AMD PRO TECHNOLOGIEN

EIN BLICK AUF AMD PRO SECURITY UND DAS AMD FRAMEWORK FÜR SICHERE, VERWALTBARE UND ZUVERLÄSSIGE BUSINESS-PCs

Der flexible, dezentrale Arbeitsplatz entwickelt sich immer weiter. Hybride Abläufe werden zur Norm und Unternehmen suchen ein ausgewogenes Verhältnis aus Zusammenarbeit im Büro und im Homeoffice, während zugleich KI in die täglichen Workflows integriert wird. Unternehmen stehen unter Druck, ihre PC-Flotten mit Systemen zu aktualisieren, die den neuen Herausforderungen, die sich aus diesen Trends ergeben, gerecht werden. Sie benötigen Lösungen, die ein Gleichgewicht zwischen Performance, Sicherheit und Manageability herstellen und sich gleichzeitig sowohl an On-Premises- als auch Cloud-basierte Umgebungen anpassen lassen.

AMD Ryzen™ PRO Prozessoren unterstützen moderne Business-PCs mit AMD PRO Technologien, einem vereinheitlichten Satz von Innovationen, um die sich ändernden Anforderungen der Unternehmen von heute zu erfüllen. In diesem Whitepaper wird die Säule der Sicherheit von AMD PRO Technologien erläutert, eine der drei grundlegenden Komponenten, die Bestandteil aller Systeme mit AMD Ryzen PRO Prozessor sind. Auch wenn Sicherheit der primäre Fokus dieses Whitepapers ist, beinhalten AMD PRO Technologien auch erweiterte Manageability und Business-Ready-Zuverlässigkeit, die zusammen eine umfassende Lösung für moderne Unternehmen bereitstellen.

Die drei Säulen werden hier kurz vorgestellt, um den Kontext für AMD PRO Technologien als Ganzes herzustellen. Dieses Whitepaper geht jedoch spezifisch auf die Sicherheitsfunktionen der nächsten Dimension der AMD Ryzen PRO Prozessoren ein, die darauf ausgelegt sind, die Business-PCs von heute vor sich entwickelnden Bedrohungen zu schützen.

PRO SECURITY: SCHUTZ FÜR DAS MODERNE UNTERNEHMEN

Eckpfeiler der AMD PRO Technologien sind stabile Sicherheitsfunktionen. Erweiterte Hardwarefunktionen, wie AMD Memory Guard[1] für eine vollständige Speicherverschlüsselung, AMD Shadow Stack zum Schutz vor Control-Flow-Angriffen und umfassende Unterstützung für den sicheren Krypto-Prozessor Microsoft Pluton bieten wichtige Schutzmaßnahmen gegen ausgeklügelte Bedrohungen. Mit integrierter Unterstützung für Secure Boot[2] und vertrauenswürdige Ausführung stärken AMD Ryzen PRO Prozessoren Geräte auf jeder Ebene und bieten vom Endpunkt bis zur Cloud Schutz für Benutzerdaten und Anwendungen.

Obwohl die modernen Sicherheitsfunktionen im Zentrum dieses Whitepapers stehen, arbeitet das weitere Framework der AMD PRO Technologien – einschließlich Manageability und Business-Ready-Zuverlässigkeit – zusammen, um Unternehmen eine vollständige Lösung für neue Anforderungen am Arbeitsplatz zu bieten.

PRO MANAGEABILITY: VEREINFACHTE IT-ABLÄUFE

Die Verwaltung verschiedener PC-Flotten ist komplex und zeitintensiv, insbesondere in hybriden Arbeitsumgebungen. AMD PRO Manageability optimiert Abläufe und auf offenen Standards basierende Tools, die Cloud-basierte Remote-Verwaltung und Endpunktüberwachung in Echtzeit ermöglichen. Diese Tools bieten ein Höchstmaß an Compliance mit offenen Standards für die Verwaltung von Remote-Systemen.[3] AMD PRO Manageability ermöglicht dem Benutzer die Kompatibilität mit branchenführenden Tools wie Microsoft Endpoint Manager und Windows Autopilot für einen konsistenten und effizienten Bereitstellungsprozess.

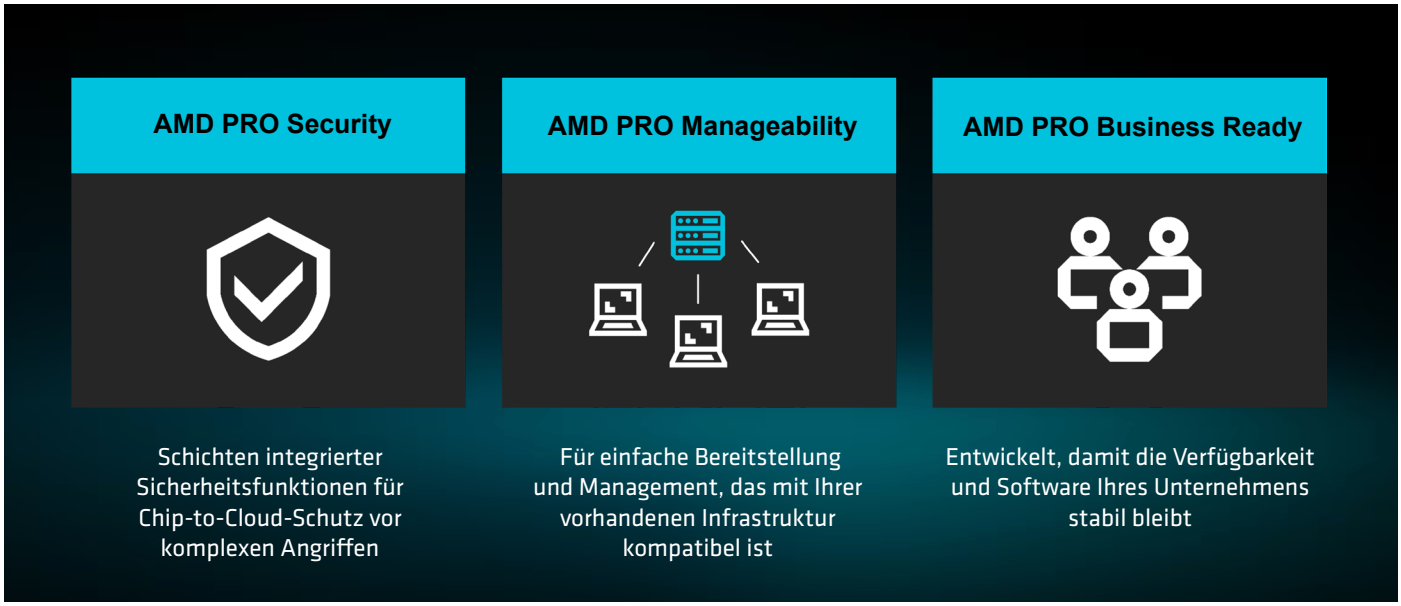
AMD PRO Manageability unterstützt die neuesten Spezifikationen von DMTF DASH (Desktop and Mobile Architecture for System Hardware, Desktop- und mobile Architektur für Systemhardware), die aktuelle Verschlüsselungs- und Authentifizierungsprotokolle wie TLS 1.2 und 1.3 beinhalten. Zudem integrieren AMD PRO Systeme hardwarebasierte Sicherheitskomponenten, einschließlich TPM 2.0, um die Speicherung und den Schutz kryptografischer Schlüssel sicherer zu gestalten. Dieser auf Standards basierende Ansatz liefert einen stärkeren Schutz und eine bessere Performance im Vergleich zu älteren, proprietären Protokollen.[4] IT-Teams profitieren von Funktionen wie Remote-Provisioning, automatisierter Patch-Bereitstellung und Echtzeitdiagnosen, die alle für kürzere Ausfallzeiten, einen besseren Endpunktzustand und einfachere Abläufe sorgen.

Aktuelle Studien heben die Auswirkungen der AMD PRO Manageability auf IT-Abläufe hervor und zeigen, dass die Bereitstellungszeiten im Vergleich zu herkömmlichen Prozessen um bis zu 41 % reduziert wurden[5] und der manuelle Arbeitsaufwand dank vereinheitlichter, intuitiver Verwaltungsschnittstellen deutlich gesenkt wurde. Dank dieser Fähigkeiten können Unternehmen Mitarbeiter genau dort unterstützen, wo sie gerade arbeiten, wodurch komplexe PC-Ökosysteme in der Verwaltung einfacher, schneller und zuverlässiger werden.

PRO BUSINESS READY: AUSSERGEWÖHNLICHE PERFORMANCE FÜR JEDE AUFGABE

AMD PRO Prozessoren mit Business-Ready-Funktionen bieten Benutzern PC-Langlebigkeit, konsistente Performance und Zuverlässigkeit für Unternehmensauslastungen. Strenge Validierungsprozesse unterstützen eine bessere Verfügbarkeit, wodurch die IT-Kosten reduziert werden können. Die erweiterte weltweite Verfügbarkeit über ein ganzes Jahr ermöglicht es Unternehmen, Systeme bei Bedarf bereitzustellen und so große Anschaffungen im Vorfeld zu minimieren. Egal, ob Unterstützung für KI-gestützte Anwendungen oder tägliche Büroaufgaben, AMD Ryzen™ PRO Prozessoren bieten die Anpassbarkeit, die Unternehmen für ihr Wachstum benötigen.

Abbildung 1. AMD PRO Technologien. Für jeden mit AMD Ryzen™ PRO Prozessor betriebenen Business-PC.



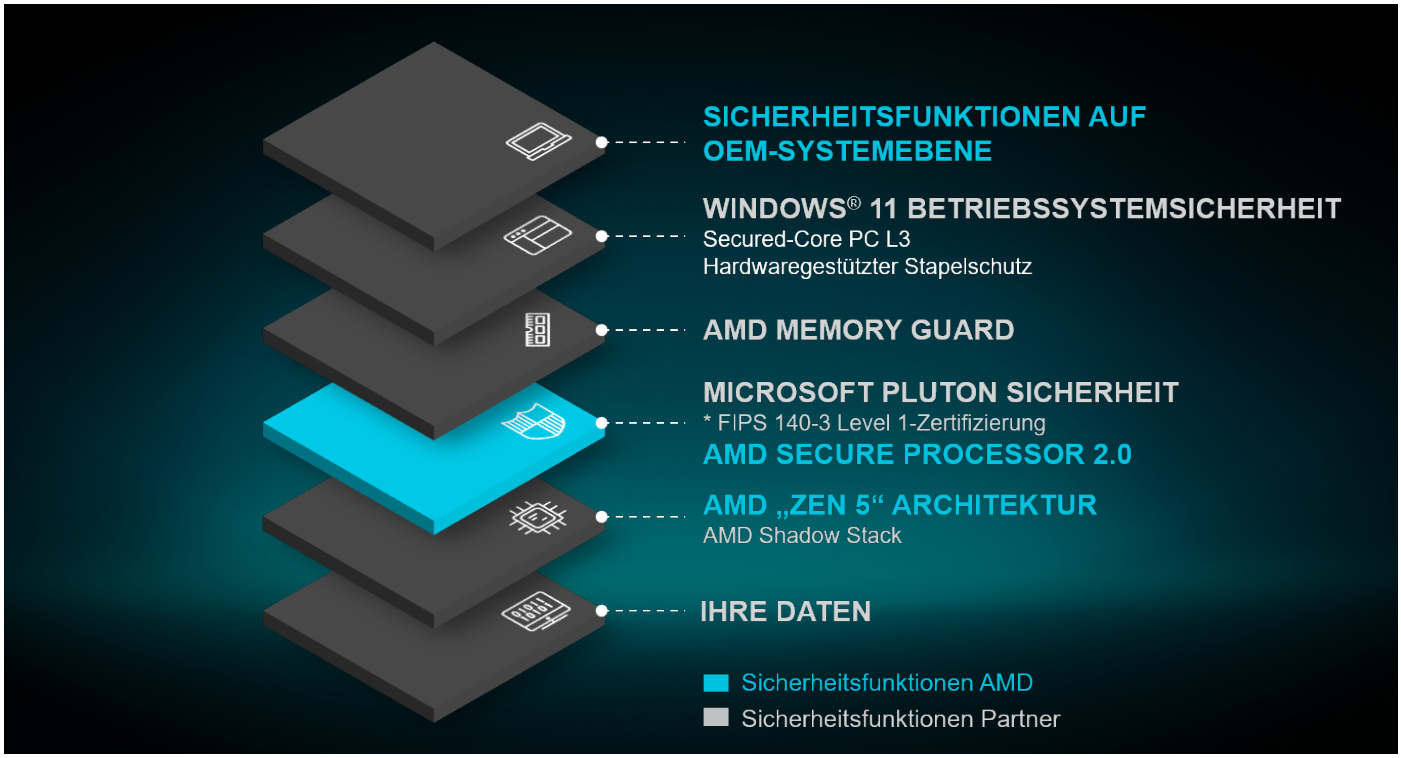
Die AMD PRO Business-Ready-Technologien erweitern diese Zuverlässigkeit, indem sie langfristige Konsistenz bereitstellen, die die IT-Planung vereinfacht und die Investitionsrentabilität maximiert. Alle AMD Ryzen™ PRO Prozessoren liefern Lösungen der Enterprise-Klasse mit:

- **Image-Stabilität:** 18 Monate geplante Softwarestabilität für flüssige Übergänge und Sicherheit für IT-Teams.
- **Qualität:** Erweiterte Plattformvalidierungsprozesse, die Qualität der Enterprise-Klasse für anspruchsvolle Unternehmensumgebungen bereitstellen.
- **Verfügbarkeit:** 24 Monate geplante Verfügbarkeit, um Hardwarekonsistenz für stabile Unternehmensabläufe aufrechtzuerhalten.
- **Zuverlässigkeit:** Kontinuierliche Plattformvalidierung für langfristige Stabilität und ein einheitliches Benutzererlebnis über mehrere Prozessorgenerationen hinweg.

Durch die Bereitstellung von Stabilität über Hardware und Software hinweg reduziert AMD PRO Business Ready die Komplexität für IT-Teams und bietet eine verlässliche Grundlage für langfristigen Unternehmenserfolg.

Für Unternehmen, die sich mit der Komplexität der Unterstützung des modernen Arbeitsplatzes auseinandersetzen müssen, bieten die AMD PRO Technologien einen entscheidenden Vorteil. Durch die Integration hochmoderner Sicherheitsfunktionen, effizienter Manageability und Business-Ready-Funktionen in jedes System mit einer AMD Ryzen PRO CPU stellt AMD Organisationen die Tools bereit, die sie benötigen, um ihre Abläufe zu schützen, die IT-Verwaltung zu optimieren und die Innovation voranzubringen.

Abbildung 2. AMD PRO Security. Neueste Sicherheitsanforderungen werden bei modernen Geräten übertroffen.



AMD PCs SIND MIT HOCHMODERNER MEHRSCHICHTIGER SICHERHEIT AUF ALLEN EBENEN KONZIPIERT

AMD arbeitet eng mit den Entwicklern von Betriebssystemen und OEMs an Sicherheitsfunktionen für Hardware zusammen, die ihr Sicherheitskonzept ergänzen und stärken.

Durch die Integration hochmoderner Sicherheitsfunktionen auf jeder Ebene, vom Chip bis zu den Betriebssystemen, ermöglicht es AMD den Organisationen, ihre wichtigsten Assets zu schützen und gleichzeitig die Ausfallzeiten zu minimieren und die IT-Komplexität zu reduzieren.

SICHERHEIT AUF JEDER EBENE

AMD PRO Technologien integrieren Sicherheit als grundlegende Säule in allen Geräten mit AMD Ryzen™ PRO Prozessoren. Konzipiert für sich entwickelnde Herausforderungen des modernen Unternehmens liefern diese Prozessoren mehrschichtigen Schutz, der mit einer stabilen Chipbasis beginnt und sich auf Firmware und Schutzmaßnahmen auf Betriebssystemebene erstreckt.

HARDWARE-VERTRAUENSANKER: INTEGRITÄT VON ANFANG AN

Die Chiparchitektur von AMD bietet einen integrierten Hardware-Vertrauensanker, mit dem Secure-Boot-Prozesse unterstützt werden. Der AMD Secure Processor 2.0[6] (ASP 2.0) festigt dieses Vertrauen, indem die Firmware und die OEM-BIOS-Integrität verifiziert werden, um vor unberechtigten Änderungen und potenziellen Firmwareangriffen zu schützen.

SPEICHERSCHUTZ NEU DEFINIERT: AMD MEMORY GUARD[7]

AMD Memory Guard verschlüsselt den gesamten Systemspeicher in Echtzeit und schützt so sensible Daten vor Kaltstart- und physischen Angriffen. Mit dedizierten Hardwareverschlüsselungs-Engines stellt diese Funktion eine stabile Verteidigung auch bei Gerätediebstahl bereit.

ARCHITEKTUR DER NÄCHSTEN GENERATION: AMD „ZEN 5“ UND DARÜBER HINAUS

Die neueste AMD „Zen 5“ Kernarchitektur führt erweiterte Sicherheitsfunktionen ein, einschließlich Supply Chain Security, die eine eindeutige Prozessor-ID nutzt, um eine sichere Verfolgung der AMD Originalhardware während ihres gesamten Lebenszyklus zu ermöglichen. Diese Innovationen stärken die Endpunktresilienz vor immer raffinierteren Cyberbedrohungen.

ABGESTIMMT AUF BRANCHENSTANDARDS

AMD PRO Prozessoren sind darauf ausgelegt, moderne Sicherheitsanforderungen, einschließlich FIPS 140-3 Stufe 1 Zertifizierung, zu übertreffen. Die Integration in Microsoft Pluton[8] verbessert den Schutz für Windows-basierte Systeme noch weiter, indem sichere Authentifizierung und kryptografischer Schutz hinzugefügt werden.

DIE AMD PRO SECURITY ARCHITEKTUR

AMD SECURE PROCESSOR 2.0:[9] EINE STÄRKERE BASIS

Im Zentrum der AMD PRO Security Architektur steht der AMD Secure Processor 2.0 (ASP 2.0). Hierbei handelt es sich um eine dedizierte Hardwarekomponente, die in jedes System-on-Chip (SoC) integriert ist. ASP 2.0 festigt einen Hardware-Vertrauensanker und unterstützt einen Secure-Boot-Vorgang, indem die Firmwareintegrität von dem Moment an geprüft wird, in dem ein Gerät eingeschaltet wird. Durch die isolierte vertrauenswürdige Ausführungsumgebung werden sensible Vorgänge vor potenziellen Angriffen geschützt. Zu den Hauptkomponenten gehören Folgende:

- **Kryptografischer Co-Prozessor (KCP):** Eine kryptografische High-Performance-Engine zur Verwaltung der Schlüsselgenerierung und kryptografischer Vorgänge in der Hardware, wesentlich für zeitkritische Sicherheitsaufgaben.
- **Boot-ROM:** Sicherer schreibgeschützter Speicher mit kritischer Firmware für die Boot-Initialisierung.
- **Static Random-Access Memory (SRAM):** Bietet Low-Power-Support für sichere Prozesse.
- **Memory Management Unit (MMU):** Regelt den Zugriff auf Boot-ROM und SRAM für die strikte Steuerung der Speicherressourcen.
- **Cloud Bare Metal Recovery:** Vereinfacht die sichere Wiederherstellung von Geräten über die Cloud und gewährleistet die Geschäftskontinuität auch in Szenarien mit katastrophalen Ausfällen.
- **Supply Chain Security:** Authentifiziert AMD Originalhardware in jeder Stufe des Lebenszyklus und schützt so vor Manipulationen oder gefälschten Komponenten.
- **Watchdog-Timer:** Schützt und mildert blockierte Prozesse auf Hardwareebene ab und verbessert so die Widerstandsfähigkeit des Systems.

Gemeinsam gehen diese Funktionen auf das erhöhte Risiko der Offenlegung sensibler Geschäftsdaten bei Reisen, im Homeoffice oder in anderen mobilen Szenarien ein.

NAHTLOSE INTEGRATION IN WINDOWS SICHERHEIT

Die AMD PRO Security Architektur fügt sich nahtlos in die Windows 11 Sicherheitsfunktionen ein, wie z. B. Secure Boot und Hardware Enforced Stack Protection, und schafft so ein umfassendes, mehrschichtiges Schutzsystem. Gemeinsam schützen sie Endpunkte vor Angriffen auf Firmware, BIOS, Treiber und das Betriebssystem.

AMD ROM ARMOR

Der SPI-Flash-Speicher (Serial Peripheral Interconnect) eines Mainboards enthält sowohl die Mainboard-UEFI als auch zusätzliche Konfigurationsinformationen, einschließlich des Status von Secure Boot.

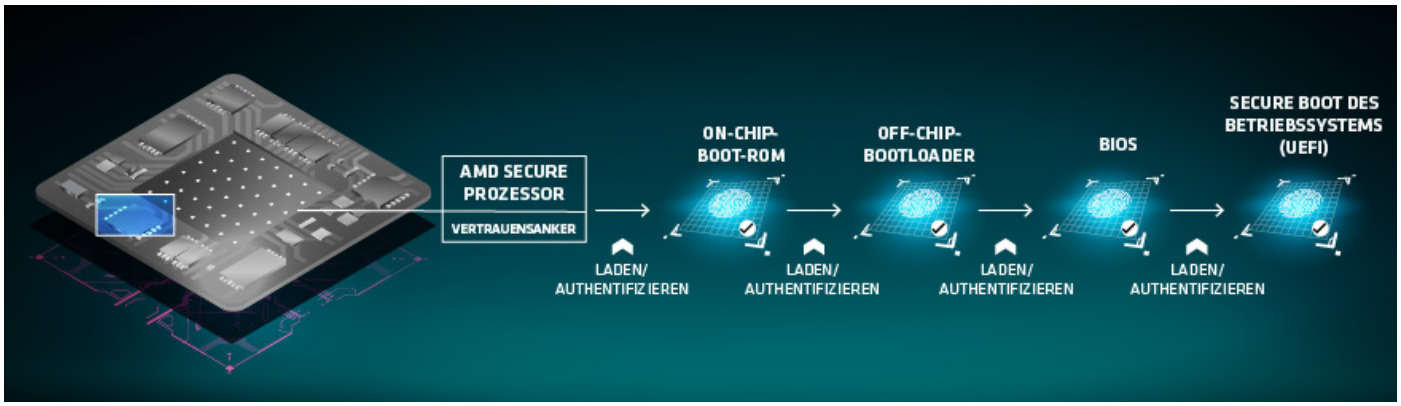
AMD ROM Armor arbeitet, bevor das Betriebssystem initialisiert wurde, und bietet Schutz vor unberechtigten Änderungen am SPI-Flash. Indem die Integrität des SPI-Flashs sichergestellt wird, bevor das Betriebssystem lädt, trägt AMD ROM Armor dazu bei, eine solide Grundlage für das System zu schaffen. Sobald AMD ROM Armor konfiguriert und aktiviert ist, wird das SPI-Flash-Gerät des Computers vor unberechtigten Schreibvorgängen geschützt.

AMD PLATFORM SECURE BOOT (PSB)

AMD Platform Secure Boot (PSB) stellt einen Hardware-Vertrauensanker bereit, der die anfängliche Firmware einschließlich des BIOS während des Bootvorgangs des Geräts authentifiziert. Wenn das System angeschaltet wird, führt ASP den ASP Boot-ROM-Code aus, der die verschiedenen ASP Bootloader-Codes authentifiziert, ehe Chip und Systemspeicher initialisiert werden. Nachdem der Systemspeicher initialisiert ist, verifiziert der ASP Bootloader-Code den OEM-BIOS-Code, wodurch andere Firmwarekomponenten vor dem Booten des Betriebssystems authentifiziert werden.

PSB ist darauf ausgelegt, die Plattformintegrität durch einen stärkeren Schutz vor bösartiger Firmware sicherzustellen, der automatisch nach Erkennung der Zugriff verweigert wird. AMD PSB hilft, den Übergang von Firmware auf niedriger Ebene zum Betriebssystem zu schützen.

Abbildung 3. AMD Platform Secure Boot.



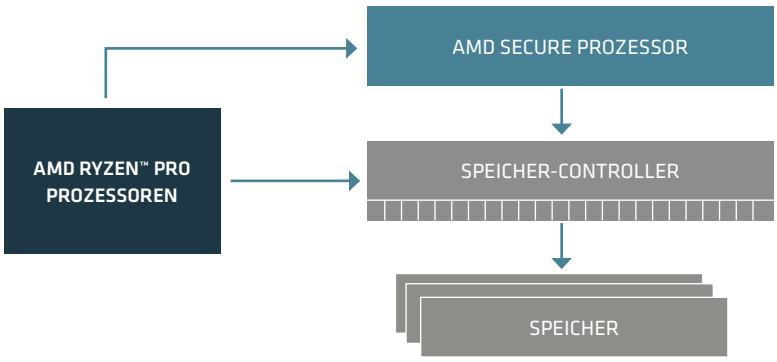
AMD MEMORY GUARD[3]

AMD Memory Guard ist eine umfassende Speicherverschlüsselungstechnologie, um Kundendaten vor physischen Angriffen zu schützen. AMD Memory Guard verschlüsselt alle DRAM-Inhalte mithilfe eines zufälligen Schlüssels. Das hilft, physische Kaltstartangriffe, DRAM-Schnittstellen-Snooping und ähnliche Angriffe abzuwehren.

Bei Systemen mit NVDIMMs hilft AMD Memory Guard außerdem beim Schutz gegen einen Angreifer, der ein Speichermodul entfernt und versucht, dessen Inhalte zu extrahieren, und wird über eine spezielle Hardware in den On-Die-Speicher-Controllern implementiert.

- Jeder Controller beinhaltet eine High-Performance-Engine mit Advanced Encryption Standard (AES), das die Daten beim Schreiben in den DRAM verschlüsselt und sie beim Auslesen wieder entschlüsselt.
- Ein 128-Bit-Schlüssel wird von einem mit On-Die NIST SP 800-90-kompatiblen Hardware-Zufallszahlengenerator generiert. Das geschieht in einem Modus, der einen zusätzlichen, auf der physischen Adresse basierenden Kniff nutzt, was dem Schutz gegen Cipher-Text-Block-Move-Angriffe dient.
- Der von der AES-Engine mit AMD Memory Guard verwendete Verschlüsselungscode wird nach jedem Zurücksetzen des Systems zufällig erstellt und ist in keiner Software sichtbar, die auf den CPU-Kernen ausgeführt wird. Dieser Schlüssel wird vollständig vom AMD Secure Processor (ASP) verwaltet.

Abbildung 4. AMD Memory Guard.



AMD SHADOW STACK

Return-Oriented Programming (ROP) ist ein zunehmend beliebter Angriffsvektor. ROP-Angriffe fügen nicht ihren eigenen Schadcode ein. Stattdessen versuchen sie, die Kontrolle über ein System zu erlangen, indem sie die Schwachstellen des legitimen Codes ausnutzen.

WIE FUNKTIONIERT DAS?

Bei der Programmierung von Computern führt eine „Routine“ ein bestimmtes Paket an Prozessen aus. Wird ein Softwareprogramm ausgeführt, wird das als Routine bezeichnet. Wenn eine Routine dann ihre Aufgabe ausführt, leitet sie eine Ausgabe an die Absenderadresse des Programms weiter. Dieser Prozess wird „jump and return“ genannt.

Bei ROP-Angriffen verändern Angreifer die Absenderadresse der Jump-Routine. Statt also zum Hauptprogramm zurückzukehren, springt sie zu anderen Routinen. Dabei werden Unterroutinen so zusammengesetzt, dass sie schädlichen Code ergeben, mit dem nun das System geschädigt werden kann. Entscheidend ist dabei, dass diese Art von Angriff unerkannt bleibt, da sie wie legitimer Code aussieht.

Die AMD PRO Security Architektur hilft beim Schutz gegen ROP-Angriffe, denn sie bietet der Software spezielle Register in der CPU, in der eine Kopie der Absenderadresse gespeichert werden kann. Anwendungen können einen parallelen Stack nutzen, den sogenannten „Shadow Stack". Damit lassen sich Softwareangriffe abwehren, die den Steuerungsablauf zu ändern versuchen. Der Shadow Stack nutzt spezielle Hardware, um eine Kopie der Absenderadressen zu speichern. Diese kann nun verwendet werden, um den normalen Programm-Stack nach Abschluss eines Prozesses zu überprüfen.

Weicht der Inhalt ab, wird eine Ausnahme generiert, die dazu beitragen kann, den Schadcode daran zu hindern, die Kontrolle über das System zu übernehmen. So hilft die Shadow-Stack-Hardware bei der Abwehr der gängigsten und gut ausnutzbaren Software-Bugs.

AMD Shadow Stack bietet robuste Abwehrmöglichkeiten gegen ROP-Angriffe. Da sich eine Kopie der Absenderadresse in der Hardware befindet, ist es für den Schadcode sehr schwer, diese zu manipulieren.

Microsoft Hardware Enforced Stack Protection wird mithilfe von AMD Shadow Stack auf der AMD PRO Security Architektur unterstützt.

MICROSOFT SECURED-CORE PC

Microsoft Secured-Core PC schützt Geräte vor Firmwareschwachstellen, sichert das Betriebssystem gegen Angriffe ab und kann unbefugten Zugriff auf Geräte und Daten mit fortschrittlichen Zugangskontrollen und Authentifizierungssystemen verhindern.

Secured-Core PC ist mithilfe verschiedener Sicherheitstechnologien und -dienste auf AMD PRO Security Architekturplattformen aktiviert:

- AMD-V™ mit 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
- Schutz durch Speicherdirektzugriff (DMA, Direct Memory Access)

AMD VIRTUALIZATION (AMD-V™) TECHNOLOGIE MIT GMET

AMD-V umfasst eine Reihe von Hardwareerweiterungen, die Virtualisierung auf AMD Plattformen ermöglichen. Guest Mode Execute Trap (GMET) ist eine Performance-Erweiterung auf Chipebene. Mit ihrer Hilfe kann der Hypervisor effizient die Codeintegrität handhaben. Das trägt zum Schutz gegen Malware bei.

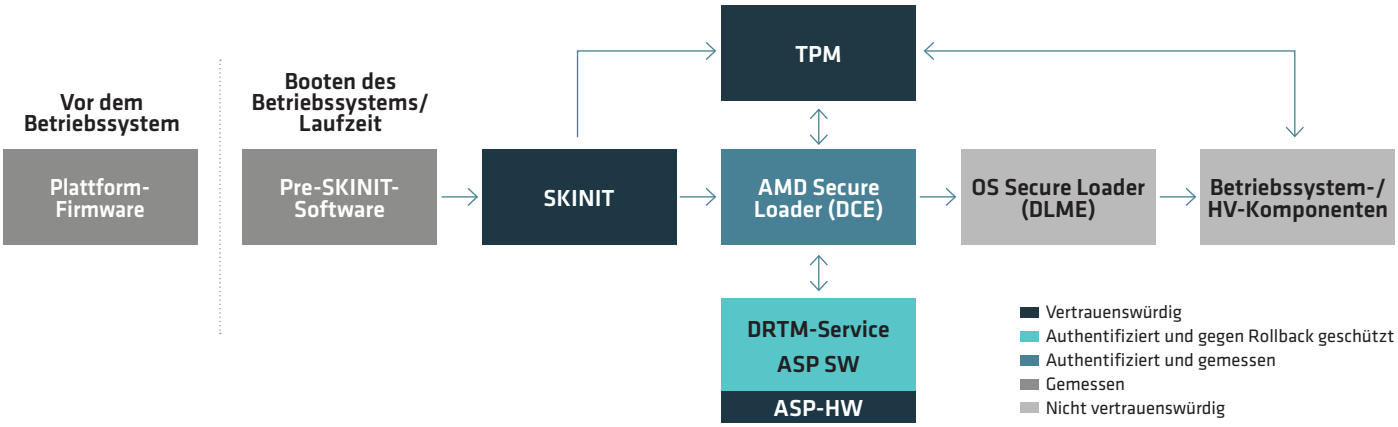
SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

Die SKINIT-Anweisung erstellt einen „Vertrauensanker“ beim Start in einem zunächst nicht vertrauenswürdigen Betriebsmodus. SKINIT reinitialisiert den Prozessor, sodass er eine gehärtete Ausführungsumgebung für Softwarekomponenten namens Secure Loader (SL) einrichtet. Dann beginnt die Ausführung des SL, die vor Manipulation schützt. SKINIT erweitert den hardwarebasierten Vertrauensanker auf den Secure Loader.

AMD SECURE LOADER (SL)

Der AMD Secure Loader ist für die Validierung der Plattformkonfiguration verantwortlich. Dazu wird die Hardware befragt, und es werden Konfigurationsinformationen vom DRMT-Dienst abgefragt, die der AMD Secure Processor bereitstellt.

Abbildung 5. DRTM-Ablauf.



An jedem Punkt, nachdem das System das Betriebssystem gebootet hat, kann Letzteres den AMD Service Block anweisen, die Werte neu zu messen und zu attestieren, ehe weitere Prozesse ausgeführt werden. Damit kann das Betriebssystem die Integrität des Systems vom Booten bis zur Laufzeit schützen.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

Der AMD DRTM-Block besteht aus der SKINIT CPU-Anweisung, ASP und SL. Dieser Block ist dafür verantwortlich, die Vertrauenskette zur Firmware zu erstellen und aufrechtzuerhalten. AMD DRTM arbeitet nach einem Konzept, bei dem die Firmware und der Bootloader unter der Annahme frei laden können, dass sie ungeschützter Code sind und dass das System kurz nach dem Start in einen vertrauenswürdigen Status wechselt, bei dem die Hardware die Firmware auf niedriger Ebene zwingt, einen vertrauten und gemessenen Codepfad zu nehmen.

Der AMD DRTM-Block besteht aus der SKINIT CPU-Anweisung, ASP und SL. Dieser Block ist dafür verantwortlich, die Vertrauenskette zur Firmware zu erstellen und aufrechtzuerhalten.

AMD DRTM arbeitet nach einem Konzept, bei dem die Firmware und der Bootloader unter der Annahme frei laden können, dass sie ungeschützter Code sind und dass das System kurz nach dem Start in einen vertrauenswürdigen Status wechselt, bei dem die Hardware die Firmware auf niedriger Ebene zwingt, einen vertrauten und gemessenen Codepfad zu nehmen.

Der DRTM-Block misst und authentifiziert den Bootloader und sammelt und speichert außerdem die folgenden Systeminformationen auf geschützte Weise. Sie werden dann weiter vom Betriebssystem u. a. zur Verifizierung und Attestierung verwendet.

- Physisches Speicherabbild
- Zuweisen des PCI-Konfigurationsraums
- Lokale APIC-Konfiguration
- E/A-APIC-Konfiguration
- IOMMU-Konfiguration/TMR-Konfiguration
- Energieverwaltungskonfiguration

GETEILTE HARDWAREVERLÄSSLICHKEIT

Das bedeutet, dass die Firmwarekomponente vom ASP-Block auf dem AMD Chip authentifiziert und gemessen wird. Die Messung wird auf geschützte Weise gespeichert und kann dann vom Betriebssystem u. a. zur Verifizierung und Attestierung weiterverwendet werden.

AMD SMM SUPERVISOR

System Management Mode (SMM) ist ein besonderer CPU-Modus in x86-Mikro-Controllern, der Energieverwaltung, Hardwarekonfiguration, thermische Überwachung und alle anderen Vorgänge auf Geräteebene handhabt. Bei einer Anforderung eines dieser Systemprozesse wird eine Unterbrechung (SMI) in der Laufzeit veranlasst, bei der der vom BIOS installierte SMM-Code ausgeführt wird. Der SMM-Code wird dabei auf höchster Rechteebene ausgeführt und ist für das Betriebssystem unsichtbar. Das macht ihn zu einem attraktiven Ziel für schädliche Aktivitäten, die potenziell für den Zugang zum Hypervisor-Speicher und die Veränderung des Hypervisors genutzt werden können.

Der SMI-Handler wird normalerweise von einem anderen Entwickler als dem des Betriebssystems bereitgestellt und hat Zugriff auf den Speicher von Betriebssystem/Hypervisor und die Ressourcen. Das bedeutet, dass ausnutzbare Schwachstellen im SMM-Code zu Beeinträchtigungen des Windows Betriebssystems, Hypervisors (HV) und der auf Virtualisierung basierenden Sicherheit (VBS – Virtualization-Based Security) führen können.

Damit der SMM isoliert werden kann, hat AMD das Sicherheitsmodul AMD SMM Supervisor entwickelt. Es wird unmittelbar vor der Übergabe der Steuerung an den SMI-Handler ausgeführt, nachdem ein SMI aufgetreten ist. Der AMD SMM Supervisor befindet sich im AMD DRTM-Serviceblock und wird verwendet, um …

- den SMM zu blockieren, sodass dieser den Speicher von Hypervisor und Betriebssystem nicht verändern kann, mit Ausnahme eines kleinen Kommunikationspuffers zwischen den beiden
- zu verhindern, dass der SMM neuen SMM-Code während der Laufzeit einfügen kann
- den SMM beim Zugriff auf DMA, E/A oder Register zu blockieren, die zu einer Kompromittierung von Hypervisor oder Betriebssystem führen können

DMA-SCHUTZ

Mit der DMA-Remapping-Technologie unterstützen AMD Plattformen Direct Memory Access (DMA) Schutz in Umgebungen vor dem Booten und mit dem Betriebssystem über AMD Secure Technologien wie Input Output Memory Management Unit (IOMMU).

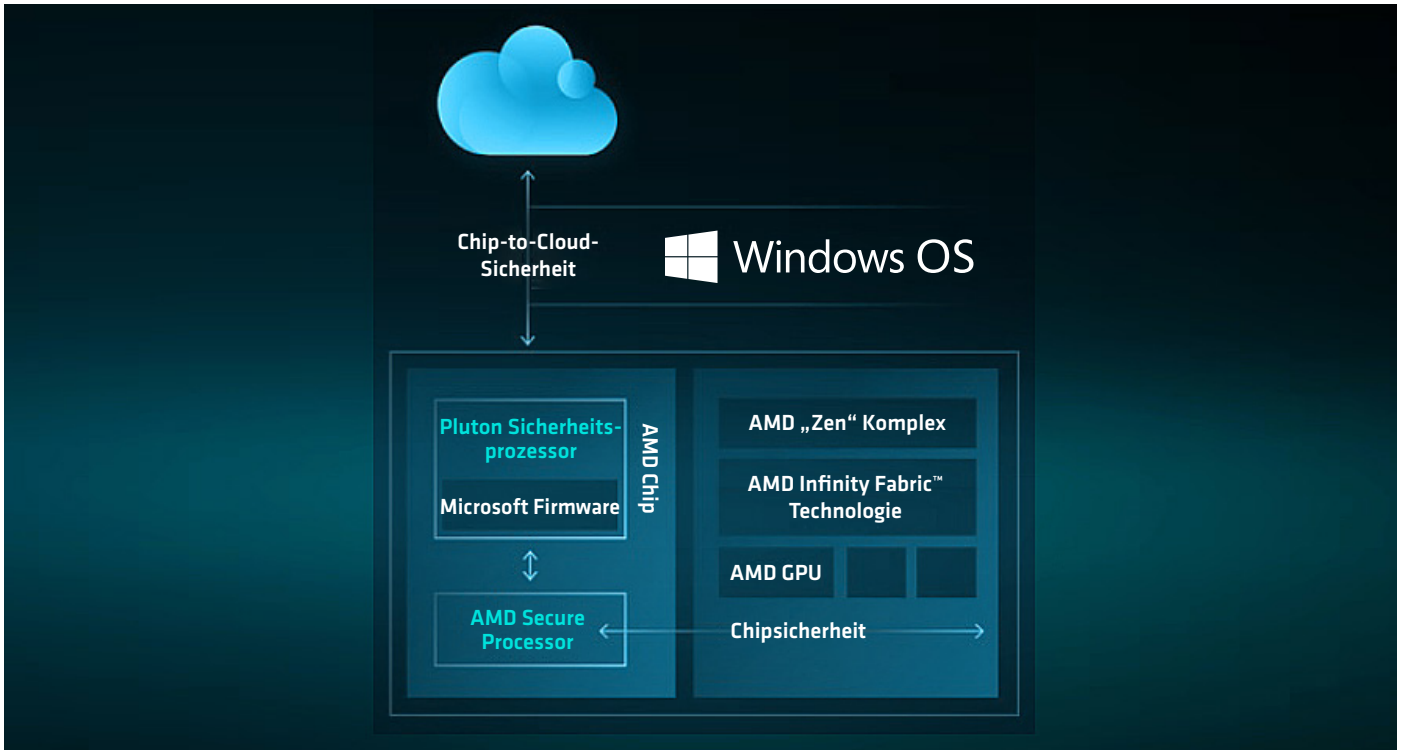
- DMA-Schutz hilft beim Schützen gegen mögliche Angriffe auf die Plattformfirmware, bei der Angreifer verbundene Geräte zur Durchführung von DMA-Angriffen nutzen können.
- DMA bietet Geräten direkten Zugang zum physischen Adressraum des Speichers für bessere Performance. Das erleichtert es der Schadsoftware allerdings auch, Malware ins System einzuschleusen, die das Betriebssystem möglicherweise nicht erkennt.

Um solche Angriffe zu verhindern, hat AMD eine Sicherheitsarchitektur entwickelt. Sie hilft bei der Verwaltung und Steuerung des DMA-Zugriffs durch Geräte über die IOMMU auf Ebene der Firmware vor dem Betriebssystem. Die DMA-Sicherheitsarchitektur übergibt die Verantwortung für die Einstellungen zum Schutz des Systemspeichers von der Firmware zum Betriebssystem, nachdem der Bootloader des Betriebssystems im Speicher eingerichtet wurde. Der DMA-Schutz mithilfe der IOMMU wird bei jedem Booten angewandt, bis das Betriebssystem selbst die Kontrolle über die IOMMU übernimmt.

MICROSOFT PLUTON SICHERHEITSPROZESSOR[8]

Microsoft Pluton wurde von Microsoft konzipiert, von Chippartnern gebaut und ist ein sicherer in die CPU integrierter Kryptografieprozessor für Sicherheit im Kern, um die Integrität des Codes und den neuesten Schutz durch die von Microsoft in Windows Update bereitgestellten Updates zu bestätigen.

Abbildung 6. Überblick über die Microsoft Pluton Sicherheitsarchitektur.



Pluton schützt die Benutzeranmeldedaten, Identitäten, personenbezogene Daten und Verschlüsselungsschlüssel. Es ist wesentlich schwieriger, Informationen zu entfernen, auch wenn ein Angreifer Malware installiert hat oder den PC vollständig in seinem Besitz hat.

Microsoft Pluton ist darauf ausgelegt, die Trusted Platform Module (TPM) Funktion bereitzustellen, und liefert weitere Sicherheitsfunktionen, die über das hinausgehen, was mit der TPM 2.0 Spezifikation möglich ist. So können zusätzliche Pluton Firmware und Betriebssystemfunktionen im Laufe der Zeit über Windows Update geliefert werden.

Der AMD Secure Processor 2.0 (ASP 2.0) und der Microsoft Pluton Sicherheitsprozessor koexistieren auf dem AMD Clientchip und kommunizieren, um die Integrität des Geräts zu schützen. Microsoft Pluton schützt Windows PC-Systeme, indem er als integrierter Hardware-Vertrauensanker für das Windows-Ökosystem fungiert. ASP 2.0 hingegen ist der Chip-Hardware-Vertrauensanker, der Integrität durch Authentifizierung der ursprünglich auf die Plattformen geladenen Firmware bereitstellt.

PLATTFORM-UPDATE

AMD PRO Prozessoren bieten Sicherheitsmaßnahmen gegen Angreifer, die in Echtzeit Zugriff auf das System erlangen wollen, und einen robusten Aktualisierungsmechanismus. Damit können Unternehmen Plattformen aktualisieren und Schwachstellen patchen, die von Hardware- oder Software-Bugs verursacht werden.

AMD arbeitet eng mit Erstausrüstern an einer soliden Plattform-Update-Architektur, die auf bewährten Methoden aufbaut und in die Plattform-Update-Lösungen von OEMs integriert werden kann. AMD PRO Prozessoren haben zusätzlich eine Funktion mit dem Namen „Firmware Anti-Rollback (FAR)“, die eine hardwarebasierte Richtlinie ermöglicht, mit der ein Downgrade der AMD Secure Processor 2.0 (ASP 2.0) Firmware blockiert wird. AMD PRO Prozessoren stellen außerdem das sichere Framework „A/B Recovery“ für die Wiederherstellung bereit. Es kann in Erstausrüsterlösungen integriert werden und ermöglicht die Wiederherstellung bei katastrophalen Ausfällen.

KRYPTO-BESCHLEUNIGER

Heutzutage sind kryptografische Prozesse wichtig, um Daten und Kommunikation zu schützen. Allerdings sind sie auch sehr rechenintensiv. AMD bietet neue, optimierte Anweisungen im Chip, um die Kosten für die Berechnung von kryptografischen Algorithmen niedrig zu halten.

Die Architekturen AMD „Zen 2“ und höher haben zusätzliche Unterstützung für vektorisierte AES-Verschlüsselung für 256-Bit (vAES256) und integrieren AES Intrinsics auf x86-Ebene. So können Benutzeranwendungen von der erweiterten kryptografischen Performance und Effizienz profitieren.

FIPS 140-3-ZERTIFIZIERUNG STUFE 1

Angesichts des sensiblen Charakters der Daten, mit denen die Behörden arbeiten, und der grundlegenden Services, die sie erbringen, steht die Endpunktsicherheit bei der Anschaffung von Notebooks für die öffentliche Verwaltung an erster Stelle. Veraltete Hardware ohne moderne Sicherheitsfunktionen kann zu hohen Kosten in Form von Datenverlusten und Dienstunterbrechungen führen.

Die Federal Information Processing Standards (FIPS) der USA sind eine Reihe von öffentlich bekannt gegebenen Standards, die das National Institute of Standards and Technology (NIST) für den Einsatz in Computersystemen für nicht-militärische, amerikanische Regierungsstellen und Auftragnehmer entwickelt hat. FIPS-Standards legen die Anforderungen für Computersicherheit und Interoperabilität fest.

AMD PRO Prozessoren haben die Industrie-Sicherheitszertifizierung **FIPS 140-3 Stufe 1**.

Abbildung 7. Programm zur Validierung kryptografischer Algorithmen für AMD Ryzen™ PRO 7000-Serie Prozessoren.

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

Das FIPS-Modul ist eine Kombination aus Hardware und/oder Software und/oder Firmware, die die zu zertifizierenden Sicherheitsfunktionen unterstützt. Auch wenn FIPS für die Verwendung durch Regierungsbehörden entwickelt wurde, nutzen im privaten Sektor viele diese Standards freiwillig, z. B. Finanzinstitute und Cloud-Anbieter. Zudem expandiert FIPS über Nordamerika hinaus, einschließlich Computerprozessoren für europäische NATO-Partner.

CLOUD BARE METAL RECOVERY

Cloud Bare Metal Recovery bietet einen sicheren Mechanismus für die Remote-Wiederherstellung von Systemen, welcher die Ausfallzeit minimiert und die Geschäftskontinuität im Falle gravierender Hard- oder Softwareausfälle unterstützt. Diese Funktion wird aktiviert, bevor das Betriebssystem bootet, um eine Systemwiederherstellung über die Cloud zu ermöglichen, ohne das Gerät einschicken zu müssen.

Durch die Integration in die AMD PRO Security Architektur trägt Cloud Bare Metal Recovery dazu bei, eine verstärkte Initialisierung und Wiederherstellung auf Hardwareebene bereitzustellen, die darauf ausgelegt ist, vor Manipulation oder Ausbeutung während des Wiederherstellungsprozesses zu schützen.

SUPPLY CHAIN SECURITY (DEVICE IDENTITY)

Supply Chain Security, ermöglicht durch AMD Device Identity, authentifiziert AMD Hardware während des gesamten Lebenszyklus von der Herstellung bis zur Bereitstellung und darüber hinaus. Diese Funktion stellt Rückverfolgbarkeit bereit und schützt vor gefälschten oder manipulierten Komponenten, was Unternehmen Sicherheit über die Integrität ihrer Hardware bietet.

AMD Device Identity stellt eine kryptografische Überprüfung des echten AMD Chips bereit, damit nur Originalhardware in die Unternehmenssysteme integriert wird. So kann man sich vor Supply-Chain-Angriffen schützen, die die Firm- oder Hardware vor der Bereitstellung gefährden könnten.

WATCHDOG-TIMER

Der Watchdog-Timer verbessert die Systemzuverlässigkeit, indem blockierte oder nicht reagierende Prozesse auf Hardwareebene erkannt und reduziert werden. Diese Funktion bietet eine zusätzliche Fehlertoleranz und ermöglicht so, dass Systeme in Betrieb bleiben und sich von potenziellen Problemen erholen.

Der Watchdog-Timer ist in die AMD PRO Security Architektur integriert und arbeitet mit Secure Boot und anderen grundlegenden Funktionen, um eine zuverlässige Fehlererkennung während der Vorgänge vor dem Booten und zur Laufzeit zu ermöglichen. Diese Fähigkeit stärkt die Systemresilienz in unternehmenskritischen Umgebungen und reduziert das Risiko einer Ausfallzeit, die durch Soft- oder Hardwareausfälle verursacht wird.

HIGHLIGHTS DER LÖSUNG

SICHERHEITSEBENE	FUNKTIONEN	VORTEILE
SYSTEM	ERSTAUS-RÜSTER-SICHERHEITS-FUNKTIONEN	Enge Zusammenarbeit von Betriebssystementwickler, Hardwareanbieter und OEM-Partnern zur Ergänzung und Ermöglichung von OEM-Sicherheitsfunktionen der Enterprise-Klasse.
BETRIEBSSYSTEM-SICHERHEIT	WINDOWS 11 SICHERHEIT	Vollständige Unterstützung für Secured-Core PC-Initiative, Hardware Enforced Stack Protection, Advanced Threat Protection, verbesserte Anmeldung, BitLocker und mehr.
HARDWARE UND FIRMWARE	AMD SECURE PROZESSOR 2.0	Spezieller Sicherheitsprozessor, der Code vor der Ausführung validiert und so die Daten- und Anwendungsintegrität unterstützt.
	AMD PLATFORM SECURE BOOT	Schützt den Bootvorgang, damit keine unbefugte Software oder Malware wichtige Systemfunktionen übernehmen kann.
	AMD MEMORY GUARD	Verschlüsselt den Systemspeicher in Echtzeit, um vor physischen Angriffen im Falle eines Verlusts oder Diebstahls des Notebooks zu schützen.
	AMD SHADOW STACK	Robuster Sicherheitsansatz, der vor Control-Flow-Angriffen schützt. Dabei wird der normale Programm-Stack mit einer Kopie im Hardwarespeicher abgeglichen und ermöglicht so Microsoft Hardware Enforced Stack Protection in der Windows 11® Sicherheit.
	MICROSOFT PLUTON SICHERHEITS-PROZESSOR	Eine Chip-to-Cloud-Sicherheitstechnologie, entwickelt und aktualisiert von Microsoft, zur Verbesserung der Sicherheit im Kern der Windows 11 PCs mit kontinuierlichem Schutz für Benutzeranmeldedaten, Identitäten, personenbezogene Daten und Verschlüsselung.
	AMD FIRMWARE TPM	Ein Firmware-TPM, das die Plattform authentifiziert und Anzeichen von Sicherheitsverletzungen erkennt.
	FIPS 140-3 STUFE 1 MODUL-ZERTIFIZIERUNG	Der Verschlüsselungsstandard, den auch Regierungen verwenden, um die Sicherheit von Kryptografiehardware in der Privatwirtschaft zu gewährleisten.
	AMD SECURE PROZESSOR 2.0	Festigt einen Hardware-Vertrauensanker. Dazu wird die anfängliche Firmware validiert und die Plattform vor unbefugtem Code geschützt.
	CLOUD BARE METAL RECOVERY	Ermöglicht eine sichere Systemwiederherstellung über die Cloud ohne Versand von Geräten. Entwickelt für minimale Ausfallzeiten bei katastrophalen Ereignissen.

ZUSAMMENFASSUNG

AMD PRO Technologien bieten eine umfassende Grundlage, um sich ändernde Anforderungen moderner Unternehmen zu bewältigen. Durch die Integration erweiterter Sicherheit, nahtloser Manageability und Business-Ready-Zuverlässigkeit in alle AMD Ryzen™ PRO Prozessoren befähigt AMD Organisationen, ihre Daten zu schützen, IT-Vorgänge zu optimieren und Produktivität der nächsten Dimension in unterschiedlichen Arbeitsumgebungen bereitzustellen.

Da Arbeitsplätze hybride Abläufe einführen und KI-gestützte Workflows integrieren, setzt sich AMD weiterhin für die Förderung von Innovationen ein. Mit jeder Generation definieren die AMD PRO Technologien die Grenzen von Sicherheit, Performance und Manageability neu, damit Unternehmen in der Lage sind, die Herausforderungen von heute zu meistern und sich auf die Möglichkeiten von morgen vorzubereiten.

HAFTUNGSAUSSCHLUSS

Die hier enthaltenen Angaben dienen ausschließlich zur Information und können ohne Vorankündigung geändert werden. Obwohl dieses Dokument mit aller Sorgfalt angefertigt wurde, kann es technische Ungenauigkeiten, Auslassungen und typografische Fehler enthalten. AMD ist nicht verpflichtet, diese Informationen zu aktualisieren oder anderweitig zu korrigieren. AMD PRODUKTE können außerdem Druckfehler enthalten, was dazu führen kann, dass der Prozessor von veröffentlichten Spezifikationen abweicht. AMD stellt solche Produktdruckfehler ohne Vorankündigung gelegentlich fest, steht aber unter keinerlei Verpflichtung, das zu tun. Advanced Micro Devices, Inc. gibt keinerlei Zusicherungen bezüglich der Genauigkeit oder Vollständigkeit dieser Inhalte und übernimmt keinerlei Haftung oder stillschweigende Gewährleistungen für die Nichtverletzung von Rechten, Marktfähigkeit oder Eignung für bestimmte Zwecke bei Betrieb oder Nutzung von AMD Hardware, Software oder anderen hier beschriebenen Produkten. Mit diesem Dokument werden keinerlei gewerbliche Schutzrechte gewährt – weder ausdrücklich noch impliziert oder durch eine Rechtswirkung. Die für den Kauf oder die Nutzung von AMD Produkten geltenden Bedingungen und Einschränkungen werden schriftlich zwischen Parteien vereinbart oder in den Standard-Verkaufsbedingungen von AMD festgelegt.

ENDNOTEN

1. Volle Systemspeicherverschlüsselung mit AMD Memory Guard ist in AMD Ryzen PRO, AMD Ryzen Threadripper PRO und AMD Athlon PRO Prozessoren enthalten. Muss durch Erstausrüster aktiviert werden. Sprechen Sie vor dem Kauf mit Ihrem Systemhersteller. GD-206.
2. Ein OEM, der die Funktion AMD Platform Secure Boot aktiviert, gibt dem eigenen kryptografisch signierten BIOS-Code die Erlaubnis, ausschließlich auf den eigenen Plattformen und mithilfe eines AMD Platform Secure Boot-fähigen Mainboards ausgeführt zu werden. Einmalig programmierbare Sicherungen im Prozessor binden den Prozessor an den OEM-Signaturschlüssel des Firmwarecodes. Ab diesem Zeitpunkt kann dieser Prozessor ausschließlich mit Mainboards verwendet werden, die denselben Signaturschlüssel für den Code verwenden. GD-192.
3. Im Vergleich zu Intel vPro implementiert AMD PRO Manageability mehr Profile der DASH-Management-Initiative, um die Verwaltung von Desktop- und Mobilsystemen mehrerer Anbieter zu unterstützen. KRKP-7.
4. Im Vergleich zu Intel vPro implementiert AMD PRO Manageability eine neuere Version des TLS (Transport Layer Security) Protokolls, das ein höheres Maß an Sicherheit und geringere Latenzzeiten bietet (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. Der AMD Secure Processor ist ein spezieller On-Chip-Sicherheitsprozessor, der in jedes von AMD entwickelte System-on-a-Chip (SoC) und ASIC (Application Specific Integrated Circuit) integriert ist. Er ermöglicht einen sicheren Start mit in der Hardware verankertem Root of Trust, initialisiert das SoC über einen sicheren Boot-Fluss und stellt eine isolierte vertrauenswürdige Ausführungsumgebung her. GD-72.
7. Volle Systemspeicherverschlüsselung mit AMD Memory Guard ist in AMD Ryzen PRO, AMD Ryzen Threadripper PRO und AMD Athlon PRO Prozessoren enthalten. Muss durch Erstausrüster aktiviert werden. Sprechen Sie vor dem Kauf mit Ihrem Systemhersteller. GD-206.
8. Microsoft Pluton ist eine Technologie von Microsoft, die an AMD lizenziert wird. Microsoft Pluton ist eine eingetragene Marke der Microsoft Corporation in den USA und/oder anderen Ländern. Weitere Informationen unter https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/. Der Microsoft Pluton Sicherheitsprozessor muss durch den Erstausrüster aktiviert werden. Erkundigen Sie sich vor dem Kauf beim Erstausrüster. AMD hat Aussagen von Dritten nicht geprüft. GD-202.
9. Der AMD Secure Processor ist ein spezieller On-Chip-Sicherheitsprozessor, der in jedes von AMD entwickelte System-on-a-Chip (SoC) und ASIC (Application Specific Integrated Circuit) integriert ist. Er ermöglicht einen sicheren Start mit in der Hardware verankertem Root of Trust, initialisiert das SoC über einen sicheren Boot-Fluss und stellt eine isolierte vertrauenswürdige Ausführungsumgebung her. GD-72.

© 2025 Advanced Micro Devices, Inc. Alle Rechte vorbehalten. AMD, das AMD Pfeillogo, AMD-V, Infinity Fabric, Ryzen und deren Kombinationen sind Marken von Advanced Micro Devices, Inc. Microsoft ist eine eingetragene Marke der Microsoft Corporation in den USA und/oder anderen Ländern. Andere Produktnamen dienen nur zur Information und können Marken ihrer jeweiligen Inhaber sein. Bestimmte AMD Technologien erfordern möglicherweise die Ermöglichung oder Aktivierung durch Dritte. Die unterstützten Funktionen können je nach Betriebssystem variieren. Bitte informieren Sie sich beim Systemhersteller über spezifische Funktionen. Keine Technologie und kein Produkt kann vollständig sicher sein.