Solution Brief

Endpoint Security

Help Shrink the Attack Surface of Endpoints with Hardware-Assisted Security

Stop advanced endpoint attacks with coordinated hardware and software defenses

Key Benefits

- **Reduce the Attack Surface by 70%[1]**
  Shut down entire classes of threats with Dell PCs running Intel® Core™ and Intel® Core™ Ultra processors on the Intel vPro® platform. Enhance and extend CrowdStrike Falcon® platform protections across the stack.
- **Enhance Threat Detection**
  Uncover early indicators of attack (IOAs) with hardware enhanced exploit detection.
- **Work with Zero Trust-Capable Solutions** Maintain device trust with full control over security posture via remote access (SaaS) to hardware telemetry and below-the-OS alerts.
- **Optimize Security Investments**
  Realize the benefits and efficiencies that come from consolidating security providers.
- **Activate with Ease**
  Deploy CrowdStrike Falcon solutions on a Dell device based on the Intel vPro platform and toggle on the capabilities to monitor your devices.

Summary

Modern threats have advanced to easily circumvent traditional point security software focused on blocking known malware, meaning that attacks often evade these legacy software security tools. What's more, attackers now employ sophisticated techniques that target different layers of the computing stack, which blend in with valid system processes. This malware-free approach now comprises 75%[2] of all attacks. To compound this, research from IBM shows that as many as 90% of successful cyberattacks originate at endpoint devices.[3]

Further, hybrid work has exposed corporate endpoints which access SaaS apps outside of the traditional network security perimeter. These combined threats have effectively increased the attack surface and accelerated the adoption of cloud-native endpoint detection and response (EDR) and extended detection and response (XDR) software. However, to stay ahead of modern, fast evolving threats, it takes deep ecosystem collaboration – across both hardware and software – to provide seamless multi-layered protection across the attack surface.

To that end, Dell, Intel and CrowdStrike have co-engineered threat detection and response capabilities that combine the power of Dell Trusted Devices, the industry's most secure commercial PCs[4], with Intel's silicon capabilities and CrowdStrike's industry-leading endpoint security and XDR platform.[5]

Working together, CrowdStrike, Dell, and Intel's layered solution reimagines endpoint security for your business, extending beyond software protections to hardware-assisted security.

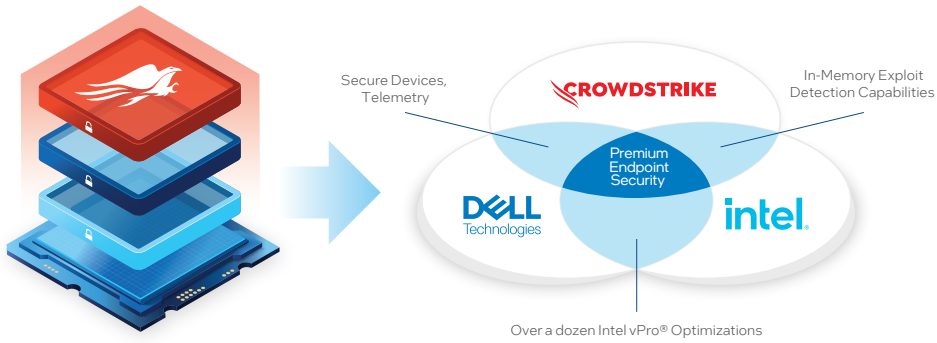

Figure 1. Multiple Layers of Protection That Work Together

The Expanding Attack Surface of the PC

As organizations harden one attack surface, threat actors move to other, softer targets. Attackers now use even 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 (LotL) binaries, and scripts.

Malware-free strategies can open the door to the stealthiest advanced persistent threats (APTs), ransomware, and prevalent dual-use tools like Cobalt Strike or Sliver C2 conduct reconnaissance ahead of attack payload execution. In particular, Cobalt Strike has shown up 161% more often in cyberattacks, having "gone fully mainstream in the crimeware world."[6]

Below-the-OS attacks similarly increased with hybrid work. In fact, in a recent survey of global IT decision makers, 69% reported at least one device/BIOS-level attack in the last twelve months. That's up 1.5 times from the 2020 study.[7]

Defense-in-Depth Evolution – Hardware-assisted Attack Surface Protections

Combatting this advanced threat craft requires a tight coupling of hardware and software protections. Given today's sophistication and volume of attacks, defense-in-depth is critical. This way, if an attack bypasses one line of defense, additional layers exist to disrupt the cybersecurity kill chain. The good news: PC hardware security has advanced to provide native protections designed to shut down entire classes of attack and feed CPU telemetry to threat management consoles for a rapid response. In fact, according to research conducted by IOActive, Dell commercial PCs with 13th Gen Intel® Core™ processors on the Intel vPro® platform have been shown to deliver a 70% attack surface reduction over 6th generation.[1]

Each new Intel vPro generation offers advances in security protections, to help make security solutions like the CrowdStrike Falcon® platform even more effective. SecOps teams that deploy CrowdStrike cybersecurity software on Dell PCs leveraging the Intel vPro platform activate a unique suite of integrated hardware and software capabilities to protect their growing attack surface.

Overview of Each Technology at Work

Intel vPro®: Built for Business

For more than 16 years, the Intel vPro platform has provided a comprehensive silicon-based solution for business PC security, deployed on more than 300 million endpoints worldwide.

Secure foundations are established at every layer: hardware, BIOS/firmware, hypervisor, VM, OS, and applications. In addition, remote keyboard/video/mouse temporary boot redirection, power controls, and seamless 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 43 built-in MITRE ATT&CK countermeasures.[8]

Included with Intel vPro, Intel® Thread Detection Technology (Intel® TDT) provides increased security performance at the hardware level. With AI-powered security capabilities, Intel TDT helps prevent ransomware, cryptomining, and even memory scanning attacks.

Dell: The Industry's Most Secure Commercial PC

Dell Trusted Workspace reduces the attack surface of a fleet with multiple layers of security. "Built-with" supply chain security establishes a trusted PC foundation. Along with a secure development lifecycle and rigorous supply chain controls, SafeSupply Chain solutions offer extra assurance of product integrity (e.g., Dell-unique Secured Component Verification).

Next, Dell-unique "built-in" hardware- and firmware-based protections like SafeBIOS work to prevent and detect foundational attacks below-the-OS, including unique features like off-host BIOS verification and Indicators of Attack (IOA). SafeID equips the device with a dedicated FIPS Level 3 security chip for credential protection and user authentication. The Dell Trusted Device (DTD) Application works in concert with these BIOS protections and the Intel® Management Engine to deliver additional Dell-only capabilities like off-host firmware verification.

Finally, "built-on" software security, delivered through an ecosystem of best-of-breed partners such as CrowdStrike, provides integrated protection against advanced threats. For those customers requiring additional support, Dell Managed Detection and Response provides 24x7 services and support.

Falcon Insight XDR/EDR: Threat Detection and Response Made Easy

CrowdStrike Falcon Insight® XDR helps to deliver complete real-time endpoint visibility across the entire organization. It accelerates security operations, allowing organizations to minimize efforts spent handling alerts and reducing time to investigate and respond to attacks. Falcon Insight XDR delivers visibility and in-depth analysis with AI-native capabilities to automatically detect suspicious activity and stop stealthy attacks – and breaches.

Leveraging cloud-native services for dynamic behavior detection and response in real time, Falcon Insight XDR delivers immediate value with CrowdStrike's innovative approach based on IOAs. Using hardware & other telemetry data from the lightweight Falcon agent, the Falcon platform is powered by IOAs targeting unknown 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 the Intel vPro platform bring new hardware security capabilities to further enable CrowdStrike's innovative IOA approach. In addition to its complex network of behavior-based IOAs, Falcon also sends AI-powered detections to the Falcon agent. 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 the Falcon agent.

How Hardware-Assisted Security Works

As illustrated in Figure 2, CrowdStrike Falcon XDR/EDR can leverage device-level telemetry from Dell commercial PCs running on Intel vPro, as well as Intel TDT to detect the stealthiest attacks.

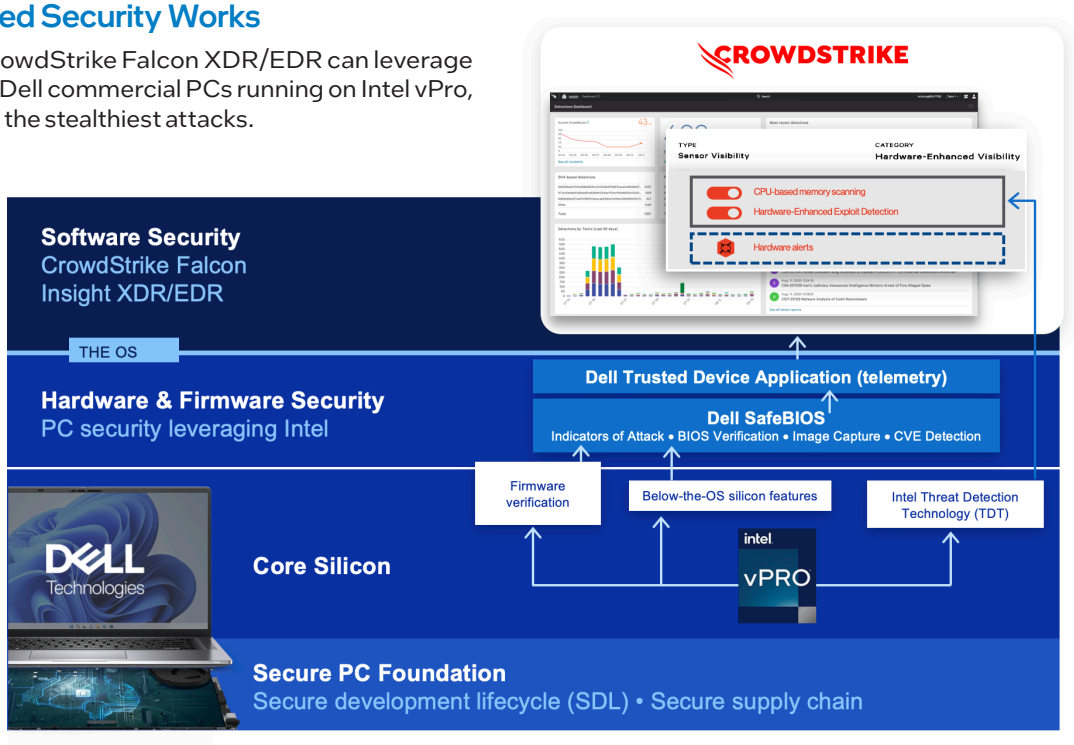

Figure 2. Tighten the 'IT-Security Gap' with hardware and software defenses that work together

Use Cases

We'll breakdown two attack scenarios to demonstrate how these joint hardware and software capabilities activate to disrupt the kill chain before they do damage:

Use Cases	Description	Hardware-Assisted Countermeasures
Fileless Malware Attacks	**Fileless Malware Attacks** are now the dominant execution method for all cyberattacks. Fileless techniques such as execution in memory and LotL (native tools/script abuse) can evade legacy EDR software solutions. For example, during an email phishing attack, clicking a link can deploy a Cobalt Strike beacon payload to execute initial access and establish a persistent back-door command and control. This may be completely undetected by legacy EDR software may look for malware signatures on disk and provide basic memory scanning, but it is not tied to AI IOAs. The ultimate cyberattack objectives could be data exfiltration through ransomware, access to the corporate VPN through DLL hijacking, coopting application memory execution through ROP attacks, or fault injection through BIOS level SMM attacks.	Dell commercial PCs help provide the visibility and actionability needed to disrupt these attacks, leveraging proprietary BIOS/firmware defenses and Intel® Control-flow Enforcement Technology (Intel® CET) to help shut down the entire class of ROP attacks. CrowdStrike's Hardware Enhanced Exploit Detection (HEED) integrates Intel® Processor Trace (Intel® PT) CPU telemetry to extend memory safety protections for coded injection techniques, across PC fleet generations. In addition, CrowdStrike has re-imagined how to stop fileless attacks early in the kill chain by using the accelerated memory scanning algorithms of Intel TDT and its ability to offload processing to the Intel® Graphics Technology integrated graphics processor. The resulting 4-7x performance[9] acceleration helps ensure a performant user experience while applying CrowdStrike's dynamic IOAs to the memory layer – and it's only available on Intel® processor-based PCs. As fileless attacks attempt to move down the stack, Dell SafeBIOS uses the Intel vPro platform's Intel® System Resource Defense technology to restrict system privileges and malicious access to the OS.
Foundational Attacks	**Foundational Attacks** are rapidly increasing as OS-level security improves. Attackers are frequently turning to rootkits and other firmware vulnerabilities to unleash devasting privilege-escalation attacks – largely undetectable by legacy EDR software alone. These foundational attacks are extremely hard to detect and remediate across remote worker fleets.	Dell commercial PCs offer a first line of defense with built-in security features. For example, SafeBIOS IOA and off-host Intel® Converged Security & Management Engine (Intel® CSME) firmware verification give IT SecOps teams enhanced visibility into the trustworthiness of a device. For improved visibility into foundational attacks, CrowdStrike Falcon Insight XDR can help reveal potential firmware tampering and deviation from the known good image by using telemetry from the Dell Trusted Device Application. For remediation, the Dell Client Command Suite uses the Intel vPro platform's out of band management capabilities to equip administrators with remote keyboard/video/mouse (KVM) to wake a device, wipe its main drive, or initiate an Intel® Firmware Guard assisted firmware update to reliably reduce the possibility of in-the-field system crashes. Dell, Intel, and CrowdStrike's coordinated capabilities provides a unique, multi-layer defense-in-depth that improves a SecOps team's effectiveness and efficiency as they protect, correct, and respond to evolving cyberthreats.

Table 1. Attack Use Cases

Simple Activation

With this three-way collaboration, the Falcon platform's user-interface for IT administrators includes a Prevention Policies screen on which administrators can enable both HEED and Accelerated Memory Scanning (AMS) capabilities. To help protect the broader fleet, IT admins also can promote policies from detection to prevention. With the Dell Trusted Device (DTD) Application enabled, below-the-OS telemetry supplements detection and response. Device-level security notifications and alerts appear in Dell consoles (via the Windows Event Viewer). Admins can also view BIOS-level weaknesses remotely in the Falcon console, leveraging that same DTD telemetry.

Get the Most from Your Security Investments

The CrowdStrike Falcon platform deployed on Dell commercial PCs based on the Intel vPro platform enhances XDR/EDR efficacy and performance. Dell customers can purchase CrowdStrike Falcon solutions at the same time as they purchase Dell Hardware 'on-the'box'. Choose the option that is right for your organization. (Table 2)

You can also add CrowdStrike Falcon solutions to your existing hardware at any time.

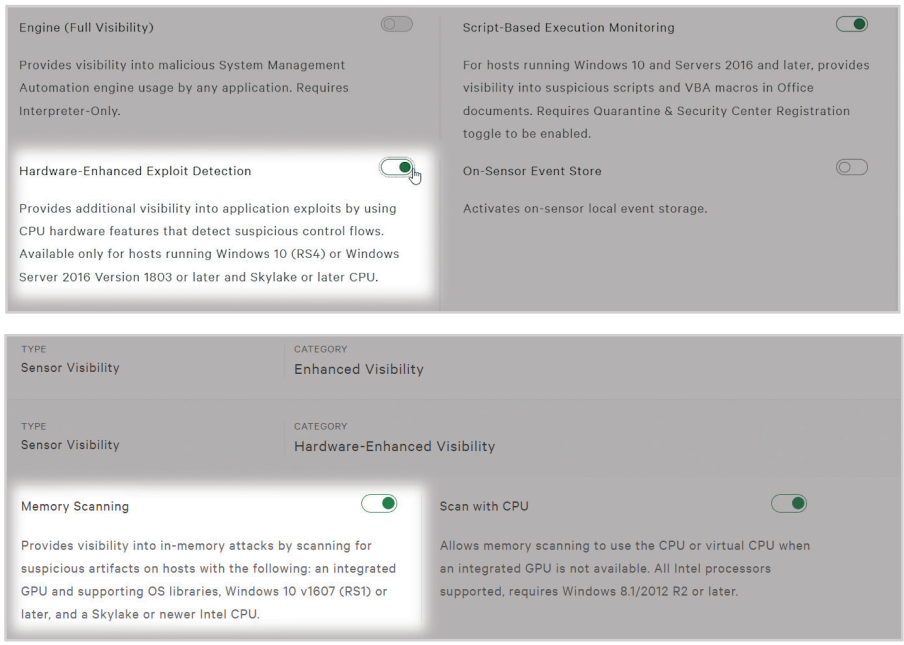

Figure 3. With Prevention Policies, administrators can enable HEED and AMS capabilities and take advantage of dual-use cases.

Target Customer	Solutions
Enterprise	Dell: Latitude, OptiPlex, Precision and Rugged, Intel vPro Enterprise

Table 2. Recommended Solution Pairing

Learn More

Watch the Demo Video

or contact: global.security.sales@Dell.com

Solution Provided By:

intel. DELL Technologies CROWDSTRIKE

[1] The latest Intel vPro based PCs provide an estimated 70% attack surface reduction compared to four-year-old devices. Based on IOActive's "Intel vPro 13th gen Attack Surface Study" published March 2023 (commissioned by Intel), which evaluates Intel vPro devices powered by 13th gen Intel Core processors against four-year-old Intel-based PCs on Windows OS. Details at www.intel.com/performance-vpro. Results may vary.

[2] Source: CrowdStrike 2024 Global Threat Report

[3] Source: IBM Endpoint Security

[4] Source: Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

[5] Source: Gartner Magic Quadrant, 2022

[6] Source: Cobalt Strike Usage Explodes Among Cybercrooks. Threatpost

[7] Source: The Futurum Group, Endpoint Security Trends, 2023

[8] Source: Intel evolves security capabilities on each platform and brings new innovation and updates to existing features. Intel has the first and only hardware-based threat detection of its kind that works to augment security software for high efficacy detection of the latest ransomware, cryptojacking, supply chain style attacks and even zero-day attacks. Additionally, Intel works with the largest eco-system to enable silicon security features as part of a defense-in-depth strategy. Furthermore, Intel and Coalfire experts have completed an analysis of hardware security capabilities available on Intel vPro systems against industry security controls (NIST, MITRE, TCG) with 43 built-in MITRE ATT&CK countermeasures.

[9] Source: CrowdStrike AMS Blog-March 2022. Crowdstrike found Intel® Threat Detection Technology can boost scanning up to 7x, resulting in faster detection of fileless attacks that are the #1 attack entry method. Falcon testing of offload memory scanning to the integrated GPU compared to CPU scanning, as described in a recent CrowdStrike blog. Details at www.intel.com/performance-vpro. Results may vary.