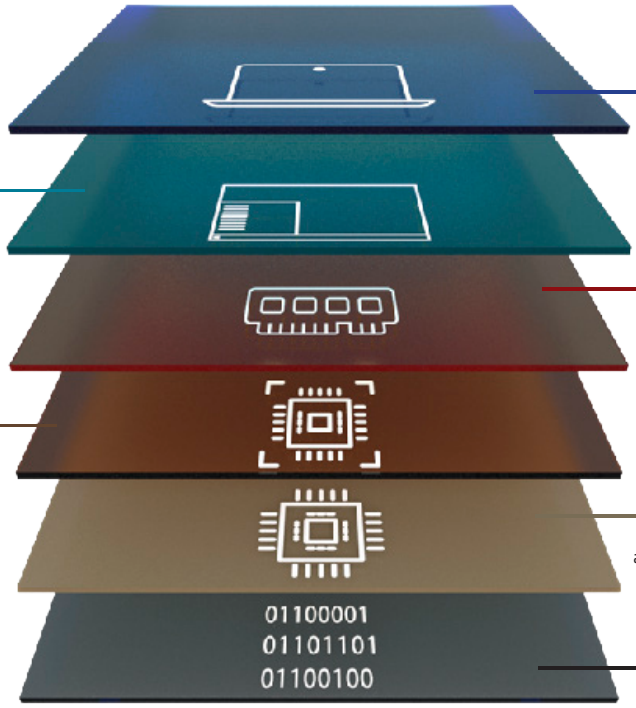
AMD PRO SECURITY

SECURITY FEATURES DESIGNED IN

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

AMD Ryzen™ PRO 6000 Series processors are the first x86 processors to integrate the Microsoft Pluton Security Processor[1,2], a chip to cloud security technology designed and updated by Microsoft, that strengthens Windows 11 devices with continuous protection for user identity, data, and apps[3].



OEM SECURITY FEATURES

Deep collaboration with OEMs to complement and enable their enterprise-grade security features

WINDOWS® 11 SECURITY

Secured-core PC offers deep integration with Microsoft and OEMs to support secure Windows PCs
Hardware Enforced Stack Protection
Microsoft Pluton Security Processor

AMD MEMORY GUARD

The world's first commercial processor family with full memory encryption as a standard security feature[2]

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

MICROSOFT PLUTON SECURITY

Integrated in AMD Ryzen™ and Ryzen™ PRO 6000 series processors.

FIPS 140-3 Level 2 Certification*

AMD ZEN 3+ ARCHITECTURE

AMD "Zen3+" Core architecture with **AMD Shadow Stack**, a robust security approach to help protect against control-flow attacks

AMD SECURE PROCESSOR

Dedicated Security Processor that validates code before it is executed to help ensure data and application integrity

YOUR DATA

*FIPS 140-3 Level 2 Certification

MICROSOFT PLUTON SECURITY PROCESSOR

ONGOING PROTECTION TO HELP KEEP DEVICES SAFE AT HOME, AT WORK, AND AT PLAY

Designed by Microsoft and integrated in AMD Ryzen™ 6000 series processors, Microsoft Pluton security processor helps deliverenhanced security features to the core of Windows 11 devices, with:

UP-TO- DATE SECURITY FEATURES AT THE CORE

Built into the CPU to deliver unified defense that helps eliminate entire vectors of attack through tightly integrated hardware and software, with latest hardware and firmware protection from Windows updates.

PROTECTION AGAINST PHYSICAL ATTACKS

The integrated design helps protect user identities, data, or encryptionkeys from sophisticated attacks when an attacker has physical possession of the device or has installed malware.

ESTABLISHED TECHNOLOGY AND PARTNERSHIPS

Built on established technology used in XBOX and Azure Sphere, Microsoft Pluton security processor is integrated with the AMD Security Processor in the CPU to help deliver chip to cloud security protection on Windows 11 devices.

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
UEFI SECURE BOOT	Helps prevent malicious code & authorized software loading during the system start up process	AMD Secure Boot
MICROSOFT PLUTON SECURITY PROCESSOR	Designed by Microsoft. Integrated on AMD Ryzen™6000 series processors. Strengthens Windows 11 devices with Microsoft Pluton which is built to support Zero Trust security strategies. Microsoft Pluton offers up-to-date security at the core of the CPU silicon, helps prevent physical attacks, and is built on established technology	Integrated Microsoft Pluton Security Processor
PLUTON TPM 2.0	Integrated TPM which is TPM2.0 compliant that supports Windows 11 usage of the TPM across scenarios like Windows Hello and BitLocker with integration with Windows Update that provides easier updates with familiar IT controls	Integrated Microsoft Pluton Security Processor
WINDOWS DEFENDER APPLICATION GUARD	Microsoft feature set which helps prevent malicious code from running in OS.	Enabled
VIRTUALIZATION BASED SECURITY	Uses hardware virtualization features to create and isolate a 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 detect signs of security breaches.	AMD Firmware TPM
RANDOM NUMBER GENERATOR	A hardware-based random number generator for cryptographic protocols. Provides cryptographic capabilities.	AMD RNRAND
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, protect device from firmware vulnerabilities, shield the operating system from attacks, and prevent unauthorized access to devices and data with advanced access controls and authentication systems	Secured-core PC compatible
CONTRL 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 a hypervisor to efficiently handle code integritycheck 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
FIPS 140-3 Level 2 Certification[3]	Government encryption standard adopted by private sector as best practice for validating the security of cryptographic hardware	Microsoft Pluton Security Processor

LAYERS OF SECURITY FEATURES
FROM ECOSYSTEM PARTNERS

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

- AMD Ryzen™ 6000 series are the world's 1st x86 processor integrating the Microsoft Pluton Security Processor to deliver hardened Windows 11 PCs with ongoing protection for identities, data, and applications
- AMD enables 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

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. As of January 2022, only AMD Ryzen™ 6000 Series processors include the Microsoft Pluton security processor, while AMD Ryzen™ 5000 Series processors and Intel's latest 11th and 12th Gen processors do not. RMB-24
2. 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/. GD-202.
3. As of January 2022, AMD has not independently verified the 3rd party claim.