Refresh to the Latest Intel-Powered Copilot+ PCs and Help Secure Your Fleet

Ten ways Intel vPro® makes a huge difference for your enterprise cybersecurity.

When upgrading to Windows 11, enterprises need a comprehensive approach to device security with software and hardware working together. Strategically upgrading to Copilot+ PCs built on Intel vPro® with hardware-enabled security can deliver a huge leap forward for your fleet's endpoint protections to stay on top of evolving threats in the era of AI.

Here are 10 reasons why:

1 Enterprises can invest in robust security now or pay more for data breaches later.

New Windows 11 PCs show a 62 percent decrease in security incidents and a threefold reduction in firmware attacks.[1] Moreover, hardware-enabled security using Intel vPro can help reduce material security breaches by up to 23 percent.[2] These improvements can help enterprises avert disruptions and mitigate losses before they have a significant impact.

2 Cyber adversaries are using techniques that can hide from security software.

Intel® Threat Detection Technology (Intel® TDT), part of Intel vPro, can fingerprint malware as it attempts to execute on the CPU microarchitecture. This innovative approach detects up to 93 percent of ransomware attacks, bolstering endpoint detection and response (EDR) detection efficacy by 24 percent over software alone.[3]

3 Built-in hardware protections don't require additional setup or configuration.

Intel vPro supports advanced Windows 11 security right out of the box. Over 30 silicon-based security capabilities enable new Windows 11 features that protect the firmware, BIOS, and operating system (OS), helping contribute to the most-secure Windows ever.[4]

4 AI can help enhance security without compromising the user experience.

Copilot+ PCs with Intel® Core™ Ultra processors use three compute engines—a CPU, GPU, and an NPU designed for AI and machine learning—to efficiently balance AI workloads. Security software vendors are taking full advantage of AI on the PC. For example, BUFFERZONE enables data isolation for sensitive content, ESET leverages AI threat detection, and Proofpoint helps prevent data loss through exfiltration.[5]

5 The most impactful security features are those proven to combat real-world attacks.

Only Intel vPro has been mapped to 150 mitigations in the MITRE ATT&CK framework and 30 mitigations in the MITRE ATLAS framework. This hardware-level mapping empowers SecOps teams with more insights into how their PC fleets can be used to effectively identify and counteract specific attack behaviors.[6]

The extensive impact of a security breach

US$4.88M

Average cost of a security breach in 2024, up 10 percent from 2023.[7]

Over 100 days

Time to full recovery by over three quarters of organizations breached.[7]

intel vPRO

6 Security demands you consider how products are developed and supported.

Security starts in the silicon but also reflects investment in people, processes, and tools through the entire product life cycle. Not only does Intel's product security assurance rank number one in the industry,[8] but Intel also proactively addressed 96 percent of reported vulnerabilities in 2024—significantly higher than other silicon providers.[9]

7 Fast Wi-Fi can support productivity *and* security.

Copilot+ PCs with Intel vPro and Intel Core Ultra processors deliver the fastest, most-secure wireless technology available. Wi-Fi 7 is five times faster than Wi-Fi 6 and delivers up to 60 percent lower latency while supporting the latest network security protocols, such as WPA3, for better protection against network-based attacks.[10]

8 Remote manageability helps enterprises recover from security incidents fast.

Intel vPro with Intel® Active Management Technology (Intel® AMT) enables chip-level recovery from devastating cyberattacks or incidents like Blue Friday.[11] With these tools, enterprises can recover downed PCs using remote keyboard, video, mouse (KVM) to reimage and reset the device, even if the OS is compromised.

9 Silicon-enabled security helps ease compliance in regulated industries.

Silicon-enabled trust helps Intel vPro satisfy key regulatory requirements in federal and public sectors, including the National Institute of Standards and Technology (NIST), Trusted Computing Group (TCG), Federated Identity Management (FIM), and Resource Identification Management (RIM) frameworks.

10 Every employee needs comprehensive protection to help keep your whole enterprise secure.

Copilot+ PCs with Intel vPro exceed Microsoft's Level 3 standard for secured-core PCs,[12] delivering the highest level of Windows 11 security and including advanced firmware protection and dynamic root of trust measurement. Copilot+ PCs built on Intel vPro provide a hardware foundation for security that helps address entire classes of vulnerabilities that cannot be addressed by software alone.

Refresh to Intel-powered Copilot+ PCs

Run the most-secure Windows ever[4] on the latest Intel® hardware to activate a defense-in-depth strategy while boosting productivity with AI. Start planning your next refresh with Copilot+ PCs built on Intel vPro today.

Learn more about Intel-powered Copilot+ PCs, visit

intel.com/businessAIPC

intel vPRO

Notices and disclaimers

1. Windows 11 Survey Report, Techaisle, September 2024. Windows 11 results are in comparison with Windows 10 devices. See learn.microsoft.com/en-us/windows/security/book/ for details.
2. Source: Forrester Consulting. "The Total Economic Impact™ of the Intel vPro® Platform." Commissioned by Intel. January 2024, intel.com/content/www/us/en/business/enterprise-computers/resources/vpro-platform-tei-case-study.html.
3. "SE Labs Intelligence-Led Testing: Enterprise Advanced Security (Ransomware)," SE Labs, February 2023, selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/.
4. As of December 2024. See cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-product-and-services/windows/windows-11/ai/MSFT_Windows_11_Pro_Security_Research_Report-EN-US.pdf for details. Results may vary.
5. Explore security and manageability use cases at intel.com/content/www/us/en/products/docs/processors/core-ultra/ai-pc-resources.html - introtext. Results may vary.
6. Todd Cramer, "Intel AI PCs Deliver an Industry Validated Defense vs Real World Attacks," Intel Community, January 5, 2025, community.intel.com/t5/Blogs/Tech-Innovation/Artificial-Intelligence-AI/Intel-AI-PCs-Deliver-an-Industry-Validated-Defense-vs-Real-World/post/1650954.
7. "Cost of a Data Breach Report 2024," IBM, accessed April 2025, ibm.com/reports/data-breach.
8. Andrew Cavalier, Jake Saunders, "Embracing Security as a Core Component of the Tech You Buy," ABI Research, February 2024, intel.com/content/www/us/en/security/security-as-a-component-of-tech.html.
9. "2024 Intel Product Security Report," Intel, February 2025, intel.com/content/www/us/en/content-details/846149/2024-intel-product-security-report.html.
10. See intel.com/performanceindex for all claim workload and configuration details. Results may vary.
11. "No More Blue Screens: Resolving Issues Like CrowdStrike update with inefi Spotlight and Intel vPro," inefi, August 2024, inefi.com/post/no-more-blue-screens-how-intel-vpro-and-inefi-spotlight-fix-crowdstrike-issues.
12. "Windows 11 Security Starts with an Intel Hardware Foundation," Intel, accessed April 21, 2025, https://www.intel.com/content/www/us/en/content-details/848494/windows-11-security-starts-with-an-intel-hardware-foundation.html?DocID=848494.

Performance varies by use, configuration, and other factors. Learn more at intel.com/performanceindex. Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure. Intel® technologies may require enabled hardware, software, or service activation.

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 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.

No product or component can be absolutely secure. Your costs and results may vary. Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

0425/MC/CMD/PDF