Solution Brief

Endpoint Security
Intel vPro® Platform

intel. + eset
Digital Security
Progress. Protected.

ESET Enhances Ransomware Protection with the Intel vPro® Platform

Multilayer security from ESET and Intel assists SMBs in the battle against ransomware.

intel vPRO®

Intel and ESET work together to help keep SMBs safe.

Intel® Threat Detection Technology and ESET Endpoint Security:

Multilayered protection
Software- and hardware-based threat detection

Seamless to use
Out-of-the-box protection

One step ahead
Advanced ML helps detect threats

SMBs face increasing cybersecurity threats

Ransomware is on the rise as attack surfaces expand with increasing numbers of remote workers and endpoints. And small and medium-sized businesses (SMBs) are a top target: 58 percent of SMBs surveyed experienced a cyberattack in the past year, while 44 percent of SMBs surveyed paid between $250,000 and $500,000 to cover breach costs.[1]

Attackers are using sophisticated techniques to evade detection by security software. These include using virtual machines to disguise ransomware or obfuscating malicious files, so they are more difficult to detect. With these aggressive approaches, organizations of all sizes are looking for ways to boost their security beyond software detection.

In response to the increasing threats, and to better support SMBs, ESET has enhanced its software-based detection technologies with hardware-based threat detection by integrating Intel® Threat Detection Technology (Intel® TDT). Intel TDT can help detect many of these new bypasses through a combination of CPU telemetry and machine learning (ML) heuristics. By integrating Intel TDT into its multilayered technology suite, ESET can help SMBs turn the tide in the battle against ransomware with silicon-level threat detection on the Intel vPro® platform.

Enhanced detection capabilities with the Intel vPro® platform

ESET has integrated Intel TDT into its endpoint protection platform and gained access to a plethora of unique hardware telemetry data to enhance protection when used in combination with the Intel vPro® platform. To keep one step ahead of bad actors, ESET can now access Intel ML heuristics, which continually evolve to detect new and changing threats.

ESET utilizes Intel TDT for the Intel vPro® platform. IT teams that manage Intel fleets and that use ESET Endpoint Protection v10 automatically benefit from Intel TDT without any extra action required.

How does ransomware work?

Ransomware works by locking a computer or encrypting its contents. A bad actor promises to unlock the device only when payment is made by the computer's owner. Many times, payment is requested in bitcoin or some other hard-to-trace cryptocurrency. Techniques used by ransomware operators can include:

- **Diskcoder ransomware:** Ransomware that encrypts an entire disk and prevents the user from accessing the operating system (OS).
- **Screen locker:** Ransomware that blocks access to the device's screen.
- **Crypto-ransomware:** Ransomware that encrypts data stored on the victim's computer.

ESET's endpoint protection platform with Intel TDT offers superior ransomware protection against these types of attack vectors.

Detection capabilities only available from Intel

Intel TDT uniquely detects ransomware and other threats through the Intel performance monitoring unit (PMU). The PMU sits beneath applications, the operating system, and virtualization layers, gathering CPU telemetry as it executes, and reinforcing ESET's multilayered security approach (see Figure 1).

ESET's endpoint protection platform with Intel TDT can now:

- Monitor malware behavior to help detect new variants
- Reduce blind spots by identifying when ransomware is seeking to avoid detection by hiding in virtual machines

With enhanced ransomware detection on their Intel-based PCs, SMBs can help reduce risks to their businesses; expanded visibility into evasion techniques helps IT teams keep data safer. End users enjoy better performance as the ESET platform offloads ML processing to the Intel integrated GPU. (See supported platforms on page 3.)

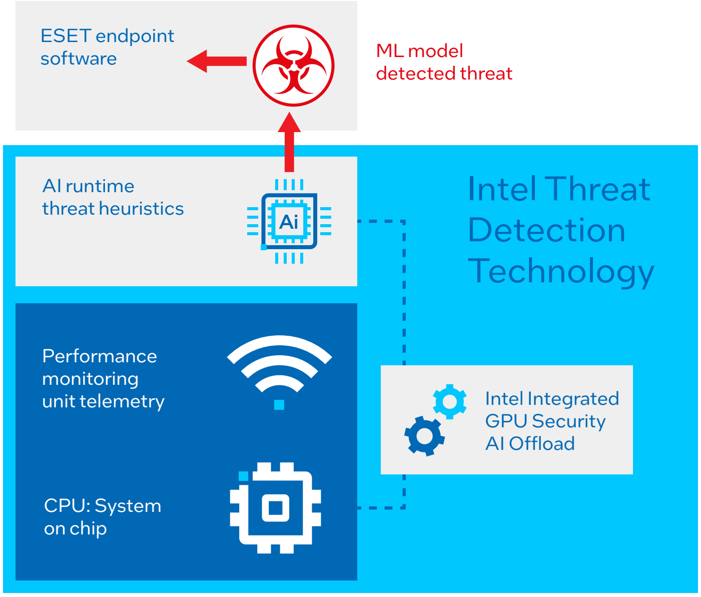

ESET endpoint software
ML model detected threat
AI runtime threat heuristics
Ai
Intel Threat Detection Technology
Performance monitoring unit telemetry
Intel Integrated GPU Security AI Offload
CPU: System on chip

Figure 1. ESET integrated Intel TDT into the ESET endpoint protection platform

ESET security leadership

ESET has researched malware and innovated security technologies for more than 30 years.[2] The company's philosophy is to track each threat over its lifecycle using key technologies to provide multiple layers of protection to endpoints.

ESET focuses on three parts of the threat lifecycle: prevention, detection, and response. This provides customers with peace of mind that most threats will be immediately warded off, and if a threat manages to penetrate prevention layers, ESET's sensors can detect the intrusion and initiate automated responses to intercept it. The result is enhanced protection for business data.

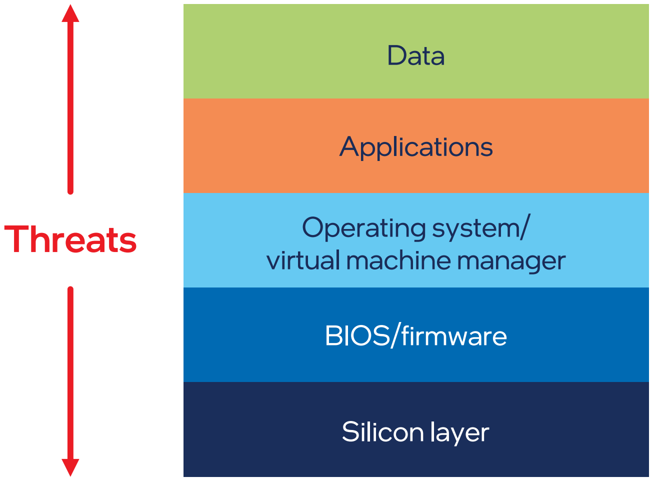
- **Prevent:** ESET offers a wealth of layered protection technologies that help block malicious code or malicious actors from entering or damaging a user's system. The data gathered from prevention methodologies is analyzed and used to further harden systems to repel future attacks.
- **Detect:** ESET provides diagnostic and investigative technology that helps identify post-execution malicious code based on its behavior, and it then triggers a response to prevent or mitigate damage.
- **Respond:** ESET delivers a suite of automated and sometimes manual actions that can halt, isolate, remove, and mitigate a threat to prevent it from spreading or doing significant harm.

What is ESET multilayer technology?

ESET protects against ransomware using key technologies that protect different layers of an endpoint. Some of the technologies that ESET uses include:[3]

- **Unified Extensible Firmware Interface (UEFI) scanner:** Enforces the security of the pre-boot firmware environment.
- **DNA detection:** Identifies malware in the application layer.
- **Advanced ML:** An array of algorithms that rapidly analyze threats across layers.

Multilayer protection



ESET's triannual threat reports provide an in-depth exploration of the key developments, trends, and threats that shape the cybersecurity landscape. Findings from ESET research labs and highlights from ESET investigations can help SMBs better respond to cybersecurity threats.

SMBs gain greater protection

By integrating Intel TDT, ESET gains access to CPU-level telemetry and ML heuristics. Now SMBs that run ESET endpoint security software on the Intel vPro® platform can experience superior protection against ransomware.

Processor support

ESET endpoint security software provides Intel TDT ransomware detection for devices with Intel® Core™ processors and the Intel vPro® platform, powered by 9th Generation and newer Intel processors.

Keep up to date on the latest security intelligence. Download ESET's latest threat report: eset.com/us/threat-report-t2-2022/

[1] Identity Theft Resource Center (ITRC). "2021 Business Aftermath Findings: Insights on Small Business Identity and Cybercrimes." October 2021. idtheftcenter.org/wp-content/uploads/2021/10/ITRC-Business-Aftermath-2021-Report-Final-102621.pdf.

[2] ESET. "Endpoint Solutions: Powerful multilayered protection for desktops, laptops and smartphones." eset.com/fileadmin/ESET/INT/Docs/Business/ESET_Endpoint_Solutions_solution_overview.pdf.

[3] ESET. "ESET industry leading technology." eset.com/int/about/technology/.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

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 does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

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 www.intel.com/Performance-vPro for details.

© 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.

Printed in USA   1122/MG/PRW/PDF   Please Recycle   353209-001US