Solution Brief

Commercial Client
Endpoint Cybersecurity

Detect Ransomware and Other Advanced Threats with Intel® Threat Detection Technology

Key Capabilities

- **CPU Threat Detection**—Equip your Endpoint Detection and Response software to go beyond signature and file-based techniques with CPU malware behavior monitoring.
- **Full-Stack Visibility**—Help close blind spots to expose ransomware from legitimate data encryption as it avoids detection in memory or hides in virtual machines.
- **Unleash AI for Better Security**—Accelerate performance-intensive AI security algorithms by offloading to the Intel® integrated graphics controller. Boost security capacity to analyze more data and do more scans.
- **Accelerate Endpoint Detection & Response**—Bolster the performance of your security vendors' client agent processing for better user experiences

Ransomware Targets Endpoints with Devasting Impact

"Ransomware is rapidly shaping up to be the defining online security issue of our era," according to a June 2020 ZDNet report. In 2019, a leading data management solutions provider estimated that attacks had increased by 97% in two years causing $20 billion in damages, with an average attack cost of $80,000. A growing concern is the fact that ransomware has evolved to bypass traditional detection techniques.

Ransomware typically is downloaded through malicious links from phishing schemes targeting susceptible users' devices. On the endpoint, it typically will encrypt files and move laterally to infect a company's servers, network appliances, and even SaaS applications. Then a ransom message demands payment (typically in a cryptocurrency such as Bitcoin) in return for decrypting the data. Upon payment, the hackers may follow through to decrypt the data.

The Intel vPro® platform comes equipped with Intel® Hardware Shield to deliver built-in below the OS, application and virtualization security, as well as advanced threat protections like Intel® Threat Detection Technology (Intel® TDT). It is integrated into leading security vendors' software to improve security capacity and performance, resulting in increased threat detection efficacy on Intel vPro platform PCs. It operates seamlessly with the ISV's solution and requires no installation or deployment-related configuration.

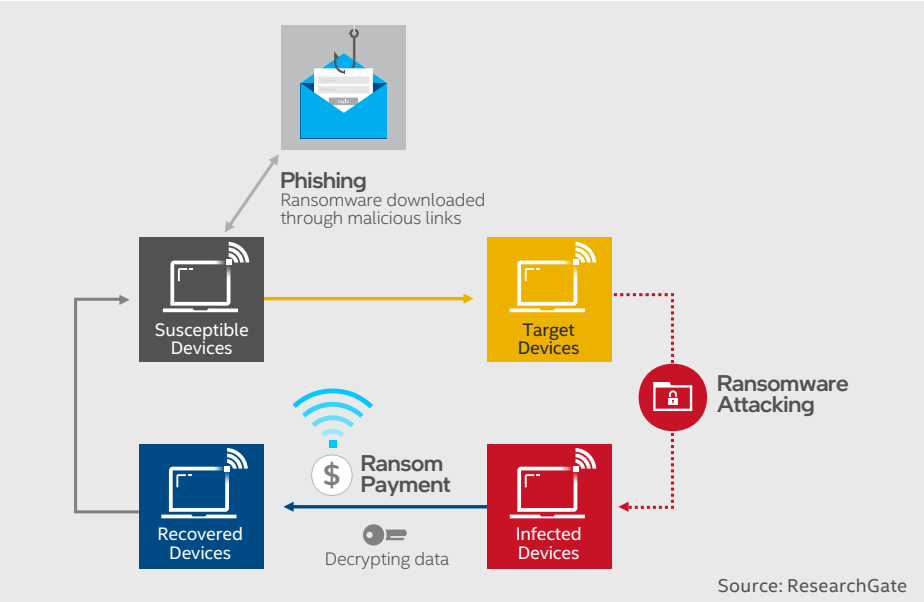

Figure 1. Ransomware attack lifecycle

Small Business, Public Sector, and Enterprise Vulnerabilities

A March 2019 Beazley Breach Response Services study shows that 70% of all ransomware attacks targeted small businesses, and a May 2019 Small Business Trends study indicates about 55% of small businesses say they'll pay ransomware demands if hit. Perhaps that's a key reason why 60% of small businesses fold within six months after such a cyberattack, according to the Chief Research Officer at the Vistage CEO Network in his May 2018, Inc., strategy piece.

Small and medium-sized businesses (SMBs) can be easy and popular targets for ransomware gangs because, unlike corporate environments, SMB users may be less sophisticated on secure browsing practices and secure data sharing techniques. SMBs often lack the defense in-depth mitigations that can be applied by a larger organization's dedicated IT security operations center, such as applying the latest patches and protections to its fleet of PCs.

Many SMBs rely on software as a service (SaaS) applications and managed service providers (MSPs) for IT support. In both cases, user PC endpoints offer a direct vector into rich targets of user data stored in the cloud. Additionally, MSPs and SaaS providers may have additional agent footprints and access to client machines across a fleet. This provides a means to move laterally to expand the threat impact: a single MSP can serve a large number of customers, so cybercriminals target MSPs to attack multiple companies, at scale.

SMBs cannot rely on cloud or local back-up storage to restore systems attacked by ransomware. Attackers often focus on infecting these commonly used disaster recovery systems in parallel attacks to ensure the system is re-infected unless the victim pays-up.

The harm wrought by ransomware is not limited to small businesses. Governments represent another tempting target for cybercriminals, with agencies at every level being especially vulnerable to ransomware attacks. "Ransomware is a particularly powerful weapon against governments, who must provide public services and cannot afford, financially or civically, to have data compromised to the point of governance paralysis," according to a May 2020 Deloitte Insights report.

A CPU Augmentation to Assist EDRs

Security software vendors offer Endpoint Detection and Response (EDR) solutions to help organizations of all sizes mitigate and recover from ransomware, malicious cryptomining and other Advanced Persistent Threats (APTs) that evade front-line defenses. EDR solutions help organizations find, contain, and remove threats quickly to help ensure endpoint security across the network. The vendors also offer companion Managed Threat Response turn-key services as an operational extension for IT.

Intel® Threat Detection Technology (Intel® TDT), as shown in Figure 2, provides an augmentation for EDRs to help increase detection efficacy, lower false positive alerts, expand visibility to catch advanced evasion techniques, and boost the overall security performance of endpoint agents. Intel TDT is not a standalone product but provides the source code that is integrated into the EDR agent to enable these CPU-assisted capabilities.

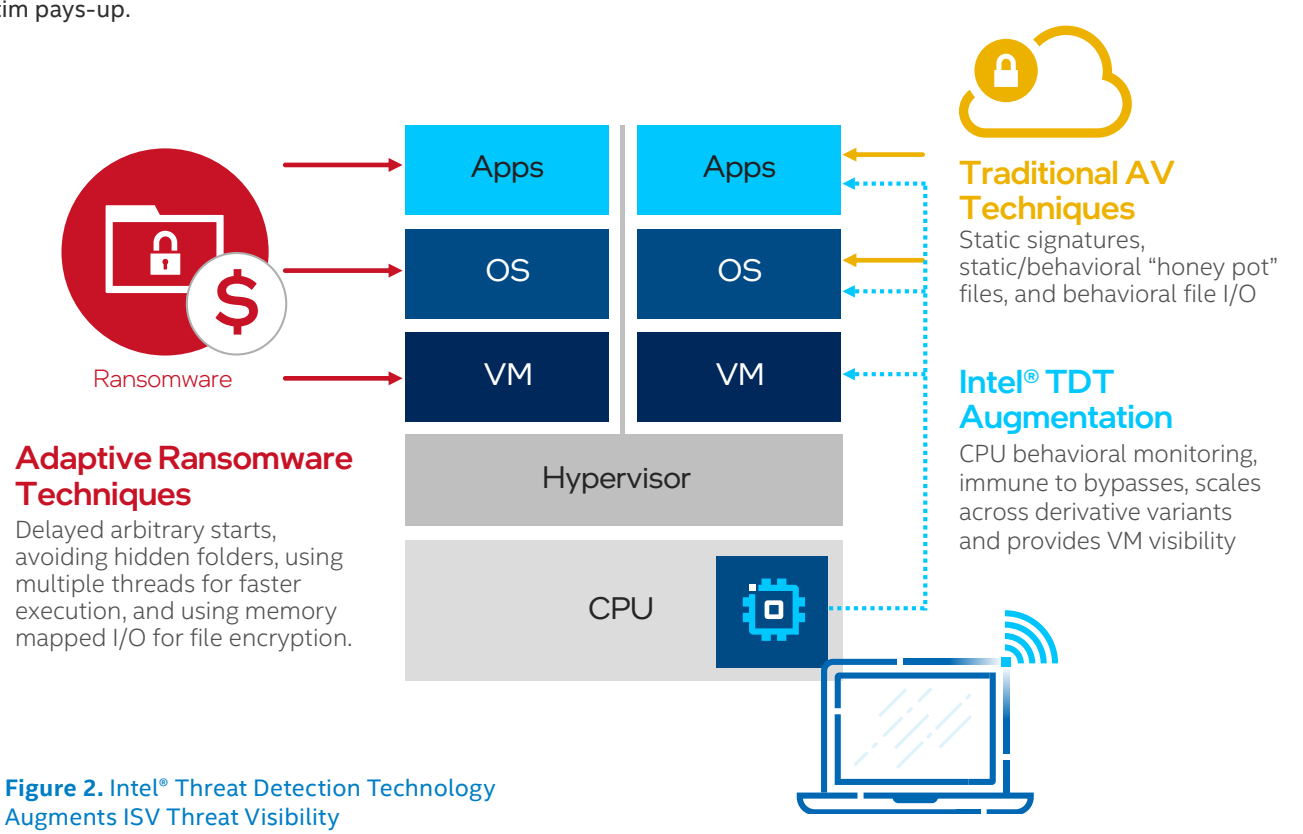

Figure 2. Intel® Threat Detection Technology Augments ISV Threat Visibility

Software-only EDR solutions often utilize performance-intensive compute operations such as AI algorithms and memory scanning that can drag down the user experience. To assist, Intel TDT offloads security workloads to the iGPU, preserving CPU resources for user productivity and increasing visibility to uncover evasion techniques that attackers are increasingly using. Commonly deployed detection techniques like static signatures, static/behavioral "honey pot" files, and behavioral file I/O all have bypasses exploited by ransomware using delayed arbitrary starts, avoiding hidden folders, using multiple threads for faster execution, and using memory mapped I/O for file encryption. The work-from-home model that increasingly leverages virtualized desktops and applications is also making enterprises more vulnerable to ransomware. Cyber criminals now target ransomware into the virtual machine (VM) layer that security vendor solutions cannot see with host OS-based scanning software.

As the frequency and severity of ransomware attacks grow, anti-virus/end-point detection and response (AV/EDR) vendors realize that CPU-based behavioral monitoring is indispensable for ransomware detection. File encryption is the fundamental operation of ransomware, and there is no relevant software/OS-level telemetry to monitor its behavior. CPU level telemetry allows Intel TDT to track encryption at the lowest level, and ML heuristics allows Intel TDT to be deterministic about singling out encryption by ransomware from other encryption behavior on the platform. CPU telemetry is immune to most bypasses, and it scales across derivative variants, common among ransomware threats. Typical EDR behavioral analysis can be susceptible to new variants of malware attacks. By looking at the run-time behavior at the CPU level, Intel TDT can help detect a new variant from its behavior.

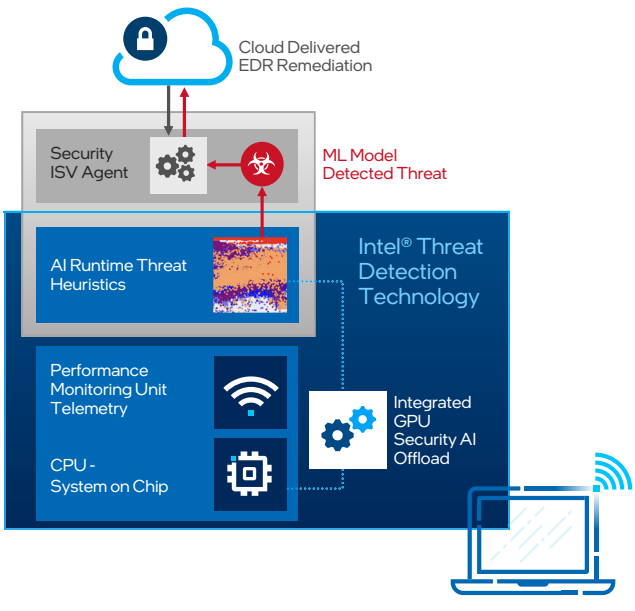

Figure 3. Intel® Threat Detection Technology

Ragnar Locker Ransomware Deploys VM to Evade OS-level Security

According to a **May 2020 Sophos News report**, Ragnar Locker ransomware was deployed in a recently detected 2020 attack inside the virtual guest machine. Its process and behaviors ran unhindered, because they were out of reach of security software on the physical host machine. The hacker gang targeted a Portuguese energy company and stole 10 terabytes of sensitive company data, demanding a ransom of 11 million US dollars.

Intel Hardware Shield, Built-in Endpoint Ransomware Protections

Although many businesses implement software-based security solutions, hackers continue to get more sophisticated, attacking the hardware layer. The Intel vPro platform offers built-in, hardware-based security features to provide a more secure foundation with protection against attacks below the operating system, coupled with remote recovery capabilities.

More than just a processor, the Intel vPro platform has integrated and validated hardware and software technologies that deliver performance, security, manageability and stability. The platforms are available from leading PC makers in thin and light mobile systems with long battery life, small form factor desktops and workstations that support a rich, visual computing environment.

Intel TDT is a key feature of the Intel vPro platform which makes profiling and detection possible across the entire device stack. Intel TDT uses a combination of CPU telemetry and ML heuristics to detect attack-behavior. It detects ransomware and other threats that leave a footprint on Intel CPU performance monitoring unit (PMU). The Intel PMU sits beneath applications, the OS and virtualization layers on the system and delivers a more accurate representation of active threats, system wide. As threats are detected in real-time, Intel TDT sends a high-fidelity signal that can trigger remediation workflows in the security vendor's code. Intel TDT issues no specialized efficacy or performance reports; rather, the data is seamlessly incorporated as a part of normal endpoint sensor reporting.

Intel TDT can parallelize multiple concurrent detectors at once. That helps increase the capacity of the security vendor to do more scans, which increases efficacy and lowers false positives inherent in threat detection.

Intel CPUs come with an integrated graphics controller (GPU), and Intel TDT can be used to offload security vendor workloads such as advanced memory scanning (AMS) to the GPU to return performance back to the CPU. ISVs leveraging Intel TDT typically use GPU offload as a default for functions such as AMS, but they also may add a configurable setting for Intel TDT testing.

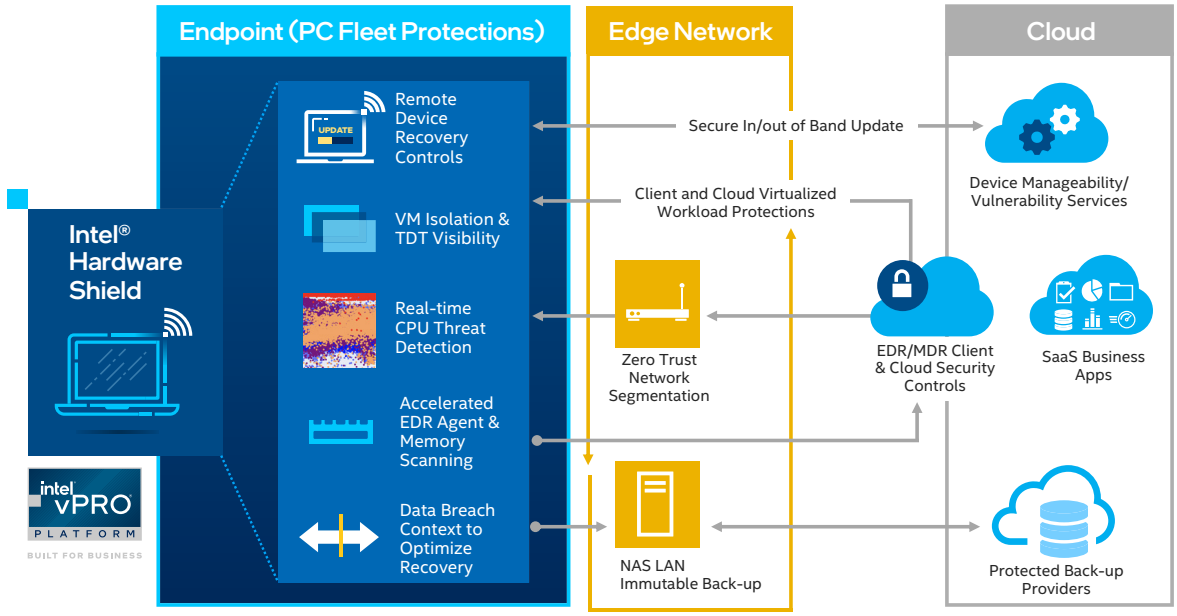

Figure 4. Intel® Threat Detection Technology Part of a Best Practice Ransomware Defense

Hardened PCs Enable Best Practices for Ransomware Defense

As an evolving threat, ransomware has proven itself adept at targeting the blind spots of security vendors' software. Intel® Core™ processor-based PCs and the Intel vPro platform have built-in CPU threat detection that should be part of a comprehensive approach to protect against ransomware.

Detection: Intel 10th Gen and newer Intel Core processor-based PCs are out-of-the-box capable to leverage Intel TDT CPU behavior monitoring and threat detection in conjunction with security vendors that have integrated the capability into their endpoint protection software. No deployment-time configuration is required to activate the feature in hardware. Intel TDT increases efficacy in detecting threats as they occur across the PC fleet.

Protection: IT departments using EDR software or outsourced MDR operations can collect additional context on Intel TDT-signaled threats to remediate with patches or segment machines using perimeter network defenses. Even when ransomware infiltrates a system, Intel vPro platform PCs with Intel Hardware Shield can help restrict lateral movement with hardware-enforced isolation of virtualized containers, memory protections, secure boot and below the OS firmware security.

Recovery: A ransomware best practice for on-prem or cloud-based back-up storage should include immutable file systems with WORM storage that only allow data to be written to storage once. Intel TDT includes early detection signals along with EDR remediation workflows to aid with better ransomware analysis-based recovery. It helps quickly identify affected data and the best recovery points. Device manageability providers leverage Intel vPro platform PCs to offer additional in- and out-of-band recovery controls such as remote patching, secure erase, re-imaging endpoints and dynamic re-launch of the OS in a hardware-secured environment.

Industry Leading Threat Detection

Intel TDT helps end-point security solutions harness CPU telemetry and hardware acceleration to help identify threats and detect anomalous activity. The PMU data and ML heuristics that Intel TDT analyzes for detection purposes are industry-leading and indispensable for comprehensive threat detection. Intel TDT can help identify polymorphic malware, file-less scripts, cryptomining, ransomware and other targeted attacks—in real-time and with little if any end-user impact.

Intel TDT is enabled by leading security vendors, including Microsoft Defender, SentinelOne Singularity, and Blackberry Optics. If you wish to enable your solution for these capabilities visit intel.com/hardwareshield.

Visit www.intel.com/vpro to learn more about how the built for business Intel vPro platform delivers the performance, security, manageability, and stability to help propel your business.

1221/MZ/DCC/PDF