What safeguards users, devices, and data in the AI era?

See why isolation technology is crucial in the changing environment

hp / AMD

Attacks have evolved—and HP Z is prepared

Even though AI advancements help optimize our daily work, they also improve opportunities for threat actors. Fortunately, HP Z AI workstations offer hardware-enforced threat containment security through Sure Click Enterprise[1] and Wolf Pro Security.[2]

93%

of security leaders anticipate daily AI attacks by 2025[3]

AI is supercharging attacks

Bad actors are using AI to make attacks (like phishing and spear phishing) more credible and harder to spot. This will make traditional security defenses too little too late and means that workstation users—whose endpoints can make particularly attractive targets, since they work with sensitive data and information—can't be expected to catch AI-powered attacks.

75% of security professionals witnessed an increase in attacks over the past 12 months, with **85%** attributing this rise to bad actors using generative AI.[4]

Factors steer endpoint protection toward isolation security

To reduce the attack surface and create a more secure experience, the focus will need to shift away from existing approaches and toward the zero-trust defenses available in HP Z Workstations.

"The traditional methods of securing data are no longer sufficient as cybercriminals constantly evolve their tactics to exploit vulnerabilities in security systems."

American Journal of Computer Architecture[5]

Why HP's threat isolation technology works

HP Z Workstations support threat isolation technology, which defeats phishing attacks, including those using AI, to stop ransomware in its tracks. This approach protects power users no matter what the attack vector (corporate or personal email, browsing, or USB drives), even if the device isn't on the internet. And it does so in ways that are scalable and unobtrusive to users.

Threat containment:

- Micro-virtual machines (μVM) securely open many commonly used file types (e.g., Microsoft Word, PDF, and HTML files) in a secure, hardwareenforced "sandbox" to effectively contain malware before it can infect the PC. Plus, when the task is completed, the μVM is deleted, taking the malware with it.
- Introspection identifies unseen attack types and provides a clear look at the malware behavior.
- Analytics and reporting surface insights into the techniques, tactics, and processes of the attack to provide security teams with updated threat intelligence.

Deliver secure remote access

HP Anyware lets power users access their HP Z workstations from any location securely without bandwidth bottlenecks.

Secure your endpoints for the AI era

Take threat management to the next level with HP Z Workstations & Solutions and AMD. Our threat containment strategy combines unique CPU-enforced isolation technology with hardware-enforced security solutions like HP Wolf Pro Security or HP Sure Click Enterprise. Learn more about the isolation security offerings from HP Wolf Security and find the one that fits your business needs.

Explore HP Z Workstations & Solutions

LEARN MORE

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

1. 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 System Requirements for HP Sure Click Enterprise for details.
2. 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, Workstation, and RPOS products. See product details for included security features.
3. NETACEA, "Cyber Security in the Age of Offensive AI," April 24, 2024, https://netacea.com/reports/cyber-security-in-the-age-of-offensive-ai.
4. Security Magazine, "Study finds increase in cybersecurity attacks fueled by generative AI," August 29, 2023, https://www.securitymagazine.com/articles/99832-study-finds-increase-incybersecurity-attacks-fueled-by-generative-ai.
5. American Journal of Computer Architecture, "Cybersecurity in the AI Era: Ensuring Your Data Stays Protected," April 27, 2023, http://article.sapub.org/10.5923.j.ajca.20231001.02.html.

/ AMD