Business Brief

Help Secure Your Most Sensitive Data.

As networks become more distributed, updated methods are needed to extend a seamless security posture across expanding attack surfaces from the data center to the cloud to the edge. At the same time, security teams must keep up with increasingly sophisticated attack techniques, the incorporation of AI into attacks as well as defenses and the challenges of rigorous privacy and regulatory requirements for sensitive data.

15% ANNUAL GROWTH IN GLOBAL CYBERCRIME[1]

EVERY **39** SECONDS THERE IS A CYBERATTACK, ON AVERAGE[2]

NEARLY **$1.8M** BREACH COST SAVINGS USING AI AND AUTOMATION[3]

Intel® Advanced Matrix Extensions (Intel® AMX) accelerate deep learning training and inference

Intel® Control-Flow Enforcement Technology (Intel® CET) protects against hard-to-detect memory attacks

Intel® Trust Domain Extensions (Intel® TDX) enhance protection of VMs and their contents

Intel® Dynamic Load Balancer (Intel® DLB) increases performance related to network data handling

Intel® QuickAssist Technology (Intel® QAT) accelerates encryption and compression operations

Intel® Software Guard Extensions (Intel® SGX) isolate sensitive data in hardware-protected memory

Intel® Xeon® processors enable three general categories of business benefits — risk, revenue and cost. Select the Risk mitigation, Revenue growth & innovation or Cost reduction icon below to explore any or all of these outcomes.

Mitigate risk

Help protect data while in use, even when shared with third parties

skip to RISK section ›

Grow revenue & innovate

Activate maximum value from sensitive or regulated data

skip to REVENUE section ›

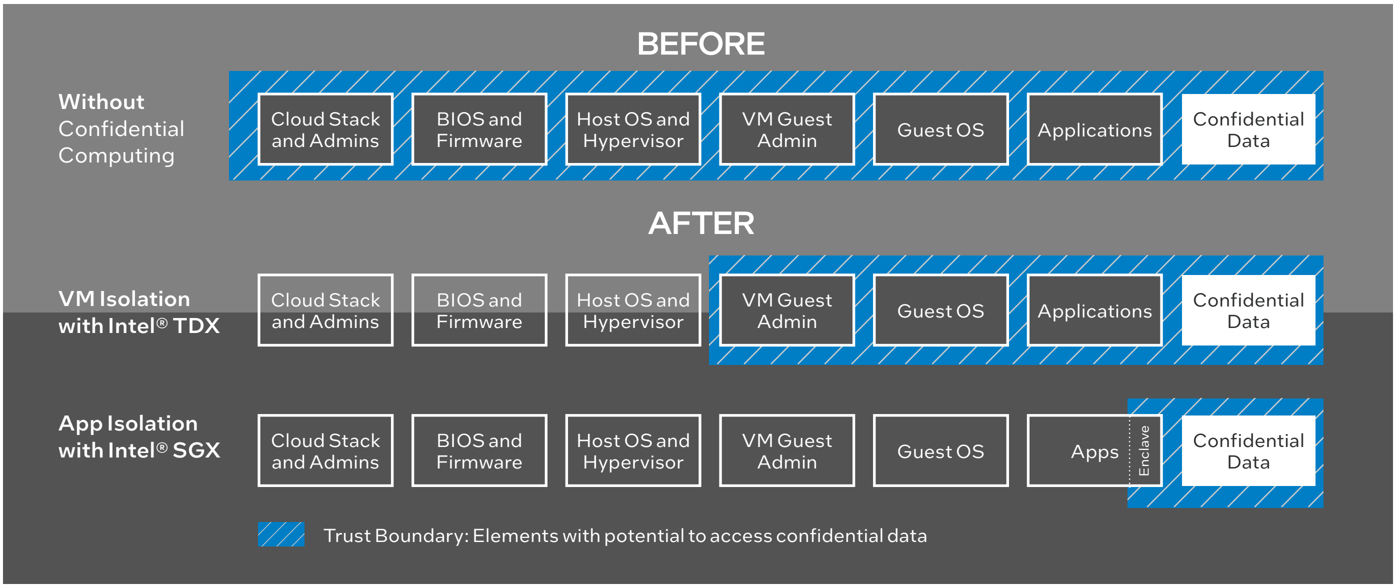
Reduce cost

Optimize the expense of protecting the business from breaches

skip to COST section ›

Mitigate risk

Confidential computing with Intel Xeon processors enables data to be processed in a hardware-protected Trusted Execution Environment (TEE), thereby reducing the likelihood that sensitive data will be compromised. TEEs are isolated from any untrusted software, including the underlying cloud stack, cloud admins and other tenants. This allows organizations to verify and control specific configurations to protect functions, further reducing attack vectors such as hackers, malware, tampering and theft.



BEFORE

Without Confidential Computing	▨ Cloud Stack and Admins	▨ BIOS and Firmware	▨ Host OS and Hypervisor	▨ VM Guest Admin	▨ Guest OS	▨ Applications	▨ Confidential Data

AFTER

VM Isolation with Intel® TDX	Cloud Stack and Admins	BIOS and Firmware	Host OS and Hypervisor	▨ VM Guest Admin	▨ Guest OS	▨ Applications	▨ Confidential Data
App Isolation with Intel® SGX	Cloud Stack and Admins	BIOS and Firmware	Host OS and Hypervisor	VM Guest Admin	Guest OS	Apps ▨ Enclave	▨ Confidential Data

▨ Trust Boundary: Elements with potential to access confidential data

Data protection must follow new methods, especially to enable data to be consumed securely across organizational boundaries. Conventional mechanisms that focused on denying access to untrusted parties are no longer useful in a world of cross-organizational workflows and shared analyses.

PERFORMANCE PROOFPOINT

UP TO **11%** HIGHER VIRTUAL MACHINE PERFORMANCE[4]

on 5th Gen Intel Xeon Scalable platform with Intel TDX vs. 4th Gen Intel Xeon Scalable platform (no Intel TDX) on integer, floating point and BERT-Large

How Intel can help

Until recently, data security has focused on protecting data at rest (in storage) and in transit (moving between locations). Confidential computing, powered by Intel® Software Guard Extensions (Intel® SGX) and Intel® Trust Domain Extensions (Intel® TDX), goes a step further, designed to protect data while it is being processed.

- **Application-level isolation**. Intel SGX is the most researched and updated confidential computing technology in data centers on the market today. For customers that need the least amount of code to access confidential data, Intel SGX provides the smallest trust boundary of any confidential computing technology in the data center today.
- **VM-level isolation**. Intel TDX offers isolation and confidentiality at the VM level. Within an Intel TDX confidential VM, the guest OS and VM applications are isolated from access by the cloud host, hypervisor and other VMs on the platform. Deploying in an Intel TDX trust domain usually does not require application code changes, offering a simpler migration path for existing applications to move to a TEE.
- **Independent attestation**. Intel provides independent attestation services in a public/private multi-cloud environment with Intel® Trust Authority. Designed to remotely verify and assert trustworthiness of compute assets such as TEEs, devices and roots of trust, the service is operationally independent from the cloud/edge infrastructure provider hosting the confidential computing workloads.

PERFORMANCE PROOFPOINT

~4x HIGHER THROUGHPUT ON VPP IPSEC (1420B)[5]

with the 5th Gen Intel Xeon Platinum 8592+ processor with integrated Intel QAT

A range of additional platform capabilities built into Intel Xeon processors complement confidential computing to provide multidimensional data protection within the TEE, including the following:

- **Accelerated encryption**. Built-in accelerators for encryption, including Intel® QuickAssist Technology (Intel® QAT) and Intel® Crypto Acceleration, help preserve performance while keeping data protected.
- **Enhanced memory protection**. Intel® Control-Flow Enforcement Technology (Intel® CET) provides hardware-based protections to help shut down an entire class of software-based attacks designed to create malicious outcomes using existing software.
- **Added protection against physical attacks**. Intel® Total Memory Encryption (Intel® TME) encrypts the platform's entire system memory with a single key for added protection against physical attacks.

Benefit *your* business

To protect more than $25B of transactions annually, Microsoft has moved its credit card processing to a cloud-based solution using Azure Confidential Computing, enabled by Intel SGX technology. The Azure-based solution meets or exceeds current Payment Card Industry Data Security Standard (PCI-DSS) guidelines for data protection and access control.

Grow revenue & innovate

New data sources open new opportunities for analysis and new services. Collaboration among multiple parties allows all participants to benefit from shared analysis or solve mutual issues, with corresponding requirements to keep data confidential and compliant.

Multi-party collaborations often require complex analyses on sensitive or regulated data while keeping it protected and out of view by unauthorized parties. These include scenarios like hospitals pooling data for drug research or disease tracking, as well as multiple banks collaborating to identify fraud and money laundering. Often, the data each party holds is sensitive or regulated, and providing unencrypted access to it would pose significant security risks.

Organizations need the means to activate this data and derive value from it while remaining compliant with regulations that require strict data protection, such as GDPR (Europe) and HIPAA (United States). For service innovations to be viable at generating value, potential risks must often be mitigated. Vulnerability to new attack vectors on data are a common result of implementing new digital capabilities. For such projects to succeed, they must incorporate data protection measures. As the level of innovation increases, so does the corresponding requirement for protecting data.

How Intel can help

Confidential computing enables you to activate sensitive and regulated data in a TEE, designed to keep it private and protected to help meet compliance. Intel SGX and Intel TDX are engineered to introduce as little overhead as possible, preserving throughput while protecting workloads. The TEE and granular access controls open possibilities for new services or collaborations using sensitive or regulated data.

Benefit *your* business

At the convergence of AI and confidential computing, Intel is driving Confidential AI to help secure sensitive data and maintain zero-trust security in environments that embrace AI transformation. These technologies are proving to be vital, following recently introduced regulations such as the European Union's AI Act and the U.S. Executive Order on the Safe, Secure and Trustworthy AI.

Reduce cost

Protecting from cyberattacks can be expensive.
But recovering from one is even more costly.

$4.5M COST OF A DATA BREACH IN 2023[6]
GLOBAL AVERAGE

$10.5T COST OF CYBERCRIME BY 2025[7]
PER YEAR

How Intel can help

To help not only mitigate the expense of implementing a cybersecurity strategy but also protect against a data breach, Intel products are designed, manufactured and maintained using the industry's best security practices. Intel product security assurance leads the silicon industry, according to a study by ABI Research, and Intel ranked No. 1 in the 2023 Forbes America's Most Cybersecure Companies list. Our innovative security capabilities and robust processes to find and address vulnerabilities are designed to help you meet today's security challenges.

Using the built-in Intel QAT as an offload engine provides a significant throughput improvement for compression, compared to the same algorithm run on processor cores. This means organizations can compress and encrypt, then decrypt and decompress on the fly, keeping data secure in motion and at rest. Intel Crypto Acceleration and Intel QAT, coupled with innovations up and down the stack, allow using fewer cores for the same security operations — saving you money while you save your customer's data from prying eyes.

PERFORMANCE PROOFPOINT

Intel® QAT Software Accelerator

UP TO **1.66x** HIGHER NGINX TLS HANDSHAKE PERFORMANCE[8]

5th Gen Intel Xeon Platinum 8592+ vs. 4th Gen AMD EPYC 9554 OOB

Intel® QAT Hardware Accelerator

UP TO **1.85x** HIGHER NGINX TLS HANDSHAKE PERFORMANCE PER CORE[8]

5th Gen Intel Xeon Platinum 8592+ with integrated QAT vs. 4th Gen AMD EPYC 9554 OOB

Innovate freely in an open ecosystem

Security and other optimizations for Intel Xeon processors are already integrated into the open source and proprietary software ecosystems, through extensive industry partnerships and collaborations, as well as Intel's longstanding status as a top contributor to high-profile open source projects such as Linux and Kubernetes. In fact, 90% of developers are using software developed or optimized by Intel.[9]

An **array of tools and resources** are available for organizations as they get started with confidential computing on Intel architecture. This includes **Gramine**, an open source library OS that simplifies adoption of Intel SGX, and **Curated Containers on Azure Marketplace** for rapid deployment of confidential containers for popular frameworks such as PyTorch, MySQL and TensorFlow.

Try the capabilities of new built-in accelerators on the **Intel Developer Cloud**, which offers easy access to the latest Intel technologies without downloads and hardware setup. Find recipes, benchmarks and other resources on how to optimize key workloads using specific built-in accelerators and other hardware features at the **Intel Optimization Hub**.

Reimagine what's possible

Forward-looking decision makers must capture the full potential of security to reduce risk, grow revenue, innovate and reduce costs. Intel uniquely provides the comprehensive hardware, software, tools and design patterns to realize that vision. Intel Xeon delivers high performance per core and per watt, to meet emerging demands while delivering on key business metrics.

Security starts with Intel.

Learn More

www.intel.com/xeon

www.intel.com/security-engines

[1] Cybercrime Magazine, May 24, 2023. "2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics." https://cybersecurityventures.com/cybersecurity-almanac-2023/.

[2] Astra IT, September 13, 2023. "160 Cybersecurity Statistics 2023 [Updated]." https://www.getastra.com/blog/security-audit/cyber-security-statistics/.

[3] IBM, August 14, 2023. "Research shows extensive use of AI contains data breaches faster and saves significant costs." https://www.ibm.com/blog/research-shows-extensive-use-of-ai-contains-data-breaches-faster-and-saves-significant-costs/.

[4] See [S1] at intel.com/processorclaims: 5th Gen Intel Xeon processors. Results may vary.

[5] See [N18] at intel.com/processorclaims: 5th Gen Intel Xeon processors. Results may vary.

[6] IBM. "Cost of a Data Breach Report 2023." https://www.ibm.com/reports/data-breach.

[7] Zippia, June 15, 2023. "30 Crucial Cybersecurity Statistics [2023]: Data, Trends And More." https://www.zippia.com/advice/cybersecurity-statistics/.

[8] See [N202] at intel.com/processorclaims: 5th Gen Intel Xeon processors. Results may vary.

[9] Global Development Survey conducted by Evans Data Corp., 2021.

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

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 does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

0424/BR/MESH/353952-002US