

Silicon-Enabled Security for AI PCs



Enterprises face a surge of AI-driven risks at the endpoint—where sensitive data and new attack techniques now converge. Intel and CrowdStrike are addressing this shift by integrating silicon-level telemetry, hardware-assisted detection, and AI-native protection directly on AI PCs powered by Intel® Core™ Ultra processors.

This integration unifies silicon insights, on-device AI inspection, and the CrowdStrike Falcon® platform's cloud-native analytics into a coordinated enforcement layer at the device, enabling stronger detection, improved data protection, and hardware-rooted resilience across enterprise fleets.

Intel vPro® adds 20+ years of commercial security innovation with over 30 hardware security capabilities and out-of-band recovery services, while Falcon brings AI-powered threat prevention and industry-leading adversary intelligence. Together, they form a more secure, high-performance foundation for modern endpoint environments.

Customer Challenges

Enterprise security teams face a structural shift as AI is deployed directly on employee PCs. This concentration of compute, data, and risk at the endpoint exposes potential security gaps that can be addressed with purpose-built hardware-assisted security controls.

Modern Attack Techniques Evade Traditional Visibility

Attackers use fileless techniques, memory-resident malware, and exploit behaviors designed to bypass signature and behavior-based software detection methods. These techniques have become more prevalent and now account for roughly 79%¹ of all attacks. To help counter this trend, modern endpoint and extended (XDR) sensor solutions integrate silicon-level acceleration and hardware-accelerated memory scanning to detect threats that evade traditional software-only defenses.

AI Introduces New Data Egress Risk at the Endpoint

AI tools create new data-egress paths, while legacy rule-based DLP lacks contextual and semantic awareness, leading to false positives and more work for SecOps teams.

AI is uniquely suited to understanding language, context, and intent, and is critical for evaluating data movement across privacy policy infractions. Data security should operate where AI interactions occur—directly on the endpoint, where user privacy can be preserved.

Endpoint Resource Constraints Limit Security Effectiveness

As AI becomes embedded across enterprise and agentic workflows, endpoint compute requirements increase. AI PCs powered by Intel provide dedicated compute resources across CPU, GPU, and NPU architectures, enabling security inspection to scale without displacing core business workloads.

Operational Resilience Requires Hardware-Level Control

Remediation should function even when OS-level access is unavailable due to cyberattacks or outages. Security sensors have also become an indispensable asset that is present on commercial endpoints, which can also deliver recovery and manageability functions, reducing the number of sensors to manage on a device.

Without chip-level manageability and recovery, incident response remains constrained when systems are compromised. Endpoint resilience is no longer optional; it is critical for it to be integrated from the silicon foundation up into the software stack.

Solution & Features

Detection Foundation: CrowdStrike Falcon Sensor on AI PCs

The CrowdStrike Falcon platform running on AI PCs that are powered by Intel integrates silicon-level capabilities directly within its endpoint security solution. AI PCs

provide CPU telemetry and GPU-accelerated offload, using Intel® Threat Detection Technology (Intel® TDT). The Falcon platform integrates these capabilities through the sensor, strengthening endpoint telemetry that feeds into CrowdStrike Falcon® Insight XDR.

Key capabilities include:

- **Advanced Memory Scanning (AMS):** Uses Intel TDT to offload memory scanning to the GPU, targeting fileless and in-memory threats.
- **Hardware-Enhanced Exploit Detection (HEED):** Uses Intel CPU telemetry to find exploit behaviors such as Return-Oriented Programming (ROP) attacks, complementing AMS with full memory safety security controls.

These hardware-assisted detections align with 93 MITRE ATT&CK techniques² because of the combined Intel and CrowdStrike integration. CrowdStrike unifies these capabilities with its extensive detection arsenal to identify and confirm attacks at the moment of attempted execution.

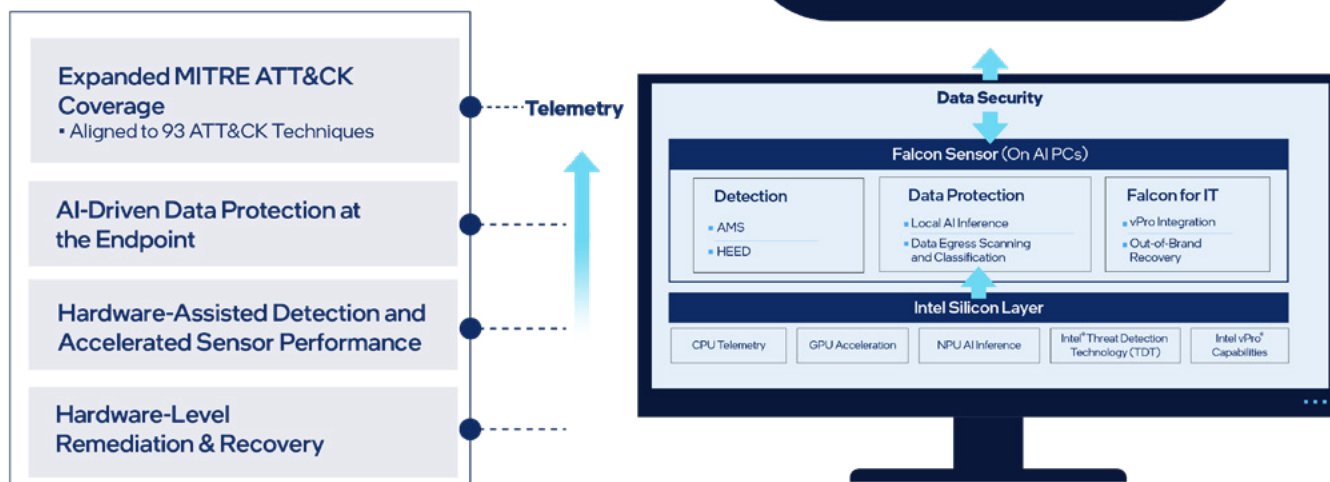
Resulting Benefits:

- Earlier detection of fileless and exploit-based attacks
- Stronger device-level signal fidelity
- Performance improvements through hardware acceleration
- Countermeasure to real-world MITRE ATT&CK threat tactics

Re-Architecting Endpoint Security with AI PCs + Falcon

Silicon-Level Telemetry

On-Device AI Enforcement | Falcon Platform Analytics



AI PCs Powered by Intel (Endpoint Hardware Foundation)

AI-Driven Data Protection: Falcon Data Security on AI PCs powered by Intel

CrowdStrike Falcon® Data Security uses AI-powered classification to identify sensitive and regulated data more accurately than static pattern matching—improving precision and reducing false positives. By using local AI inference across CPU, GPU, and NPU resources to perform semantic analysis directly on the device, security teams can identify sensitive information in free-form, unstructured content and apply protection at the point of egress across common endpoint workflows such as web-based uploads and GenAI interactions.

Resulting Benefits:

- More accurate protection than rules-based DLP
- Fast detection and response with on-device processing
- Improved privacy and regulatory compliance
- Minimized SecOps rules that work via autonomous AI detection

General availability is expected H2 2026.³

Enterprise-Grade Performance and Manageability: Falcon for IT + Intel vPro® Certification

Intel vPro® provides hardware-level manageability, out-of-band remediation, and chip-level recovery, enabling recovery even when OS-level access is unavailable. CrowdStrike Falcon® for IT integrates these capabilities directly into the Falcon sensor, which, in turn, can activate and provision PCs with Intel vPro for chip-level recovery. Additional commands and configuration can be made using the Intel + CrowdStrike Falcon® Foundry UI that is available in Falcon for IT tenants.

Falcon for IT integrates with Intel® Active Management Technology's KVM (Keyboard, Video, Mouse) feature and leverages Intel vPro® capabilities to strengthen operational resilience and enterprise confidence.

The CrowdStrike Falcon platform is optimized for Intel vPro® platforms to deliver comprehensive endpoint protection with dramatically lower system overhead—running lighter, faster, and without disrupting users. Security sensors are often criticized for degrading user experience, and IT teams must manage the cumulative impact of numerous tools across the fleet. In fact, Gartner reported in 2024 that the average enterprise runs more than 45 separate security solutions, underscoring why Intel vPro® C-certified applications are critical—validated Intel® CPU-optimized performance, stability, and low overhead at enterprise scale.

Resulting Benefits:

- Enables recovery from device outages
- Keeps security sensors performant for a seamless user experience
- Greater operational value from existing Intel vPro® fleets

Conclusion

AI is reshaping enterprise computing at the endpoint. Running the CrowdStrike Falcon platform on AI PCs that are powered by Intel strengthens detection, advances AI-driven data security, and reinforces operational performance.

This silicon-plus-software architecture positions the endpoint as a strategic enforcement layer, strengthening the security posture today while enabling confident AI adoption across the enterprise.



Contact your Connection Account Team for more information.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019
www.connection.com/Intel		



¹Source: [CrowdStrike 2025 Global Threat Report](#)

²Source: [One 93 count represents cumulative Intel vPro unique techniques/sub techniques for CrowdStrike Falcon as of January 4, 2025](#)

³Forward Looking Statement: This solution brief includes descriptions of products, features, and functionality not currently generally available. These references are provided for informational purposes only. The development, release, and timing of all features or functionality remain at our sole discretion and may change without notice. These statements are subject to risks, uncertainties, and assumptions that may cause actual results to differ materially from those expressed or implied. Customers should make purchasing decisions based only on services and features that are currently generally available. For more information on our existing offerings please talk to your CrowdStrike representative.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Performance varies by use, configuration, and other factors. Learn more at www.intel.com/PerformanceIndex.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software, or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

AI features may require software purchase, subscription, or enablement by a software or platform provider or may have specific configuration or compatibility requirements. Data latency, cost, and privacy advantages refer to non-cloud-based AI apps. Learn more at intel.com/AIPC.

All versions of the Intel vPro® platform require an eligible Intel processor, a supported operating system, Intel LAN and/or Intel WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance, and stability that define the platform. See intel.com/performance-vpro for details.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

3970521-0926