Case Studies

Finance, Healthcare, Government

Confidential Computing

Intel helps maximize the security, privacy and value of critical data.

"We're seeing a paradigm shift with Confidential Computing."

Ron Perez,
Intel Security Fellow

Executive Summary

Today, more than ever, protecting your company data is mission critical. But data usually resides in siloes, and there isn't an easy way to combine that data and pull business insights from it. *Confidential Computing,* powered by Intel® Software Guard Extensions (Intel® SGX), provides encrypted enclaves that break down these data siloes, not only within your organization, but with external entities—all without ever exposing the data to any of the parties.

Historically, collaboration of this type could expose organizations to serious levels of risk. To address this, leading companies are turning to Confidential Computing as a new approach to security technology that enables you to collaboratively process and consolidate data...without exposing it to others...so you can reap the benefits of data partnerships without compromising data privacy and security.

Intel is working with industry leaders to implement Confidential Computing across a broad range of industries, including financial, healthcare, and the public sector. We're working with a vast array of data types, such as banking information, health records, credit card data, passwords and keys, across an ever-growing number of devices and endpoints (PCs and tablets, phones, cash registers, chip readers, and the devices of tomorrow).

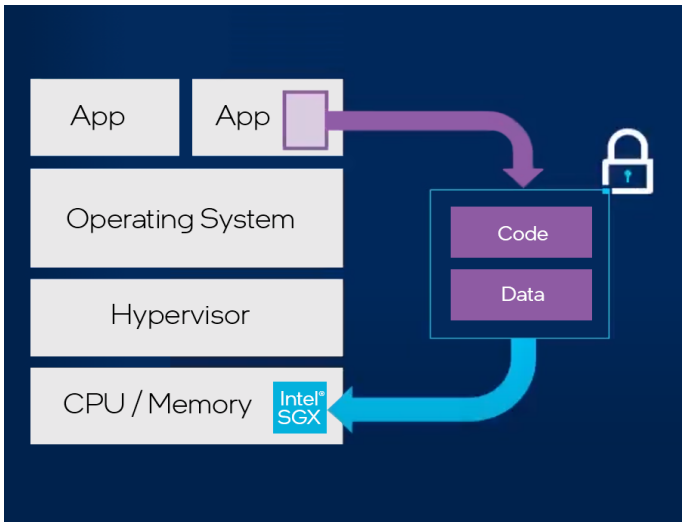
Confidential Computing

Confidential Computing is an emerging industry initiative that focuses on helping organizations keep data secure while it's in use. In essence, it's a secure platform that makes it possible for collaborating organizations to combine, analyze, and generate new knowledge from sensitive data, while ensuring that data (and the algorithms and machine learning processes analyzing it) are not visible or accessible to the rest of the system, or by any human beings—including the collaborators themselves.

Until recently, data security has focused on protecting data at rest (in storage) and in flight (while moving between locations). Confidential Computing, powered by Intel SGX, goes a step further, ensuring data is also protected while it is being processed. This is possible thanks to the creation of a Trusted Execution Environment (TEE). Not only is all critical data stored inside the TEE, but so are the applications and algorithms that access and process that data.

To achieve this, Confidential Computing takes advantage of hardware memory protection to protect against unauthorized access from other applications running on the host system, as well as the host operating system (or hypervisor). Critically, it also prevents access from system administrators, service providers, even the owner of the infrastructure—or anyone else who might gain physical access to the hardware (legitimately or otherwise).

Confidential Computing relies on the hardware it's running on. The Trusted Execution Environment is in fact a hardware-based enclave. Building the enclave in hardware is necessary because protection is needed at each layer of the compute stack, all the way down to the silicon, thus reducing the points of exposure to a minimum.



Intel SGX helps secure the entire compute stack.

The Trusted Compute Base (TCB) is a set of hardware, software, and firmware that is critical to security. Intel SGX keeps the enclave separate and outside of the trust boundary, creating the smallest attack surface to better protect your data. That's especially important in today's cloud-centric world. Even cloud providers are excluded from entry to the TEE. That means many workloads that previously were judged too sensitive to be uploaded to the cloud due to security or compliance concerns can now take advantage of the cost and accessibility benefits of cloud services.

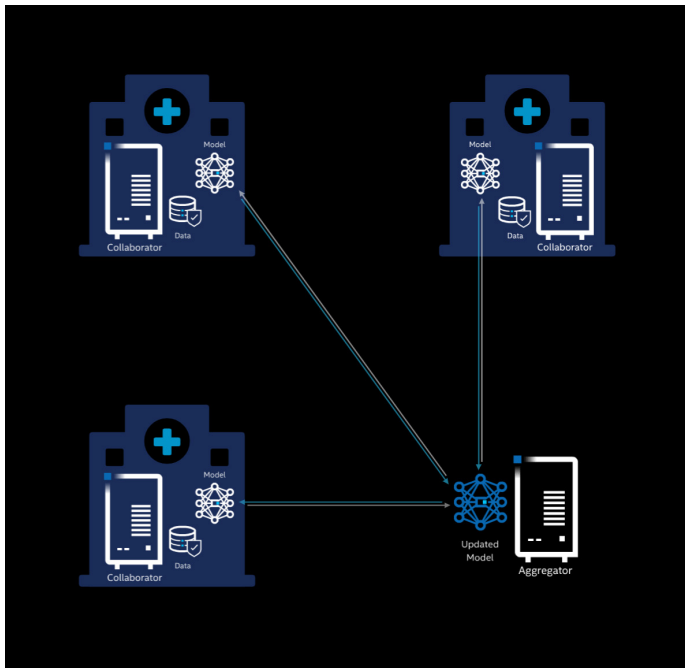
In multi-tenant cloud environments, where sensitive data is meant to be kept isolated from other privileged portions of the system stack, Intel SGX plays a large role in making this capability a reality. Available on the new 3rd Gen Intel® Xeon® Scalable processors, Intel SGX is the product of intense Intel investment in security. The latest version enables larger enclave (TEE) sizes (up to 1TB) to handle larger code and datasets.

Intel SGX also enables additional security innovations, including accommodations for AI architectures such as federated learning, a machine learning paradigm where multiple compute systems are joined together to analyze large or diverse datasets without revealing any confidential information within that dataset.

Uses of Confidential Computing

Confidential Computing enables new use cases that were simply not possible or practical previously. For instance, in many sectors where strict data security is mandatory, developers couldn't take advantage of the cloud to increase user convenience while reducing costs. Intel SGX makes that possible. Similar restrictions prevented developers from implementing solutions using blockchain technologies. Now they can. And even older, existing apps can benefit. Now developers can create secure containers within the TEE and upload the old app into that container, where it will benefit from the same level of security as any other application in the enclave, without impacting processing time using crypto accelerators. Now customers no longer need to choose between security and processing speed.

Another important use of Confidential Computing involves the ability for separate organizations to share data while at the same time knowing that their data will remain theirs and theirs alone. This provides the opportunity for companies to collaborate—even if they are competitors. For instance, two pharmaceutical companies working on vaccine development could use Confidential Computing techniques to combine their two separate research datasets into one aggregate dataset within a secure enclave. Once the data is in the enclave, even the owners of the datasets can't see the contents inside. But AI applications and algorithms can still access this new, combined dataset, train on the data in it, run inference operations, and generate new conclusions that would have been impossible previously. This type of federated learning allows separate institutions to collaborate and benefit from models with improved outcomes—while at the same time remaining confident that their data is private.



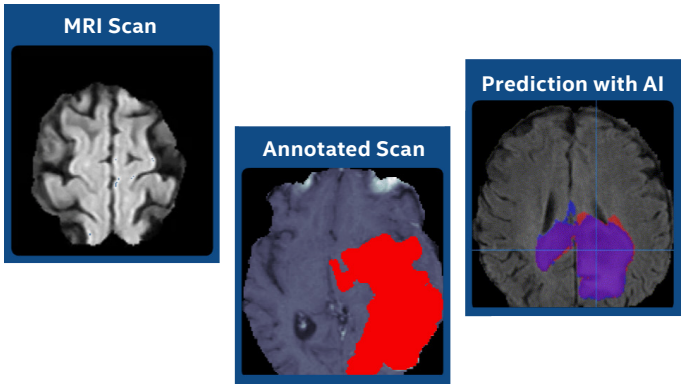
Data from multiple collaborators is shared securely in the aggregator.

A wide variety of industries can benefit from Confidential Computing...

Confidential Computing is providing new opportunities for Healthcare

Federated learning can enable medical institutions to work together to improve patient care. For instance, they could significantly improve treatment models. One example is radiologists who annotate brain MRI scans to detect and localize tumors. Scans provide the necessary data to train deep learning models to assist in this task. Federated learning now provides the ability to capture expertise from radiologists around the world in a single AI model, providing invaluable assistance to clinicians and faster diagnosis and treatment for patients. This would be especially true in AI-

enabled triage, where time-sensitive cases could be brought to the attention of a radiologist more quickly.



Other healthcare use cases include:

- Contact tracing
- Insurance fraud detection and protection
- Vaccine development

Confidential Computing is providing new opportunities for Financial organizations

Banks, brokerages, and other financial organizations can also benefit from Confidential Computing. For instance, institutions could collaborate on anti-money laundering efforts by partnering to create a governance network where they share transactional data. They could upload data to a centralized node where AI algorithms provide risk-based assessments, allowing organizations to spot high-risk individuals—without sharing full transaction history data.

Other financial examples include:

- Analyzing loan applications and granting approvals
- Detecting fraud and digital theft
- Looking for suspicious activities on commercial websites
- Calculating rates for coverages and services
- Tracking credit histories and generating credit scores
- Accessing financial products more quickly
- Taking advantage of currency and arbitrage opportunities

Confidential Computing is providing new opportunities for Governmental organizations

Public sector organizations, who often work under strict confidentiality requirements, could use Confidential Computing to solve problems that were extremely difficult (or impossible) before. Different governmental agencies working in related fields could better cooperate to serve the public good. For instance, the U.S. Center for Disease Control and the U.S. Food and Drug Administration could combine confidential datasets dealing with vaccine development and generate results that neither agency could have arrived at alone—with zero exposure of sensitive data.

Other governmental examples include:

- Public infrastructure
- Cybercrime prevention
- Intelligence analytics
- Collaboration with other countries (and other states)
- Monitoring and using digital currencies

In addition, industries such as Retail, Hospitality, Manufacturing, and Education also could benefit from promising opportunities to utilize Confidential Computing.

Intel Teams Up with Industry Leaders

In working to make Confidential Computing available to the world, Intel is collaborating with leaders in various industries to tailor solutions that will maximize the benefits of this new technology.

Intel, Swisscom, and Secretarium

Intel is working with these partners to enable customers to exchange business-critical documents via the cloud. Doing so promises to greatly accelerate critical business processes, while still meeting the highest standards of data security and confidentiality. Projects are currently underway in South America, Europe, and Asia.

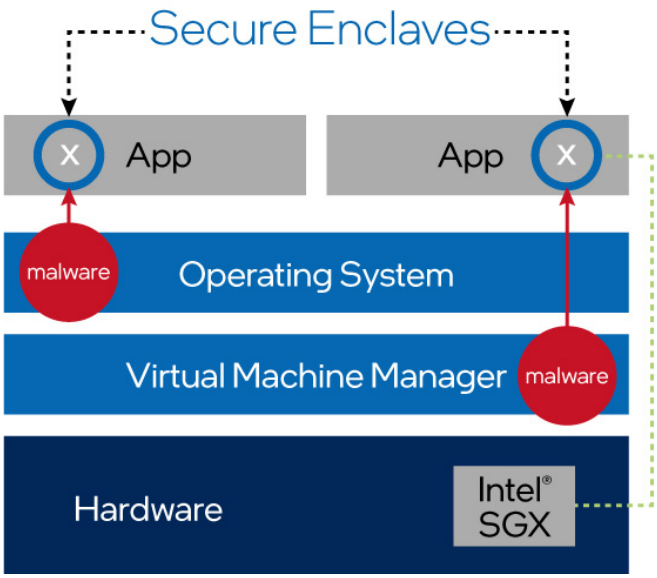
swisscom

secretarium
THE SECURE CLOUD

To meet the challenges that international trade presents, Intel, Swisscom, and Secretarium worked together to develop the Secure File Exchange (SFX) program. SFX makes possible

the fast, reliable exchange of encrypted data between companies.

SFX is easy to use and meets the highest requirements of security and confidentiality. All data resides on servers located in Swisscom data centers. Only the owner can access secure data—and that includes Swisscom, the platform developer and service provider. Intel SGX ensures that all data remains encrypted, even during processing.



Secure enclaves provide a high level of security.

Intel and Swisscom expect broad demand for the platform in the trading and finance sector. "The need for higher levels of security and confidentiality will only increase as multi-party business processes, collaboration and transactions move online," said Jason Grebe, Corporate Vice President of the Cloud and Enterprise Solutions Group at Intel. "Innovators like Swisscom that apply Intel SGX technology to their cloud services provide new levels of protection to data in-use, harnessing the industry's most tested, widely-deployed hardware-based data center trusted execution environment."

"It is a privilege for us to innovate together with leading international technology companies such as Intel to develop this platform for secure data exchange between companies."

Christoph Aeschlimann, CTO & CIO Swisscom

Intel and Consilient

Money laundering and the financing of terrorism around the world are critical issues in today's financial industry, with trillions of dollars at risk each year. But current anti-money laundering (AML) measures, like those countering the financing of terrorism (CFT), haven't kept pace with the corrosive threats and abuse of the international financial system.

To help meet this threat, Consilient has developed a new model for AML/CFT that moves beyond traditional rules-based monitoring and facilitates the secure sharing of information around the globe, while at the same time enabling collective learning about complex threats.

Based on federated learning, Consilient's solution is a behavior-based, Machine Language-driven governance model that allows its algorithms to access and interrogate data sets in different institutions, databases, and even jurisdictions without ever moving the data.

Hardware-based security technologies are critical for federated learning. Security layers can be implemented down to the silicon inside the compute node, or server, through the Trusted Execution Environment (TEE) enabled by Intel SGX. Intel SGX minimizes the trusted computing base in order to reduce the surface area for attacks (including attacks against data stored in memory). It also supports hardware-based attestation to measure and validate code and data signatures, increasing the confidence level for all partners.

Intel and eperi

More and more organizations are adopting a server-less, cloud-first architecture approach—even in highly regulated industries like finance and banking. But this process can be hampered by data security concerns and the need to comply with government rules and regulations.

When a top tier bank wanted to share and distribute restricted data internally and aggregate reports and analytics based on all types of datasets, eperi had a solution. The eperi Cloud Data Protection Solution, combined with Intel SGX, helps protect data in the cloud at all times—even when that data is being processed in analytics and AI operations.

In a proof-of-concept, the bank worked with eperi to allow data to securely move to the cloud by encrypting that data on the way out of the network using the eperi Gateway. Microsoft Azure Confidential Computing with Intel Software Guard Extensions allows computation of the data in the cloud in a privacy-preserving manner to build a cloud-based data analytics platform.

The eperi Gateway is currently the only solution in the world that supports hybrid multi-cloud environments. Cloud providers build "distributed clouds" to provide services at the point of need, giving customers new opportunities with anywhere operations.

Summary

With the constant demands being placed on data security, Confidential Computing is sure to be a critical part of leading organizations' in-depth cybersecurity defense strategy. "We're seeing a paradigm shift with Confidential Computing," said Ron Perez, Intel Security Fellow.

Given the critical nature of the challenge, once organizations have experienced the security and benefits of Confidential Computing, they will find more and more uses for it. And with this ground-breaking technology, based on Intel technologies, they will have the scalability they need to quickly and confidently take advantage of new opportunities—and meet new threats and challenges—as they arise.

Learn more

Intel.com

www.intel.com/content/www/us/en/security/confidential-computing.html

www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html

www.intel.com/content/www/us/en/big-data/partners/microsoft/overview.html

Confidential Computing Consortium

https://confidentialcomputing.io

Microsoft

https://azure.microsoft.com/en-us/solutions/confidential-compute

Swisscom

https://www.swisscom.ch/en/about/news/2020/12/09-secure-file-exchange.html

Consilient

https://consilient.com/whitepaper/federated-learning-through-revolutionary-technology

eperi

https://eperi.com