TECNOLOGÍAS AMD PRO

UNA MIRADA A LA SEGURIDAD AMD PRO Y EL MARCO AMD PARA PC EMPRESARIALES SEGURAS, MANEJABLES Y CONFIABLES

El espacio de trabajo ágil y distribuido sigue evolucionando. Las operaciones híbridas se están convirtiendo en la norma, ya que las empresas equilibran la colaboración en la oficina y el trabajo remoto, mientras integran la IA en los flujos de trabajo diarios. Las empresas se enfrentan a una presión cada vez mayor para actualizar sus flotas de PC con sistemas que aborden los nuevos retos que presentan estas tendencias. Necesitan soluciones que equilibren el rendimiento, la seguridad y la manejabilidad, a la vez que se adaptan a entornos locales y basados en la nube.

Los procesadores AMD Ryzen™ PRO dotan a las PC empresariales modernas de las tecnologías AMD PRO, un conjunto unificado de innovaciones diseñado para satisfacer las cambiantes demandas de las empresas de hoy. En este documento, se analiza el pilar de seguridad de las tecnologías AMD PRO, uno de los tres componentes fundamentales que forman parte integral de todos los sistemas con procesador AMD Ryzen PRO. Si bien la seguridad es el enfoque principal de este documento, las tecnologías AMD PRO también incluyen manejabilidad avanzada y confiabilidad empresarial, que en conjunto proporcionan una solución completa para las empresas modernas.

Los tres pilares se presentan aquí para proporcionar contexto a las tecnologías AMD PRO en su conjunto, pero el debate en este documento se centrará específicamente en las funciones de seguridad de última generación de los procesadores AMD Ryzen PRO, que están diseñados para proteger las PC empresariales actuales frente a las amenazas en constante evolución.

SEGURIDAD PRO: PROTECCIÓN DE LA EMPRESA MODERNA

La pieza clave de las tecnologías AMD PRO son las sólidas funciones de seguridad. Las funciones de hardware avanzadas, como AMD Memory Guard[1] para el cifrado completo de la memoria, AMD Shadow Stack diseñado para la protección contra ataques de flujo de control y la compatibilidad completa con el procesador criptográfico seguro Microsoft Pluton, brindan protecciones esenciales contra amenazas sofisticadas. Gracias a la compatibilidad integrada en el arranque seguro[2] y la ejecución confiable, los procesadores AMD Ryzen PRO fortalecen los dispositivos en todos los niveles, lo que proporciona al usuario protección de los datos y las aplicaciones desde el punto de conexión hasta la nube.

Si bien las funciones de seguridad avanzadas son el eje de este documento, el marco más amplio de las tecnologías AMD PRO, que incluye manejabilidad y confiabilidad empresarial, funciona conjuntamente a fin de proporcionar a las empresas una solución completa para las demandas emergentes del lugar de trabajo.

MANEJABILIDAD PRO: SIMPLIFICACIÓN DE LAS OPERACIONES DE TI

La gestión de flotas de PC diversas es compleja y requiere mucho tiempo, especialmente en entornos de trabajo híbridos. La manejabilidad de AMD PRO optimiza las operaciones con herramientas basadas en estándares abiertos que permiten la administración remota basada en la nube y la supervisión de puntos de conexión en tiempo real. Estas herramientas proporcionan el nivel más alto de cumplimiento con los estándares abiertos para la administración remota de sistemas.[3] La manejabilidad de AMD PRO ayuda a ofrecer al usuario compatibilidad con herramientas líderes en la industria como Microsoft Endpoint Manager y Windows Autopilot, lo que proporciona un proceso de implementación coherente y eficaz.

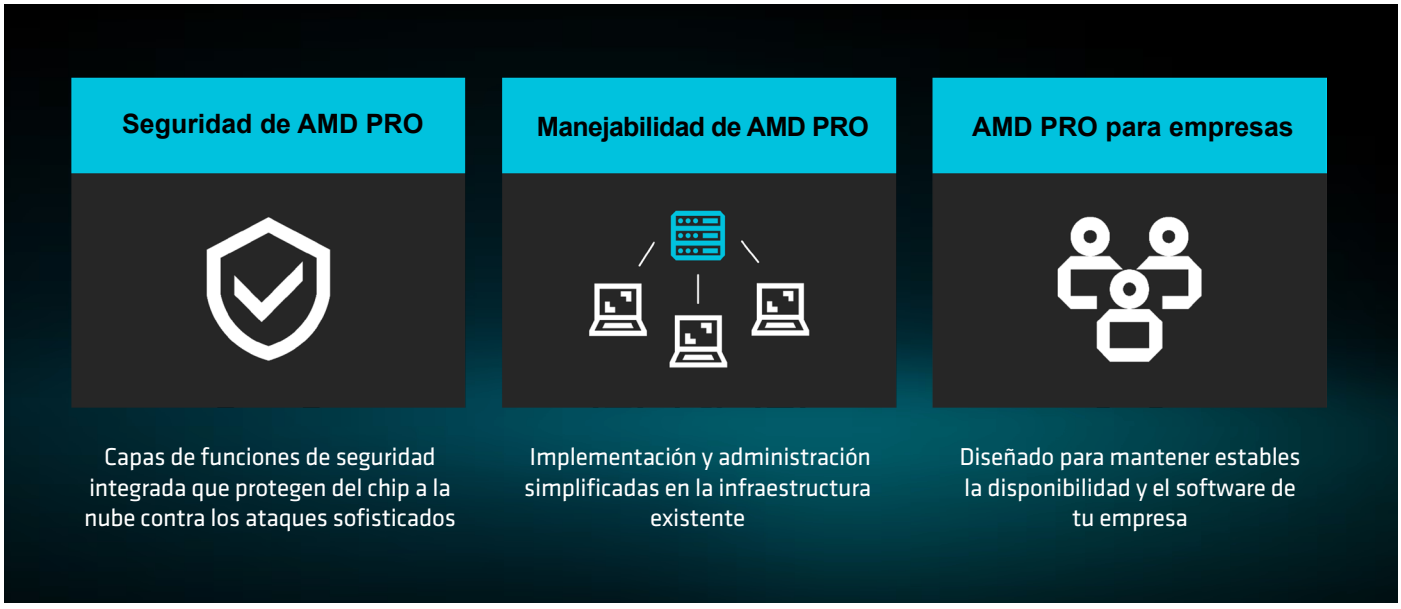
La manejabilidad de AMD PRO es compatible con las especificaciones DMTF DASH (arquitectura de escritorio y móvil para el hardware del sistema) más recientes, e incorpora protocolos de cifrado y autenticación actualizados, como TLS 1.2 y 1.3. Además, los sistemas AMD PRO integran componentes de seguridad basados en hardware, incluido TPM 2.0, para permitir mayor seguridad en el almacenamiento y la protección de claves criptográficas. Este enfoque basado en estándares ofrece una mayor protección y un mejor rendimiento en comparación con los protocolos patentados más antiguos.[4] Los equipos de TI se benefician de funciones como el aprovisionamiento remoto, la implementación automatizada de parches y el diagnóstico en tiempo real, que ayudan a reducir el tiempo de inactividad, mejorar el estado de los puntos de conexión y simplificar las operaciones.

En estudios recientes, se destaca el impacto de la manejabilidad de AMD PRO en las operaciones de TI, que muestran tiempos de implementación reducidos hasta en un 41 %[5] en comparación con los procesos tradicionales y una reducción significativa del esfuerzo práctico gracias a las interfaces de administración unificadas e intuitivas. Estas capacidades ayudan a las empresas a dar soporte a los empleados dondequiera que trabajen, lo que hace que los ecosistemas de PC complejos sean más sencillos, rápidos y confiables para administrar.

PRO PARA EMPRESAS: RENDIMIENTO CONFIABLE PARA CADA TAREA

Los procesadores AMD PRO con funciones preparadas para la empresa ayudan a dar a los usuarios una mayor vida útil de la PC, rendimiento uniforme y confiabilidad para las cargas de trabajo empresariales. Los rigurosos procesos de validación permiten un mejor tiempo de actividad, lo que puede ayudar a reducir los costos de TI. La disponibilidad ampliada en todo el mundo durante un año permite a las empresas implementar sistemas a pedido, lo que minimiza la necesidad de realizar grandes compras iniciales. Tanto si se trata de aplicaciones basadas en IA como de tareas rutinarias de oficina, los procesadores AMD Ryzen™ PRO proporcionan la adaptabilidad que las empresas necesitan para prosperar.

Figura 1. Tecnologías AMD PRO. Potenciar cada PC empresarial con un procesador AMD Ryzen™ PRO.



Las tecnologías AMD PRO para empresas mejoran esta confiabilidad mediante la entrega de coherencia a largo plazo que simplifica la planificación de TI y maximiza el retorno de la inversión. Todos los procesadores AMD Ryzen™ PRO ofrecen soluciones de nivel empresarial con las siguientes cualidades:

- **Estabilidad de imagen:** 18 meses de estabilidad de software planificada para ayudar a proporcionar transiciones sin interrupciones y tranquilidad a los equipos de TI.
- **Calidad:** Procesos de validación de plataformas mejorados que proporcionan calidad de nivel empresarial para entornos empresariales exigentes.
- **Disponibilidad:** 24 meses de disponibilidad planificada para mantener la coherencia del hardware y garantizar la estabilidad de las operaciones empresariales.
- **Confiabilidad:** Validación continua de la plataforma diseñada para ofrecer estabilidad a largo plazo y una experiencia del usuario uniforme en varias generaciones de procesadores.

Al proporcionar estabilidad en el hardware y en el software, AMD PRO para empresas reduce la complejidad para los equipos de TI y proporciona una base confiable para el éxito empresarial a largo plazo.

A medida que las empresas se enfrentan a la complejidad de dar soporte al nuevo lugar de trabajo, las tecnologías AMD PRO ofrecen una ventaja fundamental. Al integrar características de seguridad avanzadas, manejabilidad eficiente y funciones empresariales en todos los sistemas con CPU AMD Ryzen PRO, AMD equipa a las organizaciones con las herramientas que necesitan para proteger sus operaciones, optimizar la administración de TI e impulsar la innovación.

Figura 2. Seguridad de AMD PRO. Supera los últimos requisitos de seguridad para dispositivos modernos.

LAS PC CON TECNOLOGÍA AMD ESTÁN DISEÑADAS CON SEGURIDAD MULTICAPA AVANZADA EN TODOS LOS NIVELES

AMD trabaja codo a codo con los desarrolladores de sistemas operativos (SO) y los fabricantes de equipos originales (OEM) para diseñar funciones de seguridad de hardware que complementen y refuercen su diseño de seguridad.

Mediante la integración de medidas de seguridad avanzadas en todos los niveles, desde el chip hasta los sistemas operativos, AMD permite a las organizaciones proteger sus activos más importantes mientras minimiza el tiempo de inactividad y reduce la complejidad de TI.

SEGURIDAD INTEGRADA EN CADA CAPA

Las tecnologías AMD PRO integran la seguridad como pilar fundamental en todos los dispositivos con procesador AMD Ryzen™ PRO. Diseñados para los retos en constante evolución de la empresa moderna, estos procesadores ofrecen protección multicapa que comienza con una sólida base de chip y se extiende a través de defensas a nivel de firmware y sistema operativo.

RAÍZ DE CONFIANZA DE HARDWARE: INTEGRIDAD DESDE EL PRINCIPIO

La arquitectura de chip de AMD proporciona una raíz de confianza de hardware integrada que ayuda a proteger los procesos de arranque. El procesador AMD Secure 2.0[6] (ASP 2.0) refuerza esta confianza, verificando la integridad del firmware y del BIOS del OEM para defenderse de modificaciones no autorizadas y posibles ataques de firmware.

REDEFINICIÓN DE LA PROTECCIÓN DE LA MEMORIA: AMD MEMORY GUARD[7]

AMD Memory Guard cifra toda la memoria del sistema en tiempo real, lo que ayuda a proteger los datos confidenciales de los ataques físicos y de arranque en frío. Con motores de cifrado de hardware dedicados, esta función ayuda a proporcionar una defensa sólida incluso en situaciones que implican el robo de dispositivos.

ARQUITECTURA DE ÚLTIMA GENERACIÓN: AMD "ZEN 5" Y POSTERIORES

La última arquitectura de núcleo AMD "Zen 5" incorpora funciones de seguridad mejoradas, incluida la seguridad de la cadena de suministro, que utiliza una ID de procesador única para permitir un seguimiento seguro del hardware AMD original a lo largo de su ciclo de vida. Estas innovaciones refuerzan la resiliencia de los puntos de conexión frente a las ciberamenazas cada vez más sofisticadas.

CONSONANCIA CON LOS ESTÁNDARES DEL SECTOR

Los procesadores AMD PRO están diseñados para superar los requisitos de seguridad modernos, incluida la certificación FIPS 140-3 de nivel 1. La integración en Microsoft Pluton[8] mejora aún más la protección de los sistemas basados en Windows mediante la adición de seguridad de autenticación y protección criptográfica.

LA ARQUITECTURA DE SEGURIDAD DE AMD PRO

PROCESADOR AMD SECURE 2.0:[9] UNA BASE MÁS SÓLIDA

En el núcleo de la arquitectura de seguridad de AMD PRO, se encuentra el procesador AMD Secure 2.0 (ASP 2.0), un componente de hardware dedicado integrado en cada sistema en chip (SoC). ASP 2.0 refuerza una raíz de confianza de hardware y admite un flujo de arranque seguro, verificando la integridad del firmware desde el momento en que se enciende un dispositivo. Su entorno de ejecución confiable aislado ayuda a las operaciones confidenciales a permanecer protegidas de posibles ataques. Los componentes clave incluyen las siguientes opciones:

- **Coprocesador criptográfico (CCP):** Un motor criptográfico de alto rendimiento que administra la generación de claves y las operaciones criptográficas en el hardware, esencial para las tareas de seguridad urgentes.
- **ROM de arranque:** Memoria segura de solo lectura que contiene firmware esencial para la inicialización del arranque.
- **Memoria estática de acceso aleatorio (SRAM):** Proporciona soporte de baja potencia para procesos seguros.
- **Unidad de administración de memoria (MMU):** Controla el acceso a la ROM de arranque y a la SRAM para un control estricto de los recursos de memoria.
- **Cloud Bare Metal Recovery:** Facilita la recuperación segura de los dispositivos a través de la nube, lo que permite la continuidad del negocio incluso en situaciones de fallas catastróficas.
- **Seguridad de la cadena de suministro:** Autentica el hardware AMD original en cada etapa de su ciclo de vida, protegiéndolo contra la manipulación o la falsificación de componentes.
- **Temporizador de vigilancia:** Detecta y mitiga los procesos bloqueados a nivel de hardware, lo que mejora la resiliencia del sistema.

Estas funciones abordan de forma colectiva el mayor riesgo de exposición de datos empresariales confidenciales durante los viajes, el trabajo remoto u otras situaciones móviles.

INTEGRACIÓN SIN INTERRUPCIONES CON LA SEGURIDAD DE WINDOWS

La arquitectura de seguridad de AMD PRO se integra sin interrupciones en las funciones de seguridad de Windows 11, como el arranque seguro y la protección de pila aplicada por hardware, para crear un sistema de defensa multicapa integral. Juntos, fortalecen los puntos de conexión contra ataques dirigidos al firmware, el BIOS, los controladores y el sistema operativo.

AMD ROM ARMOR

La memoria flash SPI (Serial Peripheral Interconnect) de una motherboard contiene tanto la UEFI de la motherboard como información de configuración adicional, incluido el estado de arranque seguro.

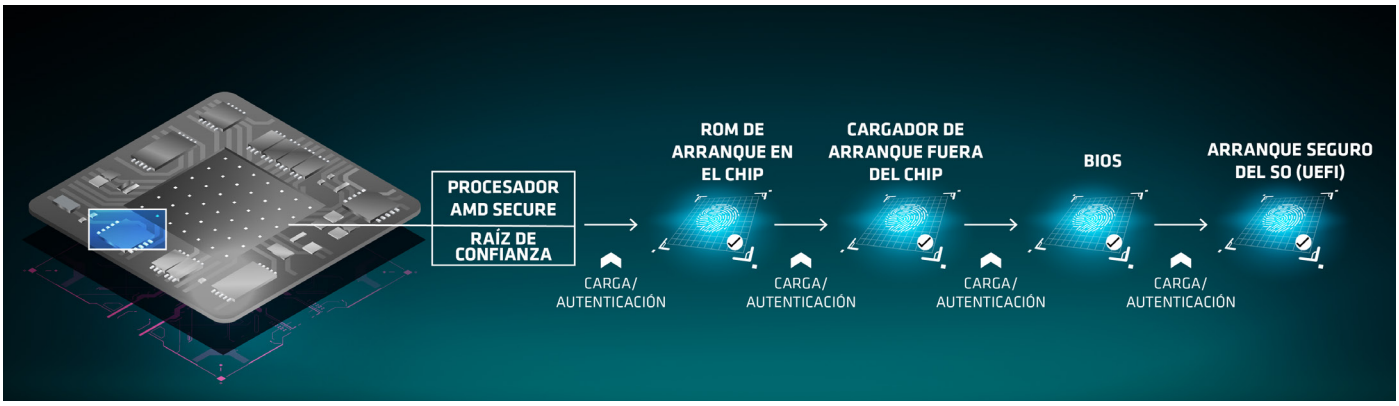
AMD ROM Armor funciona antes de que el sistema operativo se haya inicializado y proporciona protección contra modificaciones no autorizadas en la memoria flash SPI. Al proporcionar la integridad de la memoria flash SPI antes de que se cargue el sistema operativo, AMD ROM Armor ayuda a establecer una base reforzada para el sistema. Una vez que AMD ROM Armor está configurado y activado, el dispositivo flash SPI de la computadora se fortalece contra escrituras no autorizadas.

AMD PLATFORM SECURE BOOT (PSB)

AMD Platform Secure Boot (PSB) proporciona una raíz de confianza de hardware (RoT) para autenticar el firmware inicial, incluido el BIOS, durante el proceso de arranque del dispositivo. Cuando un sistema se enciende, el ASP ejecuta el código de la ROM de arranque que, a su vez, autentica diferentes códigos del gestor de arranque del ASP antes de inicializar el chip y la memoria del sistema. Una vez que inicia la memoria del sistema, el código del gestor de arranque del ASP verifica el código del BIOS del OEM, que autentica otros componentes del firmware antes de que arranque el SO.

PSB está diseñado para reforzar la integridad de la plataforma porque brinda más protección contra el firmware falso o malintencionado y le niega el acceso automáticamente cuando lo detecta. AMD PSB ayuda a proteger la transición del firmware de bajo nivel al SO.

Figura 3. AMD Platform Secure Boot.



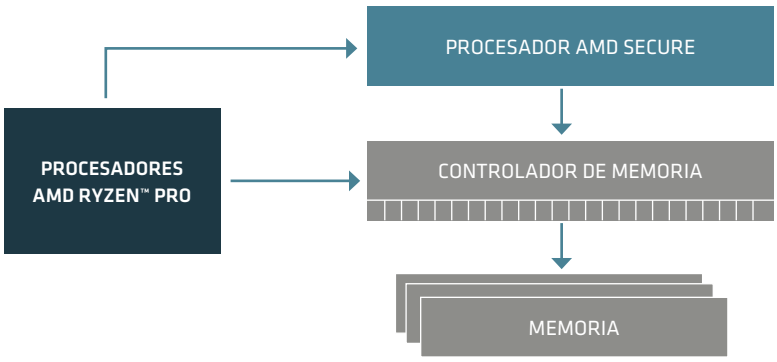
AMD MEMORY GUARD[3]

AMD Memory Guard es una completa tecnología de cifrado de memoria diseñada para proteger los datos de los clientes contra ataques físicos. Con AMD Memory Guard, se cifra todo el contenido de la DRAM con una clave aleatoria, lo que ofrece protección contra los ataques físicos de arranque en frío, el acceso no autorizado a la interfaz de la DRAM y ataques similares.

En los sistemas que utilizan NVDIMM, AMD Memory Guard también ofrece protección contra los atacantes que extraen el módulo de memoria para intentar acceder a su contenido, implementada mediante hardware exclusivo en los controladores de memoria del chip.

- Cada controlador incluye un motor con Advanced Encryption Standard (AES) de alto rendimiento que cifra los datos cuando se escriben en la DRAM y los descifra cuando se leen.
- Se genera una clave de 128 bits mediante un generador de números aleatorios por hardware que cumple con NIST SP 800-90 en chip en un modo que utiliza un ajuste basado en una dirección física adicional para ayudar a evitar ataques de movimiento de bloques de texto cifrado.
- La clave de cifrado que el motor AES utiliza con AMD Memory Guard se genera al azar en cada reinicio del sistema y no es visible para el software que se ejecuta en los núcleos de la CPU. La administración integral de la clave la lleva a cabo el procesador AMD Secure (ASP).

Figura 4. AMD Memory Guard.



AMD SHADOW STACK

La programación orientada al retorno (ROP) es un vector de ataque cada vez más popular. Los ataques de ROP no inyectan su propio código malicioso. En lugar de ello, intentan obtener el control de un sistema explotando las debilidades del código legítimo.

¿CÓMO FUNCIONA?

En programación informática, una "rutina" realiza una serie de operaciones específicas. Cuando se ejecuta un programa de software, esto se llama rutina. Cuando una rutina finaliza su trabajo, regresa al programa principal mediante la dirección de retorno. Este proceso se denomina "Saltar y regresar".

En los ataques de ROP, los ciberdelincuentes modifican la dirección de retorno de la rutina de salto. Esto significa que, en lugar de regresar al programa principal, comienza a saltar a diferentes rutinas y a unir subrutinas para generar un código malicioso que puede dañar el sistema. Lo más grave es que este tipo de ataques no se pueden detectar porque se asemejan al código legítimo.

La arquitectura de seguridad de AMD PRO ayuda a limitar los ataques de ROP porque permiten que el software acceda a registros especiales en la CPU donde se puede almacenar una copia de la dirección de retorno. Las aplicaciones pueden utilizar una pila paralela, conocida como "Pila oculta", para ayudar a limitar los ataques de software que intentan modificar el flujo de control. La pila oculta utiliza un hardware especializado para almacenar una copia de las direcciones de retorno, que se valida con la pila del programa normal en las operaciones de retorno.

Si el contenido es diferente, se genera una excepción, que ayuda a evitar que el código malicioso tome el control del sistema. De este modo, el hardware de la pila oculta mitiga algunos de los fallos de software más comunes y vulnerables.

AMD Shadow Stack refuerza el sistema contra los ataques de ROP. Dado hay una copia de la dirección de retorno en el hardware, es muy difícil que el código malicioso pueda manipularla.

La arquitectura de seguridad de AMD PRO ofrece la protección de pila aplicada por hardware de Microsoft a través de AMD Shadow Stack.

PC CON NÚCLEO SEGURO DE MICROSOFT

La arquitectura de PC con núcleo seguro de Microsoft protege el dispositivo contra vulnerabilidades de firmware, resguarda el sistema operativo de ataques e impide el acceso no autorizado a dispositivos y datos con controles de acceso y sistemas de autenticación avanzados.

La PC con núcleo seguro se habilita en las plataformas de arquitectura de seguridad de AMD PRO por medio de diferentes tecnologías y servicios de seguridad:

- AMD-V™ con GMET
- Inicialización segura y salto con atestación AMD (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- AMD System Management Mode (SMM) Supervisor
- Direct Memory Access (DMA) Protection

TECNOLOGÍA DE VIRTUALIZACIÓN AMD (AMD-V™) CON GMET

AMD-V es un conjunto de extensiones de hardware que permite la virtualización en las plataformas AMD. Guest Mode Execute Trap (GMET) es una optimización de rendimiento en el chip que permite que el hipervisor realice verificaciones de integridad de código de forma eficiente y brinda protección contra el malware.

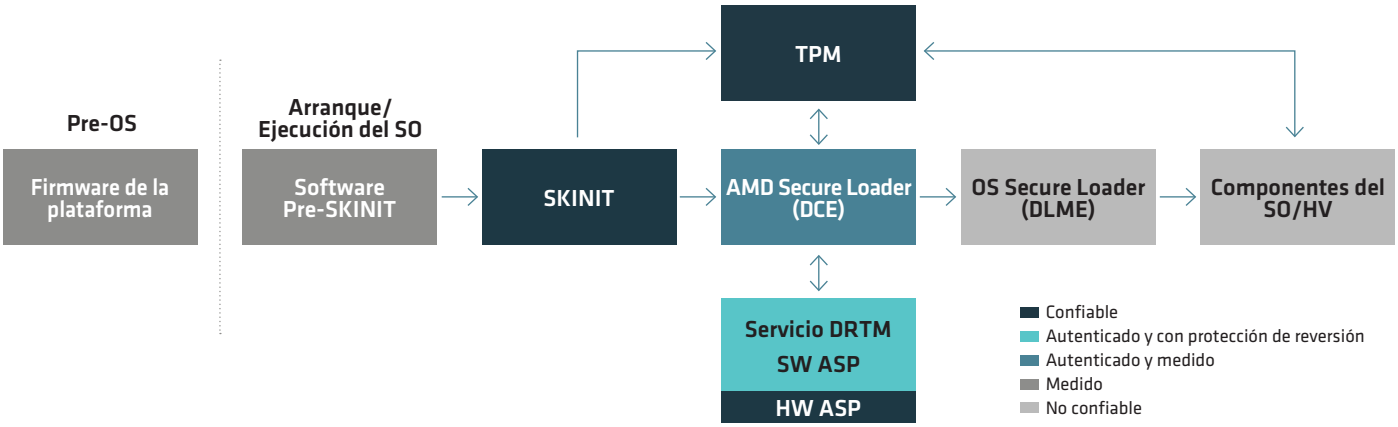
INICIALIZACIÓN SEGURA Y SALTO CON ATESTACIÓN (SKINIT)

La instrucción SKINIT ayuda a crear una "raíz de confianza" a partir de un modo de operación que no es confiable. SKINIT reinicializa el procesador a fin de establecer un entorno de ejecución reforzado para un componente de software llamado gestor de arranque seguro (SL) e inicia la ejecución de SL para evitar alteraciones en el sistema. SKINIT extiende la raíz de confianza de hardware hasta el gestor de arranque seguro.

AMD SECURE LOADER (SL)

AMD Secure Loader se encarga de validar la configuración de la plataforma, mediante la interrogación del hardware, y de solicitar la información de configuración del servicio DRTM que proporciona el procesador AMD Secure.

Figura 5. Flujo DRTM.



Una vez que el sistema ejecuta el SO, este puede solicitarle al bloque de servicio de AMD que vuelva a medir y confirmar los valores antes de ejecutar más operaciones. De esta forma, el SO puede garantizar la integridad del sistema desde el arranque hasta la ejecución.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

El bloque AMD DRTM está formado por la instrucción de CPU SKINIT, ASP y SL. Es el responsable de crear y mantener una cadena de confianza entre el firmware. AMD DRTM trabaja con la idea de que el firmware y el gestor de arranque pueden cargarse libremente y entiende que son programas desprotegidos. Sabe que, apenas arranca, el sistema pasa a un estado seguro, y el hardware fuerza el firmware de bajo nivel por una ruta de código conocida y medida.

El bloque AMD DRTM está formado por la instrucción de CPU SKINIT, ASP y SL. Es el responsable de crear y mantener una cadena de confianza entre el firmware.

AMD DRTM trabaja con la idea de que el firmware y el gestor de arranque pueden cargarse libremente y entiende que son programas desprotegidos. Sabe que, apenas arranca, el sistema pasa a un estado seguro, y el hardware fuerza el firmware de bajo nivel por una ruta de código conocida y medida.

El bloque DRTM mide y autentica el gestor de arranque, y también recopila y almacena de forma segura la siguiente información del sistema para que el SO la use en el futuro, incluida la verificación y atestación:

- Mapa de la memoria física
- Ubicación espacial de la configuración PCI
- Configuración APIC local
- Configuración APIC de E/S
- Configuración IOMMU/TMR
- Configuración de administración de energía

CONFIANZA EN HARDWARE COMPARTIDO

Significa que el bloque del ASP autentica y mide el componente de firmware en el chip AMD, y que la medición se almacena de forma segura para que el SO la use en el futuro, incluida la verificación y atestación.

AMD SMM SUPERVISOR

El modo de administración del sistema (SMM) es un modo de CPU especial en microcontroladores x86 que gestiona la administración de energía, la configuración de hardware, la supervisión térmica y otras operaciones a nivel de dispositivo. Cuando se solicita alguna de estas operaciones de sistema, se invoca una interrupción (SMI) en el momento de la ejecución y se ejecuta el código SMM que instaló el BIOS. Como el código SMM se ejecuta con los privilegios más altos y es invisible para el SO, es una excelente víctima de la actividad malintencionada, que se podría usar a fin de acceder a la memoria del hipervisor y poner en riesgo el hipervisor.

En la mayoría de los casos, el controlador de SMI es proporcionado por un desarrollador diferente del sistema operativo y tiene acceso a la memoria y los recursos del SO o hipervisor. Esto significa que las vulnerabilidades aprovechables en el código SMM pueden ponen en riesgo el SO o hipervisor (HV) de Windows y la seguridad basada en la virtualización (VBS).

Para ayudar a aislar el SMM, AMD implementó un módulo de seguridad llamado AMD SMM Supervisor, que se ejecuta justo antes de que el control se transfiera al controlador de SMI, luego de una interrupción de administración del sistema (SMI). AMD SMM Supervisor está alojado en el bloque de servicio AMD DRTM y cumple las siguientes funciones:

- Bloquea el SMM para que no pueda modificar el hipervisor o la memoria del SO, excepto un pequeño búfer de comunicación entre los dos.
- Evita que el SMM introduzca nuevo código SMM en el tiempo de ejecución.
- Bloquea el SMM para que no acceda al DMA, la E/S o los registros que pueden comprometer el hipervisor o el SO.

PROTECCIÓN DEL DMA

Con tecnología de reasignación del DMA, las plataformas de AMD protegen el acceso directo a memoria (DMA) antes del arranque y en entornos de SO por medio de las tecnologías seguras de AMD, como la Unidad de administración de memoria de entrada/salida (IOMMU).

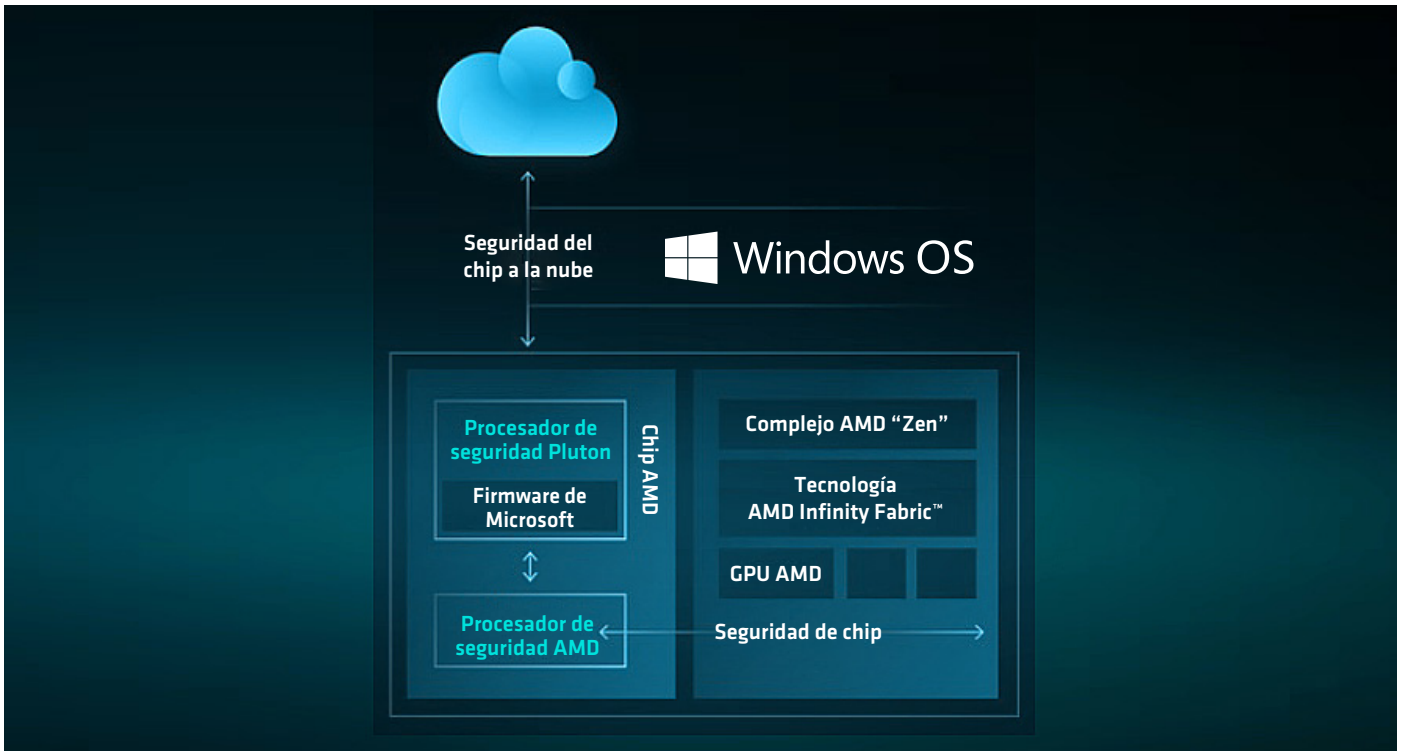
- La protección del DMA ayuda a proteger el sistema en caso de que se produzca un ataque en el firmware de la plataforma, mediante el cual los atacantes pueden usar los dispositivos conectados para intentar vulnerar el DMA.
- El DMA permite que los dispositivos accedan directamente al espacio de direcciones de la memoria física para mejorar el rendimiento. No obstante, esto también facilita que el software malintencionado inyecte malware en el sistema sin que el SO lo detecte.

Para evitar ese tipo de ataques, AMD diseñó una arquitectura de seguridad que administra y controla el acceso DMA de los dispositivos por medio de la IOMMU en el firmware al nivel pre-OS. La arquitectura de seguridad del DMA pasa la responsabilidad de los ajustes de protección de la memoria del sistema del firmware al SO, una vez que el gestor de arranque del SO se ha establecido en la memoria. En cada arranque, se aplica la protección del DMA usando IOMMU, hasta que el SO toma el control de la propia IOMMU.

PROCESADOR DE SEGURIDAD MICROSOFT PLUTON[8]

Diseñado por Microsoft y construido por Silicon Partners, Microsoft Pluton es un procesador criptográfico seguro incorporado en la CPU para ofrecer seguridad en el núcleo y ayudar a confirmar la integridad

Figura 6. Descripción general de la arquitectura de seguridad de Microsoft Pluton.



del código y la protección más reciente con actualizaciones suministradas por Microsoft a través de Windows Update. Pluton protege las credenciales de usuario, identidades, datos personales y claves de cifrado. La información es mucho más difícil de eliminar, incluso si un atacante instaló malware o tiene la posesión física completa de la PC.

Microsoft Pluton está diseñado para proporcionar la funcionalidad de módulo de plataforma segura (TPM) y ofrecer otras funciones de seguridad más allá de lo que es posible con la especificación TPM 2.0. Permite que el firmware de Pluton y las funciones del sistema operativo adicionales se distribuyan a lo largo del tiempo a través de Windows Update.

Procesador AMD Secure 2.0 (ASP 2.0) y el procesador de seguridad Microsoft Pluton coexisten en el chip de cliente AMD y se comunican para ayudar a proteger la integridad del dispositivo. Microsoft Pluton ayuda a proteger los sistemas de PC Windows actuando como una raíz de confianza de hardware integrada para el ecosistema de Windows, mientras que ASP 2.0 actúa como la raíz de confianza de hardware de chip, lo que ayuda a proporcionar integridad mediante la autenticación del firmware inicial cargado en las plataformas.

ACTUALIZACIÓN DE LA PLATAFORMA

Los procesadores AMD PRO proporcionan defensas de seguridad contra los atacantes que intentan acceder al sistema en tiempo real y un sólido mecanismo de actualización. Esto permite que las empresas actualicen sus plataformas para eliminar las vulnerabilidades que nacen de los fallos de hardware o software.

AMD colabora estrechamente con los OEM para proporcionar una arquitectura de actualización de plataforma reforzada, que cumpla con las prácticas recomendadas y pueda integrarse en las soluciones de actualización de plataforma de los OEM. Además, los procesadores AMD PRO tienen una función de antirreversión de firmware (FAR) que habilita una directiva de hardware para evitar que se pase a una versión anterior del firmware del procesador AMD Secure 2.0 (ASP 2.0). Finalmente, los procesadores AMD PRO también incluyen un marco de recuperación seguro llamado “A/B Recovery”, que se puede integrar en una solución de OEM para poder recuperar el sistema en caso de una falla catastrófica.

ACELERADOR CRIPTOGRÁFICO

En el mundo actual, las operaciones criptográficas son importantes para proteger los datos y las comunicaciones. Son esenciales, pero también exigen una gran potencia de procesamiento. AMD proporciona instrucciones nuevas y optimizadas en el chip para ayudar a reducir los costos asociados con la computación con algoritmos criptográficos.

Las arquitecturas AMD “Zen 2” y posteriores agregaron compatibilidad con el cifrado AES vectorizado para 256 bits (vAES256) e integran funciones intrínsecas AES en el nivel x86, lo que permite a las aplicaciones de usuario beneficiarse de la mejora de la eficiencia y el rendimiento criptográficos.

CERTIFICACIÓN FIPS 140-3 DE NIVEL 1

Dada la naturaleza delicada de los datos que manejan los organismos públicos y los servicios esenciales que proporcionan, la seguridad de los puntos de conexión es una de las principales preocupaciones al considerar las laptops para las compras de TI del Gobierno. El hardware obsoleto, que carece de funciones de seguridad modernas, puede provocar altos costos en términos de pérdida de datos e interrupciones del servicio.

Los Estándares Federales de Procesamiento de Información (FIPS) de Estados Unidos son un conjunto de estándares anunciados públicamente que el Instituto Nacional de Estándares y Tecnología (NIST) desarrolló para su uso en sistemas informáticos de agencias y contratistas no militares del Gobierno estadounidense. Los estándares FIPS establecen requisitos de seguridad e interoperabilidad informática.

Los procesadores AMD PRO incluyen la certificación de seguridad industrial **FIPS 140-3 de nivel 1**.

Figura 7. Programa de validación de algoritmos criptográficos para procesadores AMD Ryzen™ PRO Serie 7000.

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

El módulo FIPS es una combinación de hardware, software o firmware que admite funciones de seguridad para la certificación. Aunque FIPS se desarrolló para ser utilizado por el Gobierno federal, diversas entidades del sector privado utilizan voluntariamente estos estándares, incluidas las instituciones financieras y los proveedores de servicios en la nube. Además, FIPS se está expandiendo más allá de Norteamérica, incluidos los procesadores de computadoras para socios europeos de la OTAN.

CLOUD BARE METAL RECOVERY

Cloud Bare Metal Recovery proporciona un mecanismo seguro para recuperar sistemas de forma remota, minimizando el tiempo de inactividad y respaldando la continuidad del negocio en caso de fallas catastróficas de hardware o software. Esta función se activa antes de que se inicie el sistema operativo para permitir la recuperación del sistema a través de la nube sin necesidad de enviar el dispositivo para su reparación.

Mediante la integración en la arquitectura de seguridad de AMD PRO, Cloud Bare Metal Recovery ayuda a proporcionar una inicialización y una recuperación fortificadas a nivel de hardware, que se diseñó para proteger contra la manipulación o la explotación durante el proceso de recuperación.

SEGURIDAD DE LA CADENA DE SUMINISTRO (IDENTIDAD DE DISPOSITIVOS)

La seguridad de la cadena de suministro, habilitada mediante la identidad de dispositivos de AMD, autentica el hardware de AMD a lo largo de todo su ciclo de vida, desde la fabricación hasta la implementación y mucho más. Esta función ayuda a proporcionar trazabilidad y protege contra la falsificación y la manipulación de componentes, lo que ofrece a las empresas garantía de la integridad del hardware.

La identidad de dispositivos de AMD proporciona verificación criptográfica de chips AMD originales, de modo que solo se integra hardware auténtico en los sistemas empresariales. Esto ayuda a proteger contra los ataques a la cadena de suministro que podrían poner en peligro el firmware o el hardware antes de la implementación.

TEMPORIZADOR DE VIGILANCIA

El temporizador de vigilancia mejora la confiabilidad del sistema mediante la detección y la mitigación de los procesos bloqueados o que no responden a nivel de hardware. Esta funcionalidad proporciona una tolerancia a fallas adicional, lo que ayuda a los sistemas a permanecer operativos y a recuperarse fácilmente de posibles problemas.

Integrado en la arquitectura de seguridad de AMD PRO, el temporizador de vigilancia funciona con el arranque seguro y otras funciones básicas para proporcionar una detección de fallas sólida durante las operaciones previas al arranque y en tiempo de ejecución. Esta capacidad refuerza la resiliencia del sistema en entornos cruciales y reduce el riesgo de tiempo de inactividad causado por fallas de software o hardware.

ASPECTOS DESTACADOS DE LA SOLUCIÓN

CAPA DE SEGURIDAD	FUNCIONES	BENEFICIOS
SISTEMA	FUNCIONES DE SEGURIDAD DE OEM	Estrecha colaboración entre desarrolladores de SO, proveedores de hardware y socios OEM para complementar y permitir las funciones de seguridad de nivel empresarial de los OEM.
SEGURIDAD DE SO	SEGURIDAD DE WINDOWS 11	Compatibilidad completa con la iniciativa de PC de núcleo seguro, protección de pila aplicada por hardware, protección avanzada contra amenazas, inicio de sesión mejorado, BitLocker y mucho más.
HARDWARE Y FIRMWARE	PROCESADOR AMD SECURE 2.0	Procesador de seguridad exclusivo que valida el código antes de ejecutarlo para garantizar la integridad de los datos y las aplicaciones.
	AMD PLATFORM SECURE BOOT	Protección de arranque que evita que software no autorizado y malware tomen el control de funciones de sistema básicas.
	AMD MEMORY GUARD	Cifra la memoria del sistema en tiempo real para protegerla contra ataques físicos en caso de que te roben o extravíes tu laptop.
	AMD SHADOW STACK	Enfoque de seguridad sólido para ayudar a proteger contra los ataques de flujo de control mediante la comprobación de la pila normal del programa frente a una copia almacenada en el hardware y la activación de protección de pila aplicada por hardware de Microsoft en la seguridad de Windows 11®.
	PROCESADOR DE SEGURIDAD MICROSOFT PLUTON	Una tecnología de seguridad del chip a la nube diseñada y actualizada por Microsoft que mejora la seguridad en el núcleo de las PC Windows 11 con protección continua para credenciales de usuario, identidades, datos personales y cifrado.
	AMD FIRMWARE TPM	Un TPM de versión de firmware que proporciona autenticidad a la plataforma y controla que no se produzcan violaciones de seguridad.
	CERTIFICACIÓN DE MÓDULO FIPS 140-3 DE NIVEL 1	Estándar de cifrado gubernamental que el sector privado adoptó como práctica recomendada para validar la seguridad del hardware criptográfico.
	PROCESADOR AMD SECURE 2.0	Refuerza una raíz de confianza de hardware, validando el firmware inicial y protegiendo la plataforma contra el código no autorizado.
	CLOUD BARE METAL RECOVERY	Ayuda a permitir la recuperación segura del sistema a través de la nube sin necesidad de enviar dispositivos, diseñado para proporcionar un tiempo de inactividad mínimo durante eventos catastróficos.

RESUMEN

Las tecnologías AMD PRO proporcionan una base completa para abordar las demandas en constante evolución de las empresas modernas. Mediante la integración de seguridad avanzada, manejabilidad sin interrupciones y confiabilidad empresarial en todos los procesadores AMD Ryzen™ PRO, AMD permite a las organizaciones proteger sus datos, optimizar las operaciones de TI y proporcionar productividad de última generación en diversos entornos de trabajo.

A medida que los lugares de trabajo adoptan operaciones híbridas e integran flujos de trabajo basados en IA, en AMD seguimos comprometidos con impulsar la innovación. Con cada generación, las tecnologías AMD PRO amplían los límites de la seguridad, el rendimiento y la manejabilidad, de modo que las empresas estén equipadas a fin de afrontar los desafíos actuales y preparadas para las oportunidades del futuro.

DESCARGO DE RESPONSABILIDAD

La información que se presenta aquí solamente se ofrece con fines informativos y está sujeta a cambios sin previo aviso. Si bien se han tomado todos los recaudos necesarios en la preparación de este documento, su contenido puede contener imprecisiones técnicas, omisiones y errores tipográficos, y AMD no está obligado a actualizarlo ni corregirlo. Asimismo, los PRODUCTOS DE AMD pueden incluir erratas que provocan que el procesador difiera de las especificaciones publicadas, y, si bien la empresa identificará esas erratas ocasionalmente, sin previo aviso, no tiene obligación de hacerlo. Advanced Micro Devices, Inc. no realiza declaraciones ni otorga garantías con respecto a la exactitud o integridad del contenido de este documento, ni asume responsabilidad de ningún tipo, incluidas las garantías implícitas de no violación, comerciabilidad o idoneidad para un fin específico, respecto del funcionamiento o el uso de hardware, software u otros productos de AMD descritos aquí. Este documento no otorga ninguna licencia referente a derechos de propiedad intelectual, incluidas las implícitas o que surjan de un impedimento legal. Los términos y las limitaciones aplicables a la compra o el uso de productos AMD son los que se establecen en un acuerdo firmado entre las partes o los Términos y condiciones de venta estándar de AMD.

NOTAS FINALES

1. El cifrado integral de la memoria del sistema con AMD Memory Guard está incluido en los procesadores AMD Ryzen PRO, AMD Ryzen Threadripper PRO y AMD Athlon PRO. Requiere la habilitación del OEM. Consulta con el fabricante del sistema antes de realizar la compra. GD-206.
2. Los OEM con la función AMD Platform Secure Boot activada conceden permiso para que su código BIOS con firma criptográfica se pueda ejecutar únicamente en plataformas que usen motherboards compatibles con AMD Platform Secure Boot. Los fusibles que son programables una sola vez en el procesador unen el procesador a la clave de firma del código de firmware del OEM. A partir de ese momento, ese procesador solo se puede usar con motherboards que usen la misma clave de firma de código. GD-192.
3. En comparación con Intel vPro, Manejabilidad de AMD PRO implementa más perfiles de DASH Management Initiative a fin de admitir la administración de varios proveedores en computadoras de escritorio y sistemas móviles. KRKP-7
4. En comparación con Intel vPro, Manejabilidad de AMD PRO implementa una versión más reciente del protocolo TLS (Transport Layer Security, Seguridad de la capa de transporte) que proporciona niveles más altos de seguridad y menor latencia (TLS 1.3 frente a 1.2) KRKP-8
5. Informe de Principled Tech: https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. El procesador AMD Secure es un procesador de seguridad exclusivo en el chip integrado en cada sistema en chip (SoC) y ASIC (Application-Specific Integrated Circuit, circuito integrado para aplicaciones específicas) diseñado por AMD. Permite el arranque seguro con una raíz de confianza anclada en el hardware, inicializa el SoC mediante un flujo de arranque seguro y establece un entorno de ejecución de confianza aislado. GD-72.
7. El cifrado integral de la memoria del sistema con AMD Memory Guard está incluido en los procesadores AMD Ryzen PRO, AMD Ryzen Threadripper PRO y AMD Athlon PRO. Como requisito, el OEM debe realizar la habilitación. Consulta con el fabricante del sistema antes de realizar la compra. GD-206
8. Microsoft Pluton es una tecnología de Microsoft con licencia para AMD. Microsoft Pluton es una marca comercial registrada de Microsoft Corporation en los Estados Unidos o en otros países. Obtén más información en https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/. El OEM debe habilitar el procesador de seguridad Microsoft Pluton. Consulta con el OEM antes de realizar la compra. AMD no ha verificado la información de terceros. GD-202.
9. El procesador AMD Secure es un procesador de seguridad exclusivo en el chip integrado en cada sistema en chip (SoC) y ASIC (Application-Specific Integrated Circuit, circuito integrado para aplicaciones específicas) diseñado por AMD. Permite el arranque seguro con una raíz de confianza anclada en el hardware, inicializa el SoC mediante un flujo de arranque seguro y establece un entorno de ejecución de confianza aislado. GD-72.