Hardware-enhanced Threat Detection

Advanced Threats Require Hardened Defenses

Your company’s digital devices and systems aren’t the only things getting smarter and faster each year. Cyberattacks are as well. New forms of malware—including clever next-gen polymorphic attacks, ransomware and even CPU capture exploits for cryptocurrency mining—now threaten even well-protected computing systems. In the face of these accelerating threats, software-only cyber solutions are no longer enough. While there’s no silver bullet for security, organizations can now meaningfully reduce the chances of system compromise by integrating new hardware-based cybersecurity technologies.

The latest of these technologies is Intel® Threat Detection Technology (Intel TDT). This product enhances system protection by using your hardware to deliver two powerful and innovative capabilities: hardware-based Accelerated Memory Scanning (AMS), and Advanced Platform Telemetry.

A Memory Scan You Will Want To Keep Running

Scanning systems’ memory is a familiar technique for detecting malware. Previously, constant scanning for malware came at a high cost in system performance and power consumption. As a result, users became frustrated and memory scanning capabilities were rarely used. With Intel TDT’s AMS, the scanning for memory-based malware is offloaded from CPU to Intel Integrated graphics processor —thereby enabling CPU resources to remain focused on core processing workloads, and improving the user experience when scanning is taking place.

Moving the main processing burden from the CPU to the Intel integrated graphics enables more frequent scanning, with only negligible impact on CPU performance. Lower CPU usage means lower power consumption, even while delivering more frequent and consistent memory scanning.

Real-Time Anomaly Detection, At the Core

Enhanced system protection using hardware system data to detect unusual system events is a strong defense against malware. Intel TDT provides such protection with its new Advanced Platform Telemetry.
Everything that runs on a machine with an Intel processor generates low-level data from the CPU that can be used for detecting threats. The Intel CPU platform has many such data sources that can be tapped for real-time threat detection. With its Advanced Telemetry Platform capability, Intel TDT can identify anomalies at the most basic level without needing a connection to a blacklist running in the background.

By leveraging this new source of system data, combined with ongoing machine learning, Intel TDT provides both ISV partners and end customers with a powerful new cyber defense capability—one designed to keep up with today's ever-changing cyber threat environment.

**Threat Protection That Gets Smarter Over Time**

Intel TDT enables independent software vendors (ISVs) to collect and analyze data that continually the local picture of what is normal for each system and each machine. This enables system operators, over time, to get better and better at recognizing suspicious activity. As a result, when some advanced new type of malware strikes, Intel TDT can help them identify it quickly by observing its behavior, rather than relying on signature identification only.

**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:


For more information on how Intel is helping to protect customers and their data, please visit [www.intel.com/security](http://www.intel.com/security)

---

**Accelerated Memory Scanning**

- **Improved System Performance:** Frees up the CPU for other tasks when scanning memory
- **Lower Battery Life Impact:** Reduced power consumption with GPU-based memory scanning
- **Better Security:** Security software can scan memory for threats more frequently

---

No computer system can be absolutely secure. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Intel and the logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

© 2018 Intel Corporation.