Solution Brief

Cybersecurity
Hardware-Level Encryption

Help Prevent Data Loss with Fortanix Confidential Computing Manager

Powered by Intel® Software Guard Extensions (Intel® SGX), the Fortanix Confidential Computing Manager helps protect sensitive data, allowing businesses to better secure personally identifiable information throughout the data life cycle.

Fortanix®
The Runtime Encryption® Company

"Fortanix Confidential Computing Manager optimizes the capabilities of Intel® SGX enclaves to enable increased security for keys, data, and applications throughout the data life cycle."

—Ambuj Kumar, CEO and cofounder, Fortanix

Stop attacks before they become breaches with advanced hardware-level encryption

Personally identifiable information (PII) from financial transactions, medical records, social media sites, and other digital platforms is highly sensitive data that must be secured. When PII is exposed or stolen, consumers and businesses can be damaged on many levels and suffer significant financial losses.

For healthcare providers, financial services firms, retailers, manufacturers, and public sector agencies, securing PII is a critical function. As security technologies continue to advance, so do the tactics and technological assets of cybercriminals. Equipped with intelligent, high performance computing systems and applications, hackers today have sophisticated tools they can leverage to exploit vulnerabilities in even the most secure and trusted systems and environments worldwide.

In 2020, 155.8 million people in the United States were affected by data breaches that exposed their PII.[1] And incidents of data breaches are on the rise. Going forward, both private and public sector entities must modernize their data security solutions and strategies to keep pace with advances in cybercrime and prevent the devastating effects of data leaks and breaches.

Powered by Intel® Software Guard Extensions (Intel® SGX) security technology, Fortanix Confidential Computing Manager uses comprehensive hardware-level encryption to protect data in use, which is data that is actively being processed by a central processing unit (CPU) or in random access memory (RAM). This added layer of security is essential today as hackers continue to search for new, vulnerable points of entry into systems and applications—and as organizations increasingly migrate data processing to public clouds and other untrusted infrastructure.

Challenges: Protecting data in use and preventing cloud breaches

Data today is typically encrypted at two critical stages of its life cycle:

- At rest, when stored in persistent storage
- In transit, as it passes from one location to another—such as across the internet or through a private network

This two-part approach has historically been effective in preventing data breaches because storage and networking devices were the primary targets of hackers. As new intelligent security technologies have made it more difficult to access data at rest and in transit, hackers are refocusing their efforts on a new target: data in use. Accordingly, it is essential for businesses to take the steps needed to protect sensitive data while it is being processed by applications.

Consider also that more than 81 percent of organizations are currently using multiple cloud providers.[2] As data increasingly migrates to the cloud, gaps can form between network security and physical perimeter security solutions, leaving cloud data exposed to threats. In fact, attack patterns against cloud-based code are increasing due to insider threats, firmware compromises, and both hypervisor and container breakout. In the age of cloud computing, security strategies must be designed to protect all data throughout its life cycle, from the edge to the cloud.

The solution: Fortanix Confidential Computing Manager

To address these pressing challenges affecting all sectors of business and industry, Fortanix has developed its Confidential Computing Manager, featuring Intel SGX security technology. Built into 2nd and 3rd Generation Intel® Xeon® Scalable processors, Intel SGX allows organizations to isolate software and data from the underlying infrastructure (hardware or OS) by means of hardware-level encryption. This more secure execution environment, known as an enclave, creates a region of memory that is inaccessible to any process other than the application itself. Confidential Computing Manager manages Intel SGX enclaves by providing visibility into all running enclaves and establishing trust between them via Intel SGX's remote attestation functionality.[3]

In leveraging the capabilities of Intel SGX, Confidential Computing Manager hardens the environment for data in use and cloud data.[3]

Examples in market today

The University of California San Francisco's (UCSF) Center for Digital Health Innovation (CDHI) is using Intel SGX and Fortanix Confidential Computing Enclave Manager to help streamline certification of breakthrough medical devices with embedded artificial intelligence (AI) capabilities.

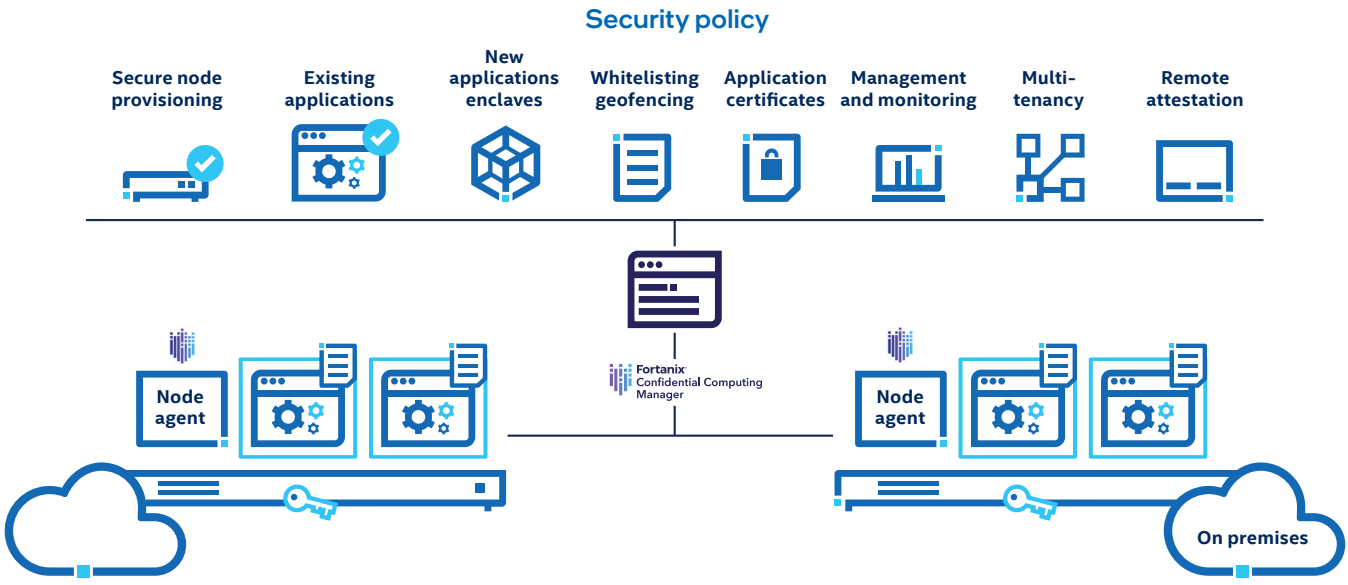
In financial services, Consilient, a company dedicated to establishing a next-generation system for anti–money laundering and countering the financing of terrorism (AML/CFT), launched a new, secure, federated learning platform powered by Intel SGX.

How it works

With Confidential Computing Manager, all code and sensitive data used in an application are stored in an Intel SGX enclave and encrypted with a key. On every boot, the 3rd Gen Intel Xeon Scalable processor randomly generates a new, unique encryption key for the enclave based on a secret already provisioned in the processor. Keys are only used by the hardware, with 3rd Gen Intel Xeon Scalable processors performing memory encryption and decryption without any software support. As a result, applications remain protected from vulnerabilities related to higher-privileged processes.

Plus, keys are not stored in any persistent storage and are not present in the random-access memory (RAM) either, further protecting the enclave from compromises.

Confidential Computing Manager also meets the needs of developers by providing a secure enclave development platform (EDP). This EDP allows developers to write to Intel SGX enclaves from scratch using the Rust programming language, which, by design, optimizes the security features in Intel SGX technology.



Ultimately, Confidential Computing Manager is so effective that Intel SGX secure enclaves remain protected from unauthorized access even when the surrounding compute infrastructure is compromised.[4] This means that data is secured when sensitive applications are run on untrusted infrastructure such as public clouds and other hosted environments. The ability to protect data and code in these types of environments makes it safer for organizations to collaborate with external entities, including their partners and customers.

Confidential Computing Manager is the only turnkey solution on the market today that manages the entire confidential computing environment and enclave life cycle, delivering these key benefits:

- Protection of data at rest, in transit, and in use
- A more secure environment for collaborating with external entities, including partners and customers
- More control over cloud data so workloads can be migrated to the cloud with confidence
- Better prevention of insider attacks and unauthorized access to sensitive data
- Attestation functionality to help ensure the integrity and confidentiality of data, code, and applications
- Better performance of existing applications, enclave-native applications, and prepackaged applications for reduced development and integration costs
- Simplified management and enforcement of security policies, including identity verification, data access control, and attestation, to protect the privacy of data, code, and applications
  - Support for geofencing and compute affinity for compliance with regulations such as GDPR
  - Access to audit logs used to verify that compliance requirements have been met
- Available as a SaaS service in Azure portal

3rd Gen Intel Xeon Scalable processors drive Intel SGX technology

Featuring Intel SGX technology, 3rd Generation Intel Xeon Scalable processors provide advanced security capabilities that can be used in concert with existing infrastructure to enhance and protect the most sensitive portions of a workload or service. Intel SGX helps protect against many known and active threats by adding another layer of defense that reduces the attack surface of the system. Intel SGX's hardware-based memory encryption isolates specific application code and data in memory. Because sensitive information is partitioned into enclaves, it is secured from both external and internal threats, including higher-privileged processes. With Intel SGX, keys are protected as well, both at rest and in use, for added security whenever data is being processed. Only Intel SGX offers such a granular level of control and protection.

Intel and Fortanix—securing data and applications wherever they are processed

Preventing data loss and breaches is essential to every industry. As hackers continue to target data in use and cloud-based code, it is vitally important to provide better protection for these critical computing assets. Fortanix leverages Intel SGX technology in its Confidential Computing Manager to protect data and applications at the highest levels. Beyond data protection, Confidential Computing Manager serves application developers with a complete solution for building and running enclave applications. By verifying the integrity of confidential computing environments and managing the enclave application life cycle, Fortanix Confidential Computing Manager enables applications to run securely anywhere they are needed, from the edge to the cloud.

About Fortanix

Fortanix is a data-first multicloud security company solving the challenges of cloud security and privacy. Fortanix empowers customers to secure their data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at rest, in motion, and in use.

fortanix.com

Learn more

Fortanix Confidential Computing Manager

Visit the website ›

Intel Software Guard Extensions

Built into 3rd Gen Intel Xeon Scalable processors, Intel SGX technology increases the security of application code and data, adding an essential layer of protection from disclosure and modification.

Learn more ›

intel + Fortanix®

1. Johnson, Joseph, "Cyber crime: Number of breaches and records exposed 2005–2020," Statista, March 3, 2021. statista.com/statistics/273550/data-breaches-recorded-in-the-united states-by-number-of-breaches-and-records-exposed/
2. Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2020. gartner.com/en/conferences/apac/infrastructure-operations-cloud-india/featured-topics/cloud
3. Fortanix Runtime Encryption Platform, Fortanix, 2019. resources.fortanix.com/hubfs/Fortanix_RTE_Platform_Whitepaper.pdf?utm_medium=email&_hsmi=76308087&_hsenc=p2ANqtz-9O25DOfa2dy8UnuQJyHq6fI7zHg-tiRsXG_PwY0d1EKyxOqnQ7B8HaCnhZoaEm5D0sDIgu8apq2-hrP7UQ1CLaMe4KYg&utm_content=76308087&utm_source=hs_automation
4. No product or component can be absolutely secure.