Business Brief

Life Sciences
Security

Integrating Security Principles to Build, Design, and Support Tomorrow's Life Sciences Innovations

Intel delivers advanced, interoperable hardware-rooted security by integrating innovative technologies to help protect against today's most sophisticated cyber attacks.

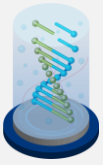
High Value Life Science Data

Patient Clinical Records

Proteomics

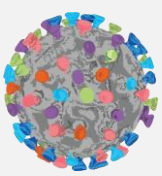
Clinical Trial Recruitment

AI Model and Analytics Workload

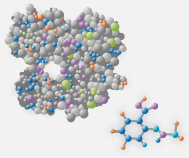


Genomics

Institutional Review Board Records



Molecular Structures



Pharmaceutical and Biologics Trade Secrets

Life Sciences Big Data Vulnerabilities

Life sciences organizations possess vast amounts of vitally important data and workloads, which normally hold highly sensitive clinical/lab information. These datasets and workloads are highly attractive to inside and outside cyber threats due to financial and legal liabilities organizations face for failing to secure these data. Data leaks can result in billions of dollars of revenue lost, supply chain infiltration, patient harm from device tampering, exposed patient information, regulatory and compliance violations, costly ransomware threats, and reverse identification of personally identifiable information (PII).

The Need for Life Sciences Data Security

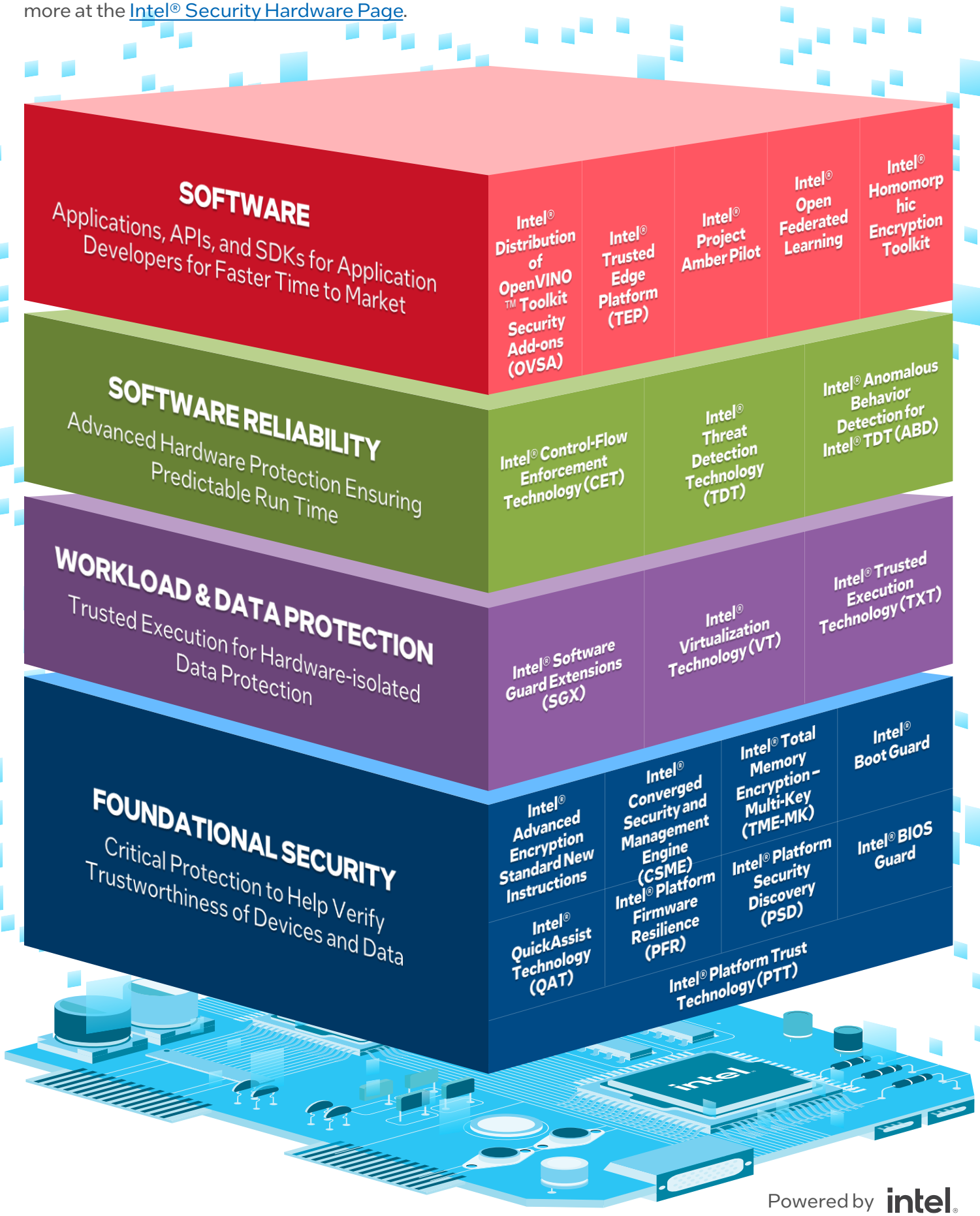
Concerns surrounding data protection, be it HIPAA, GDPR, or proprietary information, combined with regulatory compliance increases the complexity of industry collaboration and joint development. These industry obstacles have made physical collection of data a standard process for laboratory environments. And they create a need for secure solutions and technologies such as sophisticated analytics and model building to access and store sensitive data without needing to be centralized in one place to enable industry collaboration. Intel security technologies strive to standardize, embrace, and help protect the digital data ecosystem to enable easier storage, access, obtainment, analysis, collaboration, and data correlation without losing control of the environment(s).

Life Sciences Security Consideration Unlocking AI Opportunities

In today's digital world, attack sophistication is quickly evolving, which is why Intel focuses on enabling cutting edge solution architecture designed with a multi-layered security approach that extends across hardware, firmware, and software. Intel is heavily investing in confidential computing and offers a portfolio of silicon-enabled security technologies and software to help create a trusted foundation, improve software resilience, and help secure sensitive datasets and workloads.

Intel Partnerships Help Innovate Life Sciences Security

Intel offers a fully scoped stack of solution and hardware products that accelerate performance and improve security. For more product information regarding Intel® security software, software reliability, workload and data protection , and foundational security categories see page 6 or learn more at the Intel® Security Hardware Page.

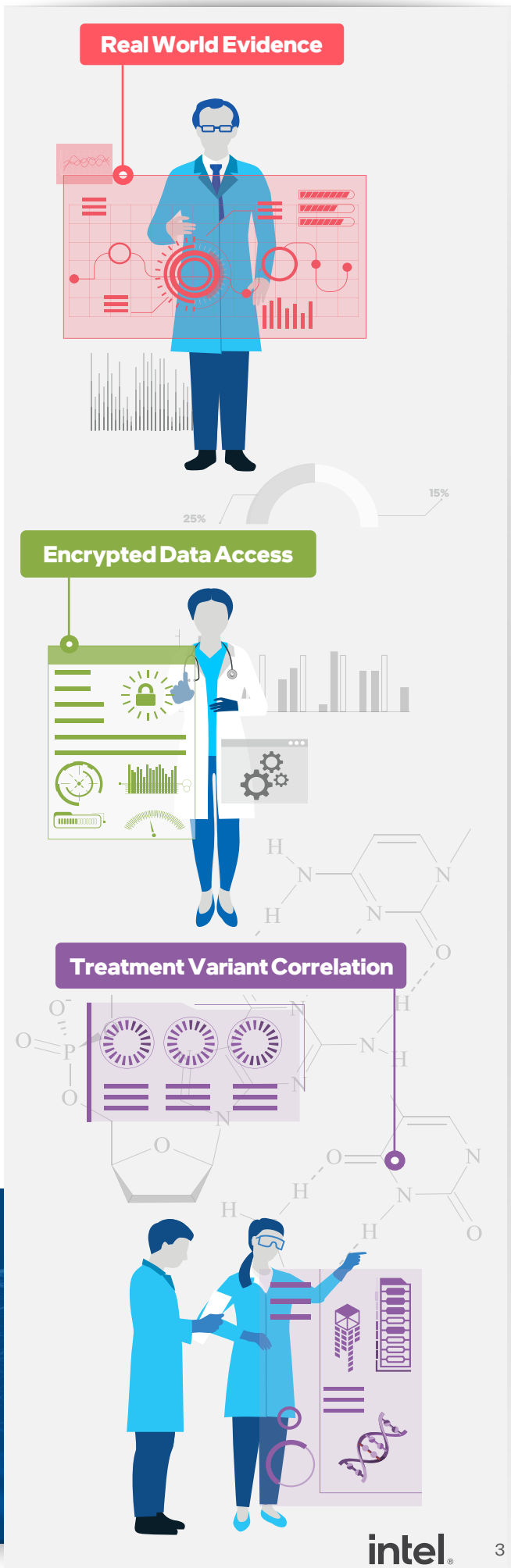


Duality Addresses Real-World Concerns by Leveraging the Value Intel Brings to Security in the Life Sciences Space

Intel is a trusted advisor in the life sciences ecosystem. When partnering with Intel in life sciences, organizations gain access to the whole industry partner ecosystem. Intel is matchmaking and building solution coalitions to address specific pain points and use cases.

For example, real world evidence studies are the engine of medical and pharmaceutical innovation – but concerns around data privacy, security, regulation, and confidentiality make collaborative medical data analysis cumbersome. To alleviate this issue, Duality created a solution, built on high performing 3rd Generation Intel® Xeon® Scalable processors with built-in AI plus encryption accelerators. By optimizing fully homomorphic encryption performance on Intel platforms, the integration makes privacy-preserving data analytics scalable, allowing enterprises to enable multiple parties to compute more securely on sensitive data while preserving privacy, confidentiality, and regulatory compliance.

Leveraging federated learning algorithms, organizations can centrally orchestrate sensitive data like linking patient health records from disparate locations. By augmenting federated learning with homomorphic encryption, Duality uniquely helps prevent leakage of intermediate federated model training results. The solution enables performing statistical analysis, fitting regression models, and applying survival analysis while the data always remains protected by federation and encryption. Then using homomorphic encryption that can be significantly faster than most cutting-edge methodologies[1], the solution enables analysis such as validating data correctness, performing statistical analysis, fitting regression models, and applying survival analysis without need for decryption. All data owners remain in control of how their data is used during the collaboration process. With Duality, customers can unleash the full value of AI while minimizing risk by making privacy-enhanced coloration a competitive advantage for the life sciences industry.



About Duality

Founded by world-renowned cryptographers and expert data scientists, Duality empowers organizations to more securely collaborate on sensitive data with their business ecosystem: customers, suppliers, and partners. By operationalizing Privacy Enhancing Technologies (PETs), Duality enables more secure analysis and AI on encrypted data—while complying with data privacy regulations and protecting valuable IP.

Intel Partnerships Help Innovate Life Sciences Security

BeeKeeperAI, Inc. and Fortanix

BeeKeeperAI, Inc. is using Fortanix Confidential Computing Manager™, integrated with Intel® Software Guard Extensions and backed by Microsoft Azure, to improve patient care and privacy while accelerating the validation of device data.[2]

Conclusion

Security will continue to be one of the top concerns for life sciences organizations. Therefore, Intel and its partners are helping build revolutionary solutions designed to more safely and securely handle environment complexity. Customers can now harness big data using advanced AI techniques that can offer valuable use cases such as treatment variant correlation all while conducting real-time detection of behavioral threats, reducing the spread of malware, and analyzing without the need of encryption.

Learn More

Find more information by contacting health.lifesciences@intel.com or through the links below:

- Intel® Healthcare and Life Sciences Home Page
- Intel® Security Hardware Page.
- Intel® Hardware – Enabled Security Web Page
- Intel® Xeon® Processors Product Page
- Intel® Virtualization Technology Product Page
- Intel® QuickAssist Technology Product Page
- Intel vPro® Product Page
- Intel® Threat Detection Technology Web Page
- Intel® Platform Firmware Resilience Product Page
- Intel® Distribution of OpenVINO™ toolkit Product Page
- Intel® Homomorphic Encryption Toolkit Product Page
- Intel® OpenFL Product Page
- Duality Website
- Duality Solution Page

Sources

1. Duality, Protecting Privacy in Genome-Wide Association Studies (GWAS), 2022
2. Intel, Intel SGX Helps BeeKeeperAI, Inc Medical Device Innovations, 2020

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.

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.

All product plans and roadmaps are subject to change without notice.

Intel® Layering Security to Meet Specific Needs

Software : Applications, APIs, and SDKs for Application Developers for Faster Time to Market

Intel® Distribution of OpenVINO™ Toolkit Security Add-ons (OVSA)
Built with Intel® Distribution of OpenVINO™ toolkit Model Server, manage AI models across software infrastructures and labs with secure packaging, licensing, and access control.

Intel® Trusted Edge Platform (TEP)
Ready-to-configure software framework to make it easier for developers to implement underlying security capabilities accelerating time to market.

Intel® Project Amber Pilot
A multi-cloud, multi-trusted execution environment service for third-party attestation. Contact ProjectAmber@intel.com for early access program information

Intel® Open Federated Learning
Enables secure data collaboration across organizations for machine learning (ML) without sharing proprietary life science data.

Intel® Homomorphic Encryption Toolkit
Toolkit to securely gain valuable insights from life sciences data using advanced HE-based cloud solutions boosted on the latest Intel platforms.

Software Reliability: Advanced Hardware Protection Ensuring Predictable Run Time

Intel® Control-Flow Enforcement Technology (CET)
CET protects against the misuse of legitimate code from hard-to-find control-flow hijacking malware through Indirect Branch Tracking (IBT) and Shadow Stack.

Intel® Threat Detection Technology (TDT)
Developers can leverage Intel® TDT detection functions to detect the latest crypto mining and ransomware threats by profiling platform telemetry in real time.

Intel® Anomalous Behavior Detection for Intel TDT (ABD)
In collaboration with TDT, protect against software supply chain attacks by ensuring continuous platform telemetry monitoring and real time alerts using Intel® ABD

Workload & Data Protection: Trusted Execution for Hardware-isolated Data Protection

Intel® Software Guard Extensions (SGX)
SGX is a method of hardware-based confidential computing for sensitive Life Sciences data/workloads to only be accessed inside a hardware-encrypted enclave in a Trusted Execution Environment (TEE).

Intel® Virtualization Technology (VT)
Intel VT allows a user to securely co-locate multiple life sciences workloads on a common set of resources while maintaining full isolation.

Intel® Trusted Execution Technology (TXT)
Intel TXT can validate the behavior of key components at system startup during the controlled launch of system software called the Measured Launch Environment (MLE).

Foundational Security: Critical Protection to Help Verify Trustworthiness of Devices and Data

Intel® Advanced Encryption Standard New Instructions (AES-NI)
IAES-NI offloads much of the computational overhead of encryption, reducing the performance impact of encryption by AES.

Intel® Converged Security and Management Engine (CSME)
CSME is both a set of hardware embedded in chipset and a firmware solution that enables platform bring up and Intel value added features including Intel® Active Management Technology, Intel® Trusted Platform Module, and Intel® Platform Trust Technology.

Intel® Total Memory Encryption – Multi-Key (TME-MK)
Built on Intel® Total Memory Encryption to encrypt memory, TME adds support for multiple encryption keys enabling hypervisors to isolate memory from different VMs.

Intel® Boot Guard
Use Intel Boot Guard as Hardware-based root of trust to help protect the integrity of the platform boot process.

Intel® Quick Assist Technology (QAT)
QAT can improve performance by the acceleration of encryption and compression of sensitive data to optimize system performance and storage.

Intel® Platform Firmware Resilience (PFR)
Intel PFR can provide resiliency by protecting platform assets, detecting corrupted firmware and malicious or erroneous behavior, and recovering the platform to a known good state.

Intel® Platform Security Discovery (PSD)
PSD helps create an interface for system firmware to display the hardware security capabilities available on the platform for upper software layers to enable.

Intel® BIOS Guard
To help reduce the risk of Flash based attacks, life sciences organizations can use BIOS Guard which reduces the size of the trust boundary for BIOS image updates to flash.

Intel® Platform Trust Technology (PTT)
Intel PTT introduces capabilities for storing keys, passwords, and digital certificates securely. PTT includes integrated Trusted Platform Module (TPM) technology provided by silicon in conjunction with CSME firmware built on crypto subsystem compliant with FIPS.

Powered by Intel® Hardware