Enterprise Strategy Group

Securing Business PCs From BIOS to Browser

PCs and laptops present customers with an array of choices and capabilities. Some systems maximize performance, while others emphasize value and an affordable price. Even as AI reshapes the entire business landscape, the critical elements of endpoint devices often boil down to the same things they always have: security, performance, and reliability.

Endpoint Security Is Becoming More Complex

Security threats are constantly evolving, and corporate PCs often represent the biggest wildcard. With employees working from anywhere and relying on multiple devices, organizational attack surfaces continue to expand. Phishing attempts are getting smarter, while vulnerability management and patching are harder to stay ahead of. It's no surprise, then, that 42% of organizations said endpoint security has grown more challenging over the past two years. There's just more to watch, more to protect, and more ways for things to slip through.

42%
of organizations find endpoint security **more difficult now than two years ago.**

40%
More complicated threat landscape

36%
Increased number of managed devices

31%
Increased number of endpoint vulnerabilities

Customers Prioritize Security Above Performance, Reliability, and Even AI

For these reasons and more, security remains the top consideration when organizations evaluate new endpoint devices—even with all the attention on AI. Performance, reliability, and cost follow closely, while dedicated AI hardware ranks much lower. **This means the foundational requirements for endpoint devices haven't changed.** Before endpoint devices can support advanced use cases, they must provide foundational safeguards to protect against complex and rapidly evolving threats. Only after these risks are addressed do features such as dedicated AI engines—or even price—begin to influence buying decisions.

58%
Security

49%
Performance

45%
Reliability

37%
Price

19%
Dedicated NPU for AI workloads

18%
Dedicated GPU for AI workloads

AMD Enables Secure Business PCs

AMD Ryzen PRO and Ryzen AI PRO processors include on-chip defensive capabilities that help organizations meet the demands of an increasingly complex security landscape. These include:

AMD Secure Processor

A dedicated security processor that validates code before it is executed, establishing a hardware-based root of trust and providing a secure boot process.

AMD Shadow Stack

Protects against control-flow attacks by maintaining a hardware-based copy of the return address stack, ensuring control-flow integrity.

AMD Platform Secure Boot[1]

Protects the security of system firmware and, coupled with AMD Secure Processor, maintains the chain of trust from hardware, to firmware, to the OS bootloader, and into the OS itself.

Microsoft Pluton Security Processor[2]

A next-generation, TPM 2.0 module that enables Windows 11 and enhanced Microsoft security features such as Windows Hello and Bitlocker.

AMD Memory Guard[3]

AMD Memory Guard – Real-time, full memory encryption aligned with Microsoft's Secured-core PCs requirements, which leverage virtualization-based security and hardware-enforced stack protection.

Conclusion

For business-class PCs, security isn't an optional add-on. It's a foundational requirement and a critical part of any endpoint strategy. AMD Ryzen™ PRO processors deliver that foundation, with hardware-based protections that help safeguard data, preserve system integrity, and support modern security frameworks like Secured-core PCs.

The PC remains one of the most important tools for getting work done. Ensuring these devices are both high-performing and protected is more important than ever—and with a platform built to support future workloads, including AI, AMD is ready to meet that need.

LEARN MORE

AMD
together we advance_

[1] GD-72: The AMD Secure Processor is a dedicated on-chip security processor integrated within each system-on-a-chip (SoC) and ASIC (Application Specific Integrated Circuit) designed by AMD. It enables secure boot with root of trust anchored in hardware, initializes the SoC through a secure boot flow, and establishes an isolated Trusted Execution Environment. GD-72.
[2] GD-202: Microsoft Pluton is a technology owned by Microsoft and licensed to AMD. Microsoft Pluton is a registered trademark of Microsoft Corporation in the United States and/or other countries. Learn more at https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/. Microsoft Pluton security processor requires OEM enablement. Check with the OEM before purchase. AMD has not verified the third-party claim. GD-202.
[3] GD-206: Full system memory encryption with AMD Memory Guard is included in AMD Ryzen PRO, AMD Ryzen Threadripper PRO, and AMD Athlon PRO processors. Requires OEM enablement. Check with the system manufacturer prior to purchase. GD-206

Source: Enterprise Strategy Group Research Report, *The Growing Role of AI in Endpoint Management and Security Convergence*, June 2025.
Source: Enterprise Strategy Group Complete Survey Results, *AI at the Endpoint: Tracking the Impact of AI on End Users and Endpoints*, April 2025