Security for AI PC

Partner Enablement Package

Enhancing PC Security with AI: Intel's Innovative Approach

intel®

Contents

- What is an AI PC?
  - Industry Analysis
  - AI PC Overview
  - Introduction to Intel® Core™ Ultra Processors
- Security for AI PC
  - Security Generates Opportunity
  - AI PC Security & Use Cases
  - Intel's AI Security Strategy
  - Intel® Threat Detection Technology
  - Intel vPro® - Built for Business
  - Empowering the Ecosystem
- Summary, Call to Action & Resources

What is an AI PC?

Industry Analysis: AI's Incredible Opportunity

WATCH NOW >

In 2024, nearly **50 million** AI PCs will ship

By 2027, it will grow to more than **167 million** – roughly **60%** of all PC shipments[1]

"Combined with an expected upcoming PC refresh cycle, there is a major opportunity to prepare the industry appropriately with well-equipped AI PCs that have the necessary…capabilities to deliver a responsive and secure AI-accelerated experience."

MOOR INSIGHTS & STRATEGY

"The role of the PC as the primary device for productivity, especially in business environments, presents a massive opportunity for embedded AI capability to deliver compelling innovation that fundamentally alters the user experience on PCs for the better."

canalys

The New Era of the AI PC

Unveiling the Future of Computing with AI PCs

[1]https://www.industryanalysts.com/021324_mars_idc_ai/#:~:text=A%20new%20forecast%20from%20International,than%20167%20million%20in%202027

What is an AI PC?

An AI PC is simply a new computer with components that are specifically designed to run powerful AI-accelerated software with great performance and quality.

With AI-acceleration built into every Intel® Core™ Ultra processor, experience enhanced collaboration, productivity, and creativity – right on the desktop.

ACCESS NOW

Intel® AI PC Advantage Guide Infographic

LEARN MORE

What is an AI PC and How Can It Help Me?

What is an AI PC - Video

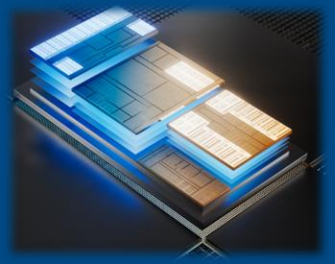
AI on the Client

Involves processing and performing tasks that typically require human intelligence, such as problem solving, reasoning, learning, understanding natural language, recognizing patterns, making decisions and generating content on PC systems.

Benefits of having AI on PC:

- Increased Privacy and Data Security
- Reduced Latency
- Online and Offline Accessibility
- Customization and Experimentation

What Makes a PC an AI PC?



The Right Engines:
CPU, GPU, NPU

The Right Frameworks

ONNX OpenVINO DirectML W3C Web Neural Network API

Open-Source Support

blender Audacity Open Broadcaster Software

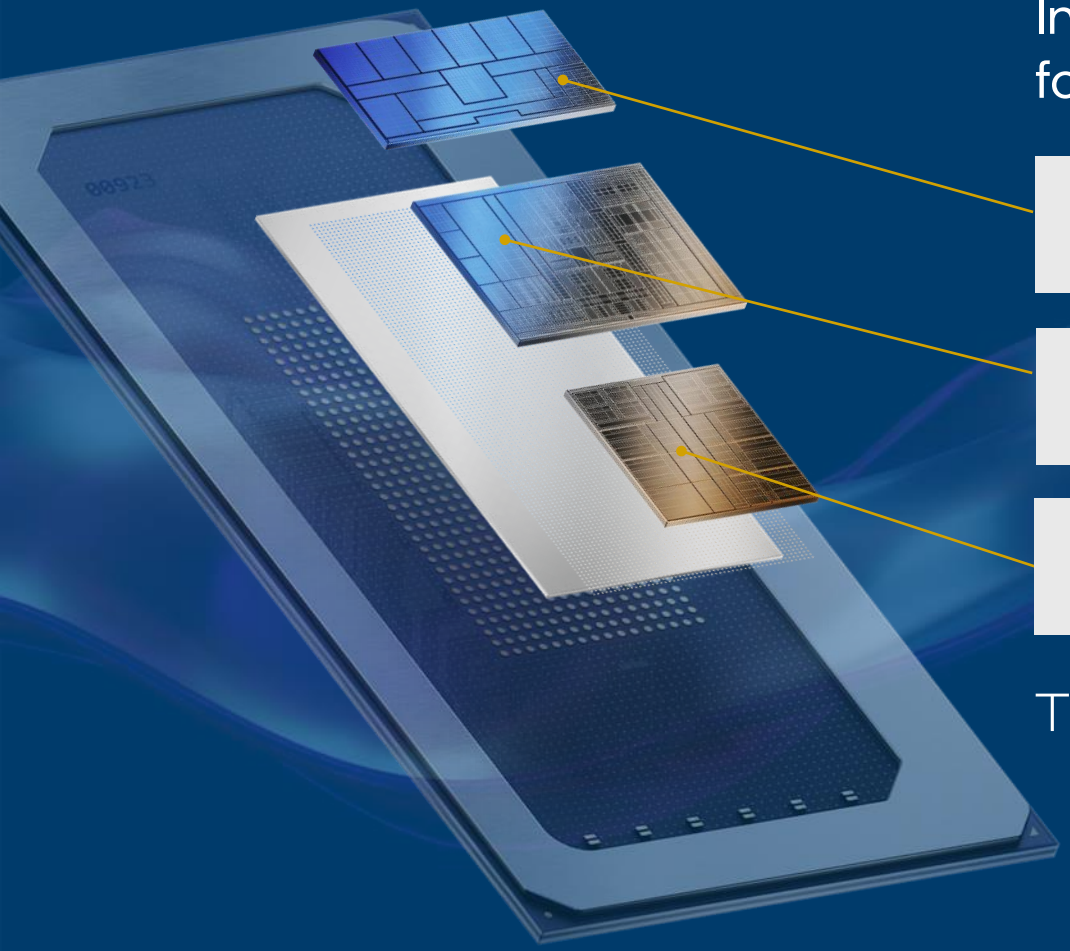
Wide ISV Enablement

Adobe SKYLUM software Stable Diffusion zoom

Intel® Core™ Ultra Processors

Client AI

PRODUCT BRIEF



Intel® Core™ Ultra Processors provide the right engines for all AI workloads

GPU	**Performance Parallelism & Throughput**	Ideal for AI infused in Media/3D/Render pipeline
NPU	**Dedicated Low Power AI Engine**	Ideal for sustained AI and AI offload for battery life
CPU	**Fast Response**	Ideal for lightweight, single-inference, low-latency AI tasks

The right balance of power and performance for AI

WATCH THE VIDEO >

Experience the Power of AI on PC with Intel® Core Ultra Processors

Security for AI PC

Security Generates Opportunity

When data is safeguarded, more is possible

Reduce Risk and Accelerate Business

Address security threats, protect IP, and reduce risk of exposing sensitive customer and employee data.

Collaborate in New Ways with New Partners

Harness business intelligence, power AI models, and partner on solutions without compromising sensitive data.

Innovate New Products

Unlock new ways of working using data securely in more places, more ways to differentiate, and deliver new solutions.

Hardware-assisted Endpoint Security is in Demand

Security threats are growing, and remote work is intensifying complexity

Remote Workers are the #1 Attack Vector

- Easy target; >90% of attacks originate at the endpoint[1]
- 62% of companies have experienced a breach that was at least partially attributable to remote working in the past three years[1]

Endpoint Detection & Response

- EDR is integral to new platform approach to security
- Customers will view EDR as mission critical to hunt, detect, and respond to attacks

Hardware's Role in Security Today

- Largely invisible, not well connected to today's "in the news" attacks
- Intel security capabilities deliver defense in depth to complement the best EDR security solutions

75% of attacks are now fileless, meaning bad actors inject malicious code directly into computer memory, where it is hard to distinguish from valid system processes[2]

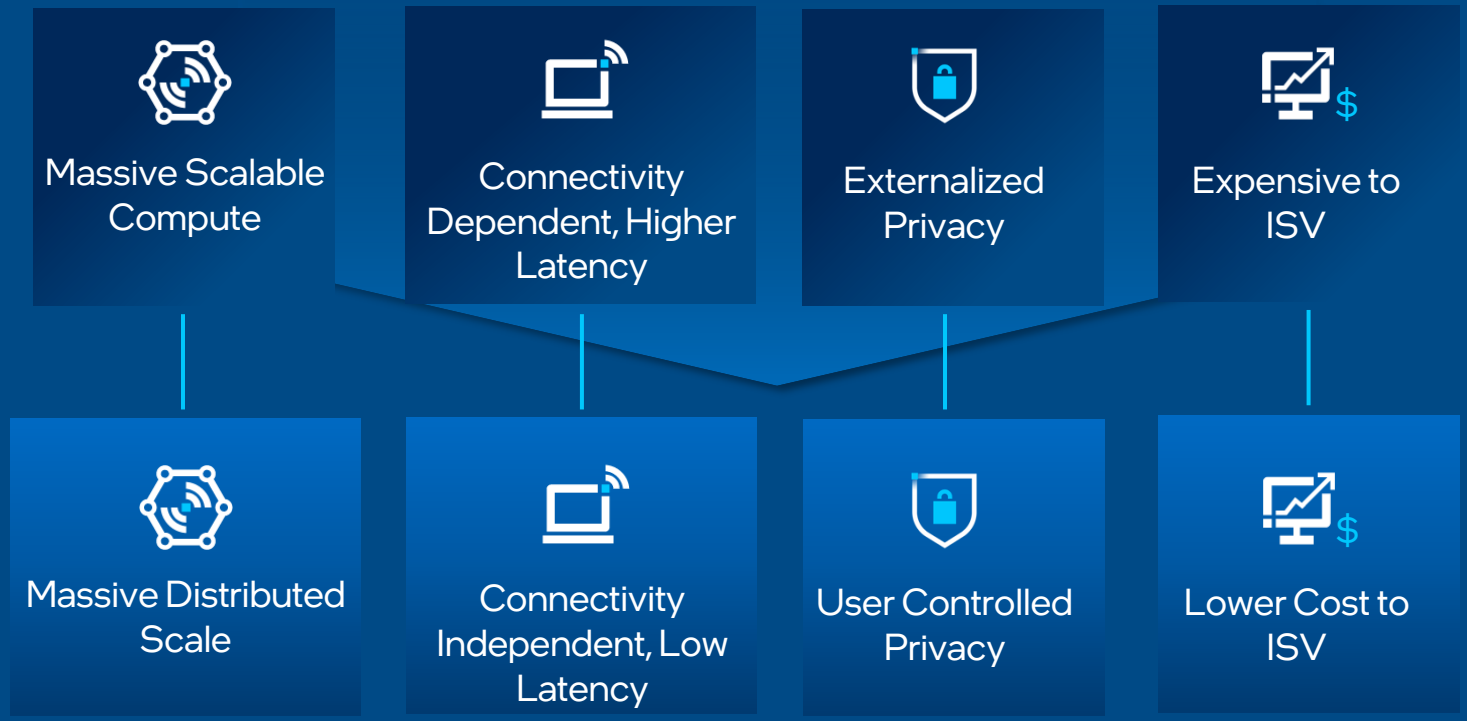
[1] Verizon, Business 2023 Mobile Security Index

2 PC Magazine. "Ransomware Attacks Rake in Over $1 Billion in 2023 for New Record." February 2024. pcmag.com/news/ransomware-attacks-rake-in-over-1-billion-in-2023-for-new-record.

AI PC Security & Use Cases

AI PCs offer more than massive productivity increases, AI capabilities can be applied to enhance security

Today: Cloud



Tomorrow: Cloud + Client + Edge

AI PC is driving a new inflection point & paradigm shift in Security

EXAMPLE USE CASES

- Federated Learning
- Data Loss Prevention
- Refactor Static & Dynamic Malware Analysis
- Anti-phishing
- Document Analysis
- Deep Fake Detection
- Email Anti-Scam
- Protect Private Data

Ecosystem Support

llmware, xcitium, Bitdefender, proofpoint, BUFFERZONE, TREND MICRO, CROWDSTRIKE, LiveDrop Technology, eset, Clarity, McAfee, Microsoft Defender

1 PC Magazine. "Ransomware Attacks Rake in Over $1 Billion in 2023 for New Record." February 2024. pcmag.com/news/ransomware-attacks-rake-in-over-1-billion-in-2023-for-new-record.

Intel's AI Security Strategy

Intel®'s latest Core™ Ultra processors take a significant step forward by incorporating an NPU (Neural Processing Unit), which enables the deployment of AI-powered security features directly on the endpoint.

CPU GPU NPU

At the core of Intel's strategy is the integration of specialized hardware components knowns as "xPUs." These hardware accelerators are designed to optimize the performance of various security-related tasks, including:

- **Cryptography and Encryption:** Accelerating the computationally intensive processes involved in secure authentication and data protection.
- **Threat Detection:** Leveraging machine learning models to identify and mitigate emerging threats, such as ransomware and crypto jacking attacks.

LEARN MORE >

- Protect Your Business with AI-based Security
- Enhancing PC Security with AI: Intel's Innovative Approach

WATCH NOW >

- The AI PC Security Revolution: Modernize Fleet Protections and Reduce Attack Surface
- Security Enhancements with AI PC

Intel is First to Market with AI Security Innovations

Intel® Threat Detection Technology is the only AI-based silicon security in deployment across a billion PCs[1]

Capabilities only work on Intel PCs (not available on Mac or AMD)

6 years of hardware-optimized software innovations

- Accelerated memory scanning for fileless malware
- AI for cryptojacking detection
- AI for ransomware detection
- CPU telemetry for anomalous behaviour detection
- NPU-optimized deep learning

Ecosystem Support

CROWDSTRIKE · Microsoft Defender · CHECK POINT · SEQURETEK SIMPLIFY SECURITY · TREND MICRO · eset · Acronis

bytesatwork · xcitium · Fidelis Security · BlackBerry · Kingsoft · 火绒安全 HUORONG SECURITY · AsiaInfo

[1]Intel® TDT provides the only silicon-enabled AI threat detection to help stop ransomware and cryptojacking attacks for Windows-based systems. Details at www.intel.com/performance-vpro. Results may vary.

Threat Detection Technology – Intel® TDT

One of the pioneering examples of Intel's hardware-accelerated security is Intel® TDT

Intel ®TDT is a software development kit (SDK) at its heart. Security ISVs use the SDK to integrate AI-based threat detection into endpoint detection and response (EDR) solutions that run on Intel® Core™ processor–based PCs from the 9th Generation onwards.

LEARN MORE

Because malware deploys obfuscation and cloaking techniques, traditional file-based threat detection techniques can miss it many of the attacks that Intel TDT can detect. However, when ISVs integrate Intel TDT into their antivirus and EDR solutions, they can detect malware earlier.

Partner Case Studies / Demos

Microsoft

Microsoft Defender for Endpoint with Intel® TDT

ESET

Intel vPro® & ESET Endpoint Security

CROWDSTRIKE

Intel vPro® & Crowdstrike Threat Detection

Intel vPro® Helps Make It Easy to Deploy Comprehensive Security

Intel® TDT is just one security component included with the Intel vPro® suite of technologies

Learn more how the Intel vPro platform can help easily support threat detection best practices across your PC fleet

Intel vPro Security
formerly Hardware Shield

Find out how this platform helps defend each layer, including hardware, BIOS/firmware, hypervisor, VMs, OS, and applications.

Advanced Threat Protections

In addition to Intel TDT, learn about other hardware-level security features included in the Intel vPro platform to protect endpoint devices from the silicon layer up.

Enhanced Endpoint Security ROI

Find out how modern, security-enhanced PC processors help keep your organization secure while lowering costs.

WATCH DEMO >

Optimizing Security Software with AI PCs on Intel vPro Platform

Intel vPro is the only business platform with built-in hardware security capable of detecting ransomware and software supply chain attacks[1]

[1]As of March 2023, Intel has the first and only hardware-based threat detection of its kind that works to augment security software for high-efficacy detection of the latest ransomware, cryptojacking, supply chain style attacks and even zero-day attacks in Windows-based systems. Based on SE Labs – Enterprise Advanced Security (Ransomware) – Intel Threat Detection Technology study published March 2023 (commissioned by Intel), which compared ransomware detection capabilities of an Intel vPro system powered by Intel Core processor against systems powered by AMD Ryzen Pro processors on Windows OS. SE Labs tested Intel's hardware approach to ransomware detection, using a wide range of ransomware attacks similar to those used against victims in recent months. Systems tested included Intel® Core™ i7-1185G7, AMD Ryzen Pro 5675U, AMD Ryzen Pro 5875U, AMD Ryzen Pro 6650U, and AMD Ryzen Pro 6850U. Visit www.intel.com/tdt to learn more. No product or component can be absolutely secure. Other names and brands may be claimed as the property of others.

Intel vPro® Platform - Built for Business

Intel vPro® delivers the features IT needs to succeed in hybrid work environments

Performance

Increase productivity and improve the employee experience wherever work happens.

Security

Intel vPro® provides the most comprehensive security for your business.[1]

Help protect your organization using multilayer, hardware-based security.

Manageability

Cost-effective device management from initial provisioning to retirement, wherever devices are.

Stability

Full platform integration and validation.

intel vPRO®

Built for Business

LEARN MORE >

Infographic - 5 Reasons to Choose Intel vPro for your Business

[1]As measured by the unrivaled combination of above and below the OS security capabilities, app and data protections, and advanced threat protections Intel vPro delivers for any sized business, as well as Intel's security first approach to product design, manufacture, and support. All business PCs built on the Intel vPro platform have been validated against rigorous specifications, including unique hardware-based security features. See www.intel.com/PerformanceIndex (Platforms) for details. No product or component can be absolutely secure

Empowering the Ecosystem

Intel actively collaborates with the broader security industry, working closely with independent software vendors (ISVs) to ensure seamless integration and optimization of their solutions on Intel-based platforms.

ENABLING THE DEVELOPER COMMUNITY

To support the developer community, Intel provides a comprehensive suite of tools and resources, including:

- Software Development Kits (SDKs)
- Optimization Frameworks
- Early Access to New Hardware Platforms

Empowering security software vendors to leverage the full potential of Intel's hardware capabilities, further strengthening the overall security ecosystem.

READ MORE

More than 500 AI Models Run Optimized on Intel® Core™ Ultra Processors

Summary & Call to Action

By combining hardware-accelerated security features, AI-enabled threat detection, and a collaborative approach with the security industry, **Intel is a key player in the ongoing effort to reduce cybercrime.**

As businesses and individuals navigate the ever-changing threat landscape, **Intel's innovative solutions offer a promising path toward enhanced PC security and resilience.**

Get Started Today

Connect with your Intel representative to further understand how our partners & their customers are using Intel AI & Security Technologies to protect against cybercrime and ultimately win more business.

AI Activation Zones

Access a comprehensive resource hub designed to help grow your business and solve your customers' most pressing business challenges. Find exclusive, value-added technical and sales enablement resources to help you build and sell solutions with Intel technology.

Technical Enablement

Sales & Marketing Enablement

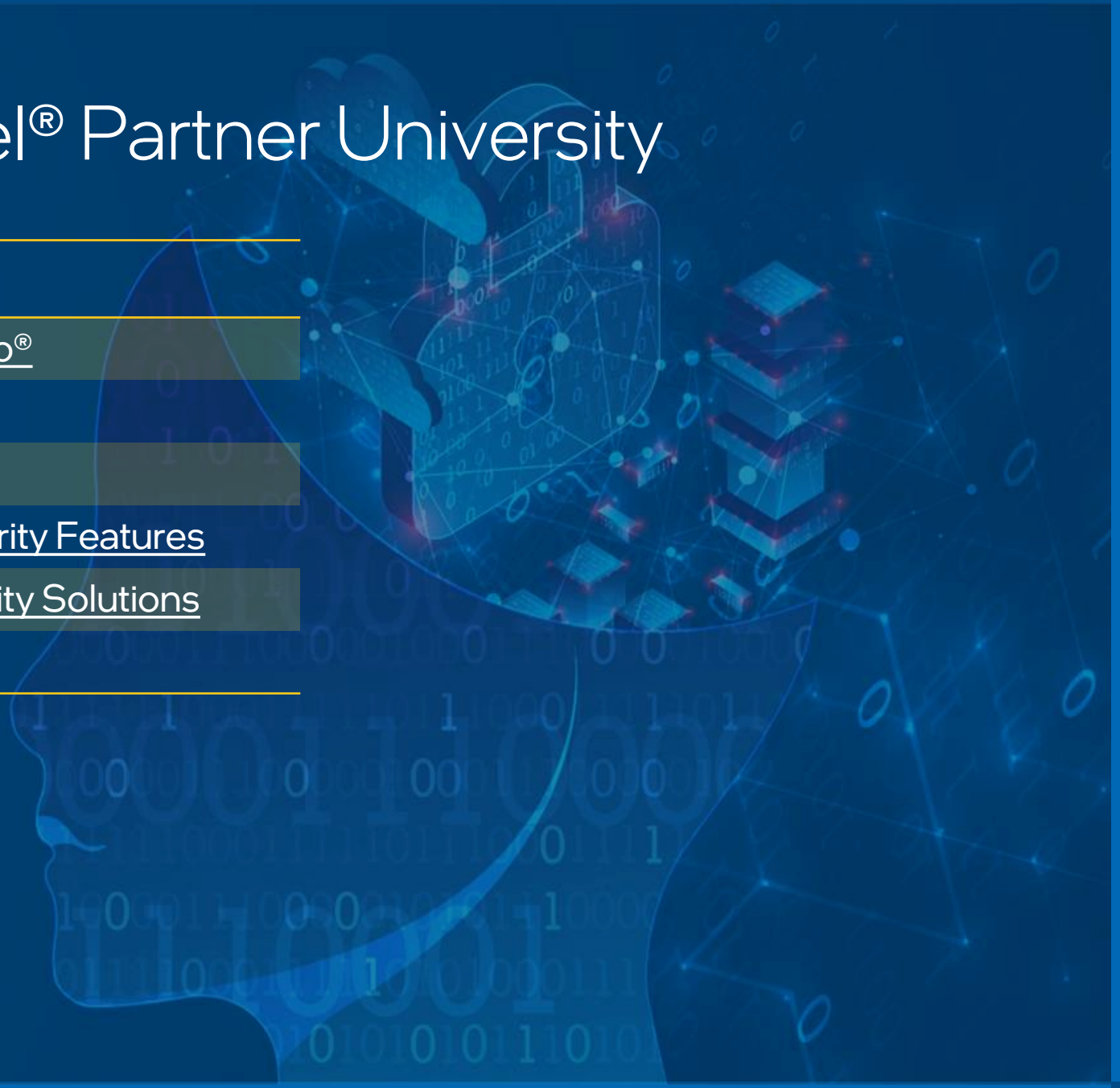
Technical Enablement

Sales & Marketing Enablement

Technical Enablement

Sales & Marketing Enablement

Training Courses on Intel® Partner University



- Strengthen Endpoint Security with Intel vPro®
- Security as a Business Imperative
- Introduction to Intel® Hardware Shield
- How to Enable Intel® Hardware Shield Security Features
- Implementing Intel® Hardware Shield Security Solutions

Notices and Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.
Your costs and results may vary.
Intel 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.

intel