE · omento solutions · GROUP WAGNER · TEDx · AGENCE eSanté LUXEMBOURG · StageAudioWorks TECHNOLOGY & ENGINEERING GROUP · ZUMIDIAN · SHOPCADA · JSDELIVR · api.video · SABER AN EMBRACER GROUP COMPANY

Contact us and go global faster

Honeypotz is an international leader in public cloud and edge computing, content delivery, hosting and security solutions.
We manage a global infrastructure designed to provide enterprise-level businesses with first-class edge and cloud-based services.

+1 305 390 0563 (US)
+41 44 585 2436 (Switzerland)
1800 409 4960 (US)
sgx@honeypotz.net
Honeypotz.net

Honeypotz