Intel's Security Technology Vision

Introduction

Security begins with Intel. We aim to empower customers with the most secure technology, software, and solutions, driven by innovation, to deliver enhanced security capabilities they trust to address today's complex challenges. Computing cannot reach its full potential until systems are trustworthy, confidential computing is ubiquitous, and security is disruption free.

Security is more than a point in time, it is in a continuous state of evolution and revolution. True security is driven by governance, processes, tools, and technologies that impact every stage of the product lifecycle: build, transfer, operate, and retire. Intel is one of the only manufacturers with the control capable of providing full lifecycle security. Protection rooted in hardware, from the component development to platform manufacturing, transport, and deployment, through support and retirement. No one is better positioned to lead this revolution than Intel.

In the last few years, trends have introduced a new era for security, shifting the industry focus from OS-level exploits to all layers, including down into firmware and hardware. Intel continues to invest in our security products, process, and people, building and driving a company-wide approach to security.

Intel's security vision encompasses a holistic undertaking to establish a first of its kind security capabilities and framework, supported across product types and families. This vision is anchored by 4 pillars:

- **Integrity and Trustworthiness** including efforts for establishing a verifiable foundation of trust in a system.
- **Any Data, Anywhere –** Workload Protection with emphasis on securing data, as it is used in new and novel ways.
- **Disruption Free Security** to tackle usability impediments to security.
- **Solutions –** Security Your Way focused on innovation and flexibility to empower choice in customers and developers.

This vision helps ensure Intel's ability to deliver best-in-class security far into the future. This security technology vision goes beyond silicon, reflecting Intel's leadership across the cloud to intelligent edge to client and all through the stack. Security begins with Intel.

Table of Contents

Uniquely Intel

Intel is a technology leader in manufacturing and development of both hardware and software.

> *"We are an industry leader, creating world-changing technology that enables global progress and enriches lives. We stand at the brink of several technology inflections – AI, 5G network transformation, and the rise of the intelligent edge – that together will shape the future of technology. Silicon and software drive these inflections, and Intel is at the heart of it all with data emerging as a transformational force in this era where an explosion of devices permeates all our interactions. That data must be moved, stored, and processed faster and more securely than ever before. We are unleashing the potential of data to unlock value for people, business, and society on a global scale."*
>
> https://www.intc.com/intel-online-annual-report

Intel plays a unique role in the technology industry due to a vast portfolio of products and end-to-end ownership in product development, to lead the industry in a security evolution. No single provider is positioned to have a larger, more comprehensive impact into product security than Intel. Intel offers platforms and products that incorporate various components and technologies, including a microprocessor and chipset, a stand-alone SoC, or a multichip package. Platform products are used in various form factors across diverse market segments. Adjacent products can be combined with platforms to form robust solutions to meet customer needs. In addition, our security solutions incorporate leading-edge capabilities such as artificial intelligence, machine learning, and threat detection, which form the foundation for securing the world's digital assets.

Intel has a strong ecosystem of partners, spanning Operating System Vendors (OSVs), Original Equipment Manufacturers (OEMs), Independent BIOSs Vendors (IBV), System Integrators (SIs), Cloud Service Providers (CSPs), and Independent Software Vendors (ISVs). Through these partnerships, Intel co-engineers' solutions to meet the industry's biggest security needs.

A Longstanding Commitment to Security

System trust is rooted in security — if hardware isn't secure, then a system cannot be secure. At Intel, our goal is to build the most secure hardware on the planet, from world-class CPUs to XPUs and related technology, enabled by software. And we have sophisticated systems to find and address security vulnerabilities in our products.

Intel's commitment to security has never been stronger. We invest in unparalleled people, processes, and products, integrating security in the ways we work and everything we work on. As we relentlessly pursue the best solutions to protect customer systems and data, you can be confident Intel is committed to:

- **Unwavering Customer Focus.** We put customer needs first in our security decisions. We listen to their challenges and use this feedback to guide everything we research, architect, build, and release. Trust is rooted in transparency. We communicate security advisories and product updates to help customers stay informed and keep their systems protected.
- **Continuous Technology Innovation.** New threats will emerge, and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security. From accelerating cryptography and Confidential Computing, to safeguarding our supply chain and manufacturing operations, we never stop innovating.
- **Robust Incident Response.** We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products. Our Bug Bounty program is a critical way we get outside perspectives, collaborating with researchers and leading academic institutions to find and address vulnerabilities. Intel role models best practices for incident response; when an issue is identified, we follow coordinated vulnerability disclosure practices to release findings and mitigations together.
- **Security by Design.** We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development. Intel has dedicated experts driving a security-first mindset that starts with research and design and doesn't stop until products reach end of servicing.
- **Community Advocacy.** It's clear no single entity can solve complex security challenges alone. We work with technology partners, academic institutions, industry organizations, and governance bodies worldwide. These efforts support development of policies, industry guidelines, standards, and research to elevate shared security goals that benefit everyone.

We actively work to deliver security without sacrificing performance. Working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver technology they trust.

View our security first pledge

Integrity and Trustworthiness

A critical focus for the computing industry over the last several years has been the establishment of methods for ensuring system integrity. Starting with manufacturing and supply chain, then system boot code, through system execution.

Supply chain-centered attacks continue to increase as malicious actors are attracted to the significant potential impact an attack at this stage can have. Such attacks can result in serious security issues at the most fundamental level of the product, potentially undercutting the entire foundation of security in computing systems. No security technology, no matter how advanced, can establish a trusted computing base if the hardware itself is not trustworthy.

Establishing an initial trusted state for the platform is only half of the problem. We then need to ensure that trust remains throughout execution and platform lifecycle. And with new multi-party/tenant paradigms in use today, we must partition the compute environment and provide assurance to each party their environment is trustworthy, without the need for the parties to trust each other.

Transparent Supply Chain

System security of a system starts from the moment sand turns into silicon. Systems are typically made of components from multiple vendors, each with differing security practices. This leads to complex responsibility for attesting to the security of the overall system.

Intel's vision is to provide not only a verifiable assurance of the integrity of every product we manufacture, but also a history of its provenance. Whether a manufacturer is looking to verify devices-maintained integrity in transit, the final system operator desires to re-affirm their system components, or there is a need to attest to a certain security posture or profile. By building technologies offering component integrity through unique manufacturer identity, the provenance of a product can be maintained through its entire lifecycle. This provenance, along with metrics regarding the generation of the associated product, will provide a foundation upon which higher level system trust, as well as advanced security capabilities and technologies, can be built, such as system identity and traceability.

System Identity/Traceability

Integrity of individual components is the basis for system identity and tracing. Component identities established through supply chain transparency serve as the root in deriving system level identification. This identity and traceability meets a multitude of evolving industry needs, such as enabling users in virtualized environments, like enterprise servers and cloud, to gain insights into the hardware systems their workloads are running on, and understand when their workload shifts between physical systems.

Intel's vision is to empower customers to add additional identities based on the system ID, which can be leveraged to provide traceable system identity, while removing vendors (such as OEM, or CSP) from the trust boundary. Verifiable and immutable system identity can be used to help address concerns about user or customer data by tying it to processing operations. Enabling customers assurance of, and insight into, the systems utilizing their data.

Intel's vision is to enable full traceability of products throughout the compute lifecycle and leverage the associated system identity to support monitoring and control of user data on platforms. These capabilities will serve as the trusted root for additional security technologies deployed across products.

Cyber Resilience

The ability to protect system firmware, detect any compromise in it, and recover from such compromises is often referred to as cyber resilience. Several industry specifications, from NIST SP800-193 to the Trusted Computing Group's Cyber Resilient Module and Building Block document , have defined the critical elements and methods for implementing cyber resilience of platform firmware. Yet cyber resilience means more than just protecting the firmware. Users and platform operators require the ability to determine at any time whether a platform is still trusted, and if not, the ability to re-establish trust.

Intel's vision includes new technology and capabilities to enable customers to meet industry best practices and standards for cyber resilience. This includes verifiable platform attestation of their current execution environment. Supporting not only local self-attestation, but also enabling out-of-band attestation to more strongly validate the attestation information provided as well as verify its accuracy. Out-of-band introspection provides a more secure and method of performing automated detection and patching of a compromised system.

Trusted Telemetry

The CPU is often the coordinator, horsepower, and enforcer of a system. Through this key role, the CPU generates and has access to a range of telemetric data. Data not only from the CPU but other discrete components such as the GPU and memory. Through novel uses of AI, ML, inferencing and data analytics, highly accurate and otherwise software-undetectable threats, and software undetectable system details such as vulnerability applicability can be identified. Intel's vision is to continue driving the industry to new capabilities of advanced security threat awareness by continuing to build upon the rich hardware telemetric data inside of discrete hardware. To further empower telemetry usability, through mutual coordination of Intel discrete components, the necessary compute power can be offloaded reducing or removing performance impact.

The compute ecosystem is ripe for the evolution of cyberattacks. Withstanding the volume, complexity, and expanded attack surface threats requires the analysis of enormous amount of data. AI is becoming an essential tool to improve the quality of data analysis, provide rapid insights to improve response time, and even predict the attacks. Hardware telemetry can enable the deep insights of computation behaviors that can be leveraged as threat sensors for AI-based solutions.

Intel's vision is to enable developers to build and optimize cutting-edge solutions that leverage the combination of the hardware telemetry, and AI/ML heuristics to reduce false positives and accelerate solutions on the best available compute unit.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf
[2] https://members.trustedcomputinggroup.org/wg/CyRes/document/

Any Data, Anywhere – Workload Protection

Computing continues to expand to more data workloads, and where compute happens continues to expand. As computational needs increased beyond what centralized systems could flexibly support, we saw the explosion of distributed networks and computing. This brought a disaggregation of data computing, spanning intelligent edge, from client to cloud, with data transitioning between them in private, public, and multi-cloud environments. The creation of high-speed telecommunications networks such as 5G, and an increased need for lower latency processing close to the consumer is pushing the boundaries even further to the edge.

Confidential Computing

Computing is becoming increasingly distributed, run across multi-tenant environments, and multi-party ecosystems. The broad adoption of cloud computing has led to security concerns of Cloud Service Providers (CSPs) to ensure confidentiality of information processed on a system where multiple parties or tenants may be simultaneously engaged. Tenants rarely have insight into who has processes executing on the same platform, or what access the CSP itself has to their data. This need for separating processing from the platform owner is not restricted to just the cloud providers, but increasingly in our distributed and disaggregated world, wherever computation takes place.

Ensuring the trust of the full operating environment quickly grows in complexity, giving way to a different approach that reduces the computing infrastructure needed to be trusted. Confidential computing is the notion of protecting data as its being processed from the operator of the platform on which it is being processed.

Trusted Execution Environments (TEEs), and advanced cryptographic techniques such as Homomorphic Encryption, enable the protection of computations of sensitive data. Intel was a pioneer in establishing confidential computing, reducing the Trusted Computing Base (TCB) to its smallest possible size. Intel's vision is to continue innovating through a portfolio of technologies in this space. Offering flexibility for virtualized and bare metal, support for all memory types, attestable integrity, and enhanced coordination between TEE's and other discrete components. Meeting the unique needs to protect data both logically and physically, for each confidential compute use case.

Artificial Intelligence (AI)

AI solutions continue to grow and proliferate diverse markets, enabling innovative use cases across the intelligent edge to cloud. AI offers businesses and end-customers new experiences and benefits, but introduces risks and trustworthiness concerns, including ethical and governance challenges. Intel is partnering with the technology industry to define a/the trustworthiness principle for AI, which aims to establish the security dependencies at each layer of AI.

At a high-level, AI consists of three critical assets: the data, the model, and the processing infrastructure. While centralized AI usage (where all assets are centrally owned and operated on) continues to be prevalent, the expansion of trusted execution capabilities has given rise to Collaborative or Federated Learning. In Federated Learning multiple parties, each with unique data, can collaboratively train an AI Model while each keeping their data private. The more unique data a model can be trained on the more affective the model will be. Federated learning enables previously impossible AI collaborations across critical industries such as healthcare, IoT, and telecommunications. Allowing a shared model to be trained by each parties' unique data, without ever exposing the information to other collaborators. In all use cases the trust and sensitivity of AI resides in protecting the data, the model, and the processing environment. Malicious parties aim to poison, steal, or manipulate at all stages of the lifecycle (development, training, deployment, and execution/inferencing).

Intel's vision is to empower trust in the Artificial Intelligence (AI) industry with a mix of software and hardware innovation, bolstering developers with tools to harden data acquisition, classification, training, inferencing, storing, ownership enforcement, and model protection.

Better Together

Security extends beyond processors and plays a role in every discrete system component. Intel's market leadership in component areas, including Memory, Networking, and Graphics, grants a unique value to customers by embracing "stronger together" security solutions.

Intel Field-Programmable Gate Arrays (FPGAs), Intel Infrastructure Processing Unit (IPU), and Intel Graphics Processing Units (GPUs) partner with the CPU to offload and accelerate security driven activities. Through this offloading the system performance impact of resource intensive activities such as advanced telemetry, exhaustive memory searching, and network operations, can be reduced. Intel FPGA/ GPU and CPU TEE coordination helps protected workloads being transferred between devices.

Intel's vision is "better together" security solutions where critical system components verify and attest to each other's integrity and trustworthiness. Allowing data to move throughout a system without ever being exposed. Compute will be re-directed to components with spare resources and accelerators enabling more powerful security computations.

Disruption Free Security

Security has historically demanded a tradeoff between usability and performance, but Intel's vision is disruption free security: the security needed without compromising on performance or usability. A trustworthy and secure system with perfect protection of data is useless if it comes at the expense of system usability. Our vision is to reduce down-time, off-load security to out-of-band elements, and deploy highly optimized, in-line security technologies to enable the security to happen, without interrupting workstreams.

No More Downtime

Security vulnerabilities will continue to evolve, and ongoing updates remain among the most foundational capabilities needed to maintain system security and performance. Every computer user understands the downtime that comes with installing updates. The ecosystem at large has recognized the importance of update delivery usability and automation in driving adoption of critical updates. Yet, for many environments there is no such thing as a convenient time to go offline to deploy an update.

Recognizing the need for disruption-free alternatives, Intel revolutionized security management and update usability solutions, bringing the first reboot-free updates to firmware patches on data center CPUs. Intel's vision is to continue expanding disruption free patching to more platforms, more patches, and more discrete hardware (GPU, memory, storage), building a future where reboot Wednesday is a thing of the past.

Security Offloading

Most security capabilities are executed within the physical execution element that processes user data. This can potentially cause performance impact to critical computing due to interrupts, context switches, and execution of the security solution itself.

Intel's vision is the introduction of active component root-of-trust, and platform-level root-of-trust to enable offloading of security functionality. Such elements will have the necessary introspection and access capabilities to execute out-of-band of the traditional OS and general compute. This enables offloaded security technologies to have minimal impact on performance or usability of the main processing element, while also providing a higher level of security through computing isolation. Intel aims to define, implement, and further expand the ability to offload security in such a manner to minimize impact on users and organizations.

Ubiquitous Crypto

Cryptography is the foundation for many security best practices: encryption to signatures to hashing. Intel continues to drive hardware-based cryptographic acceleration, including purpose-built crypto instruction sets leveraging optimized microcode flows.

Through increased computational acceleration inside the CPU, combined with closer offloading coordination with other discrete components such as GPU or FPGAs, cryptography can become ubiquitous. This is further empowered through the evolution of Intel's novel core architecture, consisting of power and efficient cores with advanced resource directing.

Intel's vision is cryptography without performance impact. Enabling a future of full memory, data caches, and inter-component communication all happening with cryptographic hardening.

Intel's vision is to lead adoption of cryptographic post-quantum (PQ) resistant computing. Intel will continue to drive the industry in PQ requirements for code signing, key management, and thought leadership in this critically maturing area.

Industry Engagement

Fostering development of industry standards is a critical part of enabling the secure, interoperable, and scalable adoption of security technologies. Intel leads and participates in industry consortiums, standard bodies, and public-private partnerships. Advancing our joint understanding of how new technologies should be designed, by defining requirements and solutions for organizations, and developing novel approaches to enhance hardware-based security. Intel also engages with policymakers and governments on proposed policies that foster the adoption of secure technologies and advance the security of the ecosystem as the threat landscape evolves.

Addressing security challenges requires the full ecosystem, and Intel's vision is to continue to expand our ecosystem engagement and standards efforts. Intel participates in international organizations driving the development of security-related standards, including

- Trusted Computing Group (TCG)
- Open Computer Project (OCP)
- Distributed Management Task Force (DMTF)
- International Standards Organization (ISO)
- International Electrotechnical Commission (IEC)
- Confidential Computing Consortium (CCC)
- 3rd Generation Partnership Project (3GPP)
- National Institute of Standards and Technology (NIST)
- Peripheral Component Interconnect Special Interest Group (PCI-SIG).

These efforts include various solutions that foster increased protections against physical attacks, encryption of data-links, definitions of system-level attestation, verification of execution integrity, and post launch servicing transparency duration among others.

Solutions – Security Your Way

Intel's security vision addresses two critical aspects: security is always evolving, and solutions are not the same for every system. Security risk is use case dependent, and context based. Processing elements are specifically designed with static specifications regarding characteristics such as execution speed, throughput, and power consumption. Security does not stay static. What was secure yesterday may not be tomorrow. As such, the final aspect of Intel's vision is customizable, configurable, and updateable security that can be tailored to the evolving needs of each customer, based on their specific deployment scenario and threat model.

Security Solutions

Intel empowers customers and users to customize and build security solutions leveraging our industry-leading technology, adapting to meet their unique needs. As users and operators are faced with ever-increasing systems, users, data, and environments, the value of complete solutions continues to rise.

Intel's vision is to continue to empower the industry through our portfolio of security technologies, but also lead the industry in solutions that solve our customers' most critical business security needs. Intel solutions will bring together the power of Intel components, mutually coordinating inside systems and across ecosystems. Leveraging the hardware's advanced capabilities, data, and telemetry, to deliver solutions that software alone cannot provide. To meet the most crucial needs in system Assurance, Trust, Migration, Attestation, and Compliance.

Custom Manufacturing

Every computing situation is unique, from the risk profile to the computational requirements. Creating a lineup of products that meet all situational needs, while a noble pursuit, is difficult. While we offer numerous SKU's, each designed to meet a

leading market need, we recognize there is still a need for customers to customize our products. With the introduction of Integrated Device Manufacturing (IDM) 2.0 and the Intel Foundry Services (IFS) organization, the opportunity to support such needs is now at our fingertips.

Intel's vision is empowering customer with choice, to customize silicon to meet their unique security and computing needs. This means allowing customers to focus on their specific risk use cases and leveraging Intel's industry leading portfolio of security technologies. Through the power of IFS, customers will be empowered with choice- the choice to use Intel security technologies, layer on their own, or fully customize.

Feature Flexibility

Threats, environments, and deployments change, and the security needs of a system might also change. Today, purchase decisions are made with an understanding of current needs and a guess at future ones. All too often, the future brings unanticipated security needs that may not align with current system capabilities.

Intel's vision is to empower customers to change the security capabilities of current systems to meet their evolving security needs. Transcending traditional software-based feature expansion, Intel's aims to enable customers to activate dormant hardware-based security features as needed, removing the pressure of anticipating every future need at the initial purchase time. Hardware that meets today's needs and can adjust to those of tomorrow.

Framework for Solutions Ecosystem

The computing industry today is met with unprecedented security challenges as malicious attackers continue to expand and exploit their advantages. Organizations continue to see unique challenges driven by characteristics such as their industry, product portfolio, or geography. Computing users and providers often struggle to keep pace and deploy sufficient mitigations and capabilities. In addition to our goal of providing security solutions, Intel believes in the power of choice and empowering the developer ecosystem to bring novel security technologies to the industry.

Intel's vision is to empower the ecosystem to build cutting edge security technologies on our platforms. By building and exposing novel frameworks that allow for elevated system telemetry, introspection, configurability, simplified interfaces, out of band communication, and robust open development ecosystems. Our goal is to empower developers and customers to harness the power of our platforms to meet their unique security needs.

Conclusion

Addressing constantly evolving threats requires an evolution in security. Security must be reimagined in ways that allow for specific deployment scenarios to be customized, configured, and continually evolve as circumstances change. Security must be rooted in foundational technologies starting at the earliest stages of the product design and continue throughout the product lifecycle.

Intel's security vision encompasses a holistic undertaking to establish a first-of-its-kind security capabilities and framework. Supported across product types and families, enabling an entire ecosystem of new security capabilities, and enhanced existing capabilities that will continuously evolve to protect against future threats.

We are working to empower our customers with the most secure systems, software, and solutions, driven by innovation, to enhance security capabilities they trust – while providing them enhanced and customized solutions to attest and demonstrate the security posture delivered by these solutions. Intel will drive computing to reach its full potential through trustworthy systems, ubiquitous confidential computing, and disruption-free security.

Now more than ever, security begins with Intel.

0222/DCC/SD