AMD PRO SECURITY

Security Features Designed In

Through a modern, multi-layered approach to security features, AMD processors help protect your sensitive data from today's sophisticated attacks, avoid downtime, and reduce resource drain.

SECURE ECOSYSTEM

- **Secured-core PC** offers deep integration with Microsoft and OEMs to support secure Windows devices
- **Collaborating with OEMs** to complement and enable their enterprise-level security features

AMD MEMORY GUARD

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

- **Full memory encryption** to help protect sensitive data against advanced physical attacks should your PC be lost or stolen

AMD SECURE PROCESSOR

- **Dedicated hardware** that validates code before it is executed to help protect data and firmware integrity
  - FIPS 140-3 Certified[2]

MODERN SECURITY ARCHITECTURE

- **AMD "Zen3" Core** architecture introduces AMD Shadow Stack, a robust security approach to help protect against control-flow attacks
- Supports **Microsoft hardware-enforced stack** protection

www.AMD.com/business

SECURITY FEATURE	BENEFIT	AMD PRO SECURITY
MEMORY ENCRYPTION	Encrypts memory to help prevent a physical attacker from reading sensitive data in memory. Helps mitigate cold boot attacks.	AMD Memory Guard
SECURE BOOT	Boot protection that helps prevent unauthorized software and malware from taking over critical system functions.	AMD Platform Secure Boot
WINDOWS 10 SECURITY	Microsoft security feature set which helps mitigate threats.	Supported
VIRTUALIZATION BASED SECURITY	Uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system.	AMD-V
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
RANDOM NUMBER GENERATOR	A hardware-based random number generator for cryptographic protocols. Provides cryptographic capabilities.	AMD RDRAND
AES-NI	Helps accelerate encryption protocols and helps protect network traffic (internet and email content) and personal data.	AMD AES
MICROSOFT SECURED-CORE PCs	Enables you to boot securely, helps protect device from firmware vulnerabilities, helps to shield the operating system from attacks, and helps prevent unauthorized access to devices and data with advanced access controls and authentication systems	Secured-core PC compatible
CONTROL FLOW ATTACK PROTECTION	Robust security approach to help protect against control-flow attacks by checking the normal program stack against a hardware-stored copy and enabling Microsoft Hardware Enforced Stack Protection as part of a comprehensive set of AMD security features to help secure PCs	AMD Shadow Stack
GUEST MODE EXECUTE TRAP	A silicon performance acceleration feature which enables hypervisor to efficiently handle code integrity check and help protect against malware.	AMD GMET
SYSTEM MANAGEMENT MODE SUPERVISOR	A security module which helps isolate System Management Mode	AMD SMM Supervisor
SECURE INIT AND JUMP WITH ATTESTATION	An instruction which helps create a “root of trust” starting with an initially untrusted operating mode	AMD SKINIT

SUPPORTING MICROSOFT SECURED-CORE WINDOWS PCS

AMD supports Secured-core PCs with security technologies like AMD-V with GMET, AMD Memory Guard, SKINIT, and SMM Supervisor

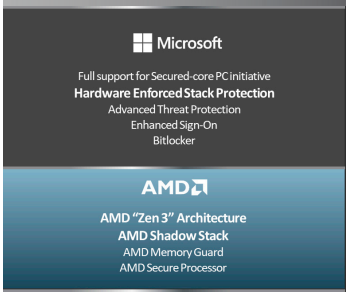
Secured-core PCs powered by AMD processors help provide protection against physical attacks with AMD Memory Guard enabled by default

LAYERS OF SECURITY FEATURES FROM ECOSYSTEM PARTNERS

AMD works closely with Microsoft and OEMs to support and complement their enterprise-level security features

OEM Partners

Enterprise-level security features integrated with OS and hardware designs to protect sensitive data



VISIT AMD.COM/PARTNER

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

To find out more about AMD for Business Processors, please visit **www.AMD.com/business**

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. FIPS 140-3 Implementation Under Test