Intel® Security Solution for Fortanix Confidential AI

Solution Snapshot

Confidential Computing with Intel + Fortanix

The Challenge

Data is your organization's most valuable asset, but how do you secure that data in today's hybrid cloud world? How do you keep your sensitive data or proprietary ML algorithms safe with hundreds of VMs or containers running on a single server?

With **Intel® Security Solution for Fortanix Confidential AI**. As a built-in collaboration with Fortanix, it is an enterprise-level, high-performance, security-enabled solution that encrypts data while in use by isolating data and code in Intel® Software Guard Extension (Intel® SGX) enclaves, without changing underlying software applications.

- **Data in transit can be secured** (Network)
- **Data at rest can be secured** (Storage)
- **Now data in compute can be secured** (Cloud – Hybrid Cloud – Edge)

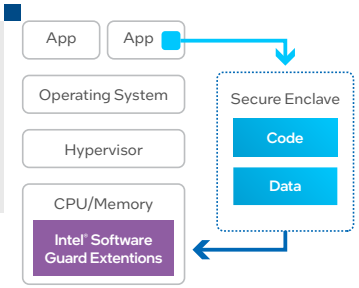
Intel® Security Solution for Fortanix Confidential AI

Security & Performance Features From intel + Turnkey Enterprise-Level Security Services From Fortanix® Confidential Computing Services

Intel® Software Guard Extensions (Intel® SGX)

Intel® SGX isolates software and data from the underlying infrastructure (hardware or OS) in hardware enclaves. Helps defend against common software-based attacks. Helps protect intellectual property (like models) from being accessed and reverse-engineered by hackers or cloud providers.

Intel® SGX is designed to prevent exposure of protected code and data even in the event of a breach in the OS and hypervisor layers.



Intel® oneAPI Analytics Toolkit

3rd Gen Intel® Xeon® Scalable Processors

Fortanix Confidential Computing Manager

A comprehensive turnkey solution that manages the entire confidential computing environment and enclave lifecycle. No application rewriting is required.

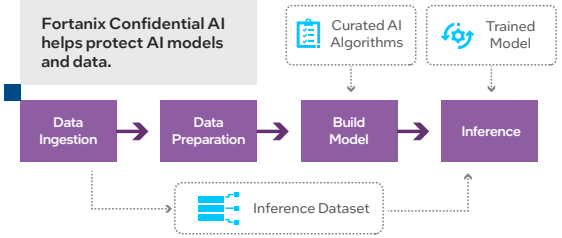
Manages and enforces security policies including identity verification, data access control, and attestation.

Fortanix Confidential AI

An easy-to-use subscription service, which provisions security-enabled infrastructure and software to orchestrate on-demand AI workloads for data teams with a click of a button.

Data teams can operate on sensitive data sets and AI models in a confidential compute environment supported by Intel® SGX enclave - the cloud provider has no visibility into the data, algorithms, or models.

Fortanix Confidential AI helps protect AI models and data.



Fortanix®

Fortanix is a data-first multicloud security company and a confidential computing pioneer. They seek to solve the challenges of data security and privacy across the entire data lifecycle for enterprises that are increasingly migrating to the cloud and hybrid models. Fortanix's unique approach allows businesses to decouple data security from infrastructure and protect data wherever it is located, even when the infrastructure itself is compromised.

Intel + Fortanix Collaboration

Learn more about the collaboration between Intel and Fortanix in these resources:

Intel and Fortanix Confidential Computing Manager — Joint Solution Brief

Data Security Manager with Intel® Software Guard Extensions — White Paper

Solution Benefits

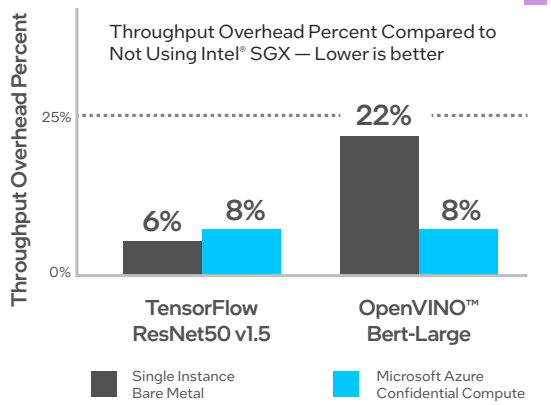
- Enables confidential computing so that (AI) models and data can be shared without exposing intellectual property and sensitive data.
- Delivers a turnkey, enterprise-level, and high-performance security solution without requiring application modifications.
- Addresses time-to-market concerns by providing a validated solution with an installation guide, containerized tools, and sample workloads.

Intel® SGX protects against thousands of known and unknown threats, many of which still do not otherwise have mitigations.[1]

Performance Remains High With Intel® SGX Enabled[2]

Implementing a multiple-instance configuration provides significant throughput gains. These performance enhancements are minimally affected by enabling Intel® SGX, meaning that organizations can simultaneously increase security and performance.

Deep Learning Workload Performance Overhead Using Intel® SGX



Learn More

Intel® Software Guard Extensions

Fortanix Confidential AI

3rd Gen Intel® Xeon® Scalable processors

Intel® Ethernet 800 Series

Intel® oneAPI Toolkit

OpenVINO™ Toolkit

Intel® Optimization for TensorFlow

Contact Your Intel Representative or Visit The Intel® SGX Overview

1 Intel® SGX is not vulnerable to most OS layer threats, and there are over 140,000 threats in the database today: https://cve.mitre.org.

2 Benchmarks were run with Intel® Software Guard Extensions (Intel® SGX) disabled versus Intel® SGX enabled and at both FP32 and INT8 precision.

BARE METAL: Test by Intel as of 01/07/2022. Single node, 2x Intel® Xeon® Platinum 8368 processor (38 cores, 2.40 GHz), Intel® Hyper-Threading Technology = OFF, Intel® Turbo Boost Technology = ON, total memory = 256 GB (16 slots/32 GB/3200 MHz), BIOS = SE5C6200.86B.0022.D64.2105220049, uCode = 0xd0002b1, OS = Ubuntu 20.04.2 LTS, kernel = 5.4.0-050400-generic, compiler version = gcc 9.3.0, Fortanix version = CCM 3.12.810 (3.13.833 for SSD-MobileNet), Node Agent = 3.12.810, framework version = Intel® Optimization for TensorFlow 2.7.0/ OpenVINO™ Toolkit 2021.4.1, Resnet50 v1.5 /SSD-MobileNet/ Bert-Large, Precision FP32/INT8

MICROSOFT AZURE CONFIDENTIAL COMPUTE: Test by Intel as of 01/14/2022. Single Standard DC4s_v3, Intel® Xeon® Platinum 8370C processor (using only 4 cores @ 2.80 GHz), Intel® Hyper-Threading Technology = OFF, Intel® Turbo Boost Technology = ON, total memory = 32 GB, BIOS = Hyper-V UEFI Release v4.1, uCode = N/A, OS = Ubuntu 20.04.3 LTS, kernel = 5.4.0-1067-azure-cvm, Fortanix version = CCM 3.12.810 (3.13.833 for SSD-MobileNet), Node Agent = 3.12.810, framework version = Intel® Optimization for TensorFlow 2.7.0/ OpenVINO™ Toolkit 2021.4.1, model: Resnet50 v1.5 /SSD-MobileNet/ Bert-Large, Precision FP32/INT8

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details.
No product or component can be absolutely secure. Your costs and results may vary.
Intel technologies may require enabled hardware, software or service activation.
© 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.