TechTarget | Custom Media
White Paper

SUPPORTING STRONG CYBERSECURITY HEALTH FOR NEXT-GENERATION PCs

Personal computers used to be an easy target for hackers, and cyberattacks on PCs accounted for considerable negative financial, operational, and regulatory impact. But today's and tomorrow's PCs benefit from substantial improvements in how they are protected, both in terms of best practices for cybersecurity hygiene and in how PCs—and their core component—are engineered.

AMD
together we advance_

Introduction: The state of cybersecurity for personal computers is...complicated.

On one hand, the use of PCs as an essential part of vast, interconnected, global networks has made them a critical point of entry for hackers, ranging from sophisticated cybercrime gangs and rogue nation states to malicious insiders. The harsh reality is that endpoints—of which PCs make up the vast majority—are a common cybersecurity target used to infiltrate applications and databases, and to navigate laterally throughout networks.

The good news, however, is that organizations now are keenly aware that PCs and other endpoints represent a critical attack vector, and have taken important steps to fortify their cybersecurity defenses across their broad landscape of PCs. Nearly half—44%—of organizations say fortifying cybersecurity is a top business priority driving their endpoint device strategy, according to TechTarget's Enterprise Strategy Group.[1] And, for organizations buying high-end PCs with "premium pricing," security is the No. 1 purchase driver for those purchases.[2]

Many of these steps constitute a growing use of best practices to protect PCs, such as improved user awareness and training on everything from avoiding suspicious hyperlinks and attachments to paying closer attention to password policies.

1 Source: Enterprise Strategy Group Research Report, Endpoint Device Trends: Evaluating a Shifting Desktop and Laptop Procurement, Management, OS, Feature, Application, and Spending Landscape, February 2024.

2 Ibid.

However, another essential step focuses on key technology advances underpinning the PC itself. Certainly, there are valuable and reliable security tools such as endpoint detection and response, encryption, data protection solutions, and more. But critical technical advancements also are being implemented on the PC itself—especially at the CPU level.

Today and in the future, the CPU is more than just the facilitator of everything from compute performance to energy management; it also is a chip-level security operations center where threats are prevented, detected, locked down, and mitigated.

What Makes a PC Vulnerable to Cyberattacks

Whether you call it PC security, as cybersecurity professionals often do, or endpoint security, organizations need to understand that personal systems are typically the preferred point of attack for attempted data breaches, ransomware, identify theft, and other hacks. Importantly, these PC-enabled attacks are often used to take down an organization's most valuable and essential systems, such as critical infrastructure, mission-critical applications, intellectual property, or personally identifiable information.

For years, PCs have been under protected against cyberattacks, too often relying on simplistic antivirus/antimalware tools. Those have proven to be wholly inadequate against increasingly sophisticated attacks and attackers, often utilizing innovative artificial intelligence tools and machine learning algorithms.

Additionally, the now-cemented trend of remote/hybrid work has further exposed PCs as a critical vulnerability, since many of those PCs are either under protected from a cybersecurity perspective, are linking to potentially vulnerable consumer-grade cloud services, or lack sufficient security support resources in real time.

Another critical cause of concern for cybersecurity professionals and IT teams is the large—and still growing—cybersecurity skills gap, putting enormous pressure on organizations to find new, innovative, and efficient ways to improve PC security. For instance, one estimate projects the cybersecurity skills gap will grow to a staggering 3.5 million positions by 2025.[3] Why is this still a problem, years after it was first identified? Research conducted by Enterprise Strategy Group and Information Systems Security Association points out that 66% of security professionals feel that working in their field has gotten harder in the last two years, while a sizeable 27% of professionals mentioned their jobs now have a high level of difficulty.[4]

With so many business professionals now working remotely at least part of their time, and with the growing number and variety of vulnerabilities targeting PCs and other endpoints, organizations are scrambling to come up with new ways to improve PC cybersecurity.

How PC CPUs Make a Difference in Cybersecurity

There are a number of ways organizations can strive to help improve the security of their users' PCs. Many of them are expensive, both in terms of capital expenditures and finding more personnel to handle things such as monitoring, management, training, and education.

Automation has helped transform many of those manual security tasks into integral parts of security processes and procedures without unduly burdening existing staff and budgets. Artificial intelligence also has helped in some areas such as threat intelligence, threat hunting, and device behavior analytics.

However, one key source of improved PC security is the PC itself. Specifically, today's PCs not only include such tools as antivirus software and data backup software

integrated at the factory, but now use components that help improve the PC's cybersecurity defenses.

For instance, many recent PCs have been engineered with CPUs, GPUs, accelerators, and storage devices that include security features that improve privacy and defense against cyberattacks. Hardware-centric approaches help by locking down private and sensitive data on a number of levels, including firmware, silicon, and operating systems.

Certain processors have been designed to act as a hardware "root of trust" when the PC leaves the factory, delivering system-level integrity by using firmware authentication upon start-up.

Other features that help provide a more secure PC environment include:

- Secure boot.
- Biometric authentication.
- Encryption.
- Support for key operating system features, including:
  - Integrated anti-malware.
  - Automatic updates.
  - Device guard.
  - Remote wipe.

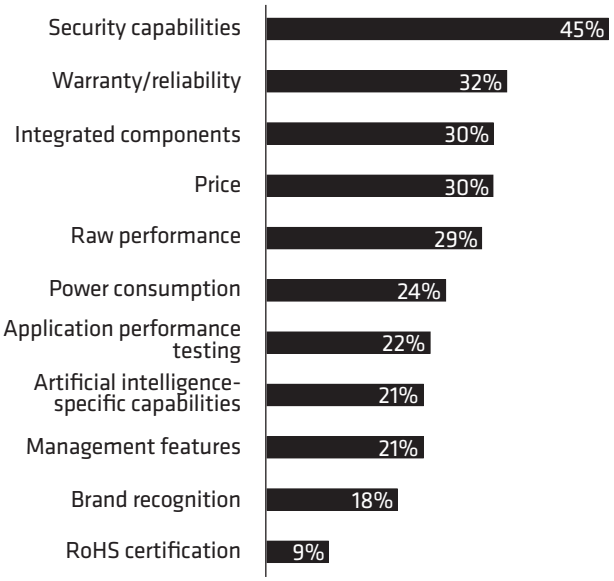
3 Source: TechTarget, "Cybersecurity Skills Gap: Why it Exists and How to Address it", January 2024.

4 Ibid.

One approach AMD has taken is to adopt a layered approach to PC security, where hardware and software are aligned to protect data at multiple levels.

Does designing security-related features into CPUs, GPUs, and other PC components make a difference? Yes, according to research from Enterprise Strategy Group. Organizations obviously want high performance, reliability, and tight integration when they evaluate CPU vendors. But organizations tell Enterprise Strategy Group that security capabilities are—far and away—their top criterion when choosing a preferred CPU vendor. In fact, nearly half—45%—of respondents indicated that security capabilities are their top priority in a CPU vendor.[5]

What are the top criteria for your organization when choosing its preferred CPU vendor? (Percent of respondents, N=354, three responses accepted)



5 Source: Enterprise Strategy Group Research Report, Endpoint Device Trends: Evaluating a Shifting Desktop and Laptop Procurement, Management, OS, Feature, Application, and Spending Landscape, February 2024.

How AMD Solutions Help Address PC Security Needs

One company devoting substantial resources to helping improve PC security for their partners and customers is AMD. As a well-established leader in microprocessors, accelerators, and other PC components, AMD has a unique perspective on ways to help improve PC security.

One approach AMD has taken is to adopt a layered approach to PC security, where hardware and software are aligned to protect data at multiple levels. For instance, AMD has teamed with Microsoft and OEMs to implement layered PC defenses with AMD Ryzen™ processors, helping to improve security from the endpoint and the edge to the cloud.

AMD Ryzen™ processors are integrated with Microsoft Pluton™ security processors to help address security concerns wherever the PCs are utilized, especially for hybrid/remote work use cases. This approach includes communication for user authentication at the chip level, instead of over the communications bus to the operating system, thus shrinking the attack vector. It also uses full system encryption for improved data protection.

Finally, AMD Ryzen™ PRO processors include such security features as:

- AMD Secure Processor, a security co-processor.
- AMD Memory Guard, which enables comprehensive system memory encryption.
- AMD Shadow Stack, a hardware-based security feature delivering control-flow protecting to help prevent malware from redirecting command flows.

Conclusion

For IT organizations and security professionals, the sometimes-harsh reality is that battling cybersecurity attacks is more challenging and carries greater potential negative impact than ever. It's also important to keep in mind that the PC is often the first point of attack for hackers, especially in this era of widespread remote work. Users' PCs may be under protected, often lacking adequate security tools and don't always adhere to recommended best practices to defend applications, data, devices, and user identities.

However, there's a silver lining: Cybersecurity now is a strategic item for all organizations, including for their C-suite executives and board members. That means that more resources are made available to secure devices, and IT professionals, security teams, and end users are far better trained and more educated on ways to harden their PC defenses.

Another positive is the important advances made by PC companies and their technology partners in building in features and capabilities that help make those client systems more prepared against cyberthreats. In particular, leading technology component companies such as AMD have made security a strong priority, designing many features into their processors and accelerators to help provide stronger PC security.

FOR MORE INFORMATION ON HOW AMD SOLUTIONS HELP ORGANIZATIONS IMPROVE THEIR PC CYBERSECURITY POSTURE, PLEASE VISIT HTTPS://WWW.AMD.COM/EN/TECHNOLOGIES/PRO-TECHNOLOGIES.

This content was commissioned by AMD, and produced by TechTarget Inc.