AMD PRO 技术

聚焦 AMD PRO 安全性技术，着眼 AMD 为商用 PC 设计的安全性、可管理性和可靠性技术框架

灵活的分布式工作场所正在不断演变。混合办公模式正在成为常态，越来越多的企业将现场办公与远程办公相结合，并逐步将 AI 集成到日常工作流程之中。面对这些趋势带来的新挑战，企业面临着升级 PC 设备的巨大压力。他们需要兼顾性能、安全性和可管理性的解决方案，同时适应本地和云端环境。

AMD 锐龙 PRO 处理器采用 AMD PRO 技术，可为现代商用 PC 提供强大助力。AMD PRO 技术可带来一整套统一的创新工具，充分满足现代企业不断变化的需求。本文将着重探讨 AMD PRO 安全性技术，在所有搭载 AMD 锐龙 PRO 处理器的系统上，这项技术都是不可或缺的三大关键组成部分之一。另外两大关键组成部分是 AMD PRO 高级可管理性技术和业务可靠性技术。这三种技术强强联合，为现代企业提供了一种全面完备的解决方案。

虽然整个 AMD PRO 技术框架由三大关键组成部分构成，但本文将着重聚焦安全性，专门介绍 AMD 锐龙 PRO 处理器的新一代安全功能，详细阐述这些功能如何帮助现代商用 PC 抵御花样不断翻新的威胁。

PRO 安全性：为现代企业保驾护航

AMD PRO 技术的基石由一系列强大的安全功能筑成。AMD PRO 安全性技术涵盖一系列先进的硬件级安全功能，包括用于全内存加密的 AMD Memory Guard[1]、专为防御控制流攻击而设计的 AMD Shadow Stack，以及对 Microsoft Pluton 安全加密处理器的全面支持等。这些功能对于抵御复杂威胁至关重要。AMD 锐龙 PRO 处理器还针对安全启动[2] 和可信执行提供高度集成的支持，因此可在每一层都为设备提供强化保护，从端点到云端全面保障用户数据和应用安全。

虽然本白皮书重点介绍的是先进安全功能，但 AMD PRO 技术框架还涵盖可管理性和业务可靠性技术，三者协同发挥作用，为企业提供满足新兴工作需求的全面解决方案。

PRO 可管理性：简化 IT 运营

管理多样化的 PC 机群既复杂又耗时，在混合办公环境下更是如此。AMD PRO 可管理性技术带来一系列基于开放标准的工具，可帮助实现基于云的远程管理和实时端点监控，从而充分简化 IT 运营。由于采用开放标准，这些工具为远程系统管理提供了超高合规性保障。[3] AMD PRO 可管理性技术广泛兼容 Microsoft Endpoint Manager 和 Windows Autopilot 等主流工具，从而为用户带来一致高效的部署体验。

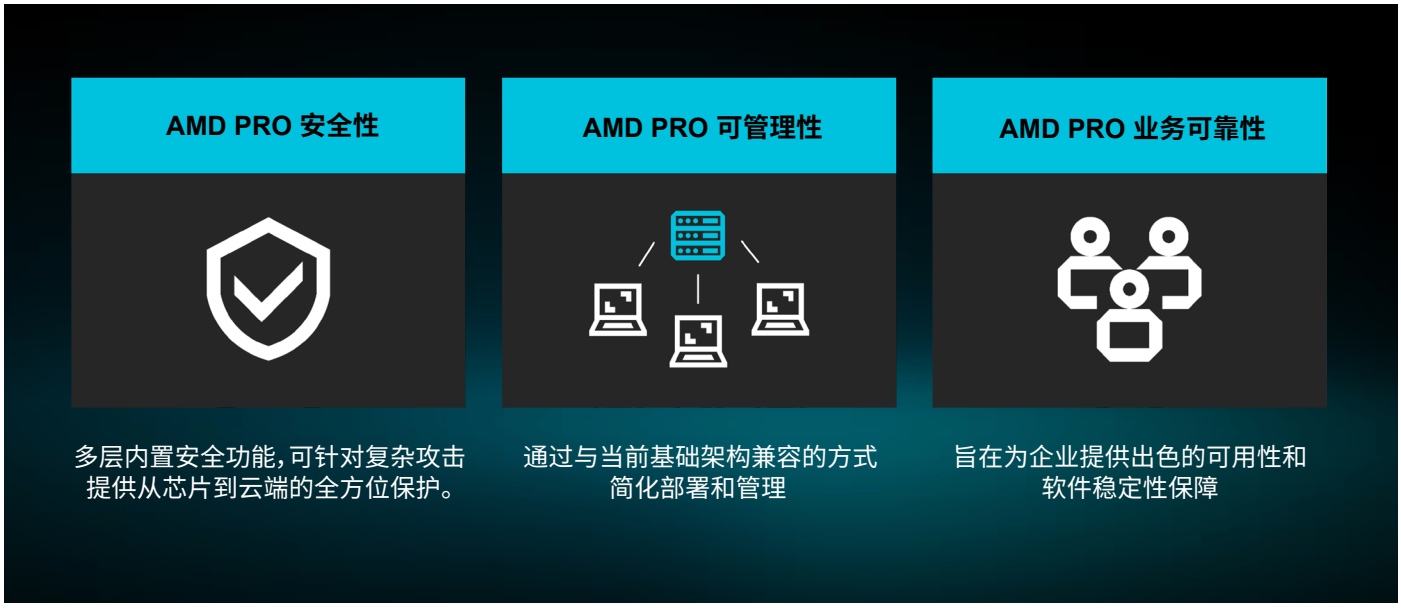
AMD PRO 可管理性技术支持全新 DMTF DASH（桌面和移动系统硬件架构）规范，其中包括最新的加密和身份验证协议，如 TLS 1.2 和 1.3。此外，AMD PRO 系统集成了基于硬件的安全组件，包括 TPM 2.0，可实现更安全的加密密钥存储和更好的保护。与早期专有协议相比，这种基于开放标准的方法能实现更强大的保护和更出色的性能。[4] 远程资源调配、自动补丁部署、实时诊断等功能均有助于减少停机时间、改善端点运行状况以及简化操作，能够为 IT 团队提供强大助益。

近期有一些调查着重研究了 AMD PRO 可管理性技术对 IT 运营的影响，调查结果表明与传统流程相比，采用此技术后部署时间缩短 41%[5]，而且由于管理界面统一直观，实际操作时间也显著减少。借助 PRO 可管理性功能，企业能够为在任何位置办公的员工提供支持，让复杂的 PC 生态系统变得更易于管理、更快速可靠。

PRO 业务可靠性：以可靠性能高效完成每项任务

依托业务可靠性功能，AMD PRO 处理器能够为 PC 带来出色的使用寿命和稳定可靠的性能，助力高效处理企业工作负载。该系列处理器采用严格的验证流程，可延长正常运行时间，从而帮助降低 IT 成本。此外，该系列处理器在全球范围内全年供应，因此企业可以按需部署系统，而无需在前期大量采购。AMD 锐龙 PRO 处理器具备卓越的适应性，无论是支持 AI 应用还是日常办公任务尽可轻松驾驭，助力企业蓬勃发展。

图 1. AMD PRO 技术。为搭载 AMD 锐龙 PRO 处理器的商用 PC 赋能助力。



AMD PRO 业务可靠性技术进一步增强了该系列处理器的可靠性，通过保障长期稳定性简化 IT 规划并充分提高投资回报。作为卓越的企业级解决方案，所有 AMD 锐龙 PRO 处理器均具备以下特性：

- **软件稳定性：**通过 18 个月的软件稳定性计划，帮助 IT 团队顺利完成过渡，让 IT 团队安心无忧。
- **质量保障：**采用经过改进的平台验证流程，以企业级质量保障满足苛刻的业务需求。
- **可靠供货：**通过 24 个月的产品供货计划，保障硬件一致性，从而帮助企业实现稳定运营。
- **可靠性：**持续进行平台验证，旨在实现长期稳定性，并确保跨多代处理器提供一致用户体验。

AMD PRO 业务可靠性技术可带来出色的软硬件稳定性，让 IT 团队的工作得以简化，为企业的长期成功奠定坚实基础。

总而言之，AMD PRO 技术能够为企业提供显著优势，帮助企业应对全新办公模式所带来的复杂挑战。通过将先进的安全功能、高效的可管理性功能以及出色的业务可靠性功能集成到搭载 AMD 锐龙 PRO CPU 的系统当中，AMD 为企业带来一系列工具，充分帮助企业实现安全运营、简化 IT 管理和推动创新。

图 2. AMD PRO 安全性。以超高安全标准为现代设备保驾护航。

AMD 先进的多层安全设计，全面保障 PC 安全

AMD 与操作系统 (OS) 开发商和原始设备制造商 (OEM) 密切合作，通过硬件安全功能来完善和加强安全设计。

从芯片层到操作系统层，AMD 在每一层都嵌入先进的安全措施，帮助组织妥善保护关键资产，同时充分减少停机时间并简化 IT 工作。

安全功能内置于每一层

在所有搭载 AMD 锐龙 PRO 处理器的设备中，AMD PRO 安全性技术均是必不可少的一个基本支柱。这些处理器经过精心设计，从芯片层一直到固件和操作系统层均内置有强大的安全防御措施，可提供多层保护，帮助现代企业应对不断变化的挑战。

硬件信任根：从始至终保障完整性

AMD 芯片架构中集成了硬件信任根，有助于通过安全启动保护所有进程。AMD 安全处理器 2.0[6] (ASP 2.0) 中内置这种信任根，用于验证固件和 OEM BIOS 的完整性，从而阻止未经授权的修改，防御潜在的固件攻击。

重新定义内存保护：AMD MEMORY GUARD[7]

AMD Memory Guard 可实时加密所有系统内存，进而帮助保护敏感数据免受冷启动和物理攻击的影响。依托专用硬件加密引擎，即使在设备被盗的情况下，此功能也能提供强大防御。

新一代架构：AMD “ZEN 5” 及更新架构

全新 AMD “Zen 5” 核心架构引入了增强的安全功能，包括供应链安全功能，该功能利用处理器唯一 ID 在整个生命周期内跟踪 AMD 硬件真伪并以此保障安全性。随着网络威胁变得日益复杂，这些创新功能使得端点防御能力得以增强。

符合行业标准

AMD PRO 处理器满足甚至超出现行的安全要求，包括 FIPS 140-3 1 级认证要求。通过与 Microsoft Pluton[8] 集成，引入了安全身份验证和加密保护措施，由此进一步增强对 Windows 系统的安全保护。

AMD PRO 安全性架构

AMD 安全处理器 2.0[9]：更强大的安全基础

AMD PRO 安全性架构的核心正是 AMD 安全处理器 2.0 (ASP 2.0)，即嵌入在每个片上系统 (SoC) 中的专用硬件组件。ASP 2.0 内置有硬件信任根，并支持安全启动流程，设备一开机便会开始验证固件完整性。ASP 2.0 具有隔离的可信执行环境，有助于保护敏感操作免受潜在攻击的影响。关键组件如下：

- **加密协处理器 (CCP)：**一个高性能加密引擎，负责管理硬件中的密钥生成和加密操作，对于时间敏感型安全任务至关重要。
- **启动只读存储器 (ROM)：**安全的只读存储器，含关键固件，用于初始化启动流程。
- **静态随机存取存储器 (SRAM)：**为安全进程提供低功耗支持。
- **存储器管理单元 (MMU)：**管理对启动 ROM 和 SRAM 的访问，用于严格控制内存资源。
- **云端裸机恢复：**通过云端实现设备的安全恢复，即使在发生灾难性故障时也能保障业务连续性。
- **供应链安全：**在 AMD 硬件生命周期的每个阶段对其进行身份验证，防止组件遭到篡改或假冒。
- **监控定时器 (Watchdog Timer)：**在硬件级别检测并处理停滞的进程，以增强系统弹性。

这些功能可协同作用，帮助解决旅途、远程工作或其他移动办公场景中敏感业务数据面临的高暴露风险。

与 WINDOWS 安全功能无缝集成

AMD PRO 安全性架构可与 Windows 11 中的安全启动和硬件强制堆栈保护等安全功能无缝集成，从而形成一个全面的多层防御系统。这两者强强联手，增强端点防御能力，全面防御针对固件、BIOS、驱动程序和操作系统的种种攻击。

AMD ROM ARMOR

主板上的 SPI（串行外围互连）闪存包含主板 UEFI 和其他配置信息，包括安全引导的状态。

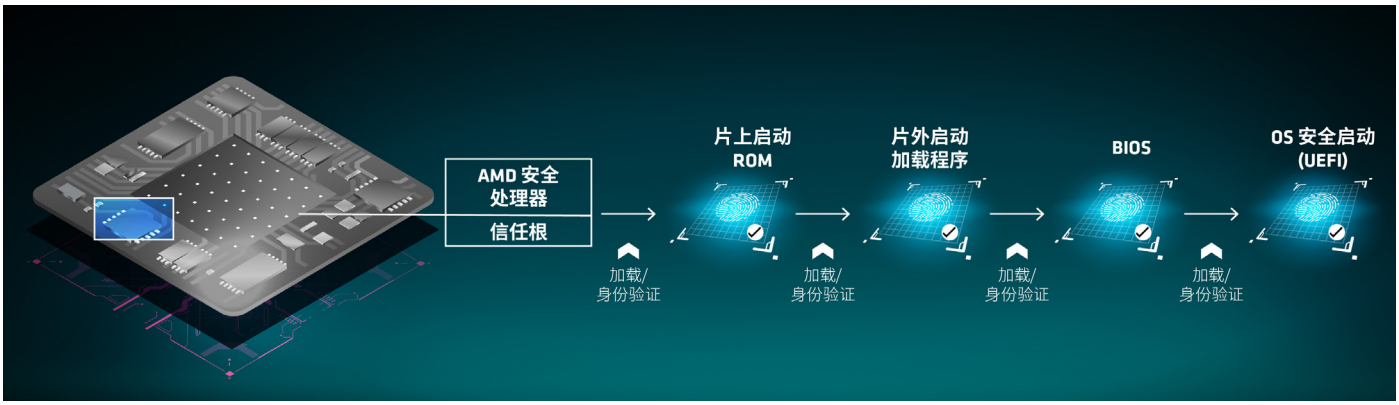
AMD ROM Armor 在操作系统初始化之前运行并提供保护，防止对 SPI 闪存进行未经授权的修改。通过在操作系统加载之前保障 SPI 闪存的完整性，AMD ROM Armor 有助于为系统建立坚实的安全基础。配置并启用 AMD ROM Armor 后，计算机中的 SPI 闪存设备将得到加强保护，防止未经授权的写入。

AMD 平台安全启动 (PSB)

AMD 平台安全启动 (PSB) 功能可提供一种硬件信任根 (RoT)，在设备启动过程中对初始固件（包括 BIOS）进行身份验证。在系统开机时，ASP 会执行 ASP 启动 ROM 代码，以便在初始化芯片和系统内存之前对各种 ASP 启动加载程序代码进行身份验证。初始化系统内存后，ASP 启动加载程序代码会验证 OEM BIOS 代码，进而在操作系统启动之前对其他固件组件进行身份验证。

PSB 旨在提供更强的保护来防御流氓或恶意固件，并在检测到这类固件时自动拒绝其访问，从而更好地保障平台完整性。AMD PSB 可提供从低级固件到操作系统的全面保护。

图 3. AMD 平台安全启动。



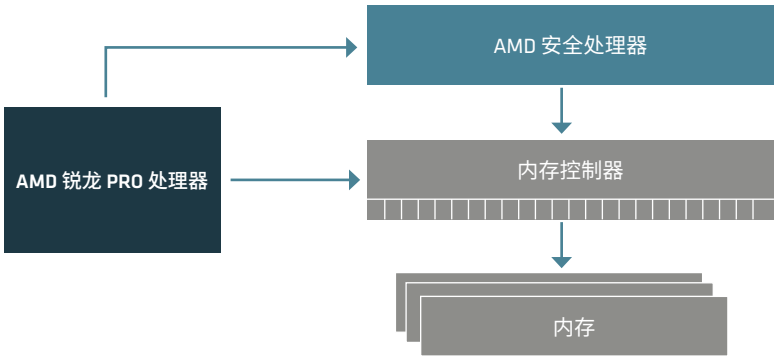
AMD MEMORY GUARD[3]

AMD Memory Guard 是一种全面的内存加密技术，旨在保护客户数据免受物理攻击。借助 AMD Memory Guard，可通过随机密钥对所有 DRAM 内容进行加密，从而抵御物理冷启动、DRAM 接口监听以及其他类似攻击。

对于采用 NVDIMM 的系统，AMD Memory Guard 还有助于防止攻击者移除内存模块并提取其中的内容，这要通过片上内存控制器中的专用硬件来实现。

- 每个控制器都有一个高性能 Advanced Encryption Standard (AES) 引擎，能够在数据写入 DRAM 时进行加密并在读取数据时进行解密。
- 符合 NIST SP 800-90 标准的片上硬件随机数生成器会生成一个 128 位密钥，该密钥利用基于物理地址的额外调整来帮助防御密文块移动攻击。
- 配备 AMD Memory Guard 的 AES 引擎所用的加密密钥会在每次系统重置时随机生成，并且对 CPU 核心上运行的任何软件均不可见。该密钥完全由 AMD 安全处理器 (ASP) 管理。

图 4. AMD Memory Guard。



AMD SHADOW STACK

返回导向编程 (ROP) 是一种越来越常见的攻击媒介。ROP 攻击者并不会自行注入恶意代码，而是试图通过利用合法代码存在的漏洞来控制系统。

工作原理

在计算机编程中，一个“例程”执行一组特定的操作。在一个软件程序执行时，就称为一个例程。当一个例程完成其工作时，它会使用返回地址返回到主程序。这个过程称为“跳转和返回”。

在 ROP 攻击中，攻击者会修改跳转例程返回地址。如此一来，例程不会返回到主程序，而是会跳转到其他例程，这会导致多个子例程合并，从而生成可能危害系统的恶意代码。更糟糕的是，由于生成的恶意代码看起来像是合法代码，这种攻击难以察觉。

AMD PRO 安全性架构允许软件访问 CPU 中用于存储返回地址副本的特殊寄存器，由此帮助降低 ROP 攻击风险。软件应用可以利用称为“影子堆栈”的并行堆栈，来抵御试图修改控制流的软件攻击。影子堆栈会使用专用硬件来存储返回地址的副本，并在执行返回操作时根据正常程序堆栈进行检查。

如果内容不同，则会生成异常，从而帮助防止恶意代码控制系统。通过这种方式，影子堆栈硬件可以帮助抵御一些容易利用的常见软件漏洞。

AMD Shadow Stack 可增强对 ROP 攻击的防御能力。原因是，通过将返回地址的副本存储在硬件中，恶意代码便很难篡改返回地址。

AMD PRO 安全性架构利用 AMD Shadow Stack，并支持 Microsoft 硬件强制堆栈保护。

MICROSOFT 安全核心电脑

Microsoft 安全核心电脑能够防御固件漏洞、保护操作系统，还能够通过先进的访问控制和身份验证系统防止未经授权访问设备和数据。

基于 AMD PRO 安全性架构的安全核心电脑将可以启用多种安全技术和服务：

- AMD-V™ 与 GMET
- AMD 基于认证的安全初始化和跳转 (SKINIT)
- AMD 安全加载器 (SL)
- AMD 动态信任根测量 (DRTM)
- AMD 系统管理模式 (SMM) 监管器
- 直接内存访问 (DMA) 保护

AMD 虚拟化 (AMD-V™) 技术与 GMET

AMD-V 是一组硬件扩展，用于支持 AMD 平台上的虚拟化操作。Guest Mode Execute Trap (GMET) 是一种芯片内性能优化功能，能够让管理程序高效处理代码完整性检查，并帮助防范恶意软件。

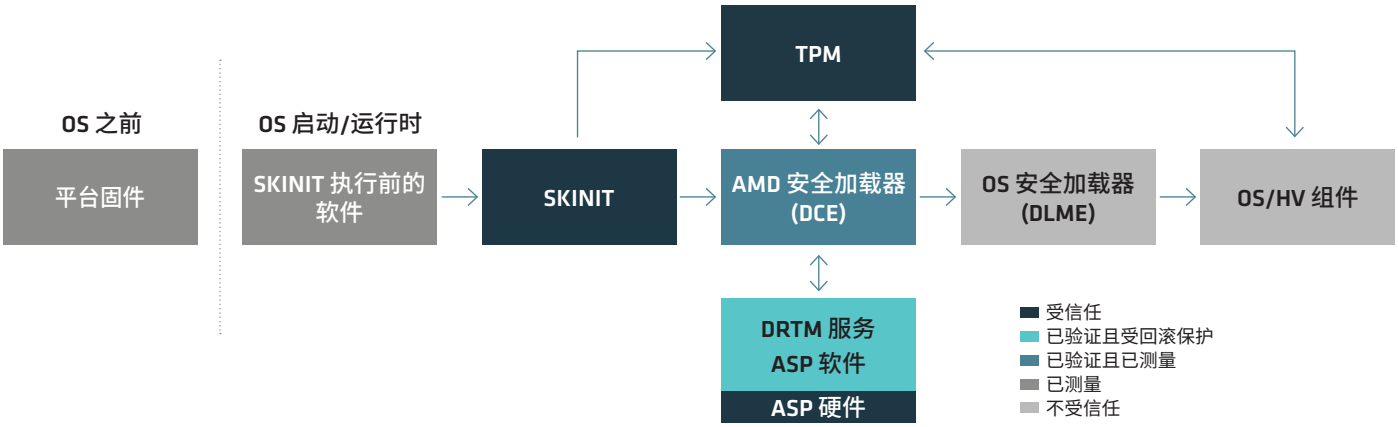
基于认证的安全初始化和跳转 (SKINIT)

借助 SKINIT 指令，可从初始不受信任的操作模式开始创建“信任根”。SKINIT 会重新初始化处理器，为称为“安全加载器”(SL) 的软件组件建立一个强化的执行环境，并开始执行 SL 以防止篡改。SKINIT 将基于硬件的信任根扩展到安全加载器。

AMD 安全加载器 (SL)

AMD 安全加载器负责质询硬件并从 AMD 安全处理器提供的 DRTM 服务请求配置信息，以此验证平台配置。

图 5. DRTM 流程。



在系统启动进入操作系统 (OS) 后，OS 随时可以请求 AMD 服务重新测量和验证相应值，然后再执行进一步操作。因此，OS 可以在从启动到运行的整个过程中保护系统完整性。

AMD 动态信任根测量 (AMD DRTM)

AMD DRTM 服务由 SKINIT CPU 指令、ASP 和 SL 组成。该服务负责建立和维护固件之间的信任链。
AMD DRTM 的工作原理是，固件和启动加载程序可以自由加载，前提是它们是不受保护的代码，并且知道在启动后不久，系统将转换为可信状态，而且硬件将迫使低级固件按照已知和可测量的代码路径运行。

AMD DRTM 服务由 SKINIT CPU 指令、ASP 和 SL 组成。该服务负责建立和维护固件之间的信任链。

AMD DRTM 的工作原理是，固件和启动加载程序可以自由加载，前提是它们是不受保护的代码，并且知道在启动后不久，系统将转换为可信状态，而且硬件将迫使低级固件按照已知和可测量的代码路径运行。

DRTM 负责测量和验证启动加载程序，并以受保护的方式收集和存储以下系统信息，以供操作系统进一步使用，包括用于进行验证和认证：

- 物理内存映射
- PCI 配置空间位置
- 本地 APIC 配置
- I/O APIC 配置
- IOMMU 配置/TMR 配置
- 电源管理配置

共享硬件可信度

这意味着，固件组件由 AMD 芯片上的 ASP 进行身份验证和测量，测量结果以受保护的方式存储，供操作系统进一步使用，包括用于进行验证和认证。

AMD SMM 监管器

系统管理模式 (SMM) 是 AMD x86 微控制器中的一种专用 CPU 模式，用于处理电源管理、硬件配置、散热监控和其他器件级操作。每当请求执行上述任一系统操作时，都会在运行时调用系统管理中断 (SMI)，以执行 BIOS 安装的 SMM 代码。SMM 代码以最高权限级别执行，对操作系统不可见，因此成为富有吸引力的攻击目标，恶意攻击者可能会利用 SMM 代码来访问管理程序内存并入侵管理程序。

SMI 处理程序可以访问操作系统/管理程序内存和资源，但通常与操作系统并不是由同一个开发商提供的。这意味着，如果 SMM 代码中的漏洞被利用，可能会导致 Windows 操作系统、管理程序 (HV) 和基于虚拟化的安全系统 (VBS) 遭受入侵。

为了帮助隔离 SMM，AMD 引入了一个名为“AMD SMM 监管器”的安全模块，该模块会在发生 SMI 后将控制权转移到 SMI 处理程序之前执行。AMD SMM 监管器位于 AMD DRTM 服务中，用途如下：

- 阻止 SMM 修改管理程序或操作系统内存，但两者之间的小型通信缓冲区除外
- 防止 SMM 在运行时引入新的 SMM 代码
- 阻止 SMM 访问可能会给管理程序或操作系统带来入侵风险的 DMA、I/O 或寄存器

DMA 保护

利用 DMA 重映射技术，AMD 平台通过输入输出内存管理单元 (IOMMU) 等 AMD 安全技术，在预启动和操作系统环境中提供直接内存访问 (DMA) 保护。

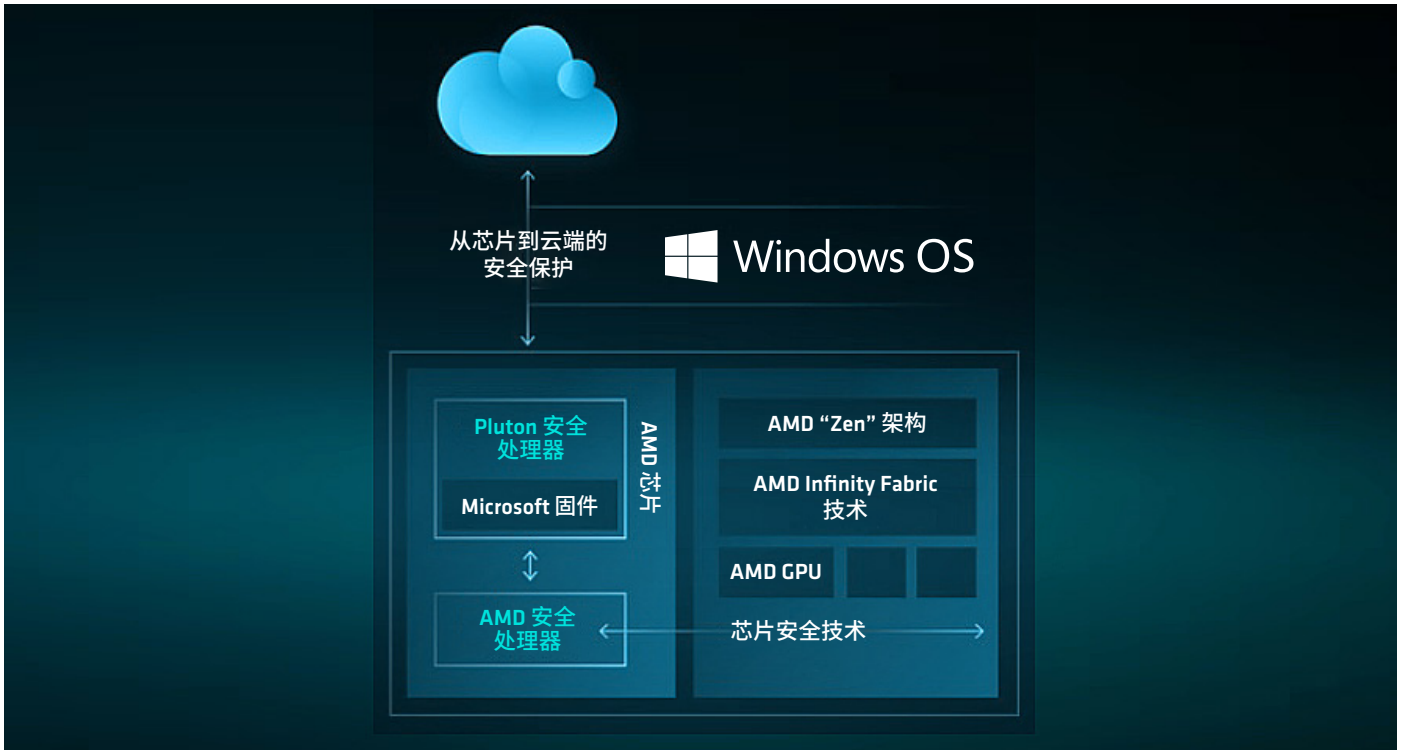
- DMA 保护有助于防御针对平台固件的潜在攻击，攻击者可能会使用连接的设备执行 DMA 攻击。
- DMA 支持设备直接访问物理内存地址空间，以此提高性能。然而，这也会使恶意攻击者更容易避开操作系统的检测，将恶意软件注入系统。

为帮助防止此类攻击，AMD 设计了一种安全架构，即在操作系统前面的固件级别通过 IOMMU 管理和控制设备的 DMA 访问。采用 DMA 安全架构，在内存中建立操作系统启动加载程序之后，系统内存保护责任便从固件转移到操作系统。每次启动时都会使用 IOMMU 进行 DMA 保护，直到操作系统控制 IOMMU 本身。

MICROSOFT PLUTON 安全处理器[8]

Microsoft Pluton 是一种内置于 CPU 中的安全加密处理器，由 Microsoft 设计，由芯片合作伙伴构建。该处理器以安全性为核心，旨在确保代码完整性，并利用 Microsoft 通过 Windows 更新助手提供的最新更新实现保护。

图 6. Microsoft Pluton 安全架构概览。



Pluton 可保护凭据、身份信息、个人数据和加密密钥。即使攻击者已安装恶意软件或实质上完全占有了电脑，想删除信息也依然很难。

Microsoft Pluton 可提供可信平台模块 (TPM) 功能，并带来可能超出 TPM 2.0 规范涵盖范围的其他安全功能。它可以通过 Windows 更新不断提供新的固件和操作系统功能。

AMD 安全处理器 2.0 (ASP 2.0) 和 Microsoft Pluton 安全处理器可在 AMD 客户端芯片上共存并相互协作，共同保障设备完整性。Microsoft Pluton 作为一种集成式硬件信任根，适用于 Windows 生态系统，可帮助保护 Windows PC 系统；ASP 2.0 则作为芯片硬件信任根，通过对平台上加载的初始固件进行身份验证来确保完整性。

平台更新

AMD PRO 处理器可提供强大的安全防御，实时阻止攻击者访问系统，而且还具有完善的更新机制。基于这种更新机制，组织能够不断更新平台，修补由硬件或软件缺陷引发的安全漏洞。

AMD 与 OEM 密切合作，提供了一种经过改进的平台更新架构，该架构符合行业最佳实践，而且可与 OEM 平台更新解决方案无缝集成。此外，AMD PRO 处理器可提供固件防回滚 (FAR) 功能，支持通过基于硬件的策略来阻止 AMD 安全处理器 2.0 (ASP 2.0) 固件降级。最后，AMD PRO 处理器还带来一种名为“A/B 恢复”的安全恢复框架，该框架可集成到 OEM 解决方案中，以便在发生灾难性故障时实现恢复。

加密加速器

在当今世界，加密操作对于保护数据和通信至关重要，但是这类操作会耗费大量计算资源。AMD 芯片采用经过优化的全新指令，可降低与加密算法计算相关的成本。

AMD “Zen 2” 及更新版本的架构支持 256 位矢量化 AES 加密 (vAES256)，并在 x86 级别集成了 AES 内部函数，能够为用户应用带来更出色的加密性能和效率。

FIPS 140-3 1 级认证

鉴于政府机构处理的数据及其提供的基本服务高度敏感，在政府 IT 部门采购笔记本电脑时，端点安全是首要的考量因素之一。由于缺乏现代安全功能，过旧的硬件可能会导致成本高昂的数据丢失和服务中断。

美国联邦信息处理标准 (FIPS) 是美国国家标准与技术研究院 (NIST) 制定的一系列公开标准，适用于非军事机构、美国政府机构和承包商所采用的计算机系统。FIPS 标准规定了计算机系统所需满足的安全性和互操作性要求。

AMD PRO 处理器包含 **FIPS 140-3 1 级**安全认证模块。

图 7. AMD 锐龙 PRO 7000 系列处理器的加密算法验证程序。

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

FIPS 模块由支持安全功能认证的硬件、软件和/或固件构成。虽然 FIPS 标准是为联邦政府机构制定的，但包括金融机构和云提供商在内的许多私营组织都自愿采用这些标准。此外，FIPS 标准的应用范围逐步扩展到北美以外地区，现涵盖面向欧洲北约伙伴国的计算机处理器。

云端裸机恢复

云端裸机恢复提供了一种远程恢复系统的安全机制，可充分减少停机时间，并在发生灾难性硬件或软件故障时保障业务连续性。此功能在操作系统启动之前激活，支持通过云端实现系统恢复，而无需寄送设备以进行维修。

云端裸机恢复功能已集成到 AMD PRO 安全性架构，能够在硬件级别提供强大初始化和恢复保障，从而防止在恢复过程中发生篡改或漏洞利用。

供应链安全（器件标识）

供应链安全功能基于 AMD 器件标识，可在从制造到部署及后续阶段的整个生命周期内对 AMD 硬件进行身份验证。此功能有助于保障可追溯性，防止硬件组件遭到假冒或篡改，从而帮助企业确保硬件完整性。

AMD 器件标识可用于对 AMD 正品芯片进行加密验证，确保只有经过验证的硬件才会集成到企业系统中。这有助于防御供应链攻击，避免固件或硬件在部署之前遭到侵害。

监控定时器 (WATCHDOG TIMER)

监控定时器可在硬件级别检测并处理停滞或无响应的进程，从而提高系统可靠性。此功能可提升系统容错能力，帮助系统在遇到问题时顺利恢复并保持正常运行。

监控定时器已集成到 AMD PRO 安全性架构，可与安全启动和其他基本功能配合使用，在预启动和运行时操作期间提供强有力的故障检测。这种检测能力可增强关键任务环境中的系统弹性，同时降低软件或硬件故障带来的停机风险。

解决方案亮点

安全层	功能特性	优点
系统	OEM 安全功能	操作系统开发商、硬件供应商和 OEM 合作伙伴之间深度合作，共同实现完善的 OEM 企业级安全功能。
操作系统安全功能	WINDOWS 11 安全功能	全面支持安全核心电脑计划、硬件强制堆栈保护、高级威胁防护、增强型安全登录、BitLocker 及更多安全功能。
硬件和固件	AMD 安全处理器 2.0	专用安全处理器会在执行代码之前验证代码，有助于确保数据和应用的完整性。
	AMD 平台安全启动	启动保护功能可防止未授权软件和恶意软件控制关键系统功能。
	AMD MEMORY GUARD	对系统内存进行实时加密，防止在笔记本电脑丢失或被盗后数据受到物理攻击。
	AMD SHADOW STACK	通过将正常程序堆栈与硬件存储的副本进行对比检查，并启用 Windows 11® 中的 Microsoft 硬件强制堆栈保护，有效防御控制流攻击，提供强大安全保障。
	MICROSOFT PLUTON 安全处理器	从芯片到云端的全面安全防护技术，由 Microsoft 设计并更新，旨在通过持续保护用户凭据、身份信息、个人数据和加密密钥来增强对 Windows 11 PC 的保护。
	AMD 固件 TPM	固件级 TPM，旨在为平台提供真实性保障，并帮助监控安全漏洞和攻击迹象。
	FIPS 140-3 1 级认证模块	私营部门采用政府加密标准来作为验证加密硬件安全性的最佳做法。
	AMD 安全处理器 2.0	内置硬件信任根，可验证初始固件并保护平台免受未经授权的代码执行攻击。
	云端裸机恢复	通过云端实现安全的系统恢复，而无需寄送设备，可在发生灾难性事件后充分缩短停机时间。

摘要

AMD PRO 技术提供了一种全面完备的解决方案，能够充分满足现代企业不断变化的需求。AMD 锐龙 PRO 处理器集高级安全功能、无缝可管理性功能和出色业务可靠性功能于一身，能够在多种办公环境中帮助组织保护数据、简化 IT 运营并提升生产力。

随着企业逐步采用混合办公模式并整合 AI 驱动的工作流程，AMD 一直致力于帮助企业推动创新。AMD PRO 技术在更新迭代的过程中不断突破限制，以更出色的安全性、性能和可管理性助力企业应对当今种种挑战，同时为迎接未来机遇做好准备。

免责声明

尾注

1. AMD 锐龙 PRO、AMD 锐龙 Threadripper PRO 和 AMD 速龙 PRO 处理器均支持通过 AMD Memory Guard 进行全系统内存加密。AMD Memory Guard 需要由原始设备制造商启用。购买前请咨询系统制造商。GD-206。
2. 原始设备制造商 (OEM) 启用 AMD 平台安全启动功能后，即授权其加密签名 BIOS 代码只能在其基于 AMD 平台安全启动主板的平台上运行。处理器中的一次性可编程熔断器会将处理器绑定到 OEM 的固件代码签名密钥。自此，该处理器只能与使用该代码签名密钥的主板一起使用。GD-192。
3. AMD PRO 可管理性技术通过部署更多 DASH Management Initiative 配置文件，为多供应商台式和移动系统管理提供强大助力。KRKP-7
4. AMD PRO 可管理性技术采用较新版本的 TLS（传输层安全）协议，即 TLS 1.3，与采用 TLS 1.2 相比可提供更高的安全性和更低的延迟。KRKP-8
5. Principled Tech 报告 - https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. AMD 安全处理器是片上专用安全处理器，集成于 AMD 系统级芯片 (SoC) 和 ASIC（应用特定集成电路）之中。处理器硬件内置信任根以实现安全启动，通过安全启动流程初始化 SoC，并建立隔离的可信执行环境。GD-72。
7. AMD 锐龙 PRO、AMD 锐龙 Threadripper PRO 和 AMD 速龙 PRO 处理器均支持通过 AMD Memory Guard 进行全系统内存加密。需要原始设备制造商启用。购买前请咨询系统制造商。GD-206
8. Microsoft Pluton 是 Microsoft 拥有并授权 AMD 使用的技术。Microsoft Pluton 是 Microsoft Corporation 在美国和/或其他国家/地区的注册商标。要了解更多信息，请访问 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 安全处理器需要原始设备制造商启用。购买前请咨询原始设备制造商。AMD 尚未验证第三方声明。GD-202。
9. AMD 安全处理器是片上专用安全处理器，集成于 AMD 系统级芯片 (SoC) 和 ASIC（应用特定集成电路）之中。处理器硬件内置信任根以实现安全启动，通过安全启动流程初始化 SoC，并建立隔离的可信执行环境。GD-72。