THE CRUCIAL ROLE OF SILICON IN ADVANCED THREAT DETECTION

By Michela Menting, Research Director, ABI Research
Commissioned by Intel

CONTENTS

Threat Detection: State of Play 1

Going Deeper into the Silicon:
True Defense in Depth........................ 2

Intel TDT 2

Indicators of Compromise............. 3
Indicators of Attack 4

Why Should Enterprises Care
about Intel TDT?.................................. 6

Call to Action 7

THREAT DETECTION: STATE OF PLAY

With returns increasingly lucrative and repercussions minimal, threat actors have much to gain from cyberattacks. Their level of sophistication is always improving, as they devise ever-more ingenious methods to evade the latest cybersecurity solutions.

Locked in a perpetual conflict with attackers, security vendors continuously seek ways to counter malicious events of an exceedingly complex nature. In the highly adversarial field of cybersecurity, nowhere is the battle more intense than in threat detection and response.

Endpoint Detection and Response (EDR) is the technology that monitors devices through software agents in order to detect and respond to threats. Emerging from the gaps left by traditional endpoint protection solutions, EDR has proved a pivotal technology to counterattack evasion techniques.

As EDR extends into networks and the cloud (XDR) to block malicious advances, attackers are adopting innovative obfuscation techniques to evade EDR monitoring.

Advanced evasion techniques today are infiltrating places where EDR software agents have trouble going. Fileless malware attacks deploying into memory and Living off the Land (LOTL) attacks coopting whitelisted systems are proving difficult to detect in a timely manner. By replicating processes that tend to be used by system administrators and injecting themselves in areas that are less closely monitored, malicious actors hope to operate under the radar. While EDR boasts extraordinary analytics and response capabilities, it is having trouble going as deep as some of the latest threats in order to counter them quickly before they take hold. As a result, these new attack vectors are actively being exploited with disastrous success.

GOING DEEPER INTO THE SILICON: TRUE DEFENSE IN DEPTH

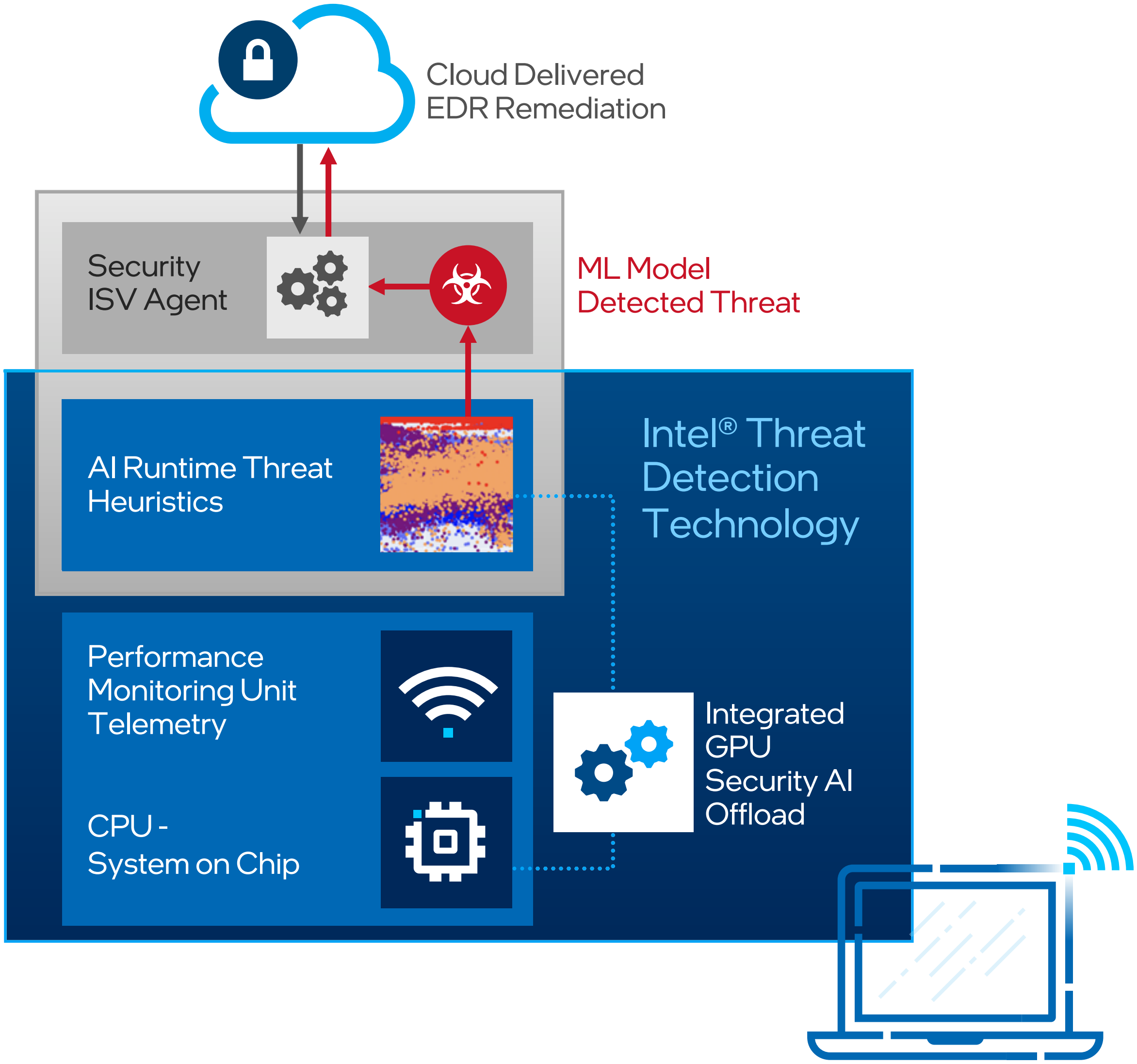
Ultimately, EDR needs better visibility in order to detect advanced evasion techniques, such as fileless malware and LOTL attacks. Fortuitously, existing technologies can be repurposed to address this limitation.

One way to augment visibility for EDR is to leverage hardware telemetry that has traditionally been used to monitor and manage the Central Processing Unit's (CPU) performance. CPU telemetry can be analyzed with Machine Learning (ML)-based correlation to reveal indicators of attack identifying an unusual or malicious payload execution. These data can then be provided to the EDR agent for further analysis in order to build a more complete picture of a potential threat.

Essentially, this capability provides a magnifying lens for EDR, enabling it to see deep within the silicon, with the additional CPU telemetry data being added to its powerful analytic capabilities. It can be the key to undermining the latest evasion techniques used by Advanced Persistent Threats (APTs), with the ability to counter ransomware, fileless malware, and software supply chain attacks.

INTEL® TDT

For the EDR agent to successfully leverage the CPU and its associated processes, the semiconductor chip manufacturer has to have developed these capabilities. Intel is one such manufacturer that has built a suite of hardware-assisted software technologies, known as Intel® Threat Detection Technology (Intel TDT), that serve to help detect malware by leveraging CPU telemetry. It is the silicon answer to expanding EDR capabilities deep within the hardware. The new data obtained can enrich an EDR's behavioral detectors and deliver better efficacy, with the Intel TDT source code integrated directly into the EDR agent.



Intel TDT is a built-in technology, available on PCs on the Intel vPro Platform.[1] It is readily available for Independent Software Vendors (ISVs) to incorporate into their EDR solutions. It offers three core capabilities that can address both known and unknown threats:

- Advanced Platform Telemetry/Targeted Exploit Behavior Monitoring
- Accelerated Memory Scanning
- Anomalous Behavior Detection

Indicators of Compromise

Advanced Platform Telemetry searches for Indicators of Compromise (IoC); it is essentially looking for specific and known types of malware and attacks, such as ransomware or cryptojacking.

[1] Intel TDT AMS, cryptojacking, and anomalous behavior detection applies to 6th Gen forward systems. Ransomware applies to 10th Gen forward systems. The iGPU is more performant with each generation. Offloading ML and AMS works best on the latest systems.

This capability leverages the Intel Performance Monitoring Unit (PMU),[2] a hardware block built into the processor to measure its performance parameters, such as instruction cycles, cache hits, cache misses, branch misses, etc. The PMU-generated telemetry can be used to characterize interaction between programmed sequences of instructions and microarchitectural sub-systems.

The PMU and its process context information serves as the telemetry sources for Intel TDT. Specific IoCs are modeled in a set of ML-powered heuristic threat detectors that can identify malicious code execution versus that of benign workloads. These ML classifier models can then infer a pre-defined threat class at runtime. Specific detection profiles are used to manage the inference characteristics of each threat variant's detector, and can be fine-tuned to meet the EDR solution's desired detection sensitivity goals. This is a unique approach in that it enables detection of zero days immediately, as the malware must execute on the CPU, enabling monitoring for its execution pattern with PMU telemetry that can see through packers or tools, as well as attacks cloaked in a Virtual Machine (VM). This can significantly speed up detection of new malware variants, which closes an attack surface gap for enterprises and helps the EDR tool up other defenses.

An added advantage is that the ML inference can be offloaded to the Intel Integrated Graphics Processing Unit (iGPU) that is part of Intel CPUs, so that Intel TDT has minimal impact on the CPU, and it is not unduly tasked. By leveraging Intel's System-on-Chip (SoC) design, Intel TDT makes the most of the available processing capabilities.

Leveraging Intel TDT's advanced platform telemetry, EDR solutions receive early detection signals on attacks happening in the OS and app layer. The parallel execution on the processes provides expanded visibility to assist EDR and allow them to quickly trigger remediation workflows.

Indicators of Attack

The other two capabilities focus on identifying Indicators of Attack (IoAs), which try to identify unknown attacks by analyzing unusual processor behavior.

Accelerated Memory Scanning (AMS) is used to detect IoAs early in the kill chain. Activated by a precise behavioral trigger, the AMS engine will scan the memory of a suspicious process to search for dynamic malicious behavior, iterating through its memory to look for artifacts, such as shellcode, unique strings, or patches.

AMS is especially well suited to catching polymorphic malware and fileless attacks that are using dual-use tools. These tools are legitimate software applications that can be subverted to conduct cyberattacks (such as Cobalt Strike, a popular penetration-testing tool) or drop fileless attacks like ransomware that can also execute in mem ory. Families like WastedLocker use polymorphism every time they run in order to look like a different entity to static scanners. This is especially true for script-based ransomware that can appear like powershell when running.

An EDR solution's use of AMS extends its detection capability and provides enhanced visibility through new memory-based telemetry data. The ISV can leverage its own threat intelligence to

[2] PMU documentation available at Intel Software Developer's Manual (Volume 13, Chapter 19).

further refine the behavioral triggers, such as types of malicious artifacts, where they are likely to be found, etc. Further, because AMS is only activated by meaningful behaviors, it minimizes system resource consumption.

AMS' main advantage is its ability to offload the memory scanning execution to the iGPU. This allows the EDR to run scans more frequently, potentially continuously, without incurring CPU overhead. As a result, the EDR can effectively monitor the system more actively and efficiently, thus providing continuous detection coverage without impacting user productivity.

Anomalous Behavior Detection (ABD) monitors the runtime execution of applications to ensure their behavior stays within normal boundaries. It leverages control-flow telemetry in the CPU, including the Intel Processor Trace (PT), Last Branch Record (LBR), and Performance Monitoring Unit (PMU), either individually or in combination to non-intrusively observe app execution behavior without ever accessing the app itself. ABD processes the telemetry with ML to ensure the applications are operating normally. Any control-flow deviation in real time is evaluated and then flagged as suspicious if it falls beyond expected boundaries.

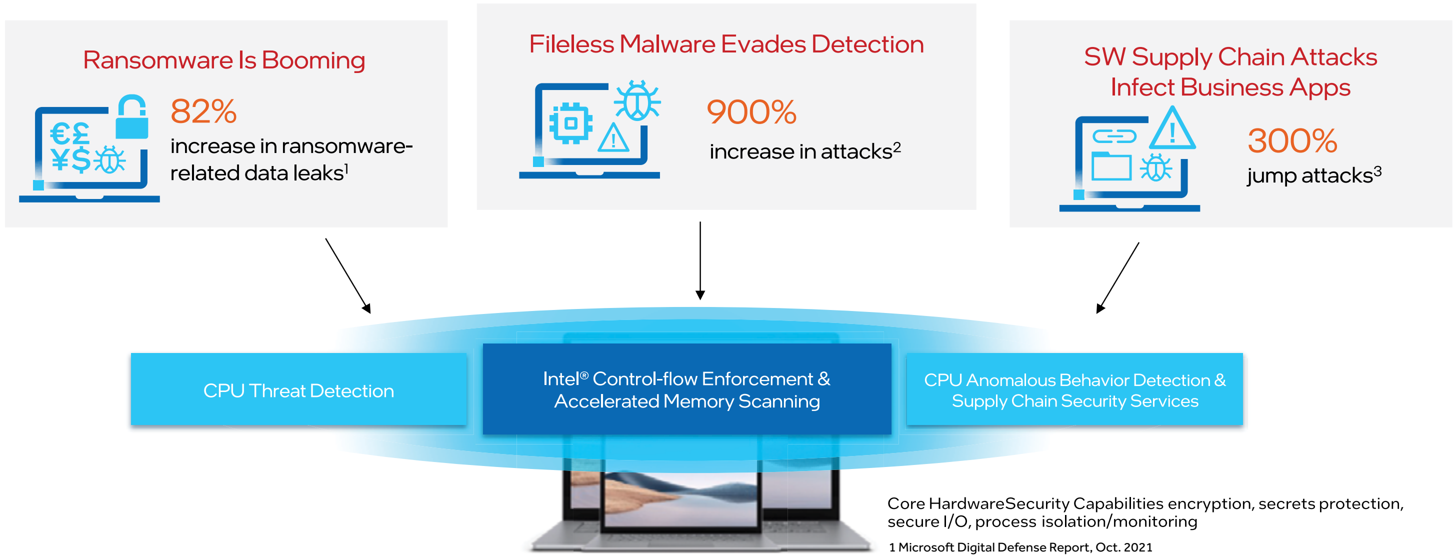
The ML used is based on a continuous learning algorithm that allows ABD to update its models through controlled incremental training. This continuous learning process can be managed and augmented by the EDR solution, with security ISVs importing additional telemetry into a base model for an app/process. ABD can also leverage static binary analysis to obtain sufficient code coverage and limit false positives if untrained code paths are used. In contrast to AMS, ABD does not use any predefined triggers due to its continuous learning ability.

Further, some of ABD's more compute-intense actions, such as the decoding of Intel PT packets, can also be offloaded to the Intel iGPU to minimize performance overhead and free up CPU resources.

ABD is highly effective at detecting control-flow and supply chain attacks, such as zero-day exploits (PrintNightmare) and live malware (Qakbot, TrickBot, and Cobalt Strike).

Current Threat Trends

Mapped to Hardware Countermeasures



Ransomware Is Booming

82%

increase in ransomware-related data leaks[1]

Fileless Malware Evades Detection

900%

increase in attacks[2]

SW Supply Chain Attacks Infect Business Apps

300%

jump attacks[3]

CPU Threat Detection

Intel® Control-flow Enforcement & Accelerated Memory Scanning

CPU Anomalous Behavior Detection & Supply Chain Security Services

Core HardwareSecurity Capabilities encryption, secrets protection, secure I/O, process isolation/monitoring

1 Microsoft Digital Defense Report, Oct. 2021
2 Watchguard, "Internet Security Report - Q4 2020," Mar 2021
3 Argon, "Supply Chain Attacks Study," Jan 2022

WHY SHOULD ENTERPRISES CARE ABOUT INTEL TDT?

Intel TDT's benefits to EDR are not just in the diversity of telemetry sources available, but also in the ML and analysis techniques used for its various capabilities. Adding to that is the effort made by Intel on minimizing overhead through the use of lightweight classifiers and the offloading of functions like ML inference and hardware telemetry decoding to the Intel iGPU. ISVs can typically gain between 4X and 7X in memory scan performance over the CPU, which is a significant metric, allowing for a broader use of scanning when needed without impacting the user experience.[3]

These capabilities significantly enhance EDR solutions, helping to solve the pernicious problem of APTs and highly evasive techniques with true defense in depth. An EDR augmented by such CPU-level features affords much better protection and higher efficacy. This allows EDR solutions to detect key threats very early in the attack cycle before they can establish command and control and drop other malicious payloads. In essence, it is about early IoA, and cutting off the threat at first contact.

Intel TDT's ransomware detection capacity is exceptional, capable of detecting 93% of known and unknown threats, including intentionally evasive ransomware. Used in conjunction with an EDR solution, the detection rate increases to 97%. When measured in head-to-head tests where the same EDR is deployed on competitive silicon that lacks these capabilities, Intel TDT showed an increased efficacy assist of 24% to the EDR.[4] These independent lab tests reveal that Intel TDT significantly augments EDR to catch top ransomware attacks and advanced 0-day evasion techniques.[5]

The advantage for enterprises is the deep integration that Intel TDT can provide with EDR; any EDR solution, in fact, as the technology is platform agnostic. Today, it is already present in a number of ISV solutions, including CrowdStrike, Microsoft Defender for Endpoint, ESET, Kingsoft, Sequretek, Fidelis, and bytesatwork, deployed already across millions of software endpoints[6]. Further, as TDT is designed into Intel vPro and Core Systems (since Intel 6th Gen), it is readily available in more than 1.3 billion machines globally. The availability of Intel TDT confers a significant competitive advantage over other solutions, extending differentiated security capabilities through the Intel vPro platform to the broader market.

Leveraging Intel TDT within EDR does not require any additional cost or effort in terms of implementation from an end-user perspective; deployment and management is taken care of by the ISV. An out-of-the-box approach like Intel TDT provides much needed simplicity in a security landscape that is highly fragmented and often overly complex. This type of integrated solution can make an immediate impact against key threats, and with hardware-based threat detection significantly amplifying the intelligence of software-based solutions, even the latest, most dangerous cyberattacks can be arrested practically in real time.

[3] *Based on offload memory scanning to the integrated GPU via Intel TDT API, which results in a 3-7x acceleration over CPU scanning methods as described in Crowdstrike blog. See www.intel.com/performance-vpro for additional details.*

[4] *Based on SE Labs Enterprise Advanced Security (Ransomware) – Intel Threat Detection Technology study published March 2023 (commissioned by Intel) analyzing ransomware detection rates with Intel TDT versus non-hardware based solutions. Additional details at www.intel.com/performance-vpro.*

[5] *SE Labs Efficacy and Detection Testing for Intel TDT, dated February 2023.*

[6] *Microsoft Ransomware Executive Testimonial Video.*

CALL TO ACTION

For enterprises, the detection work is already cut out for them; a highly efficient technology that can thwart advanced evasion techniques and persistent threats is already available through Intel TDT. But understanding its value and advantages in its association with EDR needs to be communicated by Security Operations (SecOps) to procurement.

This is not just true today for endpoint purchases like PCs and printers; increasingly, this will be necessary for any purchases of connected devices: building automation and control systems, corporate Internet of Things (IoT), etc. Comprehensive security is not just about protecting each asset in a chain, but also about designing security mechanisms deep within them as well, at their very core.

Enterprises must reassess the role of security in all procurement processes and weigh the benefits of purchasing solutions where security is ingrained. This assessment requires not only weighing the cost of security against that of a threat, but also understanding the value that can be derived from embedded protections, such as simplicity in deployment, performance in detection, and optimization in response.

Key to that is understanding the type of hardware capabilities endpoints have that can improve an enterprise's overall security posture, such as the innovative role that CPU telemetry offers, for example, in boosting EDR capabilities. It is also about understanding the interoperability and the integration between Original Equipment Manufacturers (OEMs) (from semiconductors to PC manufacturers) and ISVs; those vendors that align symbiotically on security are able to deliver better results when they matter.

SecOps needs to have a say in the hardware procurement process because of the impactful nature that advanced technologies like Intel TDT can have on security overall. For enterprises, it is a simple action to consider security during the routine task of PC purchase and refresh. The cost of doing so is low when the step is taken at this incipient stage, but it can radically augment security capabilities to counter even the most vicious threats, conferring valuable protection to enterprises facing increasingly treacherous cyberattacks.

*Both Intel® Standard Manageability and Intel® Active Management Technology (AMT) support remote out-of-band capabilities on provisioned Windows PCs, but only Intel vPro® Enterprise with AMT supports remote Key board Video Mouse control.

Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary.

Published March, 2023
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

ABOUT INTEL

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

ABOUT ABI RESEARCH

ABI Research is a global technology intelligence firm delivering actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today.

ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. The opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.