HP WOLF SECURITY

3 ways AI is raising the stakes around endpoint security

AI has made endpoint security even more challenging by accelerating attacks, raising the value of information at the endpoint, and making seemingly benign data highly sensitive.

01 AI is supercharging attacks

Generative AI is accelerating the volume and sophistication of attacks, allowing bad actors to evade traditional defenses. According to TechTarget,[1] large language models (LLMs)—AI systems that can understand and generate human language—are being used to make phishing emails more believable and urgent.

02 AI is making endpoints prime targets

Companies are embracing PC-based AI. But while this approach can improve speed, privacy, and user experience, it also significantly increases the value of data. This makes endpoints an even more attractive target for bad actors, especially because endpoints are more mobile than ever, which has amplified their exposure and made them more difficult to protect.

AI PCs will account for 22% of all PCs in 2024[2]

03

AI is triggering unprecedented threats to privacy

AI-powered inference attacks can potentially expose the decision-making process of your AI model and manipulate its outputs for malicious purposes, ultimately rendering your own AI systems untrustworthy. By piecing together more trivial data at a low-security level, these attacks can infer information at a higher security level, like health records or private information about individuals, with frightening accuracy.

75% of security professionals have seen an uptick in cybercrime in the past year, and 85% attribute this rise to the weaponization of AI[3]

Protection against the unexpected

HP Wolf Security[4] uses full-stack security to fortify your device's defenses from hardware to cloud. This vigorous approach includes threat containment technology, which isolates and contains both AI and non-AI threats before they can infect endpoints. The result is always-on protection against all types of attacks.

Trust that your workforce can work anywhere without worry, knowing HP has the industry's broadest portfolio of AI PCs[5] and an unwavering dedication to protecting you and your organization.

LEARN MORE AT HP.COM →

HP WOLF SECURITY

[1] Tech Target, "Generative AI is making phishing attacks more dangerous," December 18, 2023, https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

[2] ITPro, "AI PCs are set to surge in popularity in 2024, but vendors might find it hard to differentiate offerings," February 7, 2024, https://www.itpro.com/hardware/ai-pcs-are-set-to-surge-in-popularity-in-2024-but-vendors-might-find-it-hard-to-differentiate-offerings

[3] Gallagher, "AI: Keeping Pace With the Cybercriminals," November 2023, https://www.ajg.com/insights/ai-keeping-pace-with-the-cybercriminals/

[4] 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.

[5] Based on Intel and AMD based AI PCs with NPUs as of 3/7/2024

April 2024