How Next-Gen CPUs Enable IT Security

The benefits of the decentralized and diversified approach to IT are clear. Untethered from physical locations and monolithic architectures, organizations and individuals can embrace innovation and work with greater speed and productivity than ever.

The bulk of data will be created and processed outside of a traditional centralised data center and within clouds in the future. While the benefits are significant, there are new risks that this introduces that should keep CIOs up at night: ransomware attacks targeting edge network servers and attacks against endpoint devices are two of the biggest security challenges facing organizations today.

CIOs – and all other leaders within organizations – need to be confident that their remote and edge deployments are resistant against these types of attacks.

Security is about the stack

Security resilience within the modern IT environment relies on having full-stack approach, where data, software, and hardware all have access to layers of security.

AMD PRO security plays a critical role in this, at several levels of the stack:

- AMD “Zen” Architecture, through which AMD Ryzen™ PRO processors are designed from the ground up with security features as the priority to help reduce exposure to sophisticated attacks.
- AMD Secure Processor[1], which validates code before it is executed to help ensure data and application integrity. It helps protect systems and data from unauthorized software and applications running on the device.
- AMD Memory Guard[2], which provides real-time, full-system memory encryption. This helps protect devices that have been lost or stolen (an ever-present risk with remote technology) from data vulnerability.
- AMD Shadow Stack, which helps protect environments against control-flow attacks by checking the normal program stack against a copy stored in hardware.
- AMD Platform Secure Boot[3], which helps defend against threats to the firmware by establishing an unbroken line of trust from the AMD silicon root of trust to the BIOS.

Combined, these security features help AMD provide more secure experiences to users, regardless of their devices and locations.

AMD further leads the security conversation by partnering with other vendors that are critical in enabling the full-stack approach to security. For example, in 2020, AMD collaborated with Microsoft to help create the Microsoft Pluton security processor[4]. Microsoft Pluton is a chip-to-cloud security technology that is integrated directly into the CPU of a Windows 11 PC. It is

designed to provide hardware-based protection for critical system components, such as encryption keys, boot processes, and other security-sensitive operations.

Integrating Microsoft Pluton directly into the CPU eliminates the need for a separate, potentially more vulnerable Trusted Platform Module to store keys and system data, thereby enhancing the security capabilities of Windows PCs. By working closely with partners like AMD, Microsoft has been able to create a more streamlined and protected platform for Windows devices.

Security at a cloud level

Beyond the devices, CIOs also need to grapple with security resilience at the data center and cloud level. Decentralised IT means that employees need to be able to access applications and data remotely (and thus leverage the cloud), but this provides another attack vector for cyber criminals.

One thing that can help secure these environments are AMD CPUs, such as the AMD EPYC™ processors, that have integrated advanced security technologies like AMD Infinity Guard[5], Secure Encrypted Virtualization, and Secure Memory Encryption.

These hardware-level security features at the data center can help provide a strong foundation for protecting data and workloads in the cloud, offering IT decision makers more security resiliency in their cloud deployments.

A good example of this technology in action is MonetaGo, a company that provides financial institutions with the ability to combat fraud schemes like duplicate financing, while protecting customer and company data.

Core to the company's ability to deliver this is Secure Finance, a platform that enables banks to share sensitive lending data with MonetaGo, which then authenticates the information and flags anything that appears to be a duplicate, while maintaining data privacy across the entire process.

This wasn't technically possible until recent years, but AMD Secure Encryption Virtualization on AMD EPYC CPUs allowed Google to launch Google Cloud Confidential Computing solution, enabling the full scope of MonetaGo's vision with comprehensive security.

Another example of the power and security offered through AMD EPYC processors is Let's Encrypt, by the Internet Security Research Group (ISRG). The company is the largest Internet security certificate authority in the world, and due to the extreme nature of the security that it needs within its own systems, it has challenging limitations on how it can deliver its servers.

The company can't use the cloud or standard data center rooms. Instead, it needs special high security rooms, with their own walls, built inside data centers with biometric access. The company made the decision recently to phase out its prior servers to instead replace them with AMD EPYC systems, which were also selected because they were "significantly" more powerful, and capable of helping the company to serve 230 million websites.

Security for a cloud and distributed world

While the risks of decentralized IT are only going to accelerate, as cyber criminals continue to identify devices and computing environments outside of the core network as a less secure

environment, it's also not an opportunity that organizations can ignore. Thankfully, there are hardware and software solutions to help protect edge environments. It just requires the IT team to architect the security environment with decentralization in mind.

For more information on hardware-level security and the AMD solutions that are enabling it, click here.

---

[1] 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] 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.

[3] An OEM who has enabled the AMD Platform Secure Boot feature grants permission for their cryptographically signed BIOS code to run only on their platforms using an AMD Platform Secure Boot enabled motherboard. One-time-programmable fuses in the processor bind the processor to the OEM's firmware code signing key. From that point on, that processor can only be used with motherboards that use the same code signing key. GD-192.

[4] 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.

[5] AMD Infinity Guard features vary by EPYC™ Processor generations. Infinity Guard security features must be enabled by server OEMs and/or Cloud Service Providers to operate. Check with your OEM or provider to confirm support of these features. Learn more about Infinity Guard at https://www.amd.com/en/technologies/infinity-guard. GD-183.