White Paper

Information Technology
Cybersecurity

11th Gen Intel® Core™ vPro® Mobile Platform PCs Feature the Industry's Only Silicon-Enabled Threat Detection

Defend Against Ransomware, Cryptomining and Memory Attacks

Intel Business Client Platform Security Marketing

"Ransomware is rapidly shaping up to be the defining online security issue of our era," according to a June 2020 ZDNet report. In 2019, a leading data management solutions provider estimated that attacks had increased by 97% in two years causing $20 billion in damages, with an average attack cost of $80,000. A growing concern is the fact that ransomware has evolved to bypass traditional detection techniques.

Ransomware typically is downloaded through links from phishing schemes targeting susceptible users' devices (as is also the case with malicious cryptomining). 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.

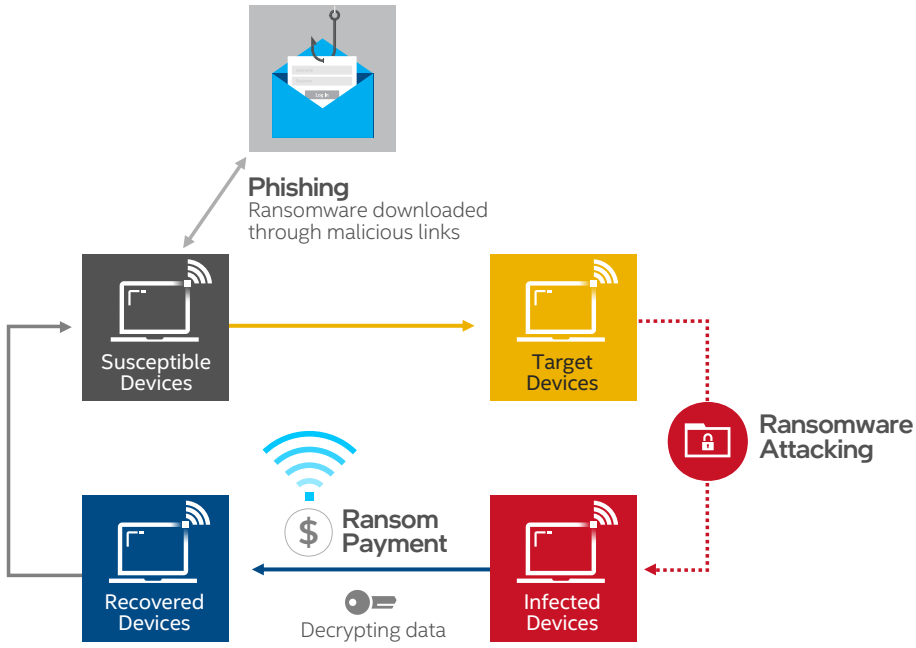

Figure 1. Ransomware attack lifecycle

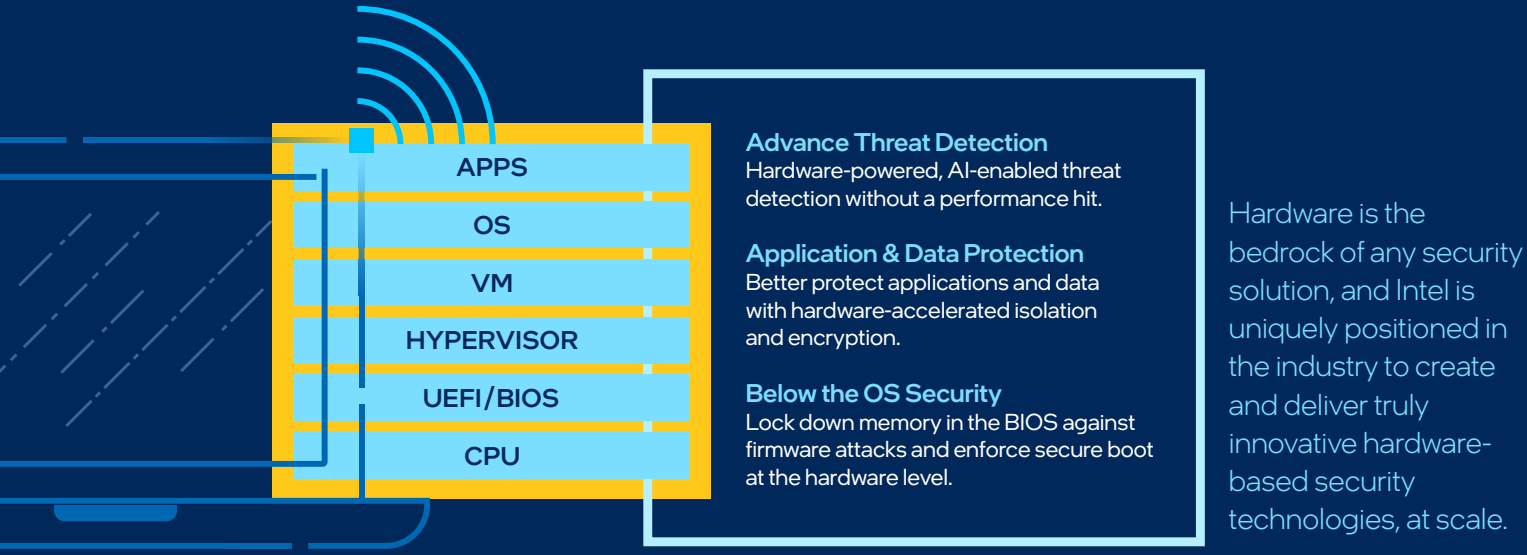

Figure 2. Intel® Hardware Shield is built into Intel vPro® mobile platform-based systems to help protect against attacks at the foundational level.

Help Protect Endpoints with the Intel® vPro Platform

Intel® Hardware Shield, a key part of the Intel vPro mobile platform, delivers built-in below the OS, application and virtualization security features, and Intel® Threat Detection Technology (Intel® TDT) for advanced threat detection. 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.

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 detection, 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. Blackberry/CyLance, Microsoft Defender, and many other End-Point Detection and Response (EDR) vendors have released or are integrating Intel TDT in their commercial solutions.

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 Graphics Technology GPU-enables offload for Accelerated Memory Scanning (AMS) & compute intensive AI algorithms

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 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 to the user experience.

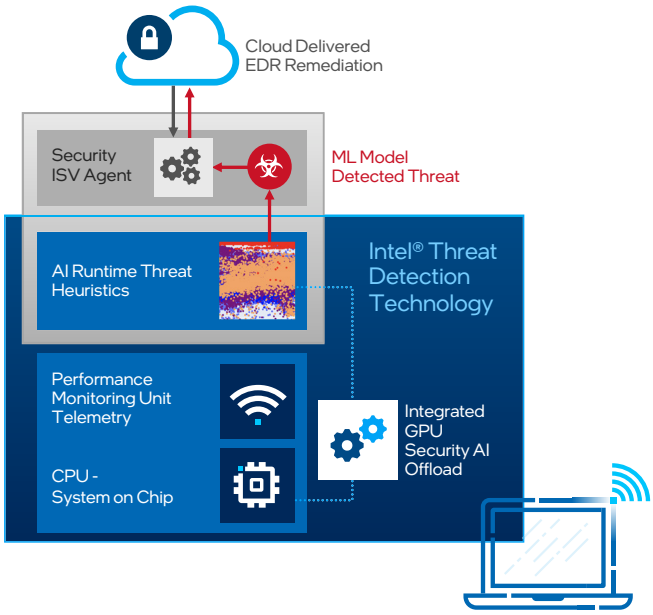

Figure 3. Intel TDT, a feature of Intel Hardware Shield, uses GPU offload and CPU telemetry to accelerate and enable advanced threat defenses such as Advanced Memory Scanning and AI-based real-time monitoring.

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 integrated GPU (which is mostly idle on enterprise clients systems). The incredible integrated GPU performance of the 11th Gen Intel Core vPro mobile 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 effecting 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 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 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 CPU to the integrated GPU.

New Intel TDT in 11th Gen Intel Core vPro mobile 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 11th Gen Intel Core vPro mobile platforms. For example, current Intel TDT cryptomining 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 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 offload.

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.

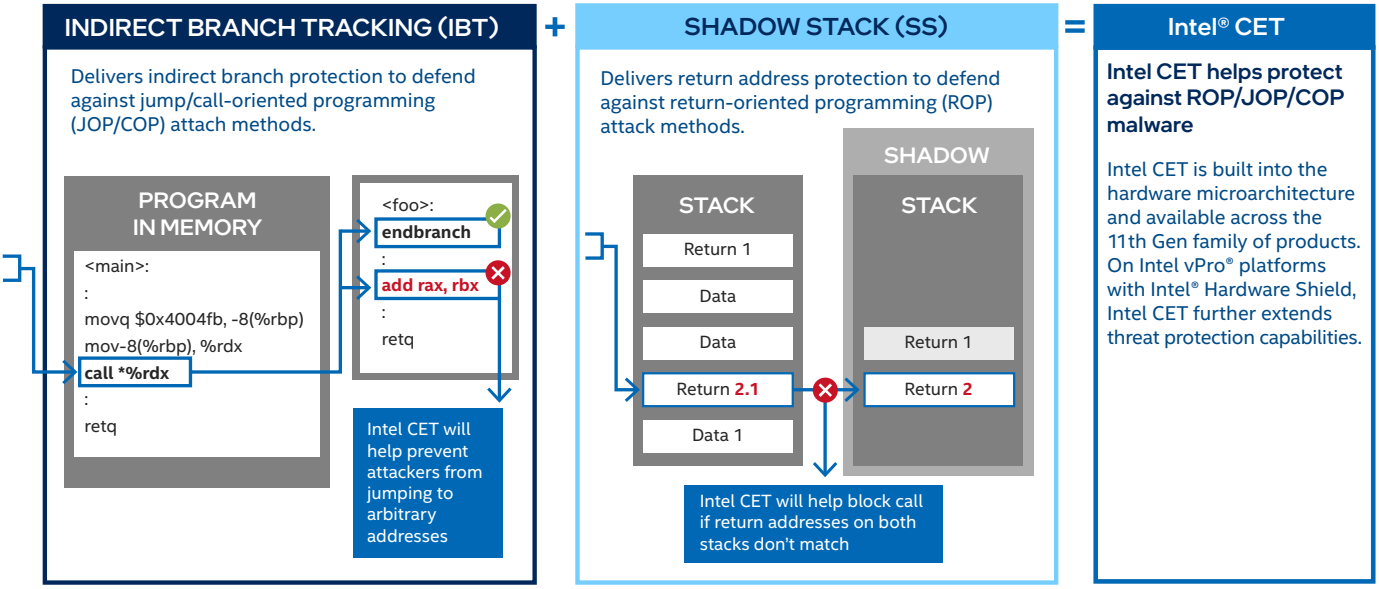

Figure 4. Intel CET offers software developers two key capabilities to help defend against control-flow hijacking malware: indirect branch tracking and shadow stack.

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.

Intel Feature	Traditional PC SKU?	Mobile SKU?	On by default?	OS enabling required?	ISV solution needed?
INTEL® CET	✓	✓	✓	✓ (requires 20H2)	✓
INTEL® TDT Advanced Threat Detection of Cryptominers	✓	✓	✓	✗	✓
Advanced Threat Detection of Top Ransomware attacks	✓	✓	✓	✗	✓
Accelerated Memory Scanning (AMS)	✓	✓	✓	✗	✓
GPU offload of ML (Intel® Iris™ Xe™ graphics)	✓	✓	✓	✗	✓

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 Enterprise Edition enable unique Intel CET capabilities in 11th Gen Intel Core mobile processors. Intel CET is straightforward to deploy and use because it is included with Intel® desktop and mobile PC silicon—no additional hardware or BIOS integration is required from the manufacturer or the user. 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 only works on systems with Intel CET—available across the 11th Gen Intel Core vPro processor family.

Like Intel CET, Intel TDT is straightforward to deploy and use because it is included with Intel desktop and mobile PC silicon with no additional hardware or BIOS integration required. 11th Gen Intel Core vPro platform desktop and mobile 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 Windows 10 Enterprise Edition and EDR solutions like Microsoft Defender Antivirus, SentinelOne Singularity, and Blackberry Optics.

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.

Related Content

Advanced Persistent Threats: Hunting the One Percent: Intel IT is committed to improving our ability to rapidly identify, contain, and remediate APTs—network attacks characterized by stealthy, unique malware designed specifically for the target environment.

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.

0421/MZ/DCC/PDF