White Paper

Information Technology Cybersecurity

Intel vPro® PCs Feature Silicon-Enabled Threat Detection

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

Intel Business Client Platform Security Marketing

While not a new cybersecurity risk, ransomware attacks have impacted people's ability to get healthcare, put gas in their vehicles, and buy groceries. According to the 2022 SonicWall Cyber Threat Report, the global volume of ransomware increased 105% year over year in 2021 and a whopping 232% since 2019.

Ransomware typically is downloaded through links from phishing schemes targeting susceptible users' devices (as is also the case with cryptojacking). On the endpoint, ransomware typically will encrypt files and move laterally to infect a company's servers, network appliances, and even SaaS applications. Then a ransom message demands payment (typically in a cryptocurrency such as Bitcoin) in return for decrypting the data. Upon payment, the hackers may follow through to decrypt the data.

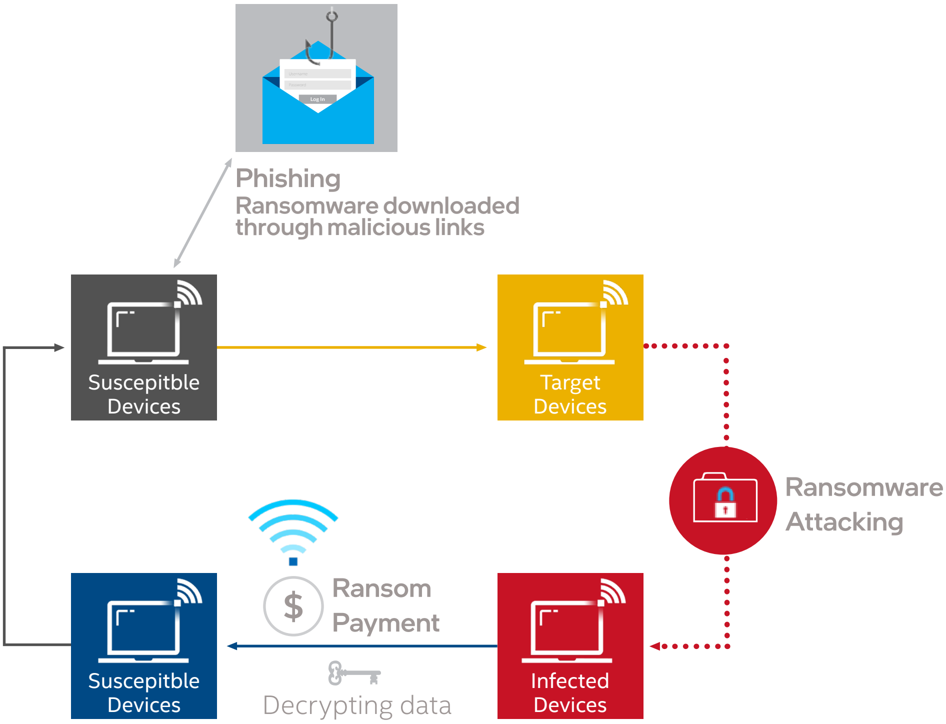
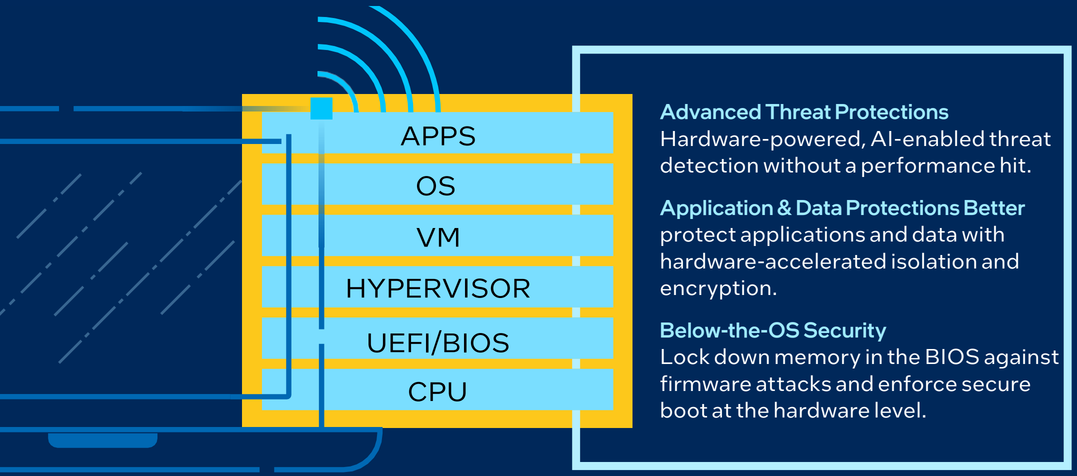


Figure 1. Ransomware attack lifecycle



Advanced Threat Protections
Hardware-powered, AI-enabled threat detection without a performance hit.

Application & Data Protections Better protect applications and data with hardware-accelerated isolation and encryption.

Below-the-OS Security
Lock down memory in the BIOS against firmware attacks and enforce secure boot at the hardware level.

Figure 2. Intel® Hardware Shield is built into Intel vPro® platform-based systems to help protect against attacks at the foundational level.

> Hardware is the bedrock of any security solution, and Intel is uniquely positioned in the industry to create and deliver truly innovative hardware- based security technologies, at scale.

Help Protect Endpoints with the Intel® vPro Platform

Intel® Hardware Shield, a key part of the Intel vPro platform, delivers built-in below-the-OS, application and virtualization security features, and Intel® Threat Detection Technology (Intel® TDT) for advanced threat protections. Intel TDT is enabled in leading security vendors' software to improve security efficacy and performance, resulting in increased threat detection efficacy on Intel vPro platform PCs. View the list of security vendors who have enabled Intel TDT as of March 2022.

The legacy model of software protecting software can't keep up with brand new variants of threats against digital security, safety and privacy. Current tools can help protect against attacks that happen at the software application and operating system (OS) level, but hackers continue to evolve their techniques.

Organizations of all sizes need to invest in better technology to help ensure security in-depth, at each layer: hardware, UEFI/BIOS, hypervisor, virtual machines (VMs), OS and applications. As the hardware-based security technology built-in to the Intel vPro platform, Intel Hardware Shield helps protect every layer of the compute stack.

Improve Endpoint Detection & Response Efficacy and Performance with Intel TDT

For advanced threat protections, the Intel TDT portion of Intel Hardware Shield operates seamlessly with enabled independent security vendors' (ISVs') solutions. Intel TDT can detect malware running on the system. CPU telemetry and optimized driver technology enables Intel TDT to identify hundreds of events (with minimal impact on the CPU), while machine learning algorithms improve efficacy. That provides high-fidelity signals to security software solutions from third-party vendors that provide remediation. Intel TDT helps Intel security partners detect threats using telemetry, machine learning and GPU-offload.

Intel TDT requires no installation or deployment-related configuration. It leverages two Intel hardware-based capabilities:

- Exploit detection platform telemetry helps profile exploits and detect their behavior in real-time
- Intel integrated GPU enables offloading from the CPU for accelerated memory scanning (AMS), compute-intensive AI algorithms, and other security workloads

Intel Exploit Detection Platform Telemetry

Intel TDT uses platform telemetry in the CPU to help profile exploits for behavioral detection. Targeted exploit detection combines machine learning algorithms with hardware telemetry unique to Intel processors. This capability adds a highly effective, low-overhead tool to the arsenal of security providers without requiring intrusive scanning techniques or signature databases, leading to improved and proactive malware detection. For example, using silicon telemetry, Intel TDT helps detect new ransomware variants not yet profiled by the security solution vendor. Likewise, a known attack may be running in a VM and be undetectable by the security vendor. Again, Intel TDT signals can be useful to the third- party solution in detecting these attacks.

Intel TDT improves the performance and efficacy of third-party EDR solutions in four ways:

1. **CPU Threat Detection—**Equips EDR software to go beyond signature and file-based techniques with CPU malware behavior monitoring.
2. **Full-Stack Visibility—**Helps close blind spots to expose and differentiate malware from legitimate data encryption as it hides in memory or in VMs to evade detection.
3. **Unleashes AI for Better Security—**Accelerates performance-intensive AI security algorithms with offload to Intel's integrated GPU. Boosts security capacity to analyze more data & do more scans.
4. **Security without Compromise—**Bolsters the performance of third-party security agent processing on the client with minimal impact on the user experience.

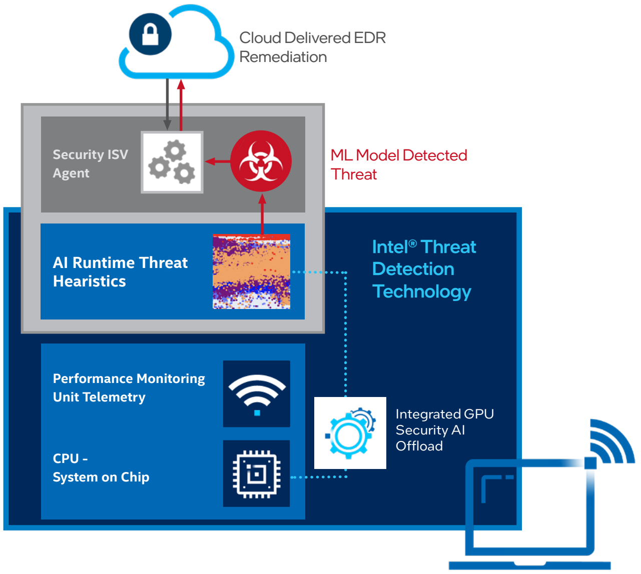

Cloud Delivered EDR Remediation
Security ISV Agent
ML Model Detected Threat
AI Runtime Threat Heuristics
Intel® Threat Detection Technology
Performance Monitoring Unit Telemetry
CPU - System on Chip
Integrated GPU Security AI Offload

Figure 3. Intel TDT, a feature of Intel Hardware Shield, uses GPU offload and CPU telemetry to accelerate and enable advanced threat defenses such as Advanced Memory Scanning and AI-based real-time monitoring.

Accelerate Endpoint Detection & Response Software with Intel TDT

Intel TDT includes a software development kit for ISVs to efficiently and easily offload some security workloads from the CPU to the Intel integrated GPU (which is mostly idle on enterprise clients systems). The Intel integrated GPU performance of Intel vPro platform, coupled with the large pool of shared system memory with the CPU, provides an opportunity to take advantage of graphics compute that is otherwise not fully utilized. Security ISVs and enterprise IT professionals need to run more security workloads to detect new classes of emerging threats. However, CPU performance can limit how much they can do without affecting the user experience. With Intel TDT, security ISVs can increase the efficacy of their solutions—how many duty cycles they can run for deeper inspection and proactive threat detection and prevention.

Advanced Memory Scanning (AMS) was the first security workload Intel TDT could offload from CPU to the Intel integrated GPU. Current scanning technologies can detect system memory-based cyberattacks, but many ISVs turn them off by default because they impact CPU performance. With AMS, offloading to the Intel integrated GPU enables EDR software solutions to scan more frequently, improving overall system security and uncovering hard-to-detect file-less attacks to the memory layer. For example, Microsoft integrates Intel TDT-enabled AMS into Microsoft Windows Defender Advanced Threat Protection's (ATP) EDR capability.

In addition to AMS, Intel TDT enables security-specific ML workloads to offload from the CPU to the Intel integrated GPU.

Intel TDT in Gen Intel Core vPro platforms target functions used for ML feature extraction and classifiers used in inference. These include:

- **Pattern Matching**—Searching for a known set of patterns in memory
- **Random Forest Classifier**—Decision Trees based classifier for inferencing
- **String Extraction**—Extracting ASCII and Unicode strings from memory
- **Entropy Calculation**—Calculate Shannon Entropy of memory blocks
- **Euclidean Distance for Clustering**—Assign sparse data points to the nearest centroids

Intel developed an initial set of ML heuristics threat detectors that will take advantage of the Intel TDT on Intel Core vPro platforms. For example, the current Intel TDT cryptojacking and ransomware detectors use the Intel integrated GPU for classification using the Random Forest Classifier toolkit workload. As Intel and ISVs add more detectors for better security, ML-offload to the Intel integrated GPU becomes a necessity to keep CPU utilization low. The value for ISVs is to help them provide enhanced security and improved user experiences by taking advantage of the increased security capacity gained from the offload.

Help Detect & Respond to Anomalous Behavior

Living off the land (LotL) and software supply chain attacks pose a significant security challenge because they blur the boundary between benign and malicious programs. It is much harder for security products to accurately identify the threat and promptly respond when legitimate programs are attacked and start to misbehave. Intel TDT Anomalous Behavior Detection (ABD) uses AI, CPU telemetry, and Intel integrated GPU performance optimizations to deliver high efficacy without significant impact on the user experience.

Anomalous Behavior Detection

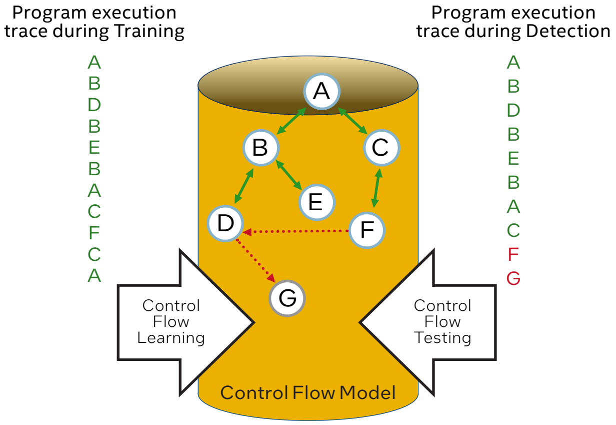


Figure 4. Using ML algorithms & Intel® processor telemetry to profile the normal control-flow behaviors of benign applications, Intel TDT ABD monitors execution and detects control-flow deviations in real-time.

ABD uses machine learning algorithms, Intel® Processor Trace (PT), Last Branch Record (LBR) and Performance Monitoring Unit (PMU) telemetry to profile the normal control-flow behaviors of benign applications. ABD then monitors application execution in production, and it detects control-flow deviations in real-time if applications are attacked or experience unexpected errors. The Microsoft Defender for Endpoint Research team evaluated ABD using a wide range of benign workloads and attack scenarios. Test results indicate that ABD can accurately detect common process hijacking techniques with very high signal-to-noise ratios. Intel is working with select security vendors to enable ABD into their solution – learn more from a joint whitepaper published in March 2022.

Help Protect Against Control-flow Enforcement Hijacking with Intel® Control-flow Enforcement Technology

Control-flow hijacking is a rapidly growing class of malware that attacks system memory, targeting operating systems (OSs), browsers, readers and many other applications. These code re-use attacks can be particularly hard to detect or prevent because the attacker hijacks existing code running from executable memory to change program behavior.

Intel developed Intel® Control-flow Enforcement Technology (Intel® CET), part of Intel Hardware Shield, to deliver effective, hardware-integrated protection with minimal impact on the user-experience. Intel CET is designed to protect against the misuse of legitimate code through control-flow hijacking.

Software developers use Intel CET to help stop code re-use threats such as Return Oriented Programming and Jump/Call Oriented Programming. Intel worked closely with Microsoft to enable Windows 10 Enterprise and developer tools, so applications and the industry at large can offer better protection against control-flow hijacking threats.

Intel CET offers software developers two key capabilities to help defend against control-flow hijacking malware: indirect branch tracking and shadow stack.

Indirect branch tracking delivers indirect branch protection to defend against jump/call-oriented programming (JOP/COP) attack methods. Shadow stack delivers return address protection to help defend against ROP attack methods where attackers use the RET (return) instruction to stitch together a malicious code flow that was not programmer-intended.

Since ROP relies on RET instructions, where the address of the next instruction to execute is fetched from a stack, stack corruption plays a critical role in ROP attacks. Intel CET enables the OS to create a Shadow Stack, which is designed to be protected from application code memory accesses, and stores copies of the return addresses.

This helps ensure that even when an attacker is able to modify/corrupt the return addresses in the data stack for the purpose of carrying out a ROP attack, the attacker is not able to modify the Shadow Stack, and the CPU detects mismatches between the address on the shadow and data stacks to help prevent the attack via an exception reported to the OS. Similarly, other indirect branch instructions, such as Call and Jump indirect can be used to launch variant attacks (COP and JOP). Intel CET adds an Indirect Branch Tracking capability to provide software the ability to restrict COP/JOP attacks.

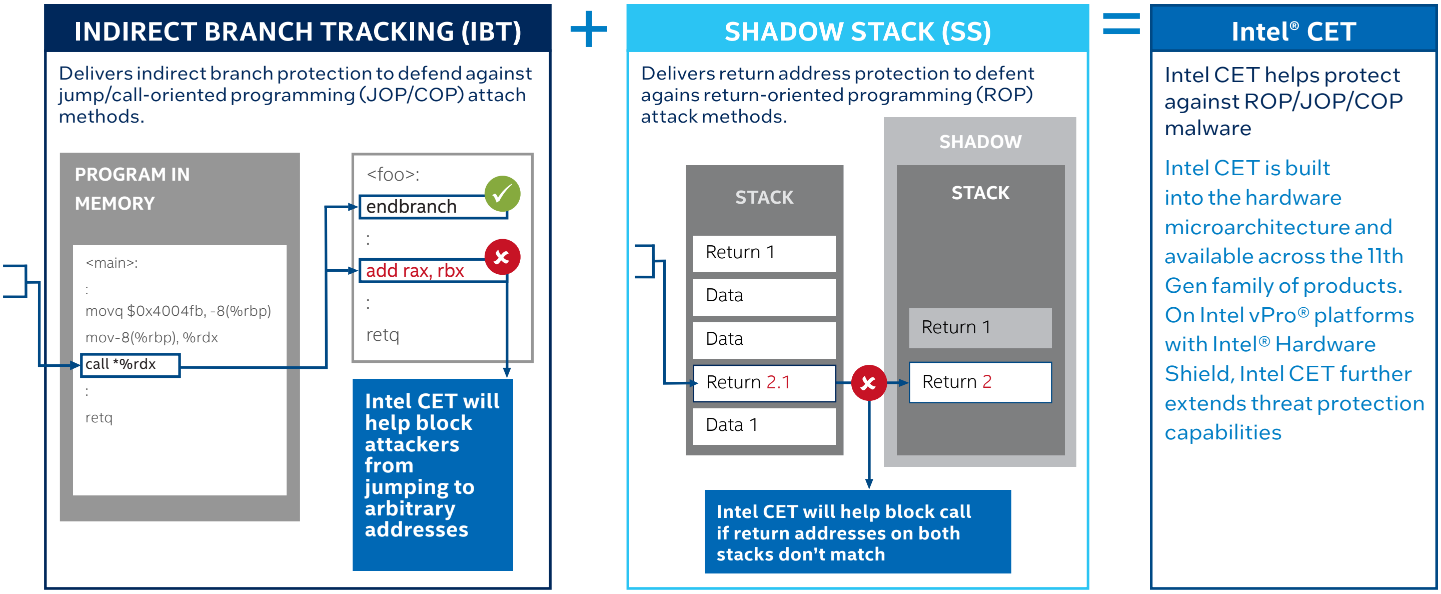

INDIRECT BRANCH TRACKING (IBT)
Delivers indirect branch protection to defend against jump/call-oriented programming (JOP/COP) attach methods.
PROGRAM IN MEMORY
<main>:
:
movq $0x4004fb, -8(%rbp)
mov-8(%rbp), %rdx
call *%rdx
:
retq
<foo>:
endbranch
:
add rax, rbx
:
retq
Intel CET will help block attackers from jumping to arbitrary addresses
+
SHADOW STACK (SS)
Delivers return address protection to defent agains return-oriented programming (ROP) attack methods.
STACK
Return 1
Data
Data
Return 2.1
Data 1
SHADOW STACK
Return 1
Return 2
Intel CET will help block call if return addresses on both stacks don't match
=
Intel® CET
Intel CET helps protect against ROP/JOP/COP malware
Intel CET is built into the hardware microarchitecture and available across the 11th Gen family of products. On Intel vPro® platforms with Intel® Hardware Shield, Intel CET further extends threat protection capabilities

Figure 5. Intel CET offers software developers two key capabilities to help defend against control-flow hijacking malware: indirect branch tracking and shadow stack.

Intel Feature	Consumer PC SKU?	Mobile SKU?	On by default?	OS enabling required?	ISV solution needed?
INTEL® CET	✓	✓	✓	✓ (requires 20H2)	✓
INTEL® TDT Advanced Threat Detection of Cryptojacking	✓	✓	✓	✗	✓
Advanced Threat Detection of Ransomware Attacks	✓	✓	✓	✗	✓
Accelerated Memory Scanning (AMS)	✓	✓	✓	✗	✓
Anomalous Behavior Detection (ABD)	✓	✓	✓	✗	✓
GPU offload to the Intel integrated GPU	✓	✓	✓	✗	✓

Table 1. As components of Intel Hardware Shield, these technologies are straightforward to deploy and use. (Chart is current as of April 8, 2021)

Deploy and Use Intel CET and Intel TDT Today

Intel Hardware Shield together with Windows 10 and Windows 11 Enterprise Edition enables unique Intel CET capabilities in Intel Core processors. Intel CET is "on" by default with Windows version 10/2004 20H1: 19041.662+ and 20H2: 19042.662+, and no OS configuration or enabling is required from the user. Microsoft's support for Intel CET is called Hardware-enforced Stack Protection. This feature works on systems with Intel CET, landing first on11th gen Intel® Core™ mobile platforms and all Intel 12th gen Intel Core platforms.

Like Intel CET, Intel TDT is straightforward to deploy and use because it is included with Intel Core and Intel vPro PCs silicon with no additional hardware or BIOS integration required. Intel Core vPro platform PCs support additional Intel TDT capabilities such as AMS and ML-based monitoring accelerated by the Intel® Xe GPU. Like Intel CET, Intel TDT is "on" by default, and there is no OS configuration or enabling required. Intel TDT is not yet part of the Microsoft Secure-core PC specification, but it is supported by Microsoft Defender for Endpoint, CrowdStrike, ESET, Fidelis Cybersecurity, bytesatwork, Sequretek, Kingsoft, Blackberry Optics, and more.

Industry support continues to grow: Intel is currently engaged with more than a dozen market-leading EDR software vendors. For more information, contact your Intel sales partner.

Learn more at Intel.com/TDT

Related Content

IDC Perspective: Intel TDT provides new tools to the cybersecurity task – The Results Could be Game Changing. Adoption of Intel TDT could lead to a measurable difference in security efficacy between Intel-based systems and the systems based on other processor vendors.

Intel Threat Detection Technology: Intel TDT enhances system protection by using your hardware to deliver hardware-based threat detection and more.

A Technical Look at Intel's Control-flow Enforcement Technology: JOP or ROP attacks can be hard to detect or prevent because the attacker uses existing code running from executable memory in a creative way to change program behavior.

Security Analysis of Processor Instruction Set Architecture for Enforcing Control-flow Integrity: Intel CET helps to defend against ROP and COP/JOP style control-flow subversion attacks.

Advanced Threat Protections

Deployment & Use

Intel Feature	Generation Introduced	Consumer SKU?	Mobile SKU?	Intel vPro® req't?	Intel vPro Enterprise?	Intel vPro Essentials?	Additional HW requirement? (Companion module, extra HW needed)	BIOS integration req't?	On by default?	OS enabling req't?	HW capability mapped to OS feature?	Secured core PC req't?	ISV solution needed?
Intel® Threat Detection Technology (Intel® TDT)Integrated GPU offload of Accelerated Memory Scanning	starts with 6th Gen	Y	Y	N	Y	Y	N	Y	Y	N	Windows	N	Reference the implementing Intel Hardware Shield document for the latest enabled ISVs
Intel® TDT Intel integrated GPU offload of Machine Learning algorithms	starts with 6th Gen	Y	Y	N	Y	Y	N	N	Y	N	Windows	N	
Intel® TDT Cryptojacking Detection	starts with 6th Gen	Y	Y	Y	Y	Y	N	Y	Y	Y	Windows	N	
Intel® TDT Ransomware Detection	starts with 9th Gen	N	Y	Y	Y	Y	N	Y	Y	N	Windows	N	
Intel® TDT Anomalous Behavior Detection	starts with 10th Gen	N	Y	Y	Y	Y	N	Y	N	Y	Windows	N	ISV eval in progress
Intel Control-flow Enforcement Technology (Intel® CET)	started on 11th Gen mobile / 12th Gen desktop mobile onwards	N	Y	Y	Y	Y	N	Y	Y	N	Windows	N	Yes, enabling is led by MSFT, security vendors will self-host when their solutions are ready

Table 1. As components of Intel Hardware Shield, these technologies are straightforward to deploy and use.

Additional Resources

Intel vPro® Platform

- Intel.com/vPro
- Intel.com/HardwareShield
- Intel vPro Expert Center

Intel vPro

- Intel.com/vPro Platform Support

[1] The Intel vPro platform delivers the first and only silicon-enabled AI threat detection to help stop ransomware and Cryptomining attacks for Windows-based systems. See www.intel.com/PerformanceIndex (platforms) for details. No product or component can be absolutely secure.

All versions of the Intel vPro® platform require an eligible Intel® Core™ processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance and stability that define the platform. See intel.com/performance-vpro for details. Intel technologies may require enabled hardware, software or service activation.

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.

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

1122/MZ/DCC/PDF