



intel®



Security Starts with Intel

Security built in. Security to build on.



Intel is a world leader in technology, and our foundational place in the compute stack provides us with a unique influence on cybersecurity. We look at security not only as a responsibility we must deliver on, but as a business opportunity for our customers and company alike. In keeping with that responsibility, we work with many of the largest and most respected companies around the world, often in the most privacy-sensitive environments.

This paper details the security practices we use and the products we deliver to help safeguard our customers.

For more information, read:
<https://www.intel.com/security>

Introduction

Today, technological innovation provides businesses with a broad range of transformative opportunities—applied analytics and AI, cloud migration, distributed services, edge deployments, blockchain, and data monetization services, to name just a few.

But to realize these opportunities, businesses face a daunting hurdle: data security. Innovation can be complicated by security and compliance requirements. Security challenges come in various guises, including cyber threats (such as malware, phishing, and data breaches), physical security threats, human threats from insiders, and cloud provider trust issues, in addition to regulatory mandates. Organizations must rigorously protect their intellectual property (IP) and fortify their supply chains. And they must implement these security measures without seriously degrading the user experience in areas such as access and performance.

Advanced threats can now outmaneuver traditional approaches to enterprise and data security. Increasingly, businesses and governments are adopting a Zero Trust strategy, based on the premise that no user or asset is inherently trustworthy. Therefore, each user, asset, application, and transaction must be continuously verified.

The foundation of an effective Zero Trust strategy is silicon-based security, rooted in the microprocessor’s privileged position in the compute stack. Intel delivers products, services, and capabilities to advance Zero Trust in the following areas:

- What we practice: Intel enterprise cybersecurity, including supply chain security. Forbes ranked Intel #1 on its 2023 “America’s Most Cybersecure Companies” list.¹
- Intel Product Security assurance practices that guide how we securely design, manufacture, and support our products were scored by ABI Research as #1 in product security assurance investments and maturity across the silicon industry.²
- Intel features provide security for our customers, enabling AI-enhanced endpoint protections.
- Intel offers the most comprehensive confidential computing portfolio in the industry.

Figure 1.
Security Assurance
Practices²

Company	Score	Overall Ranking
Intel	82.2	1
Qualcomm	68.5	2
AMD	65.0	3
Nvidia	61.7	4
ARM	45.3	5

New cyberthreats: complex, costly, and dangerous

Intel's robust security offerings are critically important in today's threat landscape. The ever-increasing scope of edge computing and the enormous growth of AI mean that threats continuously evolve in number and complexity, resulting in an expanding attack surface that must be protected. New attacks constantly appear, and criminals are reworking existing threats to increase their lethality.

The range of threats and vulnerabilities facing the enterprise is extensive:



Ransomware and Cryptojacking
Ransomware is a growing concern for cybersecurity professionals, and cryptojacking attacks increased by 659% from 2022 to 2023.⁴



Phishing Attacks
The #1 reported cybercrime in 2023.⁵



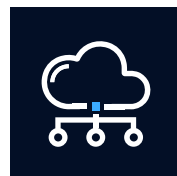
Supply Chain Corruption
Almost 55% of integrated circuit manufacturers have reported encountering counterfeit versions of their products.⁶



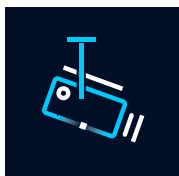
ID and Credential Theft
For a typical company, the average cost of a breach when attackers use compromised credentials is \$4.81 million.⁷



Security for AI
77% of companies reported breaches to their AI in 2023.⁸



Trusted Digital Experiences
For many companies, security is critical for sustained profitability. By 2026, 40% of revenue for G2000 companies is expected to come from digital products, services, and experiences.⁹



Video Sensors and AI
By 2026, over 346 million security cameras and sensors will be installed globally (outside China), with most recording to NVR and VMS server infrastructure.¹⁰

The risks of security breaches to customers can prove costly, resulting in outcomes such as regulatory fines, loss of sensitive data, production downtime, and potentially disastrous publicity and reputation damage. That makes security a high priority for businesses who therefore need trusted advisors across multiple security domains. Intel helps customers address their risks using silicon-enabled security to bolster Zero Trust strategies and deliver capabilities that help customers implement the right security controls for their environment.

Product security assurance: A true differentiator for Intel

At Intel, developing secure products starts from within. Intel's Security-First Pledge prioritizes customers' needs when evaluating security decisions, demonstrating Intel's commitment to advancing data protection, vulnerability management, and offensive security research. Engineering teams follow a "security-first mindset," thinking like a hacker to break what they build for optimal protection. This is critical to the design and development of secure products, and our customers can see the results.

According to a report by ABI Research,² Intel leads the silicon industry in product security assurance, ranking #1 in both innovation and implementation. The study focuses on solutions for personnel, practices, and processes that embed security considerations into product development and support.

Intel's annual Product Security Report³ illustrates ongoing industry leadership in product security assurance. It examines how investments in Intel security technology stack up competitively—and the numbers are telling. Intel's proactive product security assurance efforts resulted in discovery of 96% of the vulnerabilities addressed and 100% of the Intel processor vulnerabilities addressed were discovered through internal security research. AMD reported 4.4x more firmware vulnerabilities in their hardware root-of-trust than Intel and 1.8x more firmware vulnerabilities in their confidential computing technologies.

Intel's sophisticated security assurance framework incorporates a Security Development Lifecycle (SDL) covering all phases, from design through manufacturing and support. SDL includes incident response planning, as well as remediation strategies and a long-term retention program. While SDL is an industry best practice, Intel pioneered its implementation for hardware, firmware, and platform development, in addition to software development.

Security means you never stop looking for ways to improve. Intel employs dedicated security research experts who conduct in-depth adversarial analysis of technology architecture, focusing on system-level security spanning silicon and software layers. Specialists look at physical and fault injection attacks to resolve vulnerabilities and weaknesses. Intel works extensively with the security research community through a Bug Bounty program, live hacking events, and academic engagements. Intel also regularly collaborates with industry partners to enhance product security.

ABI Research's Vendor Matrix

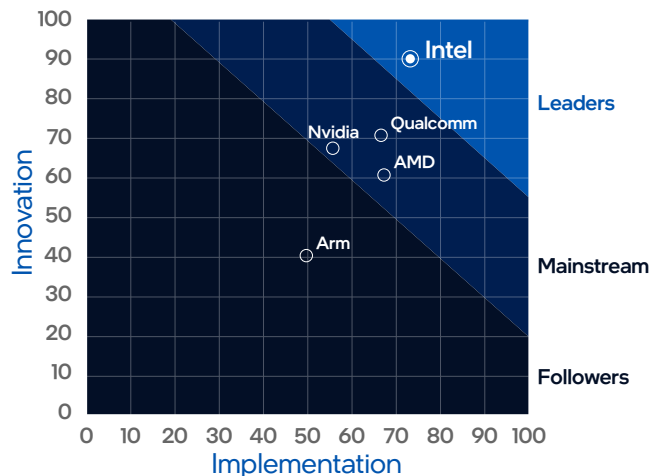


Figure 2. ABI Research's Vendor Matrix showing Intel as leader.

For more information, read: [Intel 2024 Product Security Report](#)

Intel's investments drive better security outcomes

Intel delivers products, services, and capabilities that partners and customers use to advance their Zero Trust strategy. That flexibility enables them to implement security controls they can customize to meet their specific business needs.

Intel's comprehensive security roadmap has four distinct pillars:



Endpoint Security strengthens defenses by implementing AI-powered threat detection and insights, as well as silicon-based security measures.



Network Security connects customers with the resources they need through encryption-based identity and access control.



Information and Data Security designed to isolate and protect sensitive data in use, enhancing confidentiality, integrity, and availability.



Physical Security controls direct access to cybersecurity assets, while also securing sensitive facilities, people, and physical assets.

What is silicon-enabled security?

- Security capabilities physically built in at the silicon level
- Differs from software-based protections, in which security measures are installed on top of hardware, leaving layers located below the OS vulnerable
- Meant to complement software-based security measures rather than replace them
- Designed for a multidimensional, comprehensive approach to help detect and prevent a greater range of cyberthreats

Together, these four pillars serve as a foundation of trust for Intel's industry-leading product security assurance.

For more information, read: [How Intel Contributes to Zero Trust](#)



Endpoint security

Endpoint security encompasses the strategies and technology solutions that help secure endpoint devices from digital threats and unauthorized access. Endpoint security solutions help protect devices, users, and organizations from lost productivity, increased cost, and reputation damage. According to a recent IDC study,¹¹ businesses that take advantage of comprehensive security offerings from Intel and Dell reap significant benefits. The study reported improved outcomes enabled by Intel's security capabilities, vulnerability management practices, and offensive security research. These clear and quantifiable results included:

- 26% fewer instances of major security breaches.
- 21% fewer impactful security events, in terms of the business cost associated with the security event.
- 17% greater security team efficiency.
- 14% lower 5-year cost of operations and 22% lower costs for lost productivity, PC security, and performance issues.



Comprehensive security

Intel provides comprehensive security solutions for customers. Features available with Intel vPro® processors enable in-depth defensive strategies against a variety of attacks, as illustrated in Figure 3.

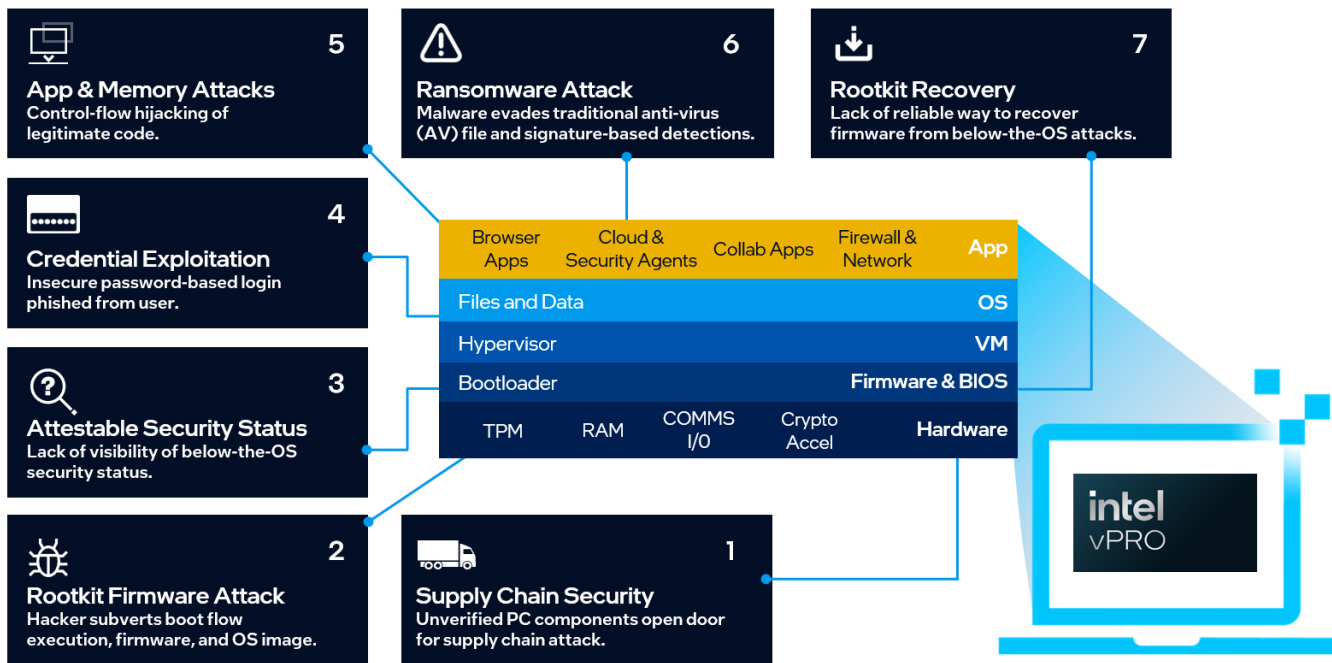


Figure 3. Attack surface protections for endpoint security.

1. Intel® Tiber™ Transparent Supply Chain guards against unverified PC components that can open the door for a supply chain attack.
2. Intel® Secure Boot and Intel® BIOS Guard help protect against rootkit firmware attacks on the OS kernel.
3. Intel® System Security Report provides visibility below the OS, attesting the software's status and checking that the boot process completes properly.
4. Intel worked with Microsoft Windows to implement enhanced sign-ins with two-factor authentication, using Intel® Virtualization Technology (Intel® VTT) to isolate phishing attacks.
5. Intel® Control Flow Enforcement Technology (Intel® CET) can help prevent control-flow hijacking of code.
6. Ransomware attacks evade traditional AV file and signature-based detections. Intel® Threat Detection Technology (Intel® TDT) helps augment existing solutions with AI-based CPU behavior monitoring and threat detection.
7. Rootkit recovery works at the firmware and BIOS levels. Intel® Active Management Technology (Intel® AMT) provides a reliable way to recover firmware from below-the-OS attacks.

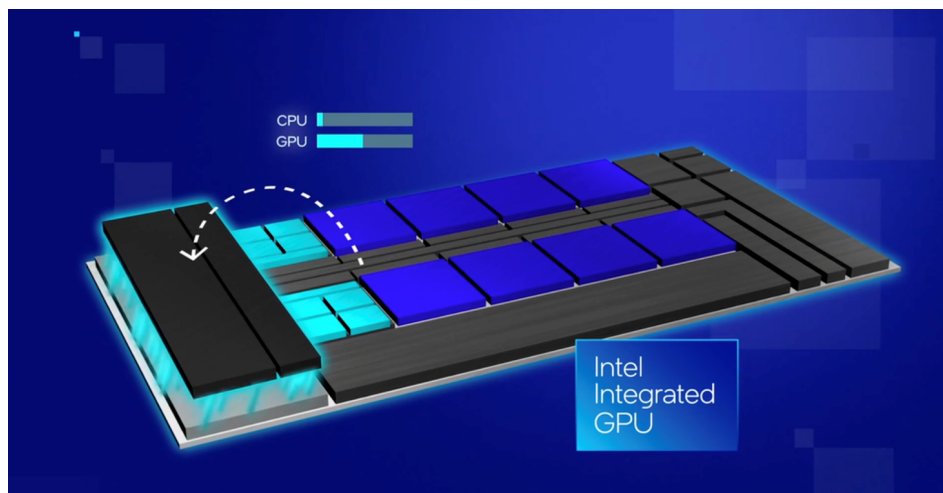
Intel TDT is an important development in security, so let's explore it more closely. It is the only AI-based silicon security deployed across a billion PCs powered by Intel® processors (but not available on Apple or AMD platforms).¹² Intel TDT can fingerprint malware as it attempts to run on the CPU. Because of its behavior-based approach, this method is immune to traditional malware cloaking or obfuscation techniques. It is a powerful tool that helps increase the efficacy and performance of security software. Intel TDT supports defensive software from a broad range of developers, including Microsoft, Check Point, Sequestek, Acronis, and CrowdStrike.

Intel TDT includes:

- Integrated GPU offload of accelerated memory scanning
- Integrated GPU offload of Machine Learning algorithms
- Cryptojacking detection
- Ransomware detection

Figure 4.

Security vendors use the Intel® Integrated GPU to offload security workloads and to scan memory.



For more information on Intel TDT, visit: <https://intel.com/tdt>



Case study

CrowdStrike is a strategic supplier and innovation partner for Intel. The [Intel Information Security \(InfoSec\) team worked with CrowdStrike](#) to leverage the power of Intel TDT through their advanced endpoint detection and response (EDR) and anti-virus capabilities.

According to the [CrowdStrike 2024 Global Threat Report](#),¹³ 75% of endpoint cyberattacks in 2023 were malware-free. These fileless attacks and APTs can evade modern attack indicators by hiding in memory. To solve that problem, CrowdStrike and Intel co-engineered a new, advanced memory scanning (AMS) capability based on Intel TDT. This hardware-accelerated solution brings an important additional layer of defense. Using Intel TDT, [CrowdStrike experienced a 4-7x performance improvement](#).¹⁴

For more information on Intel TDT and CrowdStrike, read: [Advancing Intel's Security Posture Through Partnership & Innovation with CrowdStrike](#)



Network security

International Data Corporation (IDC) reported that by 2026, Fortune 2000 companies will generate 40% of their revenue through digital products, services, and experiences.¹⁵ This projection underscores today's significant shift towards digital transformation, where companies increasingly rely on digital offerings to drive growth and remain competitive in the evolving business landscape. With that much revenue in play, it's hard to overstate the need for trusted digital processes. Intel Network Security helps meet this need by protecting and accelerating network performance, cryptography, and enhanced inferencing. Results include TCO savings, higher throughput, and improved connectivity. For example:

- Up to 40% TCO savings through NGNIX TLS Handshake¹⁶
- Up to 3.73x higher throughput with VPP IPsec using AES256¹⁷
- Up to 1.69x higher connection per second using NGNIX TLS 1.3 webserver handshake¹⁸

Case study



Deep learning models for inline threat detection

Palo Alto Networks develops and deploys deep learning models for detecting inline threats in customers' network traffic. Intel collaborated with Palo Alto Networks to incorporate analytics and AI into their security applications running TensorFlow and PyTorch. After modifying only a few lines of code, the team achieved a dramatic performance improvement in their AI inferencing model.

The incorporation of Intel optimization in the standard AI framework extended from Palo Alto Network's software foundation, PAN-OS, to their implementation in the cloud using Google Cloud with the latest Intel® Xeon® processors. Results included a 48% increase in C2 threat detection, with 96% of web-based Cobalt Strike C2 communications blocked inline.^{19,20}

For more information, watch:

["Lower TCO and increase performance on your cloud workloads easily"](#)
[\(Google Cloud Next 2023\)](#)

Case study

Post-Quantum Cryptography (PQC) Without Compromising Performance

Arqit is a cybersecurity company focused on Post-Quantum Cryptography (PQC). Future quantum computers will likely pose a risk because they can potentially break widely used cryptographic methods. The Arqit Symmetric Key Agreement Platform (SKA-Platform) is designed to protect assets from Save Now and Decrypt Later (SNDL) threats where adversaries are stealing assets today and waiting for quantum computers to become available to decrypt and access secrets.

Testing with Arqit SKA-Platform demonstrated that a quantum secure IPsec tunnel can be achieved without compromising performance.^{21,22} Intel previously demonstrated the performance of FD.io's Vector Packet Processor (VPP) combined with strongSwan (VPP-SSwan), achieving a 1.89-terabit No-Drop Rate (NDR) IPsec tunnel using a single server with 4th Gen Intel Xeon Scalable processors. The solution can also be fully deployed using the Intel® NetSec Accelerator Reference Design (i.e., a "server on a card"), opening possibilities across edge network security with its small footprint and power consumption requirements.



For more information, watch:
[Post-Quantum Cryptography \(PQC\) Without Compromising Performance | Intel® Industry Solution Builders](#)





Information & data security

Intel's approach to information and data security puts customers in control of their data; the goal is to maximize data value while designing for privacy. This is a challenge due to the realities of regulations, data sovereignty requirements, and insider threats:

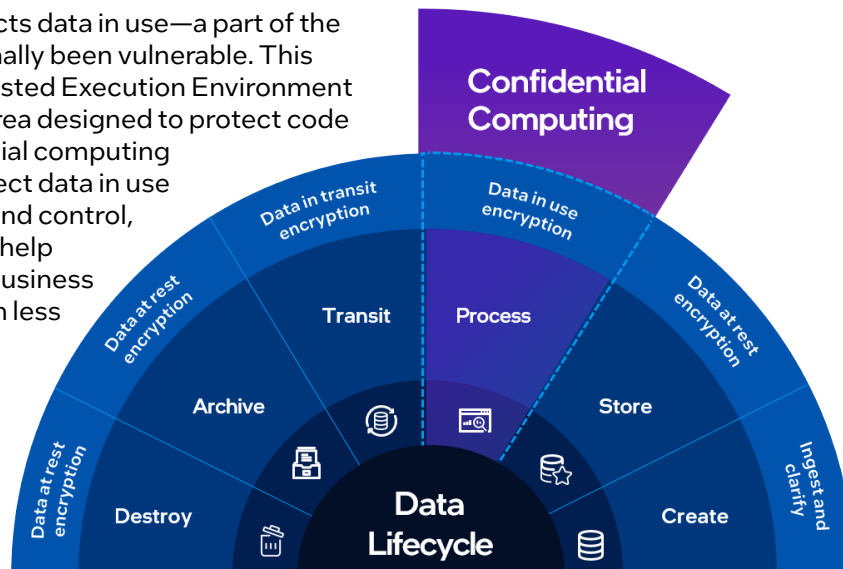
- Studies by industry analysts have shown that data and analytics leaders who share data externally gain up to 3x the economic benefits from their data when compared with those who decline to share data.²³
- 55% of logged insider threats rely on privilege escalation exploits.²⁴

A complete approach to data privacy should have technological controls to help ensure data, code, and intellectual property (IP) are handled in compliance with proper guidelines and appropriate regulatory frameworks.

Confidential computing: protecting data in use

[Confidential computing](#) protects data in use—a part of the data lifecycle that has traditionally been vulnerable. This technology focuses on the Trusted Execution Environment (TEE), a secure and isolated area designed to protect code and data in use. Intel confidential computing solutions are designed to protect data in use through isolation, encryption and control, and verification capabilities to help unlock new opportunities for business collaboration and insights, with less risk.

Figure 5. Role of Confidential Computing in the data lifecycle (Source: IDC).



Intel offers the most comprehensive security product portfolio

Intel's confidential computing portfolio includes:

Intel® Software Guard Extensions (Intel® SGX). With the smallest trust boundary of any confidential computing technology in the data center today, Intel SGX is designed to provide the highest levels of data protection and code integrity. Only the code or functions inside the protected enclave can access confidential data. Other software in the virtual machine, cloud tenants, the cloud stack, and admins are not allowed access.

Intel® Trust Domain Extensions (Intel® TDX). This technology provides hardware isolation, encryption, and isolation of VMs, designed for migration with no code changes. Intel TDX lays out a straightforward path to greater security, compliance, and control for both new and legacy applications. This VM isolation technology is generally available starting with 5th Gen Intel Xeon Scalable processors and is currently available in the cloud through Alibaba and Google Cloud. Azure offers public previews of Intel TDX-based confidential VMs, expected to be released in 2025.

Figure 6 illustrates the differences in the trust boundary between an unprotected environment, application isolation with Intel SGX, and VM isolation with Intel TDX. Without confidential computing technology, everything is inside the trust boundary, including the cloud provider's firmware, cloud stack, hypervisor, and cloud admins.

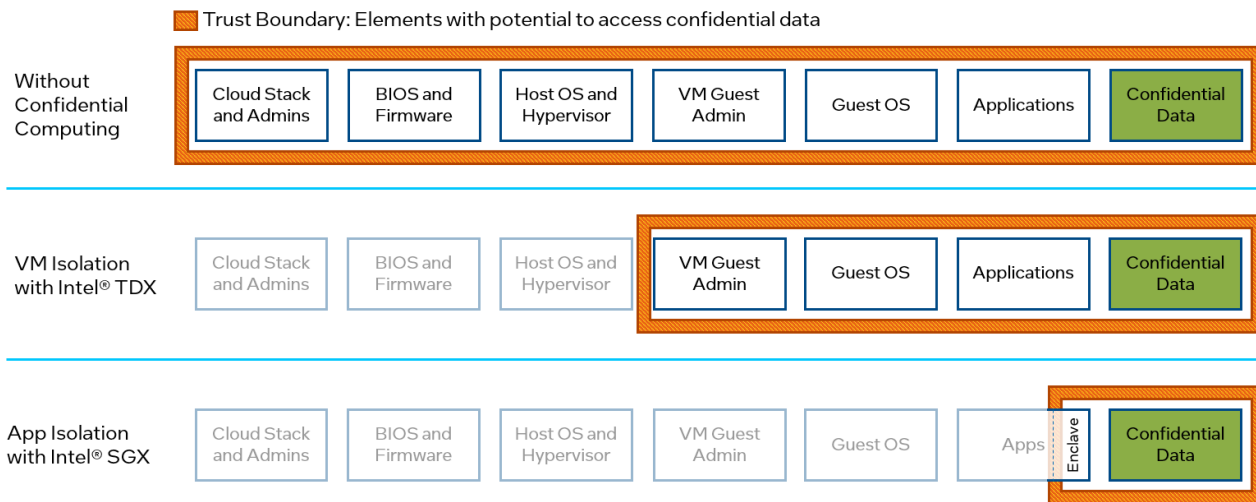



Figure 6. Comparing trust boundaries.

Both Intel SGX and Intel TDX are designed to protect the sensitive data and valuable models that are critical in the rapidly accelerating AI landscape. [Confidential AI](#) overlays confidential computing technologies onto modern techniques such as machine learning (ML) and deep learning (DL). Using Intel SGX or Intel TDX for isolation, encryption, and control, in addition to verification, provides AI practitioners with the enhanced security and confidentiality they need.

Intel® Tiber™ Trust Authority: With independent verification of the security and privacy of confidential computing environments, Intel Tiber Trust Authority puts Zero Trust within reach, delivering public cloud flexibility with private cloud security. This software attestation service enables customers to securely develop, deploy, run, manage, and scale edge solutions on standard silicon with cloud-like simplicity. Currently available on Microsoft Azure, Google Cloud, or directly from Intel, these services give organizations the tools to migrate even highly regulated data to the cloud so they can collaborate with confidence.

Case study



Microsoft deploys confidential computing to protect \$25B per year in customer payments

Microsoft's Commercial Financial Services is a payment gateway and commerce solution for e-commerce.²⁵ With support for 30 different payment methods using 80 currencies across 241 markets, it's responsible for transacting and securing \$25 billion yearly in customer payments for Microsoft products and services.

Microsoft relied on Intel SGX to implement a Level 1 Payment Card Industry Data Security Standard (PCI-DSS) compliant credit card processing and vaulting solution on Azure Cloud Services. Moving the gateway to the public cloud gave Microsoft the flexibility and scalability of a cloud-based solution and saved an estimated \$2 million in upgrade costs. Azure Confidential Computing with Intel SGX provides Microsoft with a level of security beyond that previously attainable by dedicated private or hybrid cloud solutions.

For more information, read: [Microsoft Protects \\$25B in Customer Payments](#)

Case study

Empowering US Heroes through data sovereignty, ethical AI, and precision health

[AI MINDSystems Foundation](#), in collaboration with Intel, is pioneering a secure, equitable, and person-centered data ecosystem that empowers individuals with control over their health and personal information. This transformative approach drives responsible AI advancements in healthcare, social services, and life sciences, starting with US military service members, veterans, first responders, and their families through the National HERO initiative. Its solution, WISDOM Networks, leverages Intel Xeon Scalable Processors, Intel Tiber Trust Authority, and Intel SGX.



For more information, read: [AI Aids in Decentralization of Health Data](#)





Physical security

With physical and cybersecurity increasingly interrelated, customers may find it no longer viable to separate cybersecurity and physical security policies and practices. In the past, physical security solutions had limited functionality but were more cyber-secure; for example, security cameras that once recorded images on videotape were highly secure because they were not connected to a network. Today's cameras, on the contrary, are both networked and intelligent devices and stream to a variety of solutions from edge to cloud, including Network Video Recorders (NVRs), Video Management Servers (VMS), AI Servers, and more. Safeguarding modern video security infrastructure should be a joint responsibility of the physical security/facilities personnel and the cybersecurity team.

And that's what's happening: Today, surveillance, defense, risk assessment, vulnerability assessment, business continuity, and access control are critical concerns for both physical and cybersecurity teams. By combining protections for endpoint, networking, and data privacy, Intel helps customers build a more secure video infrastructure. Holistic strategies limit access to physical assets while also implementing digital safeguards around the sensitive data on those physical systems.

The results have been impressive. One recent collaboration resulted in a 51% increase in the recovery rates of stolen goods due to more efficient monitoring, as well as a 12% decrease in criminal cases.²⁶

Software optimized for silicon

The Intel vision is to empower organizations through our portfolio of security technologies and lead the industry in providing solutions to solve customers' most critical security needs. That's true at endpoints, at the edge, and in the data center. Along with silicon, Intel invests in crucial software components that help keep pace with new threats and enable scalable AI solutions. Intel actively supports and contributes to the open-source community through a variety of projects and initiatives spanning software, silicon, and ecosystem development. Here's an overview of some key contributions in software and toolkits:

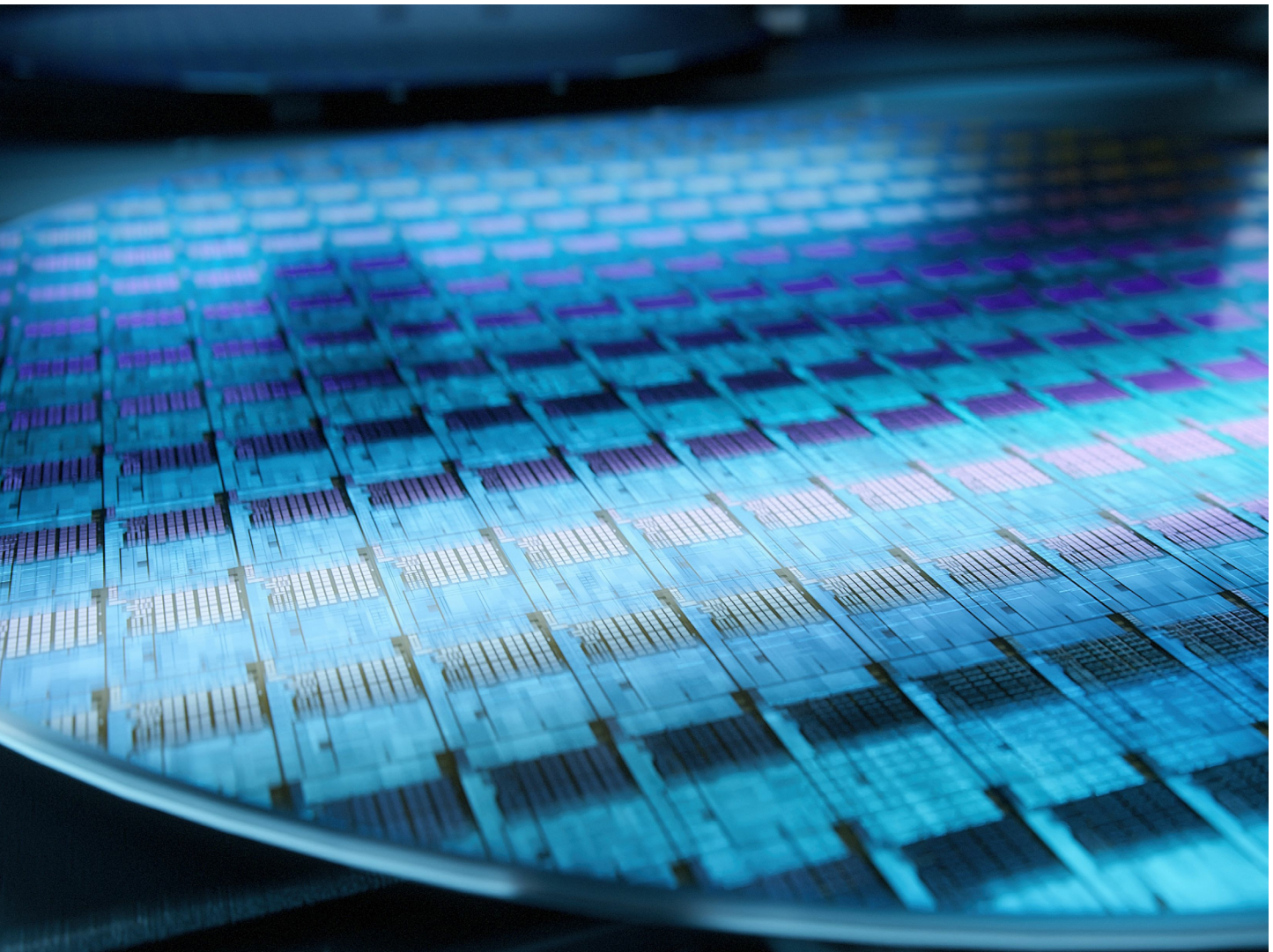
- **Intel® Tiber™ Edge Platform** enables enterprises to build, deploy, run, manage, and scale edge and AI solutions on standard silicon with cloud-like simplicity. Enterprises can onboard compute infrastructure with zero-touch provisioning in a Zero Trust environment.
- **Intel® Geti™** is a software platform that enables enterprise teams to develop vision AI models faster. By simplifying data labeling, model training, and optimization tasks, Intel Geti empowers developers to create custom AI models at scale, accelerating the deployment of intelligent solutions.
- **Intel® SceneScape** is a software platform that reaches beyond vision-based AI to realize spatial awareness from sensor data. It transforms data from many sensors to provide live updates to a 4D digital twin of any physical space. SceneScape can assimilate data from diverse sensors, derive comprehensive insights, monitor ongoing activities, and make predictive decisions.
- **Intel® Distribution of OpenVINO™ toolkit** accelerates open-source AI inference code by enabling lower latency and higher throughput while maintaining accuracy, reducing model footprint, and optimizing hardware use. It streamlines AI development and integration of deep learning in domains such as computer vision, large language models, and generative AI. Tailored for both data centers and edge devices, it enables users to harness the full potential of AI-driven video analytics.

Case study

NEC implements real-time occupancy monitoring

As one of the U.K.'s largest event venues, the National Exhibition Centre (NEC) in Birmingham, England, is heavily invested in the security of the three million people they host annually. NEC collaborated with Intel and WaitTime to address the challenge of real-time occupancy monitoring across its event spaces. Using advanced AI technology and Intel Xeon Scalable processors, WaitTime helped NEC implement a flexible crowd intelligence solution that delivers real-time occupancy data and capacity alerts, significantly improving operational efficiency and decision-making while laying the AI-powered foundation for improving guest experiences and enhancing offerings for exhibitors.

For more information, read: [NEC Implements Real-Time Occupancy Monitoring](#)



Intel:

Building a foundation of trust

Security is imperative for businesses, and customers are looking for trusted advisors to address security pain points from edge to cloud. Intel helps address these pain points using silicon-enabled security. Our solutions reduce the attack surface, protect sensitive and regulated data, and leverage AI to detect threats in both physical and cybersecurity domains. Intel can help customers implement a Zero Trust strategy, establishing silicon as the root of trust, with capabilities designed to enable robust controls for endpoint security, network security, information and data security, and physical security. The need for foundational, silicon-level security to supplement software-only protection has never been greater. Intel technology is ready to help customers overcome their security challenges.

For more information, read: [Security Starts with Intel](#)



1. Meet America's Most Cybersecure Companies 2023 (forbes.com), <https://www.forbes.com/sites/hnewman/2023/06/08/meet-americas-most-cybersecure-companies-2023/?sh=33b3f1532cf6>
2. Embracing Security as a Core Component of the Tech You Buy, <https://www.intel.com/content/www/us/en/security/security-as-a-component-of-tech.html>
3. 2024 Intel Product Security Report, intel.com/securityreport
4. 2024 SonicWall Cyber Threat Report, <https://www.sonicwall.com/resources/white-papers/2024-sonicwall-cyber-threat-report>
5. FBI Releases Internet Crime Report 2024, <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report>
6. DSIAC, Combating Counterfeit Components in the DoD Supply Chain, <https://dsiac.dtic.mil/articles/combating-counterfeit-components-in-the-dod-supply-chain/>
7. IBM, Cost of a Data Breach 2024, <https://www.ibm.com/reports/data-breach>
8. HiddenLayer, AI Threat Landscape Report 2024, <https://hiddenlayer.com/threatreport2024/>
9. IDC, Leadership in a Changing Digital World: Five Mandates | IDC Blog 2023, <https://blogs.idc.com/2023/04/28/leadership-in-a-changing-digital-world-five-mandates/>
10. Omdia, AI Outcomes in the Security Market and Beyond, <https://www.intel.com/content/www/us/en/content-details/825685/ai-outcomes-in-the-security-market-and-beyond-omdia.html>
11. Based on IDC's "The Business Value of Intel Security for PCs" report published March 2023 (commissioned by Intel), which cites a lower reported risk of significant financial impact events occurring through an Intel-based PC compared with other PCs. Additional details at: <https://www.intel.com/performance-vpro>
12. Intel TDT provides the only silicon-enabled AI threat detection to help stop ransomware and cryptojacking attacks for Windows-based systems. Details at <https://www.intel.com/performance-vpro>. Results may vary.
13. CrowdStrike 2024 Global Threat Report | Executive Summary, <https://www.crowdstrike.com/en-us/resources/reports/global-threat-report-executive-summary-2024/>
14. Enhancing Fileless Attack Detection with Memory Scanning | CrowdStrike, <https://www.crowdstrike.com/en-us/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/>
15. IDC, "Worldwide Digital Business Strategies 2022 Predictions"
16. 40% lower TCO by refreshing 5-year platform with fewer 5th Gen Intel Xeon Scalable platforms to meet the same performance requirement. See [T6] at <https://edc.intel.com/content/www/us/en/products/performance/benchmarks/5th-generation-intel-xeon-scalable-processors/>. Results may vary.
17. Up to 3.73x higher throughput with the new 5th Gen Intel® Xeon® Platinum 8592+ processor on VPP IPsec (1420B) with integrated QAT accelerator. See [N18] at <https://edc.intel.com/content/www/us/en/products/performance/benchmarks/5th-generation-intel-xeon-scalable-processors/>. Results may vary.
18. Up to 1.69x higher connections/second with 5th Gen Intel® Xeon® Platinum 8592+ processor

compared to 4th Gen Intel® Xeon® Platinum 8470N processor on NGINX TLS 1.3 ECDHE-X25519-RSA2K handshake with integrated QAT accelerator. See [N6] at <https://edc.intel.com/content/www/us/en/products/performance/benchmarks/5th-generation-intel-xeon-scalable-processors/>. Results may vary.

19. “Lower TCO and increase performance on your cloud workloads easily” (Google Cloud Next 2023), <https://www.youtube.com/watch?v=WThINi910ul&t=1094s>

20. “Stop Zero-Day Threats in Zero Time with Nebula” (paloaltonetworks.com), <https://www.paloaltonetworks.com/blog/2022/02/stop-zero-day-threats-with-nebula/>

21. Arqit and Intel Test Post Quantum Cryptography (PQC) Solution, <https://networkbuilders.intel.com/solutionslibrary/arqit-intel-test-post-quantum-cryptography-pqc-solution>

22. FD.io VPP-SSwan and Linux-CP – Integrate StrongSwan with World’s First Open Sourced 1.89 Tb IPsec Solution Technology Guide (intel.com), <https://networkbuilders.intel.com/solutionslibrary/fd-io-vpp-sswan-and-linux-cp-integrate-strongswan-with-world-s-first-open-sourced-1-89-tb-ipsec-solution-technology-guide>

23. Data Sharing is a Business Necessity to Accelerate Digital Business (gartner.com) <https://www.gartner.com/smarterwithgartner/data-sharing-is-a-business-necessity-to-accelerate-digital-business>

24. Privilege elevation exploits used in over 50% of insider attacks (bleepingcomputer.com), <https://www.bleepingcomputer.com/news/security/privilege-elevation-exploits-used-in-over-50-percent-of-insider-attacks/>

25. Azure Confidential Computing Blog, “Announcing: Microsoft moves \$25 Billion in credit card transactions to Azure confidential computing,” November 15, 2023, <https://techcommunity.microsoft.com/t5/azure-confidential-computing/announcing-microsoft-moves-25-billion-in-credit-card/ba-p/3981180>

26. Creating Globally Scalable Smart City Solutions (intel.com), June 2024, <https://networkbuilders.intel.com/solutionslibrary/creating-globally-scalable-smart-city-solutions>

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 configuration disclosure for details.

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.

© 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.

2025 ACG6640CSW