

# HP + AMD: Redefining resilience from the inside out

Innovation is accelerating and new work models are emerging: 69% of IT leaders are prioritizing digital transformation and AI over cybersecurity and cloud and data management in the next year.[1] With enormous attacks having increased 76% since the launch of ChatGPT,[2] legacy infrastructure simply can't keep up. That's where AI brings incredible opportunities—especially when paired with resilient security strategies.

But in the rush to redefine business, how do you ensure enterprise-grade security at every layer?

HP + AMD AI PCs come with the hardware-enforced, multi-layer protection of HP Wolf Security for Business, coupled with the industry-leading security features of AMD Ryzen™ PRO processors–keeping IT leaders a step ahead of evolving threats, without sacrificing performance or productivity.

**AMD Secure Processor**
Validates code before it is executed

**AMD Shadow Stack**
Protects against control-flow attacks

**AMD Platform Secure Boot**
Continues the chain of trust from the system BIOS to the OS



## Built to withstand a new era of risk

The rules of cybersecurity have changed, and upgrading PC fleets is non-negotiable. As part of the world's most secure portfolio, AMD advanced HP devices like the EliteBook X G1a Notebook come equipped with enterprise-grade protections, such as HP Wolf Security and the built-in security features of AMD Ryzen™ PRO processors. These systems are designed to detect and defend against evolving threats in real time, empowering IT to lead transformation with confidence, not compromise.

**AI protection built-in, not bolted on**
Integrated HP Wolf Security[3] and built-in security features of AMD Ryzen™ PRO processors deliver world-leading security–even for quantum hacks.

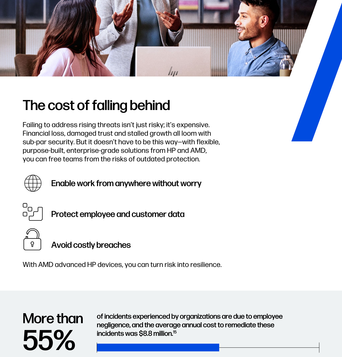
**The world's most advanced on-device AI assistant**
HP AI Companion minimizes reliance on the cloud, empowering you to analyze sensitive files, query on the go and seamlessly call with the intelligence of AI, right on your device.[4]

**Proven performance and speed**
HP + AMD AI PCs deliver up to 167% faster AI inferencing and better efficiency per watt-hour than leading competitors, with CrowdStrike reporting 7x faster memory scanning on most AI PCs than traditional computers.[5]

Equipped with features that are redefining enterprise security, AMD advanced HP PCs offer world-leading security, industry-first innovations and extreme performance–all with fleet-ready, plug-and-play simplicity.



**77%** of employees now use AI tools[6]—make sure they're using ones you can trust



## Everywhere protection for anywhere work

With 72% of organizations adopting hybrid models, endpoint protection has never been more critical.[7] Multiple networks and unmanaged devices create vulnerabilities hackers love to exploit, and 40% of organizations have reported cyber intrusions directed at their remote environments.[8]

HP + AMD AI PCs deliver hardware-enforced, multi-layered protection that locks out hackers while enabling unstoppable productivity.



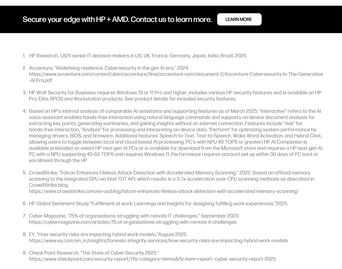
**44%**
surge in cyberattacks on organizations worldwide in 2024[9]

**True Zero-Trust coverage**
With 5GB+ web clicks, downloads and attachments protected to date without a single compromise, HP Wolf Security's[10] Threat Containment sets the Zero-Trust standard.[11]

**Full IT visibility and control**
With HP Protect and Trace with Wolf Connect, misplaced, stolen and turned-off devices can be found, locked or erased remotely, protecting sensitive data.[12]

**Detect, contain and neutralize**
HP Sure Click Enterprise[13] uses hardware-enforced isolation to contain threats and malware–without disrupting workflows. It provides stronger endpoint protection with over 150 million HP PCs shipped with no reported persistent firmware breaches.[14]

Because, in a world where work happens everywhere, endpoint security is everything.



## The cost of falling behind

Failing to address rising threats isn't just risky; it's expensive. Financial loss, damaged trust and stalled growth all loom with sub-par security. But it doesn't have to be this way–with flexible, purpose-built, enterprise-grade solutions from HP and AMD, you can free teams from the risks of outdated protection.

- Enable work from anywhere without worry
- Protect employee and customer data
- Avoid costly breaches

With AMD advanced HP devices, you can turn risk into resilience.

**More than 55%** of incidents experienced by organizations are due to employee negligence, and the average annual cost to remediate these incidents was $8.8 million.[15]

## HP + AMD: Rethink risk. Reclaim confidence

The cybersecurity landscape grows tougher everyday, but so do the solutions. AMD advanced HP devices empower your teams with the innovative, high-performing and secure technology that evolves with their needs, so you can stay prepared for what's next. Because when you unlock the power within, you can reimagine the future of work.

**Secure your edge with HP + AMD. Contact us to learn more.** LEARN MORE

1. HP Research, 1,825 senior IT decision-makers in US, UK, France, Germany, Japan, India, Brazil, 2025.
2. Accenture, "Redefining resilience: Cybersecurity in the gen AI era," 2024. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Cybersecurity-In-The-Generative-AI-Era.pdf
3. HP Wolf Security for Business requires Windows 10 or 11 Pro and higher. Includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.
4. Based on HP's internal analysis of comparable AI assistants and supporting features as of March 2025. "Interactive" refers to the AI voice assistant enables hands-free interaction using natural language commands and supports on-device document analysis for extracting key points, generating summaries, and gaining insights without an internet connection. Features include "Ask" for hands-free interaction, "Analyze" for processing and interpreting on-device data. "Perform" for optimizing system performance by managing drivers, BIOS, and firmware. Additional features: Speech-to-Text, Text-to-Speech, Wake Word Activation, and Hybrid Chat, requiring internet connectivity. Requires Windows 11 and compatible HP PCs with a dedicated NPU. Feature availability and performance may vary by device and software version. Currently available preloaded on select HP next gen AI PCs or is available for download from the Microsoft store on select Snapdragon X HP next gen AI PC with a NPU supporting 40-60 TOPS and requires Windows 11. Performance requires internet set up within 30 days of PC boot or enrollment through the HP
5. CrowdStrike, "Falcon Enhances Fileless Attack Detection with Accelerated Memory Scanning," 2022. Based on offload-memory scanning to the integrated GPU via Intel TDT API, which results in a 3-7x acceleration over CPU scanning methods as described in CrowdStrike blog. https://www.crowdstrike.com/en-us/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/
6. HP Global Sentiment Study "Fulfillment at work: Learnings and insights for designing fulfilling work experiences," 2025.
7. Cyber Magazine, "75% of organizations struggling with remote IT challenges," September 2023. https://cybermagazine.com/articles/75-of-organisations-struggling-with-remote-it-challenges
8. EY, "How security risks are impacting hybrid work models," August 2020. https://www.ey.com/en_in/insights/forensic-integrity-services/how-security-risks-are-impacting-hybrid-work-models
9. Check Point Research, "The State of Cyber Security 2025," https://www.checkpoint.com/security-report/?ltp.category=trends&ltp.item=report-cyber-security-report-2025
10. HP Wolf Security for Business requires Windows 10 or 11 Pro and higher. Includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.
11. Assumptions based on HP internal analysis of customer reported insights and installed base.
12. HP Wolf Protect and Trace is available on select HP 600, 800, 1000, 1040, Windows based Elite Dragonfly Laptops, select 800 desktops, and 27-G8 Workstations and will function when the device is powered on and connected to the Internet. HP Wolf Protect & Trace requires HP TechPulse to be installed by customer manually via a one-click download of hp.com/premium plus or by providing consent at the time of your hardware's first boot, which enables HP to install HP TechPulse to collect information related to the Device. HP TechPulse is a telemetry and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP TechPulse follows stringent GDPR privacy regulations and is ISO27001, ISO27701, ISO27017 and SOC2 Type2 certified for Information Security. Internet access with connection to TechPulse portal is required. For full system requirements, please visit http://www.hpdaas.com/requirements.
13. HP Sure Click Enterprise is sold separately. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. For full system requirements, please visit HP next-gen hyperlink to HP Sure Access Enterprise and HP Sure Click Enterprise system requirements at: https://enterprisesecurity.hp.com/s/article/System-Requirements-for-HP-Sure-Access-Enterprise
14. Based on HP's internal analysis. Over 150 million PCs shipped with HP Sure Start and no malware breaches reported.
15. Ponemon Institute, Cost of Insider Risks: Global Report 2025, https://www2.diresystems.com/c/4634212025-DI-19/583cou/464342/1749000001DNNhQ&mx/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf?_gl=1*1w18ow*_gcl_au*ODk3MzUwMDI0LjE3NDUxMTUxNjM.

© Copyright 2025 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.