Unlock Your Data:

Five Reasons for Choosing Intel® Xeon® 6 Processors with Silicon-Enhanced Security

Get more value from your data without compromising security. Enhanced security features are designed to maintain privacy and confidentiality while helping you extract value from sensitive data.

Accelerate Innovation and Enhance Data Protection

Deploying AI models based on sensitive data requires high levels of cryptographic security and enhanced access control.

Security for AI

77% of companies reported breaches to their AI in 2023[1]

Increased Regulation

82% of the world's population is covered by some form of national privacy law[2]

Due to these risks, customers need a trusted foundation—starting at the silicon—to ensure only authorized users can access their data.

Encrypting data during storage and transit is standard, but protecting it while in use poses challenges. Sensitive data like personally identifiable information (PII), medical records, and financial transactions can be vulnerable during processing. Intel Xeon 6 processors address this with integrated security features designed to protect data, preserve code integrity, and maintain high performance for demanding workloads. Their advanced crypto-acceleration enhances cryptographic security and performance without needing additional cores. Intel Xeon 6 processors allow businesses to process sensitive data in trusted execution environments, enabling new possibilities for analyzing regulated or sensitive information.

Protect Your Platform from the Ground Up

Here are five compelling reasons to choose Intel Xeon 6 processors' silicon-enabled security to help protect your data, models, and IP.

1 Control Over Sensitive Data

Intel Confidential Computing Solutions are designed to protect data in use with isolation, encryption, and attestation. This approach helps customers unlock new opportunities for business collaboration and insights.

Intel Software Guard Extensions (Intel SGX) is the most researched and updated confidential computing technology in data centers on the market today, with the smallest trust boundary.

Intel Trust Domain Extensions (Intel TDX) helps businesses increase confidentiality at the virtual machine (VM) level, enhance privacy, and gain control over their data. It enables isolation of guest OS and VM applications, designed to remove access from the cloud host, hypervisor, and other VMs on the platform from the trust boundary.

Intel's portfolio of confidential computing technologies, including Intel SGX and Intel TDX, allows businesses to choose the level of security they need to meet their business needs and regulatory requirements.

2 Encrypted I/O for Confidential AI

Intel TDX Connect enables seamless encrypted communication between a Confidential VM and an enabled PCI Express device. This capability is critical to enabling confidential usage models that extend beyond the CPU to connected devices such as GPUs, Smart NICs, or storage drives.

Intel TDX Connect, supported on Intel Xeon 6 processors, is designed to enhance confidential computing infrastructure and improve I/O virtualization performance.

With confidential AI and Intel TDX Connect, organizations can open silos containing sensitive and regulated data without hesitation and use that data to expose new insights.

3 Efficient Handling of Data for Time, Space, and Cost Savings

Accelerate data encryption and compression for applications from networking to enterprise, cloud to storage, and content delivery to database with Intel QuickAssist Technology (Intel QAT).

By offloading compute-intensive workloads, Intel QAT can free up core capacity for other workloads while helping to significantly reduce costs and compressed data footprints.

Up to

1.62x

higher NGINX performance Intel Xeon 6952P vs AMD EPYC 9655*

4 Quantum-Resistant Encryption

Some attackers are following a "harvest now, decrypt later" (HNDL) philosophy: They collect sensitive data now, intending to decrypt it in the future when quantum computing runs at scale. It's critical to increase encryption strength now to be resistant to future quantum computing attacks.

Intel co-developed one of the three NIST post-quantum cryptography algorithms (FIPS 205), based on SPHINCS+, with an international team of researchers from universities and the industry.

Intel Xeon 6 supports quantum-resistant AES-256 encryption for Intel SGX, Intel TDX, and Intel QAT.

5 More Resilient Products

Intel is a world leader in technology, and our foundational place in the compute stack gives us unique influence on cybersecurity.

Choose products designed with security in mind, protected by the best security assurance in the industry.[3]

In 2024, AMD reported

4.4x

more firmware vulnerabilities in their hardware root-of-trust than Intel.[4]

Learn about additional benefits that Intel Xeon 6 processors can deliver as your trusted foundation: https://intel.com/content/www/us/en/products/details/processors/xeon.html

See how Intel Xeon 6 processors enhance encrypted workloads for networking and infrastructure. Examine the latest workload performance metrics: https://edc.intel.com/content/www/us/en/products/performance/benchmarks/intel-xeon-6/

Review product specifications and find the best processor for your unique computing needs: https://ark.intel.com/content/www/us/en/ark/products/series/595/intel-xeon-processors.html.

Sources

[1] HiddenLayer, *AI Threat Landscape Report*, March 6, 2024. https://hiddenlayer.com/threatreport2024/

[2] Apacible-Bernardo, A, Bushey, K, *Data protection and privacy laws now in effect in 144 countries*, IAPP, January 28, 2025. https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries

[3] ABI Research, sponsored by Intel, *Embracing Security as a Core Component of the Tech You Buy*, 2024. https://www.intel.com/content/www/us/en/security/security-as-a-component-of-tech.html

[4] Intel, *2024 Intel® Product Security Report*, March 2, 2025. https://www.intel.com/content/www/us/en/content-details/846149/2024-intel-product-security-report.html

* See [9W220] at https://intel.com/processorclaims: Intel Xeon 6. Results may vary.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex. Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See https://intel.com/processorclaims for configuration details. No product or component can be absolutely secure. Your costs and results may vary. Intel technologies may require enabled hardware, software or service activation.

© 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.