Joint Solution Brief

Information Technology
Cybersecurity

Detect Threats Earlier with Hardware Assisted Security

Key Benefits

- Out-of-the-box enhancements that increase efficacy and performance on Intel processor-based PCs.
- Intel's hardware-based security capabilities help enable greater protection than software, alone.
- Uncover exploits earlier with CrowdStrike's solution optimized for hardware-based exploit detection.
- Deploy the Leader in Endpoint Protection Platforms[1] with PCs built for business: Intel vPro® provides the most comprehensive security for your business.[2]
- Enhance Fileless Attack Detection of advanced persistent threats (APTs) that attempt to evade detection in memory or infect system processes.

[2] Intel vPro® provides the most comprehensive security for your business as measured by the unrivaled combination of above and below the OS security capabilities, app and data protections, and advanced threat protections Intel vPro delivers for any sized business, as well as Intel's security first approach to product design, manufacture, and support. All business PCs built on the Intel vPro platform have been validated against rigorous specifications, including unique hardware-based security features. See www.Intel.com/PerformanceIndex (platforms) for details. No product or component can be absolutely secure.

CrowdStrike Falcon Insight on Intel vPro®: A "Better Together" Security Solution

With the evolution of fileless attacks and advanced persistent threats (APTs) that evade detection in memory, Intel and CrowdStrike collaborated to bring a unique combination of world-class technologies and expertise to co-engineer advanced threat detection and response capabilities. The resulting endpoint detection & response (EDR) solution delivers Intel's hardware leadership and CrowdStrike's cybersecurity innovations out of the box – built on industry-leading AI and machine learning.

Solutions rooted in hardware provide a great opportunity to help protect against current and future threats. The Intel vPro® platform brings a defense-in-depth hardware security foundation to help protect hardware, firmware, and software attack surfaces.

Figure 1. Combine CrowdStrike Falcon with Intel vPro to get more out of your PC fleet and endpoint security investments.

A Sustained Wave of Fileless Attacks

Attackers now use more stealthy methods for exploit/initial access, as well as for post-exploit malicious activities. Attackers often co-opt legitimate code to gain initial access – for example, by re-using instructions already loaded in memory. An increasing proportion of post-exploit malicious activities operate without attackers writing malware to the endpoint – for example, by using in-memory code injection, Living-off-the-Land binaries, and scripts.

Of all detections indexed by the CrowdStrike Security Cloud in Q4 2021, 62% were malware-free.[3] And that trend has been around for a while: 63.2% of the 1,097 vulnerabilities disclosed by ZDI from 2019 were memory safety related, targeting OS's, browsers, readers, and other applications.[4]

Malware-free strategies can open the door to the stealthiest advanced persistent threats (APTs), ransomware, and prevalent dual-use tools like Cobalt Strike that conduct reconnaissance ahead of attack payload execution. Cobalt Strike in particular has shown up 161% more, year-over-year, in cyberattacks, having "gone fully mainstream in the crimeware world."[5]

Attackers share EDR weakness and evasion techniques to circumvent detection. It takes time for traditional EDR solution updates to catch up. That contributes to a Day 0 gap, making enterprises vulnerable. Hardware-based security capabilities add powerful new ways to address these gaps.

A Modern Solution Strategy: Real-Time Indicators of Attack

After-the-fact "Indicators of Compromise" (IOC) detection strategies leave blind spots. An IOC-based approach cannot detect the increasing threats from malware-free intrusions and zero-day exploits. Zero-day vulnerabilities can only be stopped with a dynamic solution that responds to new threats in real-time, earlier in the kill chain.

Falcon Insight — EDR made easy

CrowdStrike Falcon Insight delivers complete endpoint visibility across your organization. It accelerates security operations, allowing users to minimize efforts spent handling alerts and reducing time to investigate and respond to attacks. Falcon Insight delivers visibility and in-depth analysis to automatically detect suspicious activity and stop stealthy attacks – and breaches.

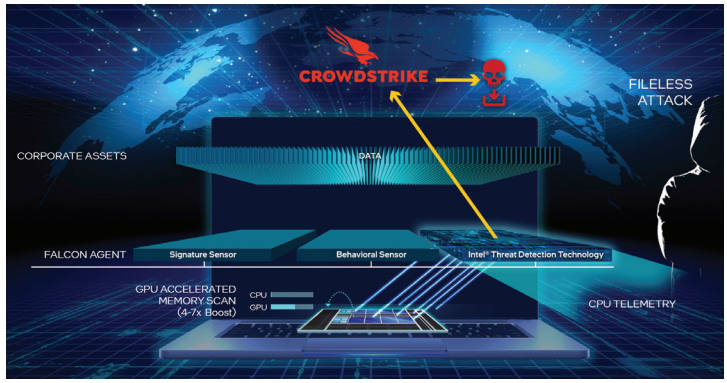

Figure 2. CPU Based Threat Detection Architecture

Leveraging cloud-native services for dynamic behavior detection and response in real time, Falcon Insight delivers immediate value with CrowdStrike's innovative approach based on Indicators of Attack (IOAs). Using telemetry data from the Falcon Agent, the Falcon platform is powered by IOAs targeting known malicious behaviors. Each IOA focuses on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used. Optimizations for Intel vPro bring new hardware security capabilities to further enable Crowdstrike's innovative IOA approach. In addition to its complex network of behavior-based IOAs, Falcon Insight also sends AI-powered detections to Falcon lightweight agents. These AI IOAs are generated from machine learning models trained on enormous data sets, including behaviors and telemetry obtained through features enhanced with Intel processors running Falcon agents.

Intel vPro: Comprehensive Hardware-based Security for Business

Intel vPro has helped set the gold standard for business PC security over the past 16 years, and it has been deployed on over 300 million endpoints in corporate fleets. Intel® Hardware Shield, a key part of the Intel vPro platform, delivers built-in below-the-OS security capabilities, application and data protections, and **Intel® Threat Detection Technology (Intel® TDT)** for advanced threat protections.

These out-of-the-box capabilities are simple to activate on Intel vPro hardware, bolstering zero-trust policies with defense in depth "device health" secure foundations at each layer: hardware, BIOS/firmware, hypervisor, VM, OS, and applications. In addition, remote keyboard/video/mouse temporary boot redirection, power controls, and seamless

Use Case	Solution	Benefits
Application Control-flow Attacks	Falcon Insight HEED capabilities use Intel CPU telemetry. Intel CET delivers CPU lock-down capabilities on modern 11th gen plus PCs. Together these capabilities help prevent attacks from redirecting the control flow of a program.	Modernize PC fleet protections to detect high volume ROP attacks.
Advanced Memory Scanning (AMS)	Falcon Insight AMS uses Intel® TDT to enhance Fileless Attack Detection of advanced persistent threats (APTs), ransomware, and dual-use tools during the earliest steps of the kill chain.	Scan broader swaths of memory to help detect earlier indicators of attack.
AI based IOAs (Indicators of Attack)	Falcon Insight HEED-based IOAs trigger AMS to help uncover stealthy, 2-stage attacks such as Cobalt Strike that might deploy a secondary ransomware payload.	Respond decisively in real time to stop attacks before they become breaches.

Table 1. Business Value

firmware updates help you manage and fix systems in remote and hybrid work environments. With validated protections tested with the broadest range of security standards, Intel vPro® platform delivers 47 built-in MITRE ATT&CK countermeasures.[6]

Combine Best-of-Breed Solutions and Industry first Enhancements for Increased Security on Intel

Falcon Insight utilizes Intel vPro's Advanced Threat Protection capabilities *(Figure 3)*. With deep hardware integration at the foundation, Falcon Insight can drive increased threat detection efficacy with minimal performance impact.

CrowdStrike's Hardware-Enhanced Exploit Detection (HEED) helps protect against sophisticated exploit techniques, including shellcode-injection, and memory attacks, such as return-oriented programming (ROP). Generally, these techniques redirect execution to an attacker-controlled location.

CrowdStrike strengthened Falcon Insight exploit protection by using Intel® Processor Trace (Intel® PT) CPU telemetry. If supported by the machine, HEED can enable execution tracing for a critical set of programs. Whenever the program executes a critical system service, the sensor will analyze the captured trace to look for suspicious operations.

The CrowdStrike Falcon agent leverages Intel CPU telemetry to deliver memory safety protections for many customers on older PCs. Such platforms lack the modern in-built protections of Intel® Control-flow Enforcement Technology (Intel® CET) and its CPU lock down approach (which starts with 11th gen Intel mobile and all 12th gen Intel vPro platforms).

Fileless attacks do not drop traditional malware or a malicious executable file to disk – they can deploy directly into memory. A fileless attack is difficult to discover because of the compute resources required for memory scan detections to be performed broadly.

Falcon Insight can help solve that with **Advanced Memory Scanning (AMS) using Intel TDT** with hardware-enhanced algorithms. Further acceleration can be gained using the Intel TDT capability to offload these performance-intensive parallel tasks to the Intel integrated GPU.

With Intel TDT and AMS, the Falcon sensor can scan large swaths of a program's virtual memory, looking for IOAs. Testing shows that Intel TDT executed the compute-heavy AMS workload at 4 to 7 times the performance of native CPU implementations,[7] helping to ensure a performant user computing experience.

Figure 3. Joint Solution

[6]See www.intel.com/PerformanceIndex (platforms) for details. No product or component can be absolutely secure.

Simple, Out-of-the-box Configuration

The Falcon Insight user-interface for IT administrators includes a Prevention Policies screen on which administrators can enable both HEED and AMS capabilities. Administrators also can implement dual-use cases where HEED-based IOAs trigger AMS to help uncover stealthy, two-stage attacks such as Cobalt Strike that might deploy a secondary ransomware payload. To help protect the broader fleet, IT admins also can promote policies from detection to prevention.

Get the Most from your CrowdStrike and Intel Investment

For increased EDR efficacy and performance, to deliver comprehensive end-to-end security for your business, ask your suppliers to bundle CrowdStrike Falcon Insight and Intel vPro.

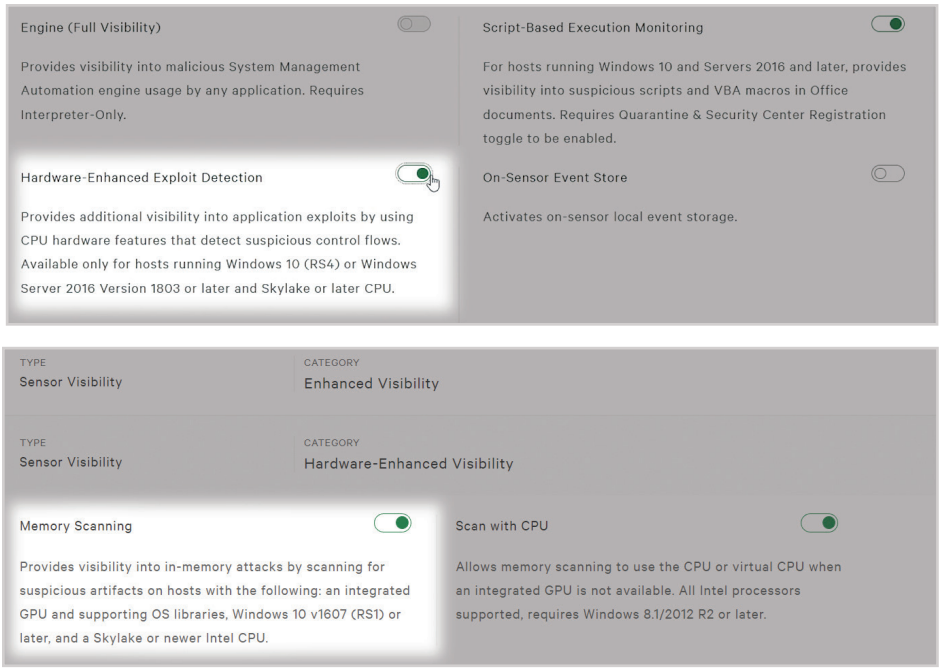

Figure 4. With Prevention Policies, administrators can enable HEED and AMS capabilities and take advantage of dual-use cases.

Minimum Endpoint Requirements:

- CrowdStrike Falcon sensor 6.37 or later with Hardware Enhanced Exploit Detection
- Windows 10 RS4 or later
- 6th gen or newer Intel® Core™ processor-based PC platform

Solution Provided By:

CROWDSTRIKE intel®

[1] Forrester Wave: Endpoint Detection And Response Providers, Q2 2022

[2] Intel vPro® provides the most comprehensive security for your business as measured by the unrivaled combination of above and below the OS security capabilities, app and data protections, and advanced threat protections Intel vPro delivers for any sized business, as well as Intel's security first approach to product design, manufacture, and support. All business PCs built on the Intel vPro platform have been validated against rigorous specifications, including unique hardware-based security features. See www.Intel.com/PerformanceIndex (platforms) for details. No product or component can be absolutely secure.

[3] 2022 CrowdStrike Global Threat Report

[4] Zero-Day Initiative Published Advisories

[5] "Cobalt Strike Usage Explodes Among Cybercrooks" June 21, 2021, Threat Post.

[6] Coalfire Report, including analysis showing the Intel vPro® platform delivers 47 built-in MITRE ATT&CK countermeasures

[7] "4-7 times faster" is based on CrowdStrike validation testing

0922/DCC/MZ/PDF