Product Brief

Intel Platform Security
Intel® Threat Detection Technology

Hardware-enhanced Threat Detection

Intel brings new hardware capabilities to threat detection

Intel® Threat Detection Technology

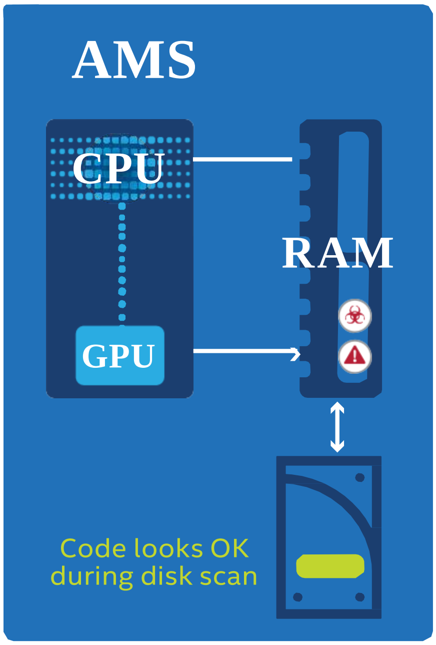

Figure 1. Accelerated Memory Scanning

Advanced threats require agile defenses

Cyber threats are increasing, attack surfaces expanding, hacker exploits getting smarter and more invasive. Bad actors are no longer just stealing data, they're commandeering computing resources on a massive scale. And through it all, the rate of change in cybersecurity keeps getting faster.

The good news: cyber defense is becoming more agile and increasingly data-driven. The best enterprise security solutions capture real-time data from a myriad of sources, and use these data to identify rapidly evolving threats. Increasingly, platform telemetry is becoming one of the most valuable sources of such data — and when combined with machine learning, memory scanning, and other hardware-enhanced capabilities, can significantly increase protection of IT systems.

Opening the doors to innovation

Intel® Threat Detection Technology (Intel® TDT) is a set of technologies that harness hardware telemetry and acceleration capabilities to help identify threats and detect anomalous activity. The raw data that Intel TDT analyzes for detection purposes is unique and valuable. Intel TDT uses these data to help identify polymorphic malware, file-less scripts, cryptomining, and other targeted attacks—in real-time, and with minimal end-user impact. Intel TDT enables developers to incorporate these capabilities to extend their own threat detection solutions in innovative ways.

More signal, less noise

In today's fast-evolving threat environment, security systems must do more than log events: they must deliver timely alerts, autonomously, and efficiently. They must also reduce false-positive alerts, long the bane of threat detection. Intel TDT uses machine learning heuristics to reduce false positives dramatically. Developers now can leverage Intel TDT's detection functions to improve threat detection, while tuning performance variables and false-positive rates that deliver the proper balance for their solution.

Memory scanning made practical

Memory scanning techniques have also been shown to be effective in identifying threats, but often go unused because of their performance overhead. Intel TDT enables certain real-time memory-scanning operations to be migrated from the CPU to the Intel integrated graphics processor. As a result, threat detection is enhanced without decreasing performance, impacting the user, experience or reducing battery life.

Where to get more information

Take the next step in protecting your enterprise by leveraging advanced Intel platform technologies to make your security software more effective. Visit Intel to learn more about Intel® Threat Detection Technology as well as the industry partners bringing it to market:

https://www.intel.com/content/www/us/en/security/hardware/threat-detection-technology-demo-video.html

For more information on how Intel is helping to protect customers and their data, please visit: **http://intel.com/hardwaresecurity**

Intel provides these materials as-is, with no express or implied warranties. All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice. Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com. Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.   Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

.