Solution Brief

Life Sciences
Security

Fortanix and Intel are Helping Secure Life Sciences Data through Confidential Computing and Enclave Processing

Fortanix Partners with Intel to Help Life Sciences Organizations Reduce Cost and Complexity, Uphold Regulatory Compliance, Centralize Control and Visibility, and Continuously Manage Security

About Fortanix

Fortanix secures data, wherever it is. Our data-first approach helps businesses of all sizes to modernize their security solutions on-premises, in the cloud and everywhere in-between. Enterprises worldwide, especially in privacy-sensitive industries like financial services, fintech, healthcare, government, and retail, trust Fortanix for data security, privacy, and compliance. Fortanix is a founding member of the Confidential Computing Consortium of the Linux Foundation. The Confidential Computing Consortium (CCC) brings together hardware vendors, cloud providers, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards.

Life Sciences Data Requires Multilayered Security

Whether it's molecular structures, manufacturing recipes, clinical trial recruitment data, or real-world evidence, life sciences datasets can unlock life-changing innovation in today's data-driven world.

The typical network and data environment for a life sciences organization is complex as companies need to store, process, and transport data and workloads across disparate locations. The sensitive nature of these datasets adds further difficulty as they become appealing to unauthorized users and runtime tampering. To further add intricacy, the datasets are often sourced or acquired through varying contractual agreements with multiple organizations and each of these organizations set their own requirements.

Securing the Entire Data Lifecycle

Data can exist in three states: at rest in storage, in use during processing, and in transit traversing across the network. Each of these stages possesses its own set of vulnerabilities for cyberattacks or unauthorized access. To help prevent cyberthreats, most security solutions leverage cryptography or encryption methods at different states of the data lifecycle, and most do not secure all three states. Securing the entire lifecycle would require integrating multiple applications and relevant components, but this often leads to significant resource investments and financial cost.

Confidential Computing Transforming Data and Workload Security

To uncover tomorrow's life sciences breakthroughs, organizations within the industry need a turnkey solution that streamline the integration of multiple infrastructure components while upholding environment confidentiality and varying regulatory compliance standards. This can be achieved through Confidential Computing and its Trusted Execution Environments (TEE), which provide a level of assurance of data integrity, data confidentiality, and code integrity. The hardware-based TEE uses a hardware-level memory encryption location, called enclaves, which isolate sensitive assets from other users or programs running on the same machine or cloud server by coding security-related instructions into a separate secure enclave processor that handles sensitive data and performs processing.

Fortanix Unlocks the Power of Confidential Computing

Fortanix has played a prominent role in advancing life sciences security measures with the Confidential Capabilities in its Data Security Manager™—a complete, intuitive solution that enables applications to run in confidential computing environments, verify the integrity of those environments and manage the enclave application lifecycle using the Enclave Development Platform.

Enclave Development Platform

Fortanix Enclave Development Platform (EDP) seamlessly integrates with Intel® Software Guard Extensions (SGX) to write enclaves from scratch. Through EDP, developers can build the application using the Rust programming language. The Rust language, combined with Intel® SGX, helps make the application more secure from development vulnerabilities and outsider attacks.

Intel® SGX

Intel® SGX technology represents one of the leading implementations of Confidential Computing. Using Intel® SGX allows life sciences organizations to isolate the software and data from the underlying infrastructure (hardware or OS) by means of hardware-level encryption.

Powering Confidential Computing through Intel® Software Guard Extensions (SGX)

Intel® SGX offers hardware-based memory encryption to protect data in use by allowing user-level code to be deployed within enclaves that isolate the application code and processed data.

The solution bypasses the operating system and virtual machine layers to enable confidential computing, while adding an additional layer of protection against today's most critical cyberattacks which include a myriad of more common software-based attacks.

Life sciences organizations can utilize Intel® SGX attestation mechanisms to enable verification requests that check for compromised applications, as well as ensuring that the CPU on which applications are running has the latest security updates.

Intel® SGX technology offers the smallest trusted computing base (TCB). This offers a clear strategic advantage for industries that have strict data privacy and security requirements.

Intel® SGX Reduces the Attack Surface Across Hardware, Virtual Machine Monitoring and Operating Systems

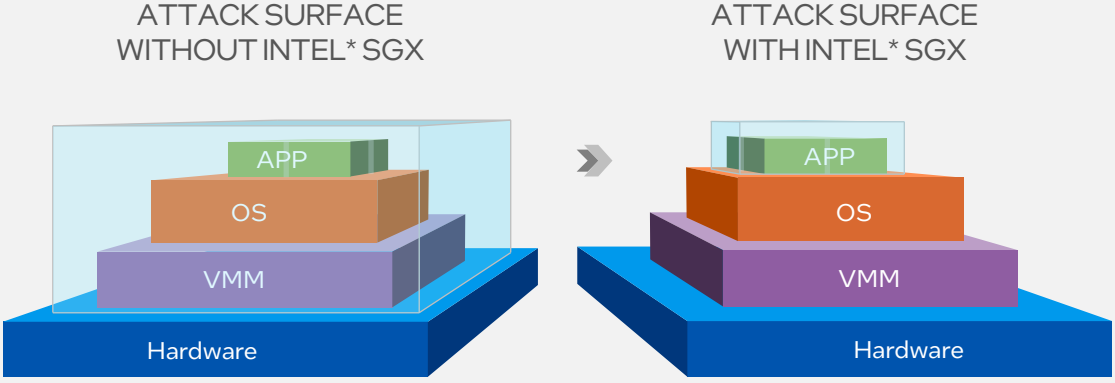

Figure 2 – REDUCTION OF ATTACK SURFACE WITH INTEL* SGX

Translating Fortanix Capabilities to Business Benefits

Leverage cutting edge security to automate and customize security to meet your specific needs.

Life Sciences Security Obstacles	Fortanix	Life Sciences Business Benefits
Manage Complex Security Manually Confidential computing requires the integration of multiple infrastructure components, rewriting applications and manually configuring and verifying applications running in enclaves across multiple environments and with varying lifecycles	**Simplify Enclave Lifecycle Management** Offers a turnkey solution that manages the entire confidential computing environment and enclave lifecycle.	**Reduce Cost and Complexity** Enables secure migration of sensitive data such as clinical records to cloud environments, ultimately consolidating or replacing multiple security solutions
Engage in Lengthy Re-write Applications Process Running an application in a secure enclave requires developers to take a significant amount of time to rewrite applications using open-source SDKs, which often discourages the use of confidential computing	**Offer Broad Set of Application Support** Enables existing applications, enclave-native applications, and pre-packaged application to run in a secure enclave in minutes. This capability in unique and enables widespread adoption of confidential computing with no development or integration costs.	**Centralize Control and Visibility** Manages multiple security services from a unified web-based user interface that segments visibility, dependent on security clearance, using features such as role-based access control for users
Build Security Stack from Scratch Securely implementing confidential computing requires critical services for authentication, encryption, attestation, and audit to ensure the integrity and confidentiality of data, code, and applications. These services are not built-into the infrastructure.	**Secure Cryptographically Enforced Policy and Auditing** Manages and enforces security policies including identity verification, data access control, and attestation to ensure the integrity and confidentiality of data, code, and applications. Using these policies, businesses can implement geo-fencing, and compute affinity to support data regulation policies such as GDPR and Schrems II. Fortanix also provides audit logs to easily verify compliance requirements.	**Protect Continuously** Manages and enforces to help secure data and application pathways even while the asset is in use, while applying multi-party analytics that can potentially help improve patient treatments and outcomes **Uphold Regulatory Compliance** Achieves HIPAA, GDPR, GXP and other organizational governance by substituting electronically protected information with anonymized information

Conclusion

Data security is essential for life sciences organizations to unleash the power of their data and gain valuable insights for tomorrow's next big breakthrough. Taking this into account, Fortanix and Intel are helping to create a safer, more connected future that allows customers to reduce cost complexity, improve regulatory compliance, centralize control and visibility, and continuously help protect the most sensitive of data.

Learn More

- Fortanix Website
- Fortanix Confidential Computing Home Page
- Fortanix Enclave Development Platform Home Page
- Intel® Software Guard Extensions Product Page
- Intel® Xeon® Processors Product Page

intel

Notices & Disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's Global Human Rights Principles. Intel® products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

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 does not control or audit third-party data. You should consult other sources to evaluate accuracy. Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

© 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.