Trend Micro and Intel Innovate to Weed Out Covert Threats

Harnessing the power of software and hardware security to drive stronger ransomware detection for businesses, released at CES 2025

DALLAS, Jan. 7, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced a new collaboration with Intel® (NASDAQ: INTC) designed to help joint enterprise customers protect critical systems from stealthy threats, including fileless malware and advanced ransomware.

When Trend's proactive security platform and Intel's technology are used together, the integrated solution can better determine if encryption behavior is legitimate—such as a user backing up files or malicious—ensuring the appropriate action is taken to protect critical systems.

This news coincides with the CES 2025 (Consumer Electronics Show), which is the most influential tech innovation event for enterprises and society as a whole, where Intel and Trend will be present. Trend invites corporate attendees to join a panel discussion on Thursday, January 9th, entitled "Data Collection, Privacy and Why You Should Care," to learn how to safeguard a digital footprint as cybercriminals increasingly target critical data. Register now at: https://spr.ly/6044vmkSQ.

Carla Rodriguez, Intel VP: "Threat actors are increasingly targeting endpoints with sophisticated attacks that evade traditional software-based security. Trend's integration of Intel® Threat Detection Technology provides a hardware-accelerated detection layer to uncover stealthy threats. This technology, deployed across a billion PCs, is the only AI-based silicon security solution of its kind. Our mutual customers will benefit from enhanced protection with Trend's AI-powered Trend Vision One™ – Endpoint solutions on Intel AI PCs."

Protecting critical assets across endpoints, email, networks, and cloud workloads is increasingly challenging as malicious actors favor covert threats such as fileless malware, which was reportedly present in 40% of attacks in 2023. These can be used to deploy ransomware, steal sensitive data, and cause significant financial and reputational damage.

Fileless attacks are particularly dangerous as they rely on in-memory execution, reside in the registry, or abuse legitimate tools like PowerShell and Windows Management Instrumentation.

That's why Trend and Intel are teaming up by combining the AI-powered Trend Vision One. This collaboration provides organizations with powerful tools to detect and respond to ransomware and fileless attacks before they can cause damage.

Rachel Jin, Chief Enterprise Platform Officer at Trend:"Proactive security has long been desired but just recently feasible. Through our work with Intel, we're redefining what's possible in cybersecurity—empowering enterprises to proactively safeguard their systems, data, and operations against an increasingly complex threat landscape."

How AMS works:

- Intel® TDT offloads advanced memory scanning (AMS) workloads from CPU to GPU.
- This enables Trend endpoint security solutions to scan more deeply and more often to uncover fileless attacks before they can launch malicious payloads.
- Using fewer CPU resources enhances threat detection and response without affecting performance, slowing down PCs, or reducing battery life.

Trend Vision One™ – Endpoint Security leverages AMS to improve memory scanning capacity by 7 to 10X[1]. This means that organizations can scan more and detect more threats.

CPU-based threat detection:

Advanced ransomware is increasingly capable of evading EDR detection thanks to packing and obfuscation techniques and VM cloaking. EDR solutions are too often playing catchup with behavior-based approaches, which take time to get up to speed.

Intel® TDT augments Trend's behavioral analysis, runtime machine learning, and expert rules by providing critical visibility into the hardware layer, increasing ransomware detection efficacy by 24% over software alone.

It does this by:

- Using CPU telemetry and Intel® AI, offloading Intel AI and memory scanning from the CPU to the integrated GPU to provide a detection assist to Trend's ransomware defenses which won't disrupt the user experience.
- Integrating Intel TDT source code directly into the Trend Micro agent to deliver deeper insights from CPU telemetry. This enables instant discovery of zero-day attacks and new, fast-moving variants.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

---

[1] Trend Micro, Fileless Attacks Prompt Intel's Next-Gen Security,https://www.trendmicro.com/en_us/research/24/d/fileless-malware-attack-solution.html.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---