Security @ Intel

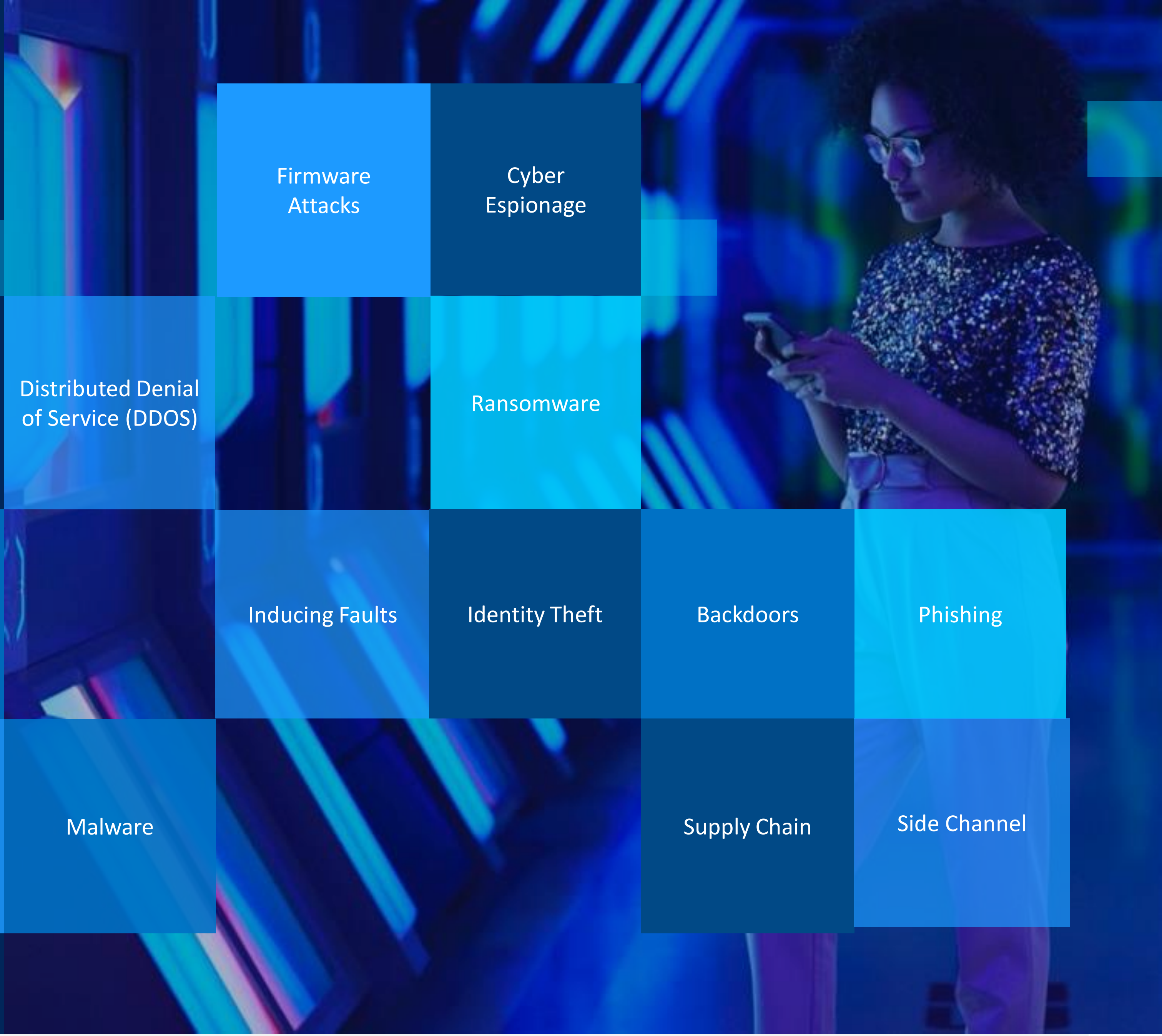
Understanding our investments in security assurance practices and technology

intel® security

Addressing The Security Landscape

Threat Landscape

External threats are growing in complexity and precision



Firmware Attacks

Cyber Espionage

Distributed Denial of Service (DDOS)

Ransomware

Botnets

Inducing Faults

Identity Theft

Backdoors

Phishing

Counterfeiting

Physical Tampering

Malware

Supply Chain

Side Channel

Source: IBM, Cost of Data Breach Report 2020

Consequences have never been higher

315 days

Average time
to detect
and contain
a malicious data breach

- ⚠ Fraud, loss of sensitive data or IP
- ⚠ Legal and compensation costs
- ⚠ Regulatory fines
- ⚠ Brand and reputational damage

Governments are working to regulate, in order to mitigate threats and vulnerabilities and manage risk.

Source: IBM, Cost of Data Breach Report 2020

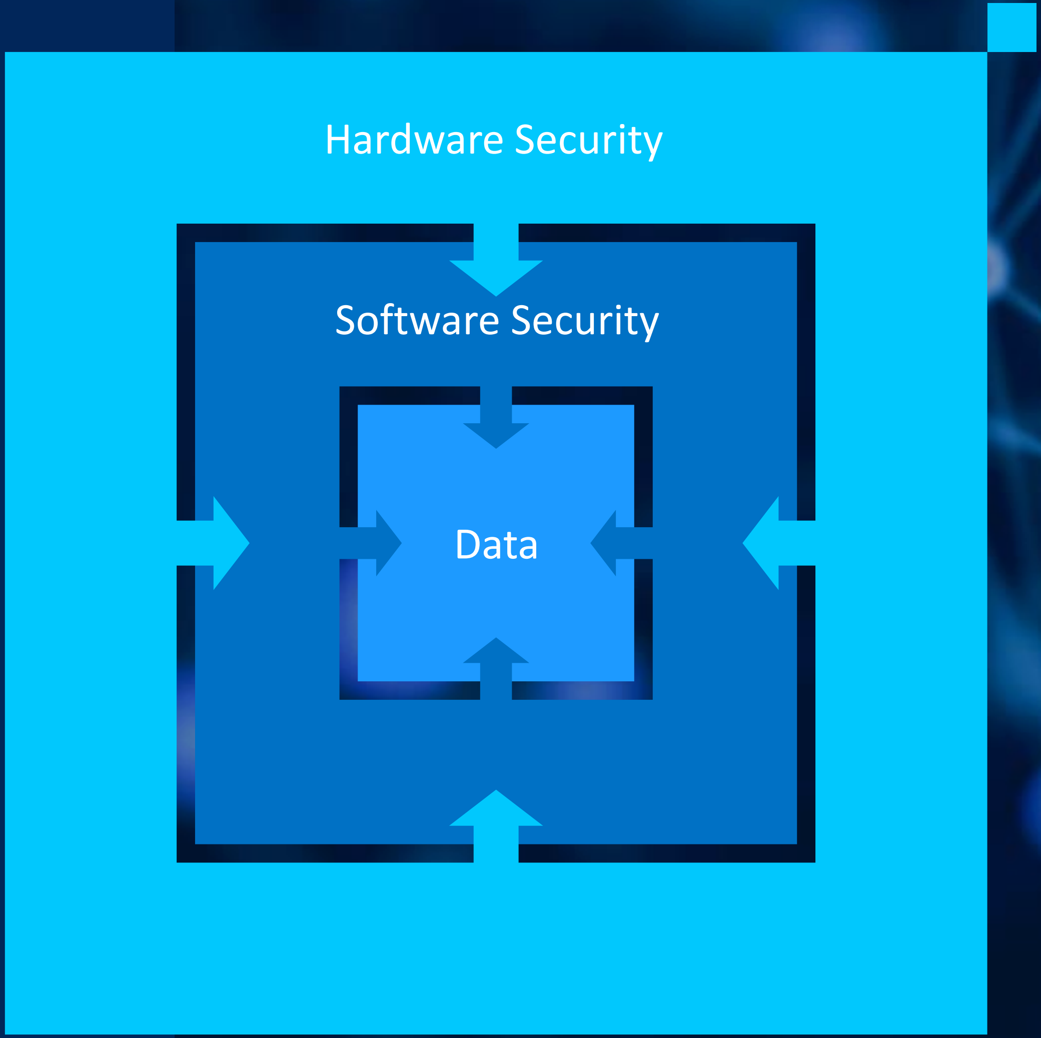
Securing hardware is foundational to all security efforts

Provides a trusted foundation to protect data.

Empowers software to provide protection while reducing performance impact

Enables software security to deliver functionality with a basis in hardware.

Attackers are increasingly targeting hardware, as attacks at this level can gain greater control.



Intel’s Security Commitments

At Intel, security comes first

In the way we work:

Practices

Our culture and practices guide everything we build with the goal of delivering the highest performance and optimal protections

- Secure Development Practices
- Threat Discovery & Response
- Community & Policy Advocacy

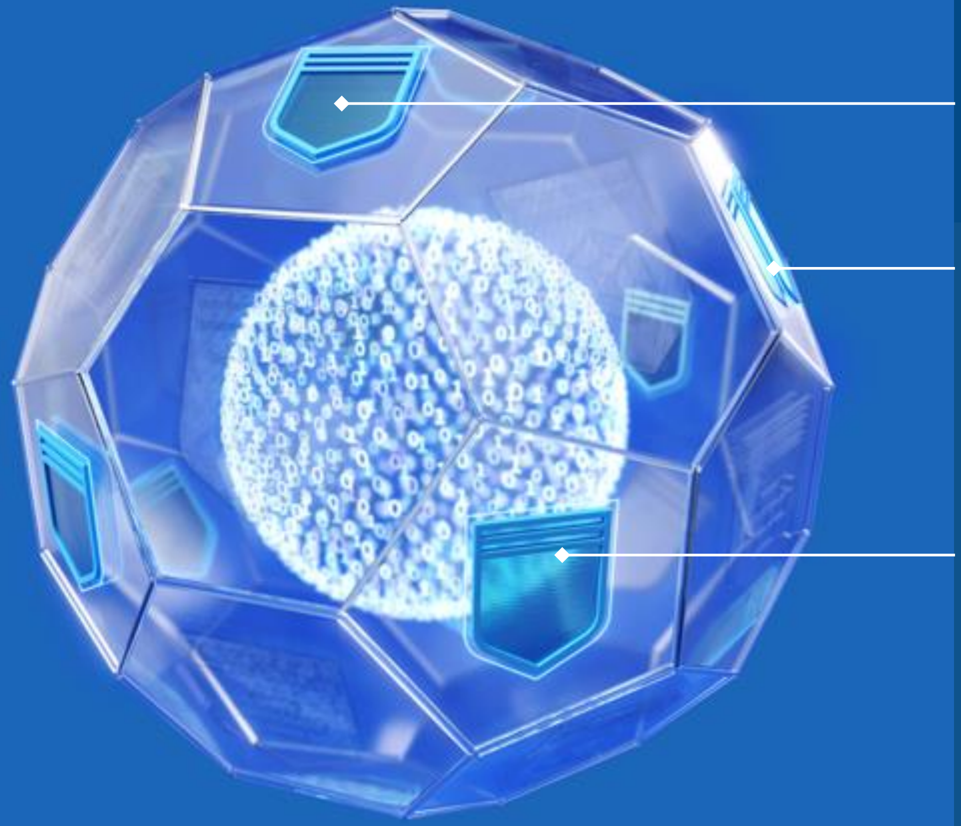
In what we work on:

Technology

We are relentless in our pursuit of innovations, taking a security-centric approach, that enables our customers to tackle today's toughest challenges

- Software Reliability
- Workload Protection
- Foundational Security

At Intel, security comes first



The way we work:

Practices

Our culture and practices guide everything we build with the goal of delivering the highest performance and optimal protections

Secure Development Practices

Integrating security principles at every lifecycle stage to help ensure products are built with security in mind

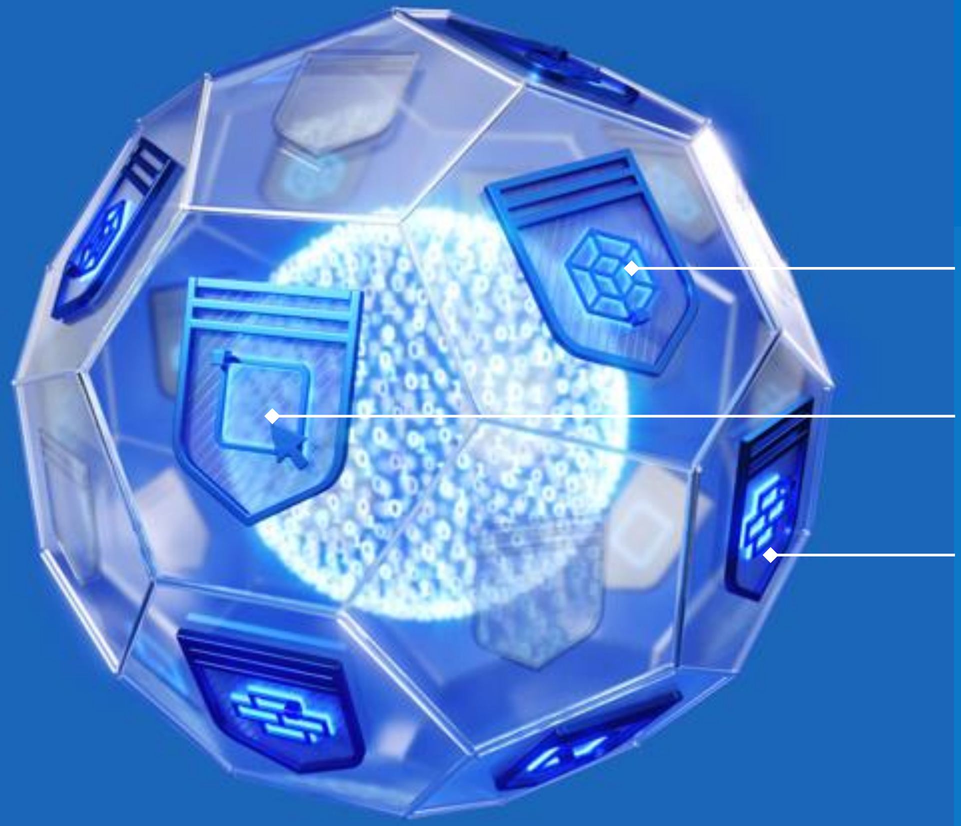
Threat Discovery & Response

Delivering discovery through offensive security research, Product Security Incident Response (PSIRT) and bug bounty.
Routinely sharing security mitigations and updates.

Community & Policy Advocacy

Leading cross-industry efforts to advance standards, government policies and industry best practices

At Intel, security comes first



What we work on:

Technology

We are relentless in our pursuit of innovations, taking a security-centric approach, that enables our customers to tackle today’s toughest challenges

Foundational Security

Hardware-based security creates a trusted foundation for helping protect data in all its phases: at rest, in flight, and in use

Workload Protection

A trusted execution environment designed for hardware-isolated protection of data, flexible to fit any workload

Software Reliability

Hardware embeds protections against common and emerging software attacks, aiming to lower your risks while preserving performance

Security is more than technology

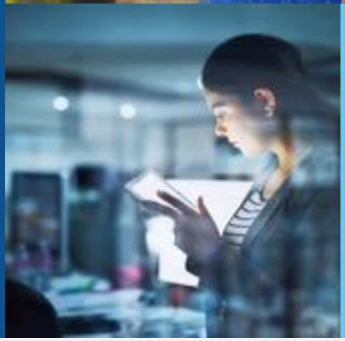
Intel builds genuine partnerships with our customers and ecosystem to understand their needs and collaborate on security solutions designed to generate time and cost savings.

Intel’s security approach creates empowerment, enablement and partnership

Partnering through security integration and attestation support

Enabling security in our partners’ processes beyond integration

Empowering through information sharing: regular reporting and guidance



Partnering through security integration and audit support

Compressing integration time, reducing development time and increasing confidence

- Security configuration auditing tools
- Security-backed advanced debugging
- Robust reference code, open source libraries, and SDKs
- Development and Customer Reference Boards
- Security-focused community with dedicated Intel support

Enabling security in our partners’ processes beyond integration

Intel helps customers to deliver enhanced security capabilities to end users

- Predictable rollup security patch cycles
- Transparent supply chain security and assurance
- Robust reference code, open source libraries, and SDKs
- Transparent support timelines, and clear end of life
- Partnering on passthrough security messaging
- End to end product assurance

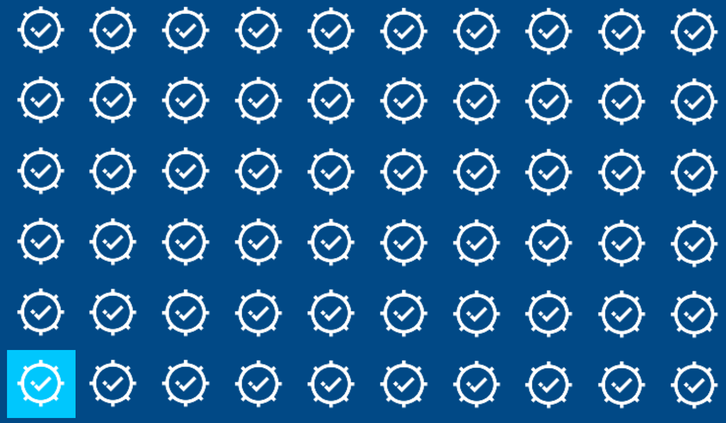
Empowering through information sharing: regular reporting and guidance

Helping customers better assess their security posture and make informed decisions to protect systems and data

- Annual product security report
- Monthly security rollup bulletins
- Disclosure process for internal and external findings
- Coordinated Vulnerability Disclosure
- Impactful security advisories, whitepapers
- Comprehensive mitigation details and guidance

Security disclosures mean Intel is closing gaps before they can be exploited

intel



Self-disclosed vulnerabilities mean Intel has successfully closed off opportunities for exploitation

Competitor

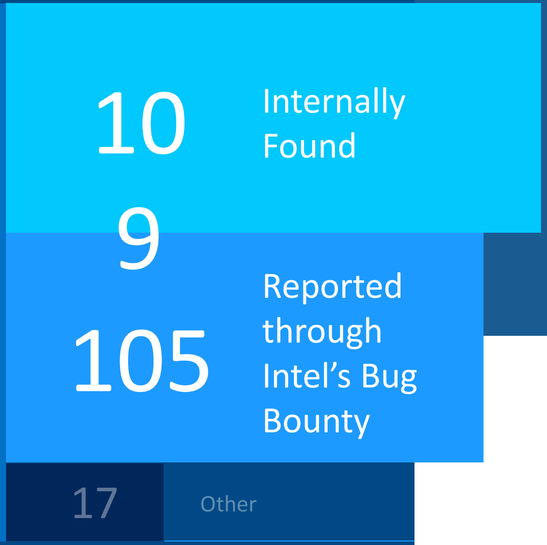
Undisclosed – and undiscovered - vulnerabilities leave organizations open to attack

More disclosures ≠ more issues

Intel discloses numerous vulnerabilities because we invest heavily in finding, mitigating and reporting them.

All pictures are for illustrative purposes only and are not intended to reflect actual results

Our customers can rely on us to address vulnerabilities, before they become attacks



92%

vulnerabilities addressed through Intel channels

In 2020, 92% of vulnerabilities addressed were found as the result of Intel's proactive investments in security research

None of these vulnerabilities have led to a known attack

Source: 2020 Intel Product Security Report

Security
at Scale

The scale of Intel's security capabilities is unmatched.

500+
Dedicated product security staff

987
PSIRT tickets closed in 2020

7000
Active projects tracked in Intel's Security Development Lifecycle system

400
Max. security tasks per project

In 2020

116
Public security whitepapers

120
Hackathons held

40+
Academic research teams funded

Intel's Security Advantage

Seasoned

5 decades of experience delivering high-performing, robust products

Pioneer

Deploying Secure Development Lifecycle in hardware and software,
at scale

Mature

13 years of an industry leading and respected PSIRT program

Dedicated

Purpose-built teams of Offensive Security Researchers partnered with industry researchers

Advocate

Partnering with industry and government to advance security best-practices, and advance innovation

Innovator

Worldwide leader in supply chain security and assurance

How seriously does your vendor take product security?

Do they disclose CVEs for issues found in their products, including those found internally?

1

Do they apply Security Development Lifecycle practices to their range of products?

2

Do they have a dedicated PSIRT to effectively manage security incidents?

3

Do they have a Bug Bounty program to encourage external security research on their products?

4

Do they have offensive security research expertise to identify vulnerabilities in their products?

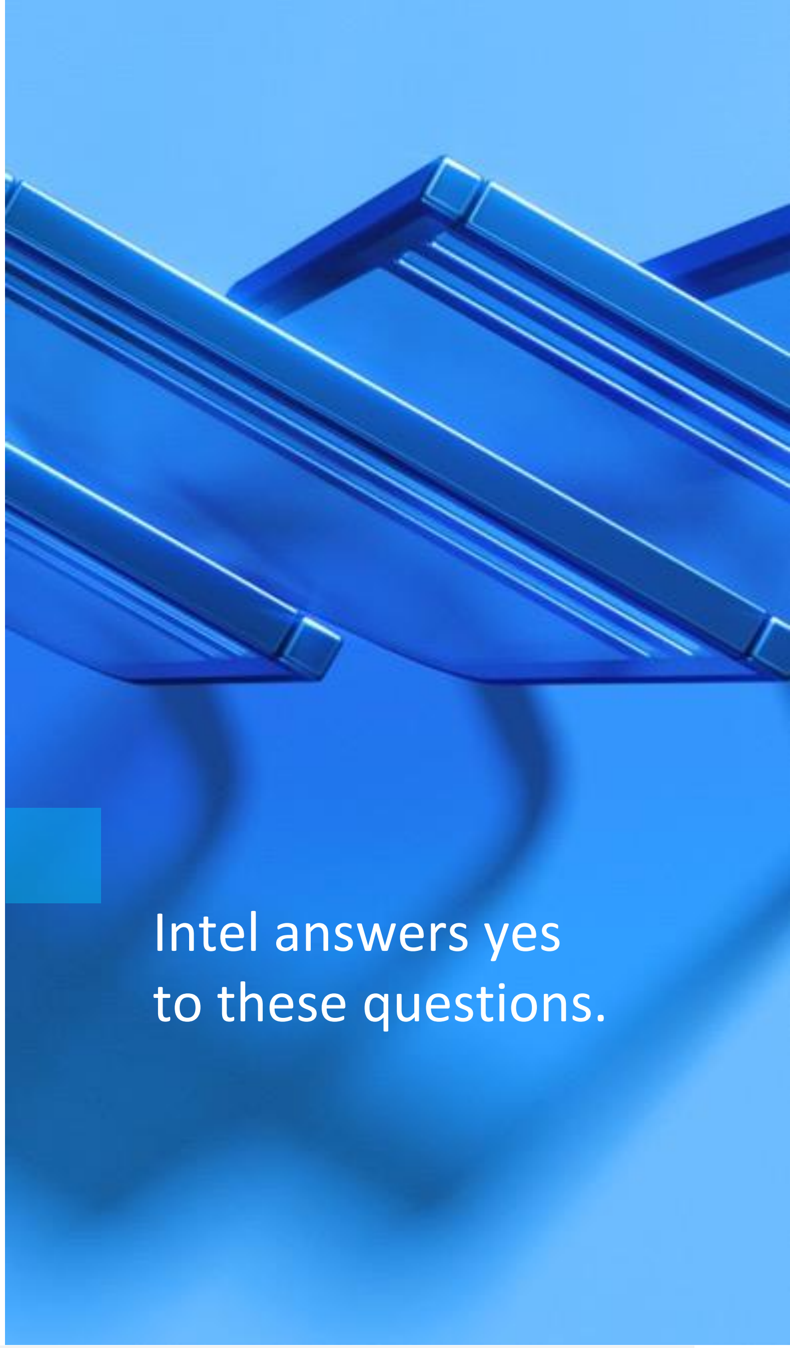
5

Are they open about communicating security updates and mitigations?

6

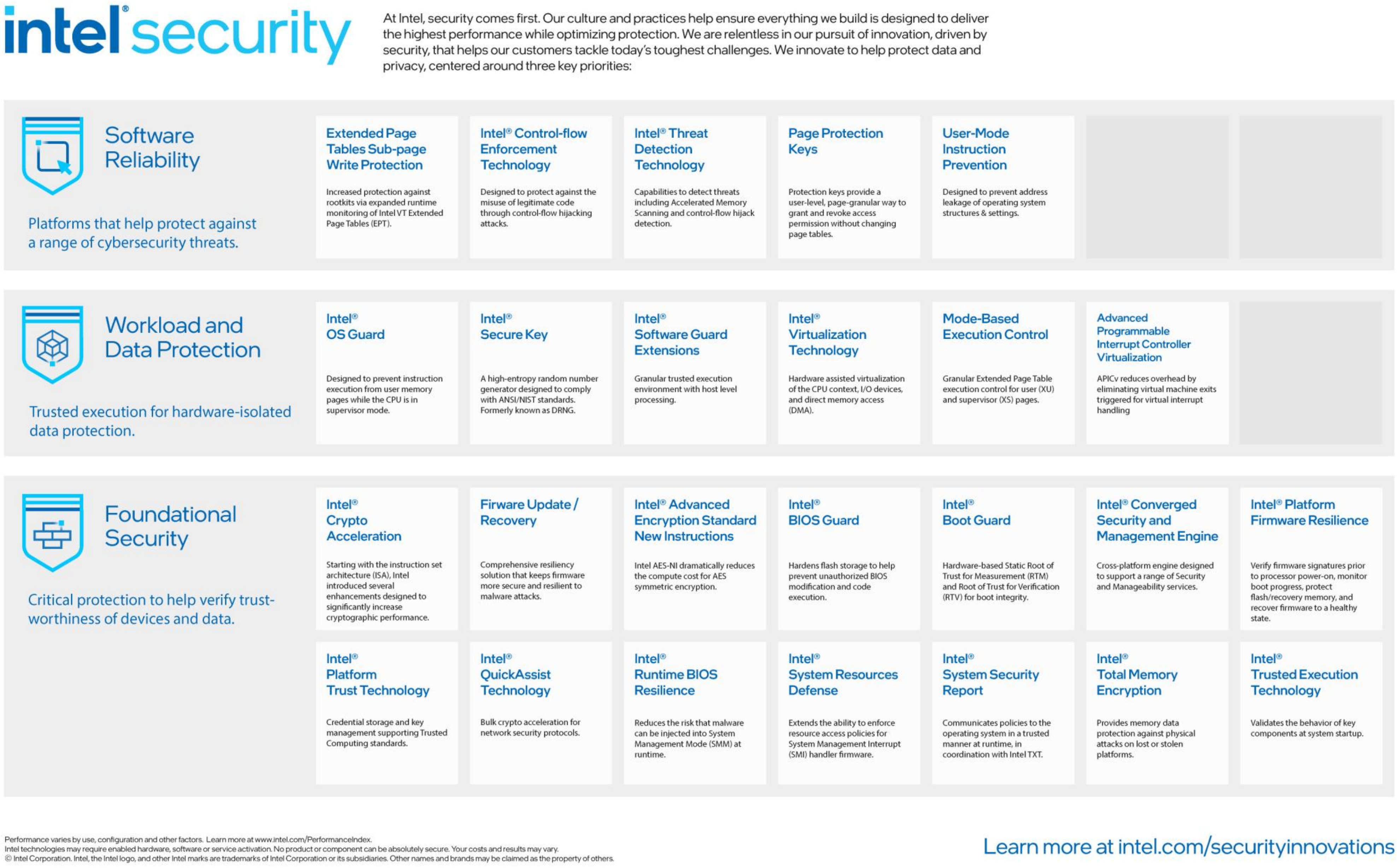
Do they have access to their range of products going back 10+ years to test and triage?

7



Intel answers yes to these questions.

Appendix:
Detailed Overviews



intel security

At Intel, security comes first. Our culture and practices help ensure everything we build is designed to deliver the highest performance while optimizing protection. We are relentless in our pursuit of innovation, driven by security, that helps our customers tackle today's toughest challenges. We innovate to help protect data and privacy, centered around three key priorities:

Software Reliability

Platforms that help protect against a range of cybersecurity threats.

Extended Page Tables Sub-page Write Protection

Increased protection against rootkits via expanded runtime monitoring of Intel VT Extended Page Tables (EPT).

Intel® Control-flow Enforcement Technology

Designed to protect against the misuse of legitimate code through control-flow hijacking attacks.

Intel® Threat Detection Technology

Capabilities to detect threats including Accelerated Memory Scanning and control-flow hijack detection.

Page Protection Keys

Protection keys provide a user-level, page-granular way to grant and revoke access permission without changing page tables.

User-Mode Instruction Prevention

Designed to prevent address leakage of operating system structures & settings.

Workload and Data Protection

Trusted execution for hardware-isolated data protection.

Intel® OS Guard

Designed to prevent instruction execution from user memory pages while the CPU is in supervisor mode.

Intel® Secure Key

A high-entropy random number generator designed to comply with ANSI/NIST standards. Formerly known as DRNG.

Intel® Software Guard Extensions

Granular trusted execution environment with host level processing.

Intel® Virtualization Technology

Hardware assisted virtualization of the CPU context, I/O devices, and direct memory access (DMA).

Mode-Based Execution Control

Granular Extended Page Table execution control for user (XU) and supervisor (XS) pages.

Advanced Programmable Interrupt Controller Virtualization

APICv reduces overhead by eliminating virtual machine exits triggered for virtual interrupt handling

Foundational Security

Critical protection to help verify trust-worthiness of devices and data.

Intel® Crypto Acceleration

Starting with the instruction set architecture (ISA), Intel introduced several enhancements designed to significantly increase cryptographic performance.

Firware Update / Recovery

Comprehensive resiliency solution that keeps firmware more secure and resilient to malware attacks.

Intel® Advanced Encryption Standard New Instructions

Intel AES-NI dramatically reduces the compute cost for AES symmetric encryption.

Intel® BIOS Guard

Hardens flash storage to help prevent unauthorized BIOS modification and code execution.

Intel® Boot Guard

Hardware-based Static Root of Trust for Measurement (RTM) and Root of Trust for Verification (RTV) for boot integrity.

Intel® Converged Security and Management Engine

Cross-platform engine designed to support a range of Security and Manageability services.

Intel® Platform Firmware Resilience

Verify firmware signatures prior to processor power-on, monitor boot progress, protect flash/recovery memory, and recover firmware to a healthy state.

Intel® Platform Trust Technology

Credential storage and key management supporting Trusted Computing standards.

Intel® QuickAssist Technology

Bulk crypto acceleration for network security protocols.

Intel® Runtime BIOS Resilience

Reduces the risk that malware can be injected into System Management Mode (SMM) at runtime.

Intel® System Resources Defense

Extends the ability to enforce resource access policies for System Management Interrupt (SMI) handler firmware.

Intel® System Security Report

Communicates policies to the operating system in a trusted manner at runtime, in coordination with Intel TXT.

Intel® Total Memory Encryption

Provides memory data protection against physical attacks on lost or stolen platforms.

Intel® Trusted Execution Technology

Validates the behavior of key components at system startup.

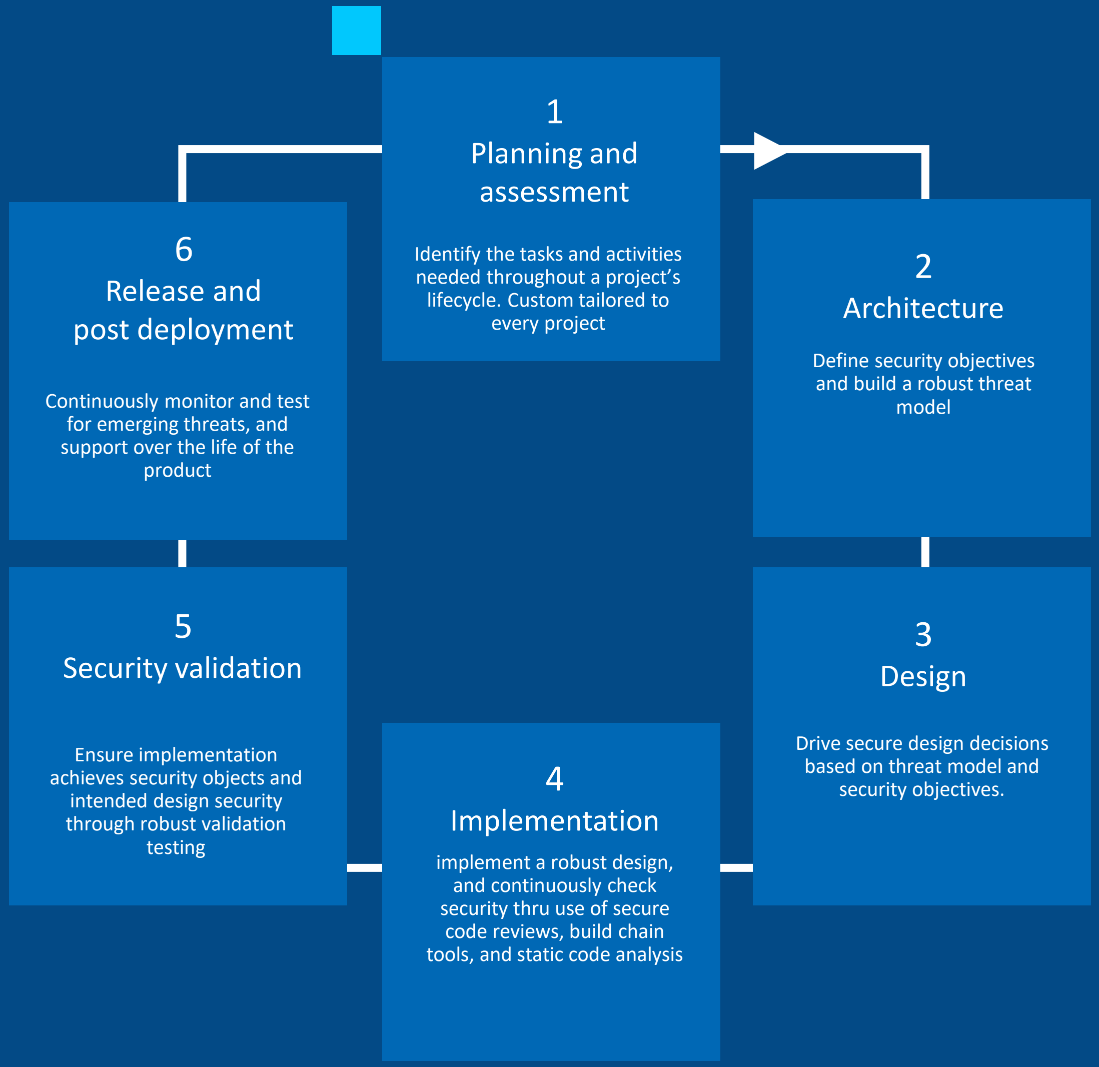
Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex.
Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary.

Learn more at intel.com/securityinnovations

Source link

Security Development Lifecycle (SDL)

The Intel Security Development Lifecycle (SDL) guides us in applying privacy and security practices across hardware and software (including firmware) throughout the product lifecycle.



1
Planning and assessment

Identify the tasks and activities needed throughout a project's lifecycle. Custom tailored to every project

2
Architecture

Define security objectives and build a robust threat model

3
Design

Drive secure design decisions based on threat model and security objectives.

4
Implementation

implement a robust design, and continuously check security thru use of secure code reviews, build chain tools, and static code analysis

5
Security validation

Ensure implementation achieves security objects and intended design security through robust validation testing

6
Release and post deployment

Continuously monitor and test for emerging threats, and support over the life of the product

Offensive Security Research (OSR)

Ensuring we are continually finding, mitigating and reporting security issues in our products.

Proactive Research

Dedicated researchers continually monitor and probe Intel products and platforms for known, emerging, and novel threats and attacks.

- Intelligence Insights
- Architecture Reviews
- Threat Model ++
- Vulnerability & Exploitation
- Systemic Mitigations

Reactive Research

Intel acts swiftly when a new vulnerability or exploit is discovered, quickly working to develop systemic mitigations.

- Triage incoming PSIRTs
- PSIRT mitigation effectiveness

Capabilities & Culture

Solutions to instill the security-first mindset within every Intel architect, developer, designer and validator.

- Immersive Mentoring
- Security Belts
- Tools
- Purple Teams
- Training
- SDL

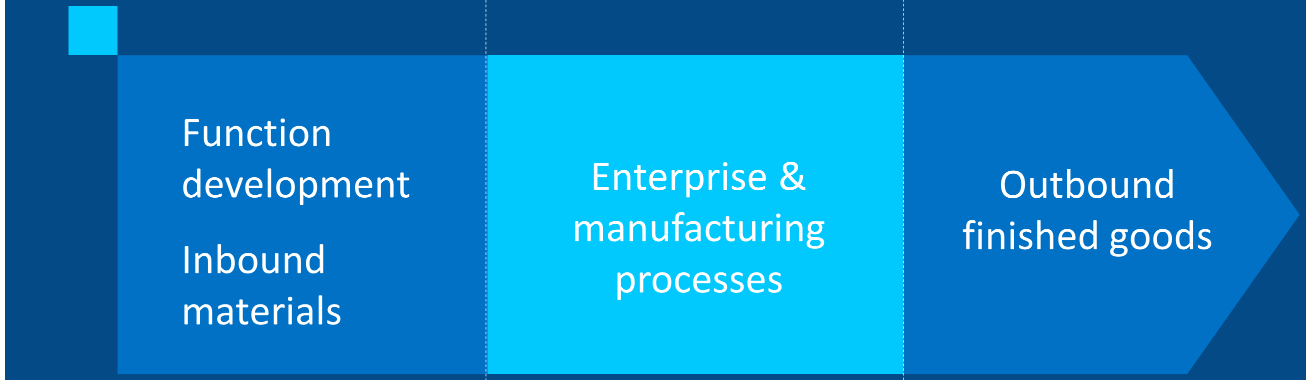
Researcher & Community Outreach

Investments to engage the global research community in industry and academia.

- Listening Events
- Research Sponsorship
- Diversity & Inclusion

Manufacturing & Supply Chain Security

Intel's supply chain spans 28 countries and ~14,000 suppliers, orchestrated to deliver ~2 billion units of Intel product annually. Intel has extensive controls to help maintain security in manufacturing and supply chain.



Function development

Inbound materials

Enterprise & manufacturing processes

Outbound finished goods

Design and Research

Protecting essential IP to help ensure designs and data are not compromised, whether in-house or outsourced.

Sourcing

Integrating security across our global supply chain, through selection criteria, contractual security expectations, ongoing remediation of vendor vulnerabilities, and regular audits.

Manufacturing and Test / Assembly

Copy exactly methodology limits introduction of unknown variables that could pose a security risk.

ISO 9001 device level traceability to efficiently track issues to their source.

Information Technology

Daily scanning of over 650,000 devices, automated protections and a robust incident response strategy.

Physical Security

Restricting authorized access to and monitoring of manufacturing facilities, warehouses, offices, networks and materials

Distribution and Logistics

C-TPAT, TAPA compliant transport and storage

Industry leading anti-counterfeit methods and research.

Vulnerability Management

Systematic management and response tactics – including internal and external research teams, and work across the industry – continually working to strengthen the security of our products.

Intel Product Security and Incident Response Team (PSIRT)

Central point for managing security vulnerabilities response. Now in its 13th year, the team continues to define industry best practices in identification, management and disclosure of vulnerabilities.

Intel Bug Bounty Program

Encouraging external security researchers to report vulnerabilities they find in Intel products and coordinate on disclosure. It is one of the top programs in the industry for its breadth, ranking #4 in 2020 for total payouts.

Coordinated Vulnerability Disclosure (CVD)

Industry driver for adoption and maturation of CVD processes. Responsibly disseminating information to stakeholders, and only publicly disclosing after mitigations are deployed.

Intel Platform Update (IPU)

The Intel Platform Update (IPU) helps ensure Intel products remain up to date in the field. Designed to have predictable and consistent timelines, and transparent messaging.

Community & Policy Advocacy

Intel partners with a range of industry-leading organizations, academic institutions and governance bodies to accelerate our shared secure, data-centric vision.

Technology Vendor Partnerships

Intel spear-heads a cross-industry council with 20+ industry influencing companies to accelerate our collective understanding of the latest security threats, validate potential impacts, develop mitigations and coordinate vulnerability disclosures.

Industry Initiatives

Intel is active in initiatives that focus on data security and privacy. Intel contributes to numerous industry consortiums, with emphasis on developing industry-wide standards for technology, security assurance and development.

Policy & Government

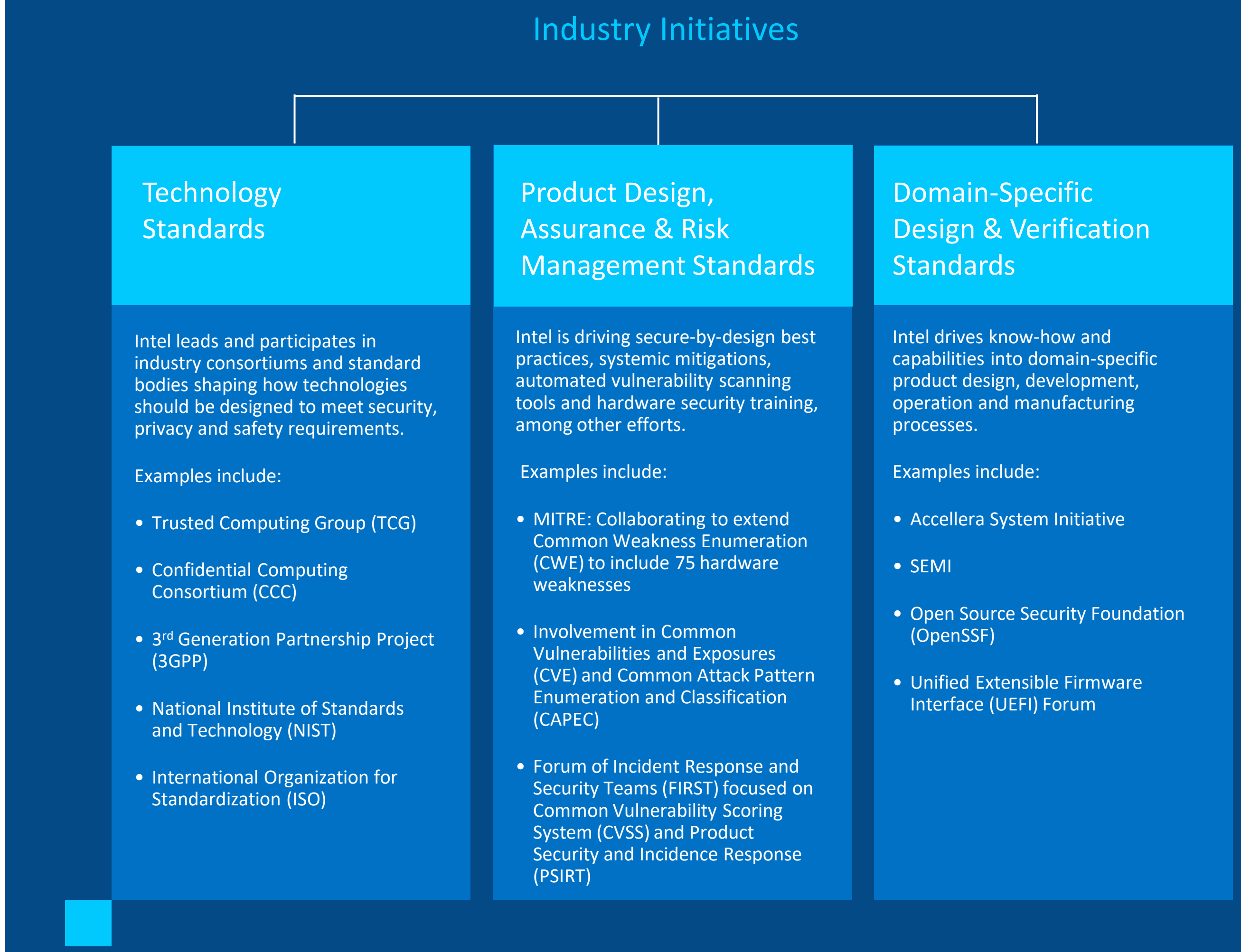
Intel advises policymakers and governments on strategies to advance product security through regulatory compliance, external advocacy and supply chain best practices. We advocate for public-private partnerships and policies that support scalable, global standards.

Academic Investment & Partnerships

Intel believes collaboration through academic investments and partnerships is critical to fueling innovation. Our relationships with leading security research institutions allow us to work with top talent around the world.

Collaboration with Industry

Intel is active in industry initiatives focused on aspects of data security and privacy, with emphasis on developing technology, security assurance and development standards.



Industry Initiatives

Technology Standards

Intel leads and participates in industry consortiums and standard bodies shaping how technologies should be designed to meet security, privacy and safety requirements.

Examples include:

- Trusted Computing Group (TCG)
- Confidential Computing Consortium (CCC)
- 3rd Generation Partnership Project (3GPP)
- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)

Product Design, Assurance & Risk Management Standards

Intel is driving secure-by-design best practices, systemic mitigations, automated vulnerability scanning tools and hardware security training, among other efforts.

Examples include:

- MITRE: Collaborating to extend Common Weakness Enumeration (CWE) to include 75 hardware weaknesses
- Involvement in Common Vulnerabilities and Exposures (CVE) and Common Attack Pattern Enumeration and Classification (CAPEC)
- Forum of Incident Response and Security Teams (FIRST) focused on Common Vulnerability Scoring System (CVSS) and Product Security and Incidence Response (PSIRT)

Domain-Specific Design & Verification Standards

Intel drives know-how and capabilities into domain-specific product design, development, operation and manufacturing processes.

Examples include:

- Accellera System Initiative
- SEMI
- Open Source Security Foundation (OpenSSF)
- Unified Extensible Firmware Interface (UEFI) Forum

intel®