AMD GUARDMI TECHNOLOGY

A Built-in Security Guard for Every Business

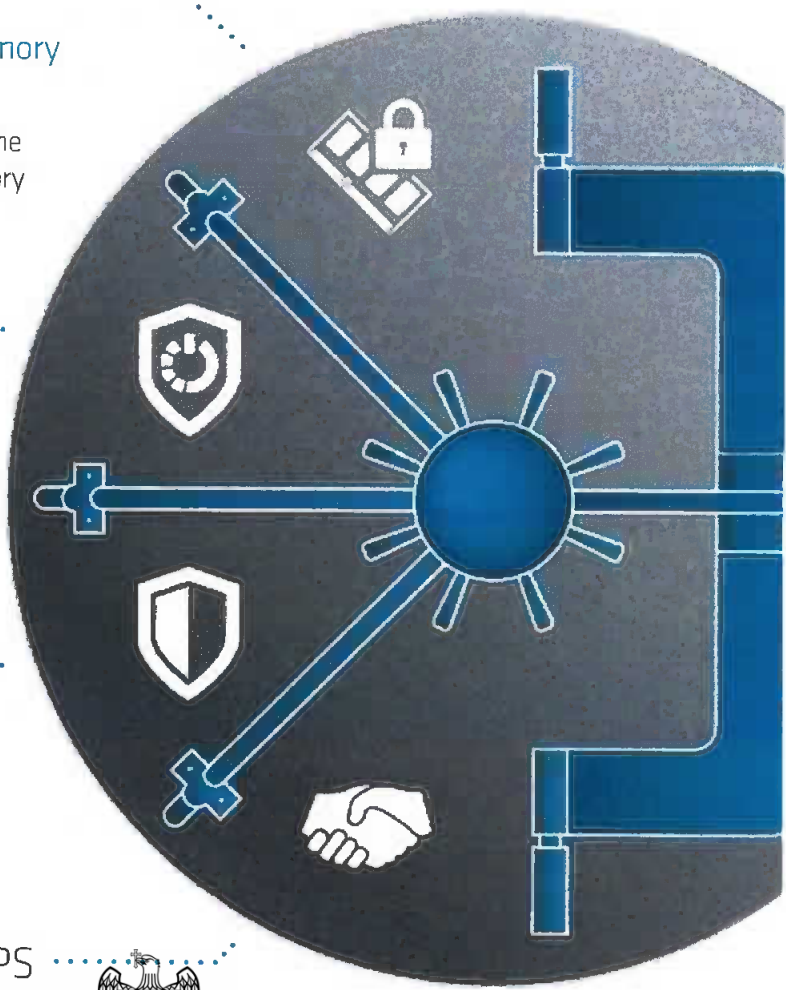
AMD processors are architected with a focus on security. As a result, AMD GuardMI Technology was designed with features to help customers address cybersecurity concerns.

WORLD'S FIRST

AMD MEMORY GUARD

The world's only processor family with full memory encryption as a standard security feature[1]

- **Helps defend against cold boot attacks** with real-time encryption and decryption of all your system's memory



AMD SECURE BOOT

- Enables a secure boot process to **help secure the PC**
- **Helps prevent threats** from reaching critical software

ENHANCED OS SECURITY

- Support of **Windows 10 security features**: Device Guard, Credential Guard, TPM 2.0, VSB, and others

COLLABORATIVE RELATIONSHIPS

- Helping ensure **latest security feature integration and support**

Digitally signed by Dimitriu Alina
Date: 2020.05.18 13:48:13 EEST
Reason: MoldSign Signature
Location: Moldova

www.AMD.com/GuardMI

AMD

AMD SECURE PROCESSOR (ASP)

- Helps **secure the processing and storage** of sensitive data and trust applications

SECURITY FEATURE	BENEFIT	AMD GUARDMI	INTEL VPRO
MEMORY GUARD	Encrypts memory to prevent a physical attacker from reading sensitive data on the memory like keys. Helps mitigate cold boot attacks.	✓ AMD Memory Guard	No Equivalent Offering
SECURE BOOT	Boot protection that helps prevent unauthorized software and malware from taking over critical system functions.	✓ AMD Secure Boot	✓ Intel Boot Guard
UEFI SECURE BOOT	Helps prevent malicious code & unauthorized software loading during the system start up process.	✓ AMD Secure Boot	✓ Intel BIOS Guard
MICROSOFT DEVICE GUARD	Microsoft feature set which helps prevent malicious code from running in OS.	✓	✓
VIRTUALIZATION BASED SECURITY	Enables virtualized environments.	✓ AMD-V	✓ Intel Virtualization (VT-d/VT-x)
FIRMWARE TPM	A firmware version instead of real hardware which provides authenticity to the platform and helps ensure that there are no signs of security breaches.	✓ AMD Firmware TPM	✓ Intel Platform Trust Technology
RANDOM NUMBER GENERATOR	A hardware-based random number generator for cryptographic protocols. Provides cryptographic capabilities for added security.	✓ AMD (RNRAND)	✓ Intel Secure Key
AES-NI	Helps accelerate encryption protocols and helps protect network traffic (internet and email content) and personal data.	✓ AMD AES-NI	✓ Intel Advanced Encryption

AMD.com/partner

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

Contact your local AMD representative to learn more, or go to **www.AMD.com/GuardMI**

AMD