AMD PRO TECHNOLOGIES

A LOOK AT AMD PRO SECURITY AND THE AMD FRAMEWORK FOR SECURE, MANAGEABLE, AND RELIABLE BUSINESS PCS

The agile, distributed workplace continues to evolve. Hybrid operations are becoming the norm, with businesses balancing in-office collaboration and remote work while integrating AI into daily workflows. Enterprises face increasing pressure to refresh their PC fleets with systems that address the new challenges presented by such trends. They require solutions that balance performance, security, and manageability while adapting to both on-premises and cloud-based environments.

AMD Ryzen™ PRO processors empower modern business PCs with AMD PRO Technologies, a unified set of innovations designed to meet the changing demands of today's enterprises. This paper explores the security pillar of AMD PRO Technologies, one of three foundational components integral to all AMD Ryzen PRO processor-powered systems. While security is the primary focus of this paper, AMD PRO Technologies also include advanced manageability and business-ready reliability, which together provide a comprehensive solution for modern enterprises.

The three pillars are introduced here to provide context for AMD PRO Technologies as a whole, but the discussion in this paper will focus specifically on the next-level security features of AMD Ryzen PRO processors that are designed to protect today's business PCs against evolving threats.

PRO SECURITY: SAFEGUARDING THE MODERN ENTERPRISE

The cornerstone of AMD PRO Technologies is robust security features. Advanced hardware features, such as AMD Memory Guard[1] for full memory encryption, AMD Shadow Stack designed for protection against control-flow attacks, and comprehensive support for the Microsoft Pluton secure crypto-processor, provide critical safeguards against sophisticated threats. With integrated support for secure boot[2] and trusted execution, AMD Ryzen PRO processors fortify devices at every layer, giving the user data and applications protection from endpoint to cloud.

While state-of-the-art security features are the focus of this paper, the broader AMD PRO Technologies framework—including manageability and business-ready reliability—works together to provide enterprises with a complete solution for emerging workplace demands.

PRO MANAGEABILITY: SIMPLIFYING IT OPERATIONS

Managing diverse PC fleets is complex and time-intensive, especially in hybrid work environments. AMD PRO Manageability streamlines operations with open-standards-based tools that enable cloud-based remote management and real-time endpoint monitoring. These tools provide the highest level of compliance with open standards for remote systems management.[3] AMD PRO Manageability helps give the user compatibility with industry-leading tools like Microsoft Endpoint Manager and Windows Autopilot, delivering a consistent and efficient deployment process.

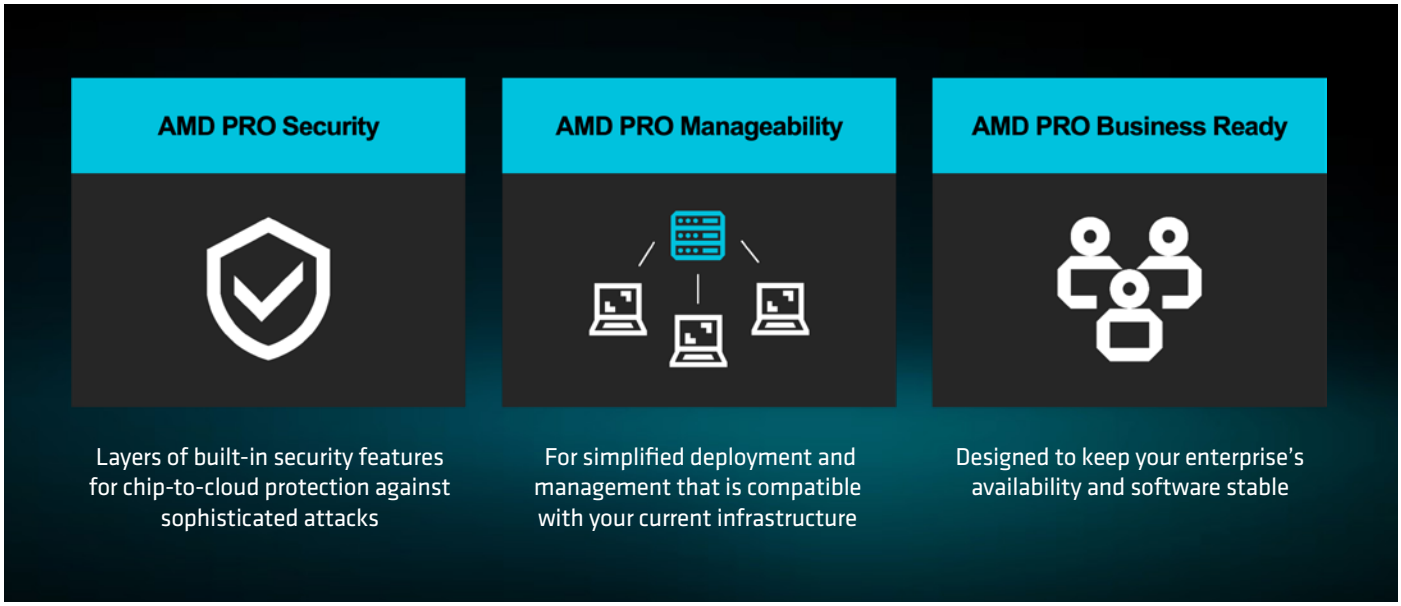
AMD PRO Manageability supports the latest DMTF DASH (Desktop and Mobile Architecture for System Hardware) specifications, incorporating up-to-date encryption and authentication protocols such as TLS 1.2 and 1.3. In addition, AMD PRO systems integrate hardware-based security components, including TPM 2.0, to enable safer cryptographic key storage and protection. This standards-based approach delivers stronger protection and better performance compared to older, proprietary protocols.[4] IT teams benefit from features like remote provisioning, automated patch deployment, and real-time diagnostics, all of which help reduce downtime, improve endpoint health, and simplify operations.

Recent studies highlight the impact of AMD PRO Manageability on IT operations, showing deployment times reduced by up to 41%[5] compared to traditional processes and a significant reduction in hands-on effort thanks to unified, intuitive management interfaces. These capabilities help give enterprises the ability to support employees wherever they work, making complex PC ecosystems more straightforward, fast, and reliable to manage.

PRO BUSINESS-READY: RELIABLE PERFORMANCE FOR EVERY TASK

AMD PRO processors with business-ready features help give users PC longevity, consistent performance, and reliability for enterprise workloads. Rigorous validation processes support better uptime, which can help reduce IT costs. Extended worldwide availability over a full year allows businesses to deploy systems on demand, minimizing the need for large up-front purchases. Whether supporting AI-driven applications or routine office tasks, AMD Ryzen™ PRO processors provide the adaptability businesses need to thrive.

Figure 1. AMD PRO Technologies. Empowering every AMD Ryzen™ PRO processor powered business PC.



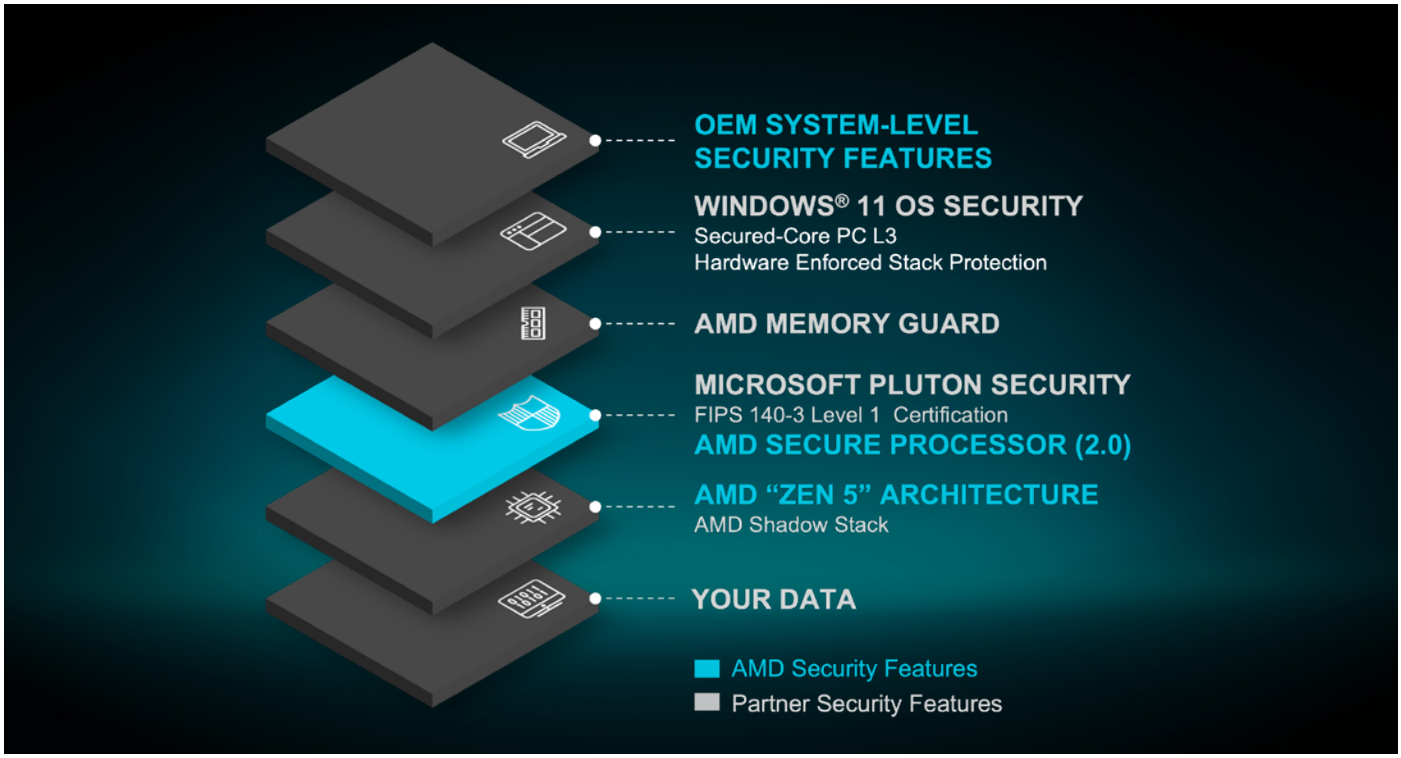
The AMD PRO Business Ready technologies enhance this reliability by providing long-term consistency that simplifies IT planning and maximizes return on investment. All AMD Ryzen™ PRO processors deliver enterprise-grade solutions with:

- **Image Stability:** 18 months of planned software stability to help provide smooth transitions and peace of mind for IT teams.
- **Quality:** Enhanced platform validation processes that provide enterprise-grade quality for demanding business environments.
- **Availability:** 24 months of planned availability to maintain hardware consistency for stable enterprise operations.
- **Reliability:** Continuous platform validation designed for long-term stability and a consistent user experience across multiple processor generations.

By providing stability across both hardware and software, AMD PRO Business Ready reduces complexity for IT teams and provides a dependable foundation for long-term enterprise success.

As enterprises navigate the complexities of supporting the new workplace, AMD PRO Technologies offers a critical edge. By integrating cutting-edge security features, efficient manageability, and business-ready features into every AMD Ryzen PRO CPU-powered system, AMD equips organizations with the tools they need to help protect their operations, streamline IT management, and drive innovation.

Figure 2. AMD PRO Security. Exceeding the latest security requirements for modern devices.



AMD POWERED PCS ARE DESIGNED WITH CUTTING-EDGE MULTILAYERED SECURITY AT ALL LEVELS

AMD works closely with operating systems (OS) developers and original equipment manufacturers (OEMs) to provide hardware security features that complement and strengthen their security design.

By embedding cutting-edge security measures at every level, from silicon to operating systems, AMD empowers organizations to protect their most critical assets while minimizing downtime and reducing IT complexity.

SECURITY BUILT INTO EVERY LAYER

AMD PRO Technologies integrate security as a foundational pillar across all AMD Ryzen™ PRO processor-powered devices. Designed for the evolving challenges of the modern enterprise, these processors deliver multilayered protection that starts with a robust silicon foundation and extends through firmware and operating system-level defenses.

HARDWARE ROOT OF TRUST: INTEGRITY FROM THE START

Silicon architecture from AMD provides an integrated hardware root of trust that helps secure boot processes. The AMD Secure Processor 2.0[6] (ASP 2.0) anchors this trust, verifying firmware and OEM BIOS integrity to defend against unauthorized modifications and potential firmware attacks.

MEMORY PROTECTION REDEFINED: AMD MEMORY GUARD[7]

AMD Memory Guard encrypts all system memory in real-time, helping to safeguard sensitive data from cold boot and physical attacks. With dedicated hardware encryption engines, this feature helps provide robust defense even in scenarios involving device theft.

NEXT-GENERATION ARCHITECTURE: AMD "ZEN 5" AND BEYOND

The latest AMD "Zen 5" core architecture introduces enhanced security features, including Supply Chain Security, which leverages a unique processor ID to enable secure tracking of genuine AMD hardware throughout its lifecycle. These innovations strengthen endpoint resilience against increasingly sophisticated cyber threats.

ALIGNED WITH INDUSTRY STANDARDS

AMD PRO processors are built to exceed modern security requirements, including FIPS 140-3 Level 1 certification. Integration with Microsoft Pluton[8] further enhances protection for Windows-based systems by adding secure authentication and cryptographic safeguards.

AMD SECURE PROCESSOR 2.0:[9] A STRONGER FOUNDATION

At the core of the AMD PRO Security Architecture is the AMD Secure Processor 2.0 (ASP 2.0), a dedicated hardware component embedded in every system-on-a-chip (SoC). ASP 2.0 anchors a hardware root of trust and supports a secure boot flow, verifying firmware integrity from the moment a device powers on. Its isolated Trusted Execution Environment helps sensitive operations remain protected from potential attacks. Key components include:

- **Cryptographic Co-processor (CCP):** A high-performance cryptographic engine that manages key generation and cryptographic operations in hardware, essential for time-sensitive security tasks.
- **Boot ROM:** Secure read-only memory containing critical firmware for boot initialization.
- **Static Random-Access Memory (SRAM):** Provides low-power support for secure processes.
- **Memory Management Unit (MMU):** Governs access to Boot ROM and SRAM for strict control over memory resources.
- **Cloud Bare Metal Recovery:** Facilitates secure recovery of devices via the cloud, enabling business continuity even in catastrophic failure scenarios.
- **Supply Chain Security:** Authenticates genuine AMD hardware at every stage of its lifecycle, protecting against tampering or counterfeit components.
- **Watchdog Timer:** Detects and mitigates stalled processes at the hardware level, enhancing system resilience.

These features collectively address the heightened risk of sensitive business data exposure during travel, remote work, or other mobile scenarios.

SEAMLESS INTEGRATION WITH WINDOWS SECURITY

The AMD PRO Security Architecture aligns seamlessly with Windows 11 security features, such as Secure Boot and Hardware Enforced Stack Protection, to create a comprehensive, multilayered defense system. Together, they fortify endpoints against attacks targeting firmware, BIOS, drivers, and the operating system.

AMD ROM ARMOR

The SPI (Serial Peripheral Interconnect) flash memory on a motherboard contains both the motherboard UEFI and additional configuration information, including the status of Secure Boot.

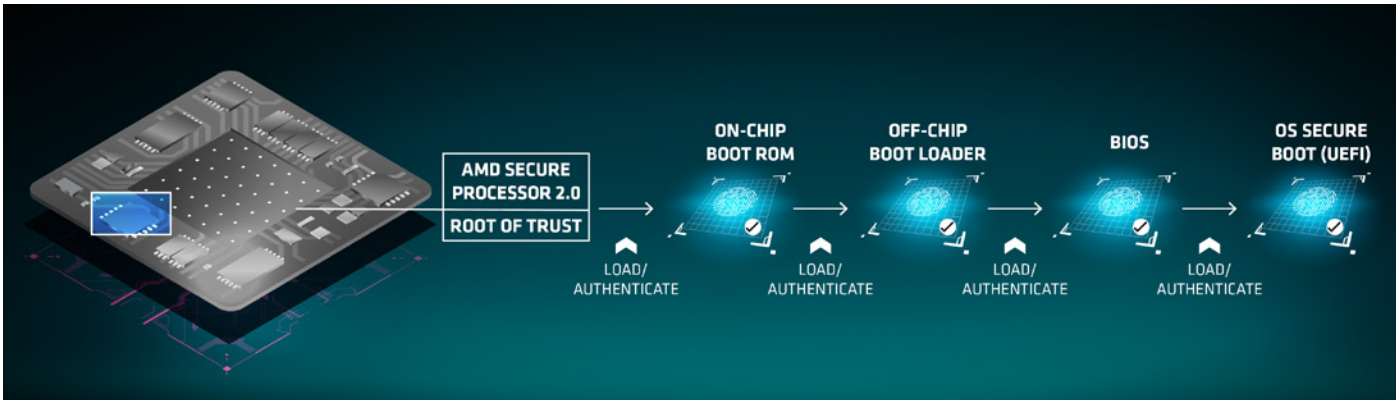
AMD ROM Armor operates before the OS has initialized and provides protection against unauthorized modifications to the SPI flash. By providing the integrity of the SPI flash before the operating system loads, AMD ROM Armor helps establish a fortified foundation for the system. Once AMD ROM Armor is configured and enabled, the computer's SPI flash device is strengthened against unauthorized writes.

AMD PLATFORM SECURE BOOT (PSB)

AMD Platform Secure Boot (PSB) provides a hardware root of trust (RoT) to authenticate the initial firmware, including BIOS, during the device's boot process. When a system powers on, ASP executes the ASP boot ROM code, which authenticates various ASP boot loader codes before initializing silicon and system memory. Once system memory is initialized, the ASP boot loader code verifies the OEM BIOS code, authenticating other firmware components before the OS is booted.

PSB is designed to enforce platform integrity by providing stronger protection from rogue or malicious firmware, automatically denying them access upon detection. AMD PSB helps protect the transition from low-level firmware to OS.

Figure 3. AMD Platform Secure Boot.



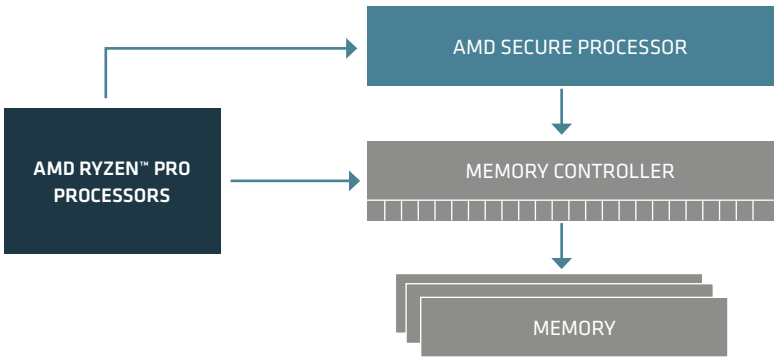
AMD MEMORY GUARD[3]

AMD Memory Guard is a comprehensive memory encryption technology designed to safeguard customer data against physical attack. With AMD Memory Guard, all DRAM contents are encrypted utilizing a random key, which helps protect against physical cold boot, DRAM interface snooping, and similar attacks.

For systems with NVDIMMs, AMD Memory Guard also helps protect against an attacker removing a memory module and attempting to extract its contents, implemented 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.
- A 128-bit key is generated by an on-die NIST SP 800-90 compliant hardware random number generator in a mode that utilizes an additional physical-address-based tweak to help protect against ciphertext 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 (ASP).

Figure 4. AMD Memory Guard.



AMD SHADOW STACK

Return-Oriented Programming (ROP) is an increasingly popular attack vector. ROP attacks don't inject their own malicious code. Instead, they try to gain control of a system by exploiting weaknesses in legitimate code.

HOW DOES THIS WORK?

In computer programming, a “routine” performs a particular set of operations. When a software program executes, it is called a routine. When a routine finishes its job, it returns to the main program using the return address. This process is called “jump and return.”

In ROP attacks, attackers modify the jump routine return address. So, instead of going back to the main program, it jumps around to different routines, stitching together subroutines to create malicious code that can now harm the system. Most importantly, this type of attack goes undetected, as it looks like legitimate code.

The AMD PRO Security Architecture helps mitigate ROP attacks by providing software access to special registers in the CPU where a copy of the return address can be stored. Applications can utilize a parallel stack, known as the "shadow stack," to help mitigate software attacks that attempt to modify the control flow. The shadow stack uses specialized hardware to store a copy of return addresses, which is checked against the normal program stack on return operations.

If the content differs, an exception is generated, which can help prevent malicious code from gaining control of the system. This way, shadow stack hardware can help mitigate some of the most common and exploitable software bugs.

AMD Shadow Stack adds robustness against ROP attacks. Because a copy of the return address is in the hardware, it is very difficult for malicious code to tamper with.

Microsoft Hardware Enforced Stack Protection is supported on AMD PRO Security Architecture using AMD Shadow Stack.

MICROSOFT SECURED-CORE PC

Microsoft Secured-Core PC helps protect your device from firmware vulnerabilities, shields the operating system from attacks, and can prevent unauthorized access to devices and data through advanced access controls and authentication systems.

Secured-Core PC is enabled on AMD PRO Security Architecture platforms using various security technologies and services:

- AMD-V™ with GMET
- AMD Secure Init and Jump with Attestation (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- AMD System Management Mode (SMM) Supervisor
- Direct Memory Access (DMA) Protection

AMD VIRTUALIZATION (AMD-V™) TECHNOLOGY WITH GMET

AMD-V is a set of hardware extensions that enable virtualization on AMD platforms. Guest Mode Execute Trap (GMET) is an in-silicon performance enhancement that enables the hypervisor to efficiently handle code integrity checks and help protect against malware.

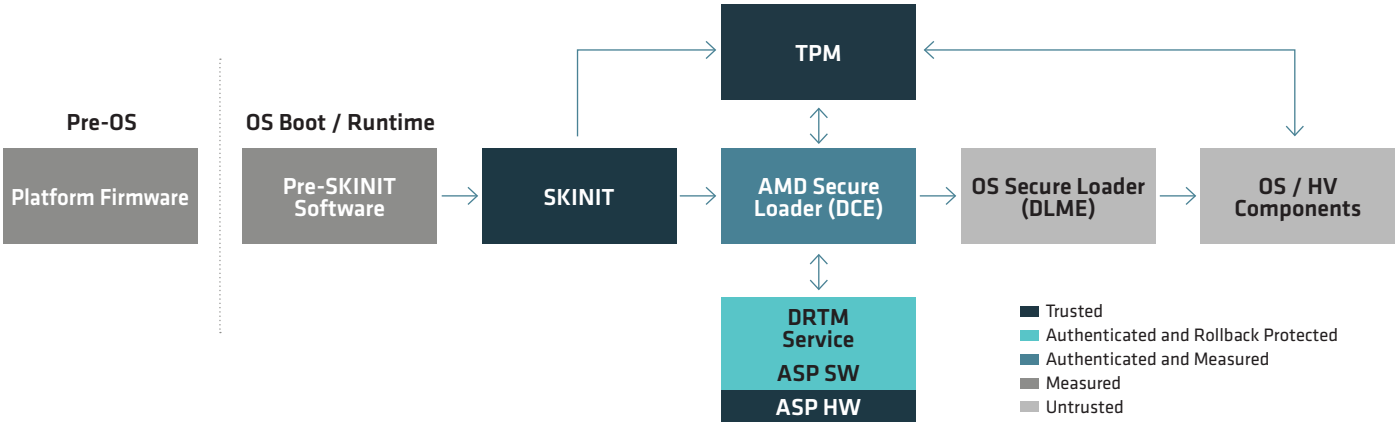
SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

The SKINIT instruction helps create a "root of trust," starting with an initially untrusted operating mode. SKINIT reinitializes the processor to establish a hardened execution environment for a software component called the secure loader (SL) and starts execution of the SL to help prevent tampering. SKINIT extends the hardware-based root of trust to the secure loader.

AMD SECURE LOADER (SL)

The AMD Secure Loader is responsible for validating the platform configuration by interrogating the hardware and requesting configuration information from the DRTM service provided by the AMD Secure Processor.

Figure 5. DRTM Flow.



At any point after the system has booted into OS, the operating system can request AMD service block to remeasure and attest the values before executing further operations. Thus, the OS can help protect the integrity of the system from boot to run time.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

AMD DRTM block is made up of the SKINIT CPU instruction, ASP, and SL. This block is responsible for creating and maintaining a chain of trust between firmware. AMD DRTM works on the concept that the firmware and boot loader can load freely with the assumption that they are unprotected code, knowing that shortly after launch, the system will transition into a trusted state with the hardware forcing low-level firmware down a well-known and measured code path.

AMD DRTM block is made up of the SKINIT CPU instruction, ASP, and SL. This block is responsible for creating and maintaining a chain of trust between firmware.

AMD DRTM works on the concept that the firmware and boot loader can load freely with the assumption that they are unprotected code, knowing that shortly after launch, the system will transition into a trusted state with the hardware forcing low-level firmware down a well-known and measured code path.

The DRTM block measures and authenticates the bootloader and gathers and stores the following system information in a defended manner for further use by the OS, including verification and attestation:

- Physical memory map
- PCI configuration space location
- Local APIC configuration
- I/O APIC configuration
- IOMMU configuration / TMR configuration
- Power management configuration

SHARED HARDWARE CONFIDENCE

This means that the firmware component is authenticated and measured by the ASP block on AMD silicon, and the measurement is stored in a protected manner for further use by the OS, including verification and attestation.

AMD SMM SUPERVISOR

System Management Mode (SMM) is a special-purpose CPU mode in x86 microcontrollers that handles power management, hardware configuration, thermal monitoring, and other device-level operations. Whenever one of these system operations is requested, an interrupt (SMI) is invoked at runtime, executing SMM code installed by the BIOS. SMM code executes in the highest privilege level and is invisible to the OS, making it an attractive target for malicious activity that could potentially be used to access hypervisor memory and compromise the hypervisor.

The SMI handler is typically provided by a developer different from the operating system and has access to OS/hypervisor memory and resources. This means exploitable vulnerabilities in SMM code could lead to compromises of Windows OS, Hypervisor (HV), and Virtualization-Based Security (VBS).

To help isolate SMM, AMD introduces a security module called AMD SMM Supervisor that executes immediately before control is transferred to the SMI handler after an SMI has occurred. AMD SMM Supervisor resides in the AMD DRTM service block and is used to:

- Block SMM from being able to modify hypervisor or OS memory, except for a small communication buffer between the two
- Prevent SMM from introducing new SMM code at runtime
- Block SMM from accessing DMA, I/O, or registers that can compromise the hypervisor or OS

DMA PROTECTION

With DMA remapping technology, AMD platforms support direct memory access (DMA) protection in pre-boot and OS environments via AMD secure technologies like Input Output Memory Management Unit (IOMMU).

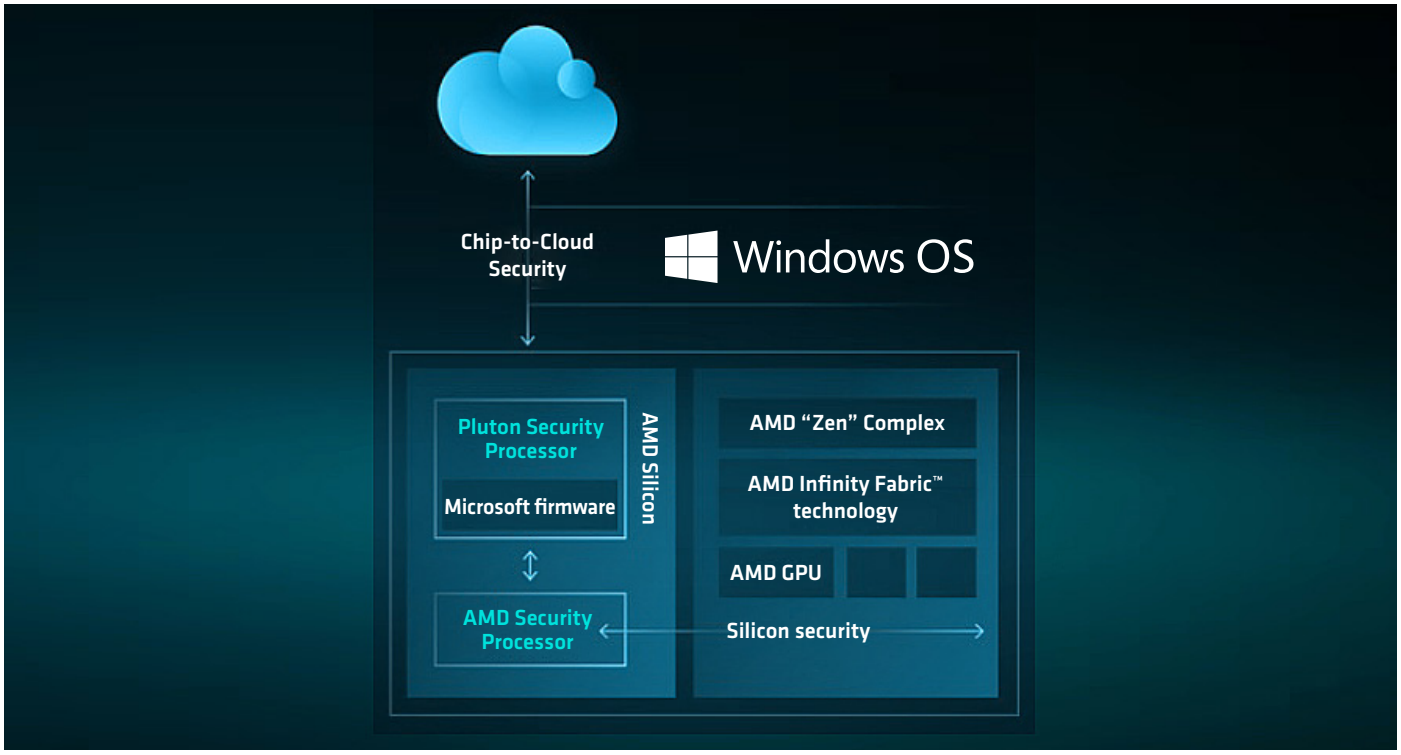
- DMA protection helps safeguard against a possible attack on the platform firmware, where adversaries can use connected devices to perform DMA attacks.
- DMA provides devices with direct access to the physical memory address space for improved performance. However, this also makes it easier for malicious software to inject malware into the system, which can go undetected by the OS.

To help prevent such attacks, AMD has designed a security architecture to manage and control device DMA access via the IOMMU at the pre-OS firmware level. The DMA security architecture hands over responsibility for system memory protection settings from the firmware to the OS after the OS boot loader has been established in memory. The DMA protection using IOMMU is applied on each boot until the OS takes control of the IOMMU itself.

MICROSOFT PLUTON SECURITY PROCESSOR[8]

Designed by Microsoft and built by silicon partners, Microsoft Pluton is a secure cryptography processor built into the CPU for security at the core to help confirm code integrity and the latest protection with updates delivered by Microsoft through Windows Update.

Figure 6. Microsoft Pluton Security Architecture overview.



Pluton protects credentials, identities, personal data, and encryption keys. Information is significantly harder to remove even if an attacker has installed malware or has complete physical possession of the PC.

Microsoft Pluton is designed to provide the Trusted Platform Module (TPM) functionality and deliver other security functionality beyond what is possible with the TPM 2.0 specification. It allows additional Pluton firmware and OS features to be delivered over time via Windows Update.

The AMD Secure Processor 2.0 (ASP 2.0) and the Microsoft Pluton security processor co-exist on AMD client silicon and communicate to help protect the device's integrity. Microsoft Pluton helps protect Windows PC systems by acting as an integrated hardware root of trust for the Windows ecosystem, while ASP 2.0 acts as the silicon hardware root of trust, which helps provide integrity by authenticating initial firmware loaded on the platforms.

PLATFORM UPDATE

AMD PRO processors provide security defenses against attackers trying to gain access to the system in real-time and a robust update mechanism. This enables organizations to update platforms to patch vulnerabilities created by hardware or software bugs.

AMD works closely with OEMs to provide a fortified platform update architecture, one that complies with best practices and can be integrated into OEM's platform update solutions. AMD PRO processors additionally have a Firmware Anti-Rollback (FAR) feature that enables hardware-based policy to block the downgrade of AMD Secure Processor 2.0 (ASP 2.0) firmware. Finally, AMD PRO processors also provide a secure recovery framework called A/B Recovery, which can be integrated into an OEM solution to enable recovery in the event of catastrophic failure.

CRYPTO ACCELERATOR

In today's world, cryptographic operations are important to help protect data and communications. While cryptographic operations are essential, they are also very compute-intensive. AMD provides new, optimized instructions in silicon to help provide low costs associated with cryptographic algorithm computation.

The AMD "Zen 2" and beyond architectures have added support for vectorized AES encryption for 256-bit (vAES256) and integrate AES intrinsics at the x86 level, allowing user applications to benefit from enhanced cryptographic performance and efficiency.

FIPS 140-3 CERTIFICATION LEVEL 1

Given the sensitive nature of the data government agencies handle and the essential services they provide, endpoint security is a top concern when considering laptops for government IT purchases. Outdated hardware lacking modern security features can cause high costs in terms of data loss and service interruptions.

The Federal Information Processing Standards (FIPS) of the United States are a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed for use in computer systems of non-military, American government agencies and contractors. FIPS standards establish requirements for computer security and interoperability.

AMD PRO processors include **FIPS 140-3 Level 1** industry security certification.

Figure 7. Cryptographic Algorithm Validation Program for AMD Ryzen™ PRO 7000 Series processors.

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Implementation Name	AMD Ryzen PRO 7000 Series PSP Cryptographic CoProcessor (SHA2_RSAPSS_SIGVER)
Description	The AMD PSP Cryptographic CoProcessor provides cryptographic algorithm support for the Ryzen PRO 7000 Series processor. The following cipher implementation is covered: SHA2-384 and RSA-PSS sigver implementation.
Version	bc0c0140FIPS001
Type	HARDWARE
Vendor	Advanced Micro Devices (AMD) 2485 Augustine Drive Santa Clara, CA 95054 USA
Contacts	FIPS Contact FIPS@amd.com +1 408-749-4000

A3018 First Validated: 11/18/2022

Collapsed | Expanded | Aggregated

Operating Environment	Algorithm Capabilities
AMD Ryzen PRO 7330U (100-000000950)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7530U (100-000000949)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7730U (100-000000948)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7330U (100-000000950)	SHA2-384
AMD Ryzen PRO 7530U (100-000000949)	SHA2-384
AMD Ryzen PRO 7730U (100-000000948)	SHA2-384

The FIPS module is a combination of hardware, and/or software and/or firmware that supports security functions to be certified. Although FIPS was developed for use by the federal government, many in the private sector voluntarily use these standards, including financial institutions and cloud providers. Additionally, FIPS is expanding beyond North America, including computer processors for European NATO partners.

CLOUD BARE METAL RECOVERY

Cloud Bare Metal Recovery provides a secure mechanism for recovering systems remotely, minimizing downtime and supporting business continuity in the event of catastrophic hardware or software failures. This feature activates before the OS boots to enable system recovery via the cloud without requiring the device to be shipped for service.

By integrating with the AMD PRO Security Architecture, Cloud Bare Metal Recovery helps provide fortified initialization and recovery at the hardware level, which is designed to protect against tampering or exploitation during the recovery process.

SUPPLY CHAIN SECURITY (DEVICE IDENTITY)

Supply Chain Security, enabled by AMD Device Identity, authenticates AMD hardware throughout its lifecycle, from manufacturing to deployment and beyond. This feature helps provide traceability and defends against counterfeit or tampered components, offering assurance to enterprises about the integrity of their hardware.

AMD Device Identity provides cryptographic verification of genuine AMD silicon, so that only authentic hardware is integrated into enterprise systems. This helps safeguard against supply chain attacks that could compromise firmware or hardware before deployment.

WATCHDOG TIMER

The Watchdog Timer enhances system reliability by detecting and mitigating stalled or unresponsive processes at the hardware level. This functionality provides additional fault tolerance, helping systems remain operational and recover gracefully from potential issues.

Integrated into the AMD PRO Security Architecture, the Watchdog Timer works with Secure Boot and other foundational features to provide robust fault detection during pre-boot and runtime operations. This capability strengthens system resilience in mission-critical environments and reduces the risk of downtime caused by software or hardware failures.

SOLUTION HIGHLIGHTS

SECURITY LAYER	FEATURES	BENEFITS
SYSTEM	OEM SECURITY FEATURES	Deep collaboration between OS developer, hardware vendor, and OEM partners to complement and enable OEM enterprise-grade security features.
OS SECURITY	WINDOWS 11 SECURITY	Full support for Secured-core PC initiative, Hardware Enforced Stack Protection, Advanced Threat Protection, Enhanced Sign-On, BitLocker, and more.
HARDWARE & FIRMWARE	AMD SECURE PROCESSOR 2.0	Dedicated security processor that validates code before it is executed to help ensure data and application integrity.
	AMD PLATFORM SECURE BOOT	Boot protection that helps prevent unauthorized software and malware from taking over critical system functions.
	AMD MEMORY GUARD	Delivers real-time encryption of system memory to help defend against physical attacks should your laptop be lost or stolen.
	AMD SHADOW STACK	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 in Windows 11® security.
	MICROSOFT PLUTON SECURITY PROCESSOR	A chip-to-cloud security technology, designed and updated by Microsoft, that enhances security to the core of Windows 11 PCs with continuous protection for user credentials, identities, personal data, and encryption.
	AMD FIRMWARE TPM	A firmware version TPM that provides authenticity to the platform and helps monitor for signs of security breaches.
	FIPS 140-3 LEVEL 1 MODULE CERTIFICATION	Government encryption standard adopted by private sector as best practice for validating the security of cryptographic hardware.
	AMD SECURE PROCESSOR 2.0	Anchors a hardware root of trust, validating initial firmware and protecting the platform against unauthorized code.
	CLOUD BARE METAL RECOVERY	Helps enable secure system recovery via the cloud without requiring shipping of devices, designed to provide minimal downtime during catastrophic events.

SUMMARY

AMD PRO Technologies provide a comprehensive foundation for addressing the evolving demands of modern enterprises. By integrating advanced security, seamless manageability, and business-ready reliability into every AMD Ryzen™ PRO processor, AMD empowers organizations to protect their data, streamline IT operations, and provide next-level productivity across diverse work environments.

As workplaces embrace hybrid operations and integrate AI-driven workflows, AMD remains committed to driving innovation. With each generation, AMD PRO Technologies push the boundaries of security, performance, and manageability, so that businesses are equipped to meet today's challenges and prepare for tomorrow's opportunities.

DISCLAIMER

ENDNOTES

1. 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.
2. 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.
3. Compared to Intel vPro, AMD PRO Manageability implements more profiles of the DASH Management Initiative to support multi-vendor management for desktop and mobile systems. KRKP-7
4. Compared to Intel vPro, AMD PRO Manageability implements a newer version of TLS (Transport Layer Security) protocol which provided higher levels of security and lower latency (TLS 1.3 vs. 1.2) KRKP-8
5. Principled Tech report - https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. 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.
7. 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
8. 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.
9. 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.