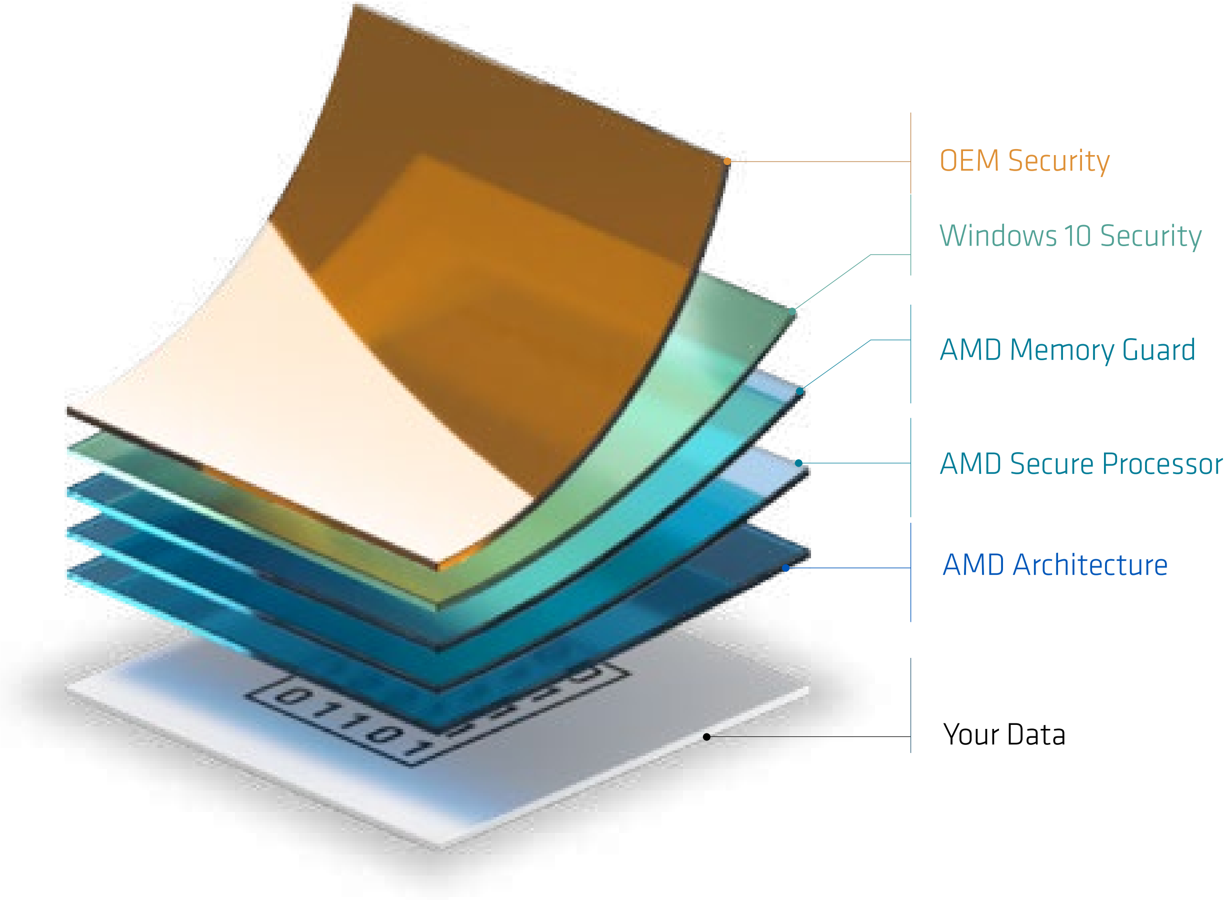
AMD MEMORY GUARD

The World’s Only Processor Family with Full Memory Encryption as a Standard Security Feature[1]

Whether you are a large corporation or small business, protecting your customers and business data is important. There are numerous reports of computers being lost or stolen containing very sensitive information such as banking records, individuals’ health information and even government FBI investigations. With modern notebooks and desktop PCs that are never fully turned off, the threat of this data being stolen from a physical attack (sometimes referred to as a “Cold Boot Attack”) is high. Many security mechanisms, even drive encryption, can be defeated through this type of attack.

Through a modern, multi-layered approach to security, AMD processors help protect your sensitive data from today’s sophisticated attacks, avoid downtime, and can reduce resource drain. AMD provides a set of silicon and firmware level security features that we then build on with our industry ecosystem partners at the OS and system levels. In particular, AMD Memory Guard brings a new set of security features to help address an old industry problem.



DID YOU KNOW?[2,3]

Every
53
Seconds
A laptop is stolen

80%
Of the average cost associated with the loss of a laptop is due to a data breach

3x
Data breaches increased from 2018

When users login to their computer many of the system secrets are stored within the DRAM, un-encrypted. With physical access to a PC an attacker may be able to chill the memory, reset the system bypassing memory clearing functions, and read the contents. As a result, the keys used for drive encryption and user passwords stored in memory can be extracted. Unfortunately, this has been an industry problem going back more than 10 years. While in recent years DDR4 memory scrambling techniques have helped somewhat they have been publicly proven to not provide an effective protection against a physical memory attack.

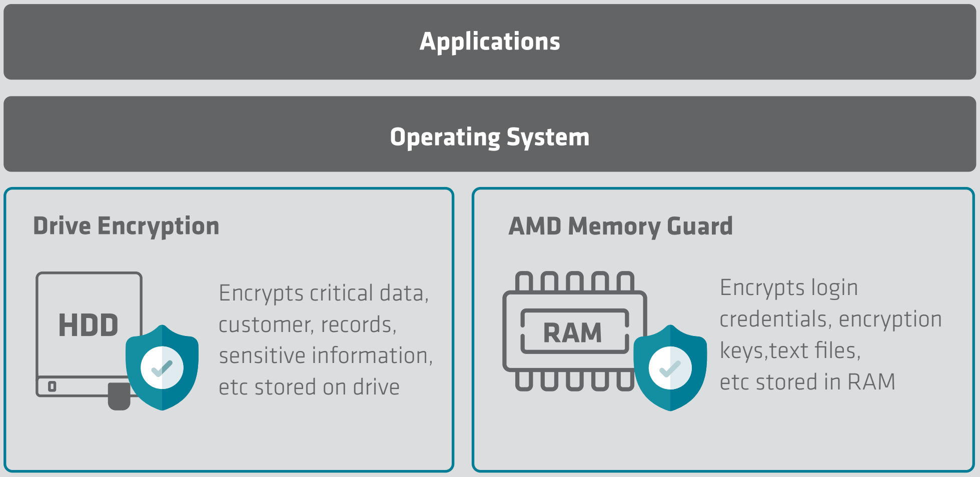
Up until AMD Memory Guard the only way to help protect against this type of attack was to completely turn the PC off after each use. In fact, many storage encryption vendors still recommend this approach today. While effective, the problem is end users expect a more and more responsive computing experience with the ability to leave and resume their work without ever turning their computer off. The industry responded by pushing towards the widescale use of modern standby where a PC stays in standby mode ready to resume functioning where the user left off within seconds. This greatly improves the user experience and productivity, but it also brought back into focus the risk from physical attacks. Finding a solution to this dilemma between productivity and data security is the type of technology challenge AMD is dedicated to help customers solve.

Businesses must look at all aspects of endpoint security as essential tools in their security defenses while also being mindful of how the modern PC is being used. With AMD PRO security technology, users get the benefit of **AMD Memory Guard**, which enables system memory encryption to help reduce the threat of physical memory attacks even if a system is left in standby mode. When used in combination with other technologies, like drive encryption, TPM, and system authentication businesses can continue to help protect data while also allowing users to be more productive by not having to shut down their PC after every use.

How AMD Memory Guard Helps Augment End Point Security by Encrypting System Memory

Inside every AMD Ryzen™ PRO processor is a dedicated on-chip security co-processor called the AMD Secure Processor (ASP). The ASP forms the foundation of the root of trust for critical security functions and features of AMD PRO security technology including AMD Memory Guard.

AMD Memory Guard is a memory encryption technology providing a simple yet compelling model for many computing systems, especially when physical attacks on the system are a concern. With AMD Memory Guard, all DRAM contents are encrypted utilizing the random key which helps provide protection against physical cold boot, DRAM interface snooping, and similar types of attacks. For systems with NVDIMM, AMD Memory Guard also helps provide protection against an attacker removing a memory module and attempting to extract its contents.



Applications

Operating System

Drive Encryption

Encrypts critical data, customer, records, sensitive information, etc stored on drive

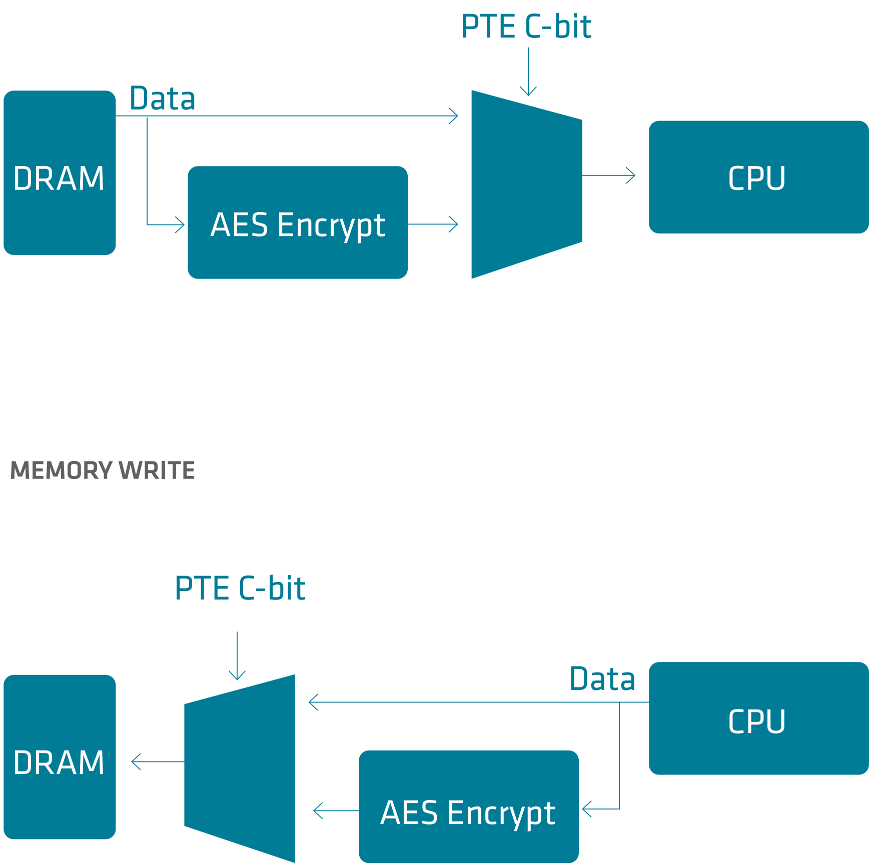
AMD Memory Guard

Encrypts login credentials, encryption keys,text files, etc stored in RAM

Architectural Advantages from AMD

Main memory encryption, AMD Memory Guard, is performed via dedicated hardware in the on-die memory controllers. Each controller includes a high-performance Advanced Encryption Standard (AES) engine that encrypts data when it is written to DRAM and decrypts it when read as shown in Figure 1. By being part of the memory controller the solution has the added benefit of being completely transparent to the OS and any application level software.

FIGURE 1.


MEMORY READ

MEMORY WRITE

5 Things to know about AMD Memory Guard:

1. Does not require any software modifications
2. Will run on any OS version
3. Works with any application
4. No significant impact to system performance
5. AMD has the ONLY commercial processors with full memory encryption as a standard security feature[1]

Memory Encryption Behavior

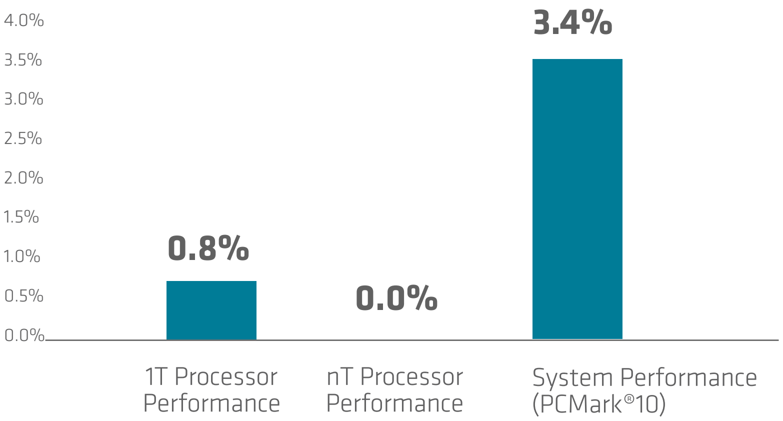
The encryption of data is done with a 128-bit key generated by an onboard NIST SP 800-90 compliant hardware random number generator in a mode which utilizes an additional physical address-based tweak to help protect against cipher-text block move attacks. The encryption key used by the AES engine with AMD Memory Guard is randomly generated on each system reset and is not visible to any software running on the CPU cores. This key is managed entirely by the AMD Secure Processor.

Small Impact on System Performance

The AMD architecture has several advantages by providing a cryptographically strong cipher that is integrated within the processor itself, making it more difficult to breach via a physical attack. Importantly, it also has only a small impact on overall system performance.

The chart to the right shows an approximate amount of reduction in processor performance as well as overall system performance when AMD Memory Guard is turned on versus a baseline score without memory encryption. The chart shows the processor performance and overall system performance are very close with virtually no noticeable impact to the user.

Performance Impact with AMD Memory Guard Turned On[4,5]



An Essential Feature of a Comprehensive Security Solution

Physical Cold Boot attacks have been around for more than 10 years with the only solution that addressed that security threat was to either physically secure a PC or completely turn it off after every use. Neither solution is particularly convenient especially as notebooks become more prominent and users keep their systems in a standby state to increase usability.   But now with AMD Memory Guard, important data can be encrypted in system memory to help mitigate against physical memory attacks. With the increasing need to protect sensitive data against cyber threats, AMD now provides another tool that as part of a comprehensive security solution can help address security threats.

VISIT AMD.COM/PARTNER

Your source for tools, training, news, reviews, and much more!

Learn more about AMD PRO security at **WWW.AMD.COM/PROSECURITY**

[1] For general business laptops and desktops AMD Memory Guard, full system memory encryption, is included in AMD Ryzen PRO and Athlon PRO processors. PP-3
[2] https://www.ibm.com/security/data-breach
[3] http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches
[4] Testing as of 3/26/2020 by AMD Performance Labs on a Ryzen 5 PRO 350U (Lenovo T495). Results may vary. PP-23.
[5] Testing as of 3/26/2020 by AMD Performance Labs on a Ryzen 5 PRO 350U (Lenovo T495). Results may vary. PP-24.

PCMark is a registered trademark of Futuremark Corporation.