TECHNOLOGIES AMD PRO

DÉCOUVREZ LA SÉCURITÉ AMD PRO ET LA STRUCTURE AMD POUR DES PC PROFESSIONNELS SÉCURISÉS, FACILES À GÉRER ET FIABLES

L'espace de travail agile et distribué ne cesse d'évoluer. Les opérations hybrides deviennent la norme, les entreprises jonglant entre la collaboration sur site et le travail à distance tout en intégrant l'IA dans les workflows quotidiens. Ainsi, les entreprises sont confrontées à une pression croissante pour moderniser leurs parcs de PC avec des systèmes capables de répondre aux nouveaux défis posés par ces tendances. Elles ont donc besoin de solutions alliant performance, sécurité et gérabilité, adaptées aussi bien aux environnements sur site qu'aux infrastructures cloud.

Les processeurs AMD Ryzen™ PRO équipent les PC professionnels modernes des technologies AMD PRO, un ensemble unifié d'innovations conçues pour répondre aux exigences en constante évolution des entreprises d'aujourd'hui. Ce document explore le pilier de la sécurité des technologies AMD PRO, l'un des trois composants fondamentaux qui caractérisent tous les systèmes équipés de processeurs AMD Ryzen PRO. Bien que la sécurité soit le sujet principal de ce livre blanc, les technologies AMD PRO offrent également une gérabilité avancée et une fiabilité adaptée aux entreprises, fournissant ainsi une solution complète aux entreprises modernes.

Ces trois piliers sont présentés ici afin de présenter le contexte global des technologies AMD PRO, mais ce document se concentrera spécifiquement sur les fonctionnalités de sécurité de nouvelle génération des processeurs AMD Ryzen PRO, conçues pour protéger les PC professionnels actuels contre les menaces en constante évolution.

SÉCURITÉ PRO : PROTÉGER L'ENTREPRISE MODERNE

Les technologies AMD PRO reposent sur des fonctionnalités de sécurité robustes. Les fonctionnalités hardware avancées, telles qu'AMD Memory Guard[1] pour le cryptage complet de la mémoire, AMD Shadow Stack pour la protection contre les attaques de flux de contrôle ou encore la prise en charge complète du processeur cryptographique sécurisé Microsoft Pluton, offrent des protections essentielles contre les menaces sophistiquées. Grâce à la prise en charge intégrée du démarrage sécurisé[2] et à une exécution fiable, les processeurs AMD Ryzen PRO renforcent les appareils à tous les niveaux, garantissant ainsi aux utilisateurs une protection des données et des applications, du terminal au cloud.

Bien que les fonctionnalités de sécurité ultra-modernes soient au cœur de ce livre blanc, la structure générale des technologies AMD PRO (incluant une gérabilité et une fiabilité adaptée aux entreprises) fonctionne de concert afin de fournir aux entreprises une solution complète pour répondre aux nouvelles exigences professionnelles.

GÉRABILITÉ PRO : SIMPLIFICATION DES OPÉRATIONS INFORMATIQUES

La gestion de parcs de PC divers est complexe et fastidieuse, en particulier dans les environnements de travail hybrides. La gérabilité AMD PRO rationalise les opérations grâce à des outils basés sur des normes ouvertes qui permettent une gestion à distance basée sur le cloud et une surveillance des terminaux en temps réel. Ces outils offrent le plus haut niveau de conformité aux normes ouvertes pour la gestion des systèmes à distance[3]. La gérabilité AMD PRO permet à l'utilisateur de bénéficier d'une compatibilité avec des outils de pointe tels que Microsoft Endpoint Manager et Windows Autopilot, garantissant ainsi un processus de déploiement cohérent et efficace.

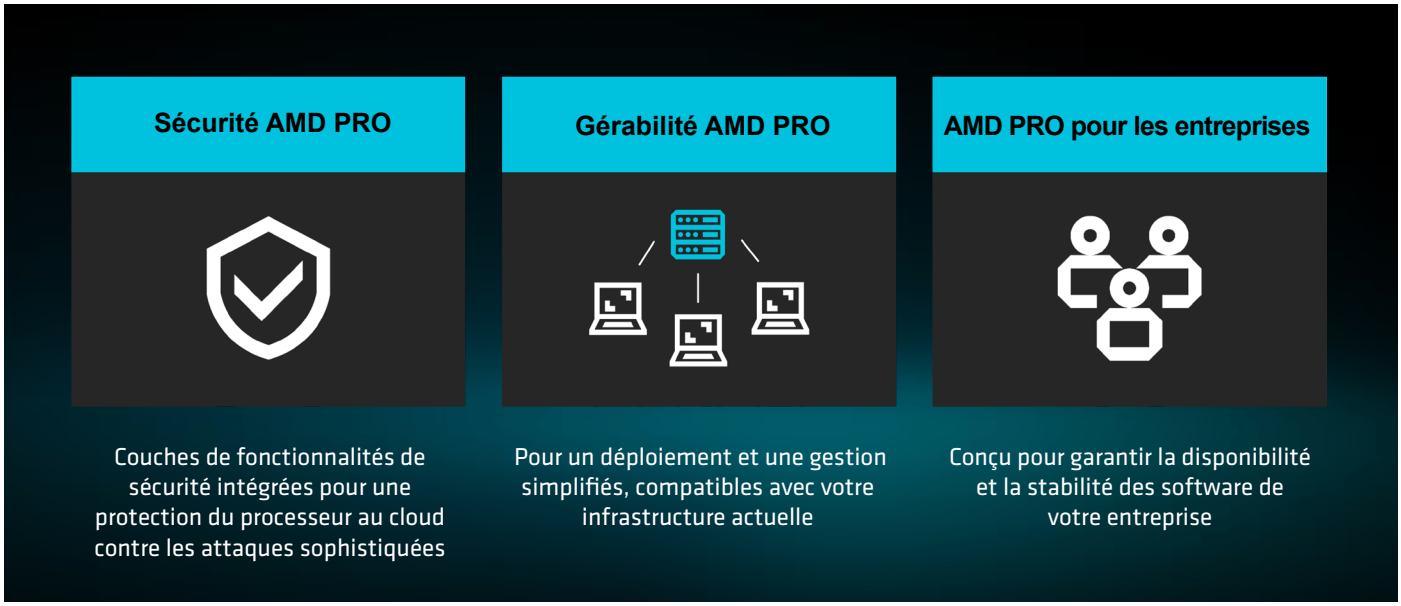
La gérabilité AMD PRO prend en charge les dernières spécifications DMTF DASH (Desktop and Mobile Architecture for System Hardware), intégrant des protocoles de cryptage et d'authentification à jour tels que TLS 1.2 et 1.3. En outre, les systèmes AMD PRO intègrent des composants de sécurité hardware, notamment TPM 2.0, pour un stockage et une protection des clés cryptographiques plus sûrs. Cette approche basée sur des normes offre une protection renforcée et de meilleures performances par rapport aux protocoles propriétaires plus anciens[4]. Les équipes informatiques bénéficient de fonctionnalités telles que le provisionnement à distance, le déploiement automatisé des correctifs et les diagnostics en temps réel. Ces dernières contribuent à réduire les temps d'arrêt, à améliorer la santé des terminaux et à simplifier les opérations.

Des études récentes mettent en évidence l'impact de la gérabilité AMD PRO sur les opérations informatiques, avec des temps de déploiement réduits jusqu'à 41 %[5] par rapport aux processus traditionnels, ainsi qu'une réduction significative des efforts manuels grâce à des interfaces de gestion intuitives et unifiées. Ces fonctionnalités permettent aux entreprises d'aider leurs employés où qu'ils se trouvent, rendant ainsi la gestion des écosystèmes de PC complexes plus simple, plus rapide et plus fiable.

PRO POUR LES ENTREPRISES : DES PERFORMANCES FIABLES POUR TOUTES LES TÂCHES

Les processeurs AMD PRO dotés de fonctionnalités adaptées aux entreprises garantissent la longévité des PC, tout en offrant aux utilisateurs des performances constantes et une grande fiabilité pour les charges de travail professionnelles. Des processus de validation rigoureux assurent un meilleur fonctionnement, ce qui peut contribuer à réduire les coûts informatiques. Une disponibilité mondiale étendue sur une année complète permet aux entreprises de déployer des systèmes à la demande, limitant ainsi les achats initiaux importants. Qu'il s'agisse de prendre en charge des applications basées sur l'IA ou des tâches bureautiques courantes, les processeurs AMD Ryzen™ PRO offrent l'adaptabilité dont les entreprises ont besoin pour prospérer.

Figure 1. Technologies AMD PRO. Au service de chaque PC d'entreprise équipé d'un processeur AMD Ryzen™ PRO.



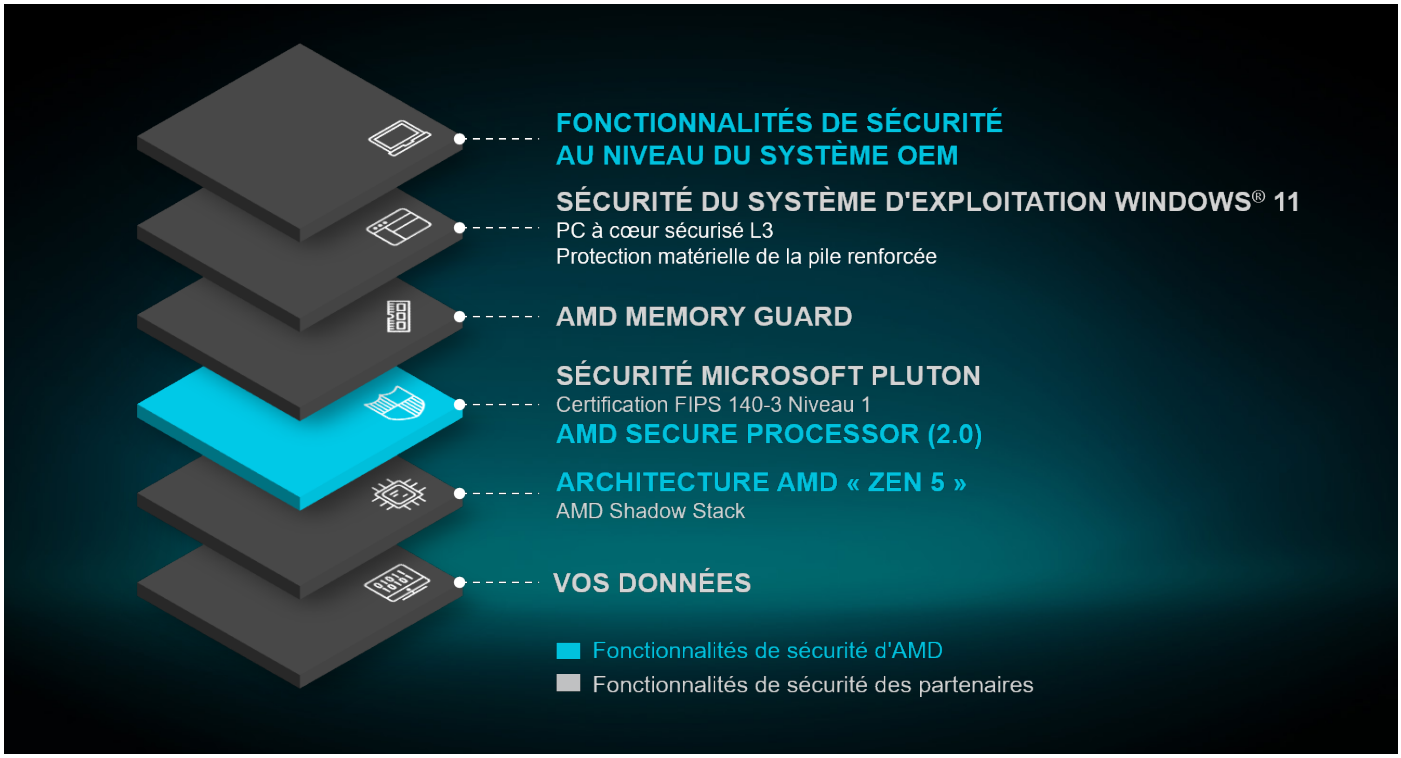
Les technologies AMD PRO pour les entreprises améliorent cette fiabilité en garantissant une cohérence à long terme qui simplifie la planification informatique et optimise le retour sur investissement. Tous les processeurs AMD Ryzen™ PRO offrent des solutions professionnelles avec les caractéristiques suivantes :

- **Stabilité d'image :** 18 mois de stabilité software planifiée pour garantir des transitions fluides et offrir une tranquillité d'esprit aux équipes informatiques.
- **Qualité :** des processus de validation des plateformes améliorés offrant une qualité professionnelle pour les environnements de travail exigeants.
- **Disponibilité :** 24 mois de disponibilité planifiée pour maintenir la cohérence du hardware et assurer la stabilité des opérations d'entreprise.
- **Fiabilité :** une validation continue des plateformes pour assurer une stabilité à long terme et une expérience utilisateur cohérente sur plusieurs générations de processeurs.

En assurant la stabilité hardware et software, les technologies AMD PRO pour les entreprises réduisent la complexité pour les équipes informatiques et fournissent une base fiable pour assurer la réussite à long terme de l'entreprise.

Alors que les entreprises s'efforcent de s'adapter à de nouvelles conditions de travail, les technologies AMD PRO leur apportent un atout stratégique. En intégrant des fonctionnalités de sécurité de pointe, une gérabilité efficace et des fonctionnalités adaptées aux entreprises dans chaque système basé sur un CPU AMD Ryzen PRO, AMD fournit aux entreprises les outils dont elles ont besoin pour protéger leurs opérations, rationaliser la gestion informatique et stimuler l'innovation.

Figure 2. Sécurité AMD PRO. Surpasser les dernières exigences de sécurité pour les appareils modernes.



LES PC ÉQUIPÉS DE PROCESSEURS AMD SONT CONÇUS AVEC UNE SÉCURITÉ MULTICOUCHE DE POINTE À TOUS LES NIVEAUX

AMD travaille en étroite collaboration avec les développeurs de systèmes d'exploitation (OS) et les fabricants d'équipement d'origine (OEM) pour fournir des fonctionnalités de sécurité matérielles qui complètent et renforcent leur conception de sécurité.

En intégrant des mesures de sécurité de pointe à chaque niveau, du silicium aux systèmes d'exploitation, AMD permet aux organisations de protéger leurs actifs les plus critiques tout en limitant les temps d'arrêt et en réduisant la complexité informatique.

SÉCURITÉ INTÉGRÉE À CHAQUE COUCHE

Les technologies AMD PRO intègrent la sécurité comme un pilier fondamental sur tous les appareils équipés de processeurs AMD Ryzen™ PRO. Conçus pour répondre aux défis en constante évolution de l'entreprise moderne, ces processeurs offrent une protection multicouche qui commence à la base par un silicium robuste et s'étend jusqu'aux défenses au niveau du micrologiciel et du système d'exploitation.

RACINE DE CONFIANCE HARDWARE : INTÉGRITÉ DÈS LE DÉMARRAGE

L'architecture du silicium d'AMD fournit une racine de confiance hardware intégrée qui aide les processus de démarrage sécurisé. L'AMD Secure Processor 2.0[6] (ASP 2.0) renforce cette confiance en vérifiant l'intégrité du micrologiciel et du BIOS de l'OEM pour assurer une protection contre les modifications non autorisées et les attaques potentielles ciblant le micrologiciel.

PROTECTION DE LA MÉMOIRE REDÉFINIE : AMD MEMORY GUARD[7]

AMD Memory Guard crypte toute la mémoire système en temps réel, ce qui permet de protéger les données sensibles contre les attaques par démarrage à froid et les attaques physiques. Grâce aux moteurs de cryptage hardware dédiés, cette fonctionnalité offre une protection renforcée, même dans les cas de vol d'appareils.

ARCHITECTURE NOUVELLE GÉNÉRATION : AMD « ZEN 5 » ET AU-DELÀ

La dernière architecture de cœur AMD « Zen 5 » introduit des fonctionnalités de sécurité améliorées, notamment Supply Chain Security, qui exploite un ID de processeur unique pour permettre un suivi sécurisé du hardware AMD authentique tout au long de son cycle de vie. Ces innovations renforcent la résilience des terminaux face aux cybermenaces de plus en plus sophistiquées.

CONFORMITÉ AUX NORMES DU SECTEUR

Les processeurs AMD PRO sont conçus pour dépasser les exigences de sécurité modernes, notamment la certification FIPS 140-3 Niveau 1. L'intégration avec Microsoft Pluton[8] renforce encore la protection des systèmes Windows en ajoutant des mécanismes d'authentification et de cryptage sécurisés.

L'ARCHITECTURE DE SÉCURITÉ AMD PRO

AMD SECURE PROCESSOR 2.0[9] : UNE BASE PLUS SOLIDE

Au cœur de l'architecture de sécurité AMD PRO se trouve l'AMD Secure Processor 2.0 (ASP 2.0), un composant hardware dédié intégré dans chaque système sur puce (SoC). ASP 2.0 constitue une racine de confiance hardware et prend en charge un flux de démarrage sécurisé, qui vérifie l'intégrité du micrologiciel dès la mise sous tension de l'appareil. Son environnement d'exécution de confiance isolé protège les opérations sensibles contre les attaques potentielles. Voici ses principaux composants :

- **Coprocesseur cryptographique (CCP) :** moteur cryptographique hautes performances qui gère la génération de clés et les opérations cryptographiques au niveau hardware, essentiel pour les tâches de sécurité urgentes.
- **ROM de démarrage :** mémoire sécurisée en lecture seule contenant le micrologiciel nécessaire à l'initialisation du démarrage.
- **Mémoire vive statique (SRAM) :** fournit une prise en charge à faible consommation des processus sécurisés.
- **Unité de gestion de la mémoire (MMU) :** régule l'accès à la ROM de démarrage et à la SRAM afin d'assurer un contrôle strict des ressources mémoire.
- **Cloud Bare Metal Recovery :** facilite la restauration sécurisée des appareils via le cloud, garantissant la continuité des activités même en cas de panne critique.
- **Supply Chain Security :** authentifie le hardware AMD authentique à chaque étape de son cycle de vie, protégeant ainsi les composants contre toute altération ou contrefaçon.
- **Watchdog Timer :** détecte et atténue les processus bloqués au niveau hardware, améliorant ainsi la résilience du système.

Ces fonctionnalités répondent collectivement au risque accru d'exposition des données sensibles de l'entreprise en cas de déplacement, de travail à distance ou dans d'autres scénarios de mobilité.

INTÉGRATION FLUIDE À LA SÉCURITÉ WINDOWS

L'architecture de sécurité AMD PRO s'aligne de manière fluide aux fonctionnalités de sécurité de Windows 11, notamment le démarrage sécurisé et la protection hardware de la pile, afin de créer un système de défense multicouche complet. Ensemble, ces fonctionnalités renforcent les terminaux contre les attaques ciblant le micrologiciel, le BIOS, les pilotes et le système d'exploitation.

AMD ROM ARMOR

La mémoire flash SPI (Serial Peripheral Interconnect) d'une carte mère contient à la fois l'UEFI de la carte mère et des informations de configuration supplémentaires, notamment l'état du démarrage sécurisé.

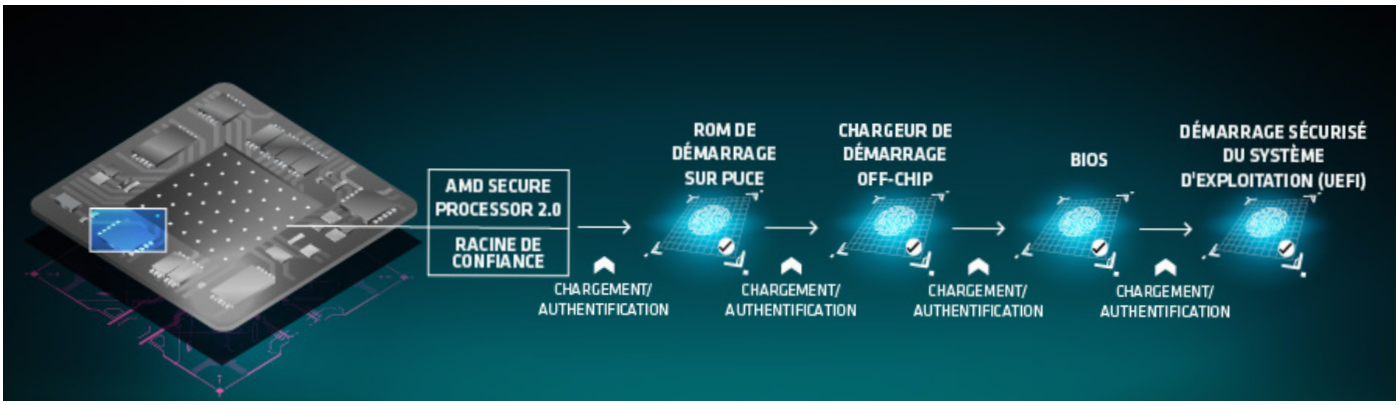
AMD ROM Armor fonctionne avant même l'initialisation du système d'exploitation et fournit une protection contre les modifications non autorisées de la mémoire flash SPI. En assurant l'intégrité de la mémoire flash SPI avant le chargement du système d'exploitation, AMD ROM Armor contribue à établir une base renforcée pour le système. Une fois configurée et activée, cette fonctionnalité renforce la protection du périphérique flash SPI de l'ordinateur contre les écritures non autorisées.

DÉMARRAGE SÉCURISÉ DE PLATEFORME (PSB) AMD

Le démarrage sécurisé de plateforme (PSB) d'AMD fournit une racine de confiance (RoT) hardware afin d'authentifier le micrologiciel initial, y compris le BIOS, lors du processus de démarrage de l'appareil. Lors de la mise sous tension d'un système, ASP exécute son code ROM de démarrage, qui authentifie plusieurs codes de chargement de démarrage d'ASP, avant d'initialiser la puce et la mémoire système. Une fois que la mémoire système est initialisée, le code de chargement de démarrage d'ASP vérifie le code du BIOS de l'OEM et authentifie d'autres composants des micrologiciels avant de démarrer le système d'exploitation.

PSB est conçu pour assurer l'intégrité de la plateforme en fournissant une protection supérieure contre les micrologiciels intempestifs ou malveillants, en leur interdisant automatiquement l'accès dès leur détection. Il sécurise ainsi la transition du micrologiciel de bas niveau au système d'exploitation.

Figure 3. Démarrage sécurisé de plateforme AMD.



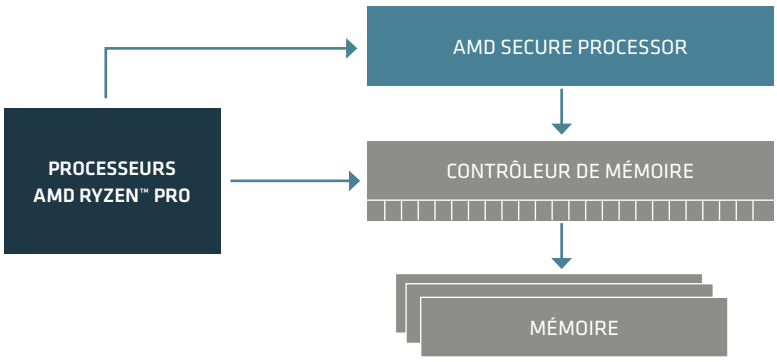
AMD MEMORY GUARD[3]

AMD Memory Guard est une technologie complète de cryptage de la mémoire conçue pour protéger les données des clients contre les attaques physiques. Avec AMD Memory Guard, tout le contenu de la mémoire DRAM est crypté à l'aide d'une clé aléatoire pour assurer une protection contre les attaques physiques par démarrage à froid, l'espionnage d'interface DRAM et d'autres attaques similaires.

Pour les systèmes avec NVDIMM, AMD Memory Guard aide aussi à se protéger contre les attaques consistant à retirer un module de mémoire et à tenter d'en récupérer le contenu. Cette protection est mise en œuvre par un hardware dédié dans les contrôleurs de mémoire sur puce.

- Chaque contrôleur comprend un moteur Advanced Encryption Standard (AES) hautes performances, qui crypte les données lors de leur écriture dans la DRAM, pour les décrypter à la lecture.
- Une clé 128 bits est produite par un générateur hardware de nombres aléatoires conforme à la norme NIST SP 800-90 dans un mode qui utilise un réglage à base d'adresse physique supplémentaire pour mieux se protéger contre les attaques par déplacement de blocs de cryptogrammes.
- La clé de cryptage utilisée par le moteur AES avec AMD Memory Guard est générée de manière aléatoire à chaque réinitialisation du système. De plus, elle est invisible pour tous les software exécutés sur les cœurs de CPU. Cette clé est entièrement gérée par AMD Secure Processor (ASP).

Figure 4. AMD Memory Guard.



AMD SHADOW STACK

La programmation orientée retour (ROP) est un vecteur d'attaque de plus en plus populaire. Les attaques ROP n'injectent pas leur propre code malveillant. Au lieu de cela, ils essaient de prendre le contrôle d'un système en exploitant les faiblesses du code légitime.

FONCTIONNEMENT

En programmation informatique, une « routine » consiste à réaliser une série spécifique d'opérations. Lorsqu'un programme software s'exécute, cela s'appelle une routine. Une fois sa tâche accomplie, la routine retourne au programme principal à l'aide de l'adresse de retour. Ce processus comprend un saut (jump) et un retour (return)

Dans les attaques ROP, les attaquants modifient l'adresse de retour après le saut de routine. Au lieu de retourner au programme principal, elle passe à d'autres routines, et assemble des routines secondaires en vue de créer un code malveillant susceptible de nuire au système. Et surtout, ce type d'attaque échappe aux détections, car il semble utiliser un code légitime.

L'architecture de sécurité AMD PRO aide à atténuer les attaques ROP en donnant au software un accès à certains registres du CPU où une copie de l'adresse de retour peut être stockée. Les applications peuvent utiliser une pile parallèle, appelée pile cachée ou « shadow stack », pour empêcher les attaques logicielles qui tentent de modifier le flux de contrôle. La pile cachée utilise du hardware spécialisé pour stocker une copie des adresses de retour, qui sont ensuite comparées aux opérations de retour de la pile de programmation normale.

Si le contenu diffère, une exception est générée pour empêcher le code malveillant d'accéder au contrôle du système. Ainsi, le hardware de la pile cachée peut aider à atténuer les dysfonctionnements logiciels les plus courants et exploitables.

AMD Shadow Stack est un renfort supplémentaire face aux attaques ROP. Comme une copie de l'adresse de retour se trouve dans le hardware, un code malveillant aura énormément de mal à la modifier.

La protection Microsoft hardware de la pile, intitulée Microsoft Hardware Enforced Stack Protection, est prise en charge par l'architecture de sécurité AMD PRO grâce à AMD Shadow Stack.

PC À CŒUR SÉCURISÉ MICROSOFT

La technologie de PC à cœur sécurisé de Microsoft protège votre PC contre les vulnérabilités des micrologiciels, les attaques contre les systèmes d'exploitation et les accès non autorisés aux appareils et données, au moyen de contrôles d'accès et de systèmes d'authentification avancés.

Cette technologie est activée sur les plateformes à architecture de sécurité AMD PRO à l'aide de divers services et technologies de sécurité :

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

TECHNOLOGIE DE VIRTUALISATION AMD (AMD-V™) AVEC GMET

AMD-V est un ensemble d'extensions matérielles qui permettent la virtualisation sur les plateformes AMD. Guest Mode Execute Trap (GMET) est une amélioration des performances intégrée à la puce, qui permet à l'hyperviseur de gérer efficacement des contrôles d'intégrité de code et ainsi de se protéger contre les malware.

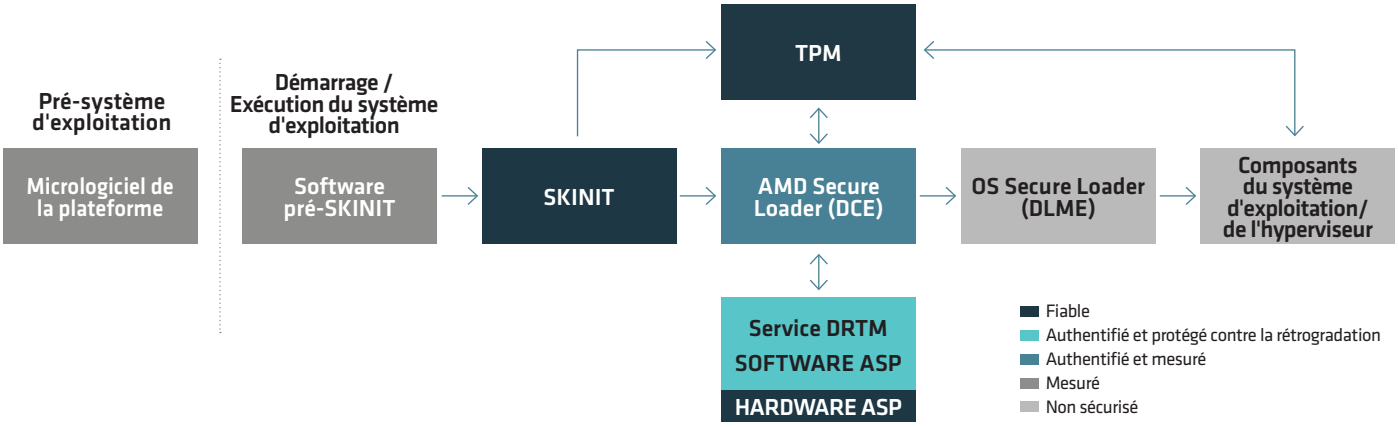
SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

L'instruction d'initialisation et de saut sécurisés avec attestation (SKINIT) permet de créer une « racine de confiance » commençant par un mode opérationnel initialement non sécurisé. SKINIT réinitialise le processeur pour établir un environnement d'exécution renforcé, destiné à un composant software de chargement sécurisé (Secure Loader, SL), et démarre l'exécution du SL pour éviter toute altération. SKINIT étend la racine de confiance hardware jusqu'au SL.

AMD SECURE LOADER (SL)

AMD Secure Loader est chargé de valider la configuration de la plateforme en interrogeant le hardware et en demandant des informations de configuration au service DTRM fourni par AMD Secure Processor (ASP).

Figure 5. Flux DRTM.



À tout moment après le démarrage du système d'exploitation, celui-ci peut demander au bloc de service AMD de re-mesurer et d'attester les valeurs avant de procéder à d'autres opérations. Le système d'exploitation est donc en mesure de protéger le système, du démarrage à l'exécution.

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

Le bloc AMD DRTM se compose de l'instruction SKINIT du CPU, de l'ASP, et du SL. Il est chargé de créer et de préserver une chaîne de confiance entre les micrologiciels. Le bloc AMD DRTM laisse le micrologiciel et le chargeur de démarrage se charger librement, car ce sont des codes sans protection, mais juste après leur lancement, le système adoptera un état de confiance basé sur le hardware qui renverra le micrologiciel sur un trajet de code mesuré et bien connu.

Le bloc AMD DRTM se compose de l'instruction SKINIT du CPU, de l'ASP, et du SL. Il est chargé de créer et de préserver une chaîne de confiance entre les micrologiciels.

Le bloc AMD DRTM laisse le micrologiciel et le chargeur de démarrage se charger librement, car ce sont des codes sans protection, mais juste après leur lancement, le système adoptera un état de confiance basé sur le hardware qui renverra le micrologiciel sur un trajet de code mesuré et bien connu.

Le bloc DRTM mesure et authentifie le chargeur de démarrage, et collecte et enregistre de manière sécurisée les informations système suivantes, qui serviront plus tard au système d'exploitation, notamment à des fins de vérification et d'attestation :

- Carte de la mémoire physique
- Emplacement de l'espace de configuration PCI
- Configuration APIC locale
- Configuration APIC des E/S
- Configuration IOMMU / Configuration TMR
- Configuration de la gestion de la consommation énergétique

CONFIANCE MATÉRIELLE PARTAGÉE

Cela signifie que le composant micrologiciel est authentifié et mesuré par le bloc ASP au niveau du silicium AMD, et que la mesure est sauvegardée et protégée en vue d'une utilisation ultérieure par le système d'exploitation, notamment à des fins de vérification et d'authentification.

SUPERVISEUR AMD SMM

Le mode de gestion du système (SMM) est un mode de CPU spécial dans les microcontrôleurs x86 qui gère l'alimentation, la configuration hardware, la surveillance thermique et d'autres opérations au niveau de l'appareil. À chaque demande d'exécution d'une de ces opérations système, une interruption (SMI) est invoquée lors de l'exécution et le code SMM installé par le BIOS s'exécute. Le code SMM s'exécute avec le niveau de priorité le plus élevé, sans être visible par le système d'exploitation, car c'est une cible idéale des activités malveillantes qui pourraient l'utiliser pour accéder à la mémoire de l'hyperviseur afin d'en compromettre le contenu.

Le gestionnaire SMI est habituellement fourni par un autre éditeur que celui du système d'exploitation, et il a accès à la mémoire et aux ressources du système d'exploitation et de l'hyperviseur. Cela signifie que des vulnérabilités exploitables dans le code SMM peuvent conduire à des failles du système d'exploitation Windows, de l'hyperviseur (HV) et de la sécurité à base de virtualisation (VBS).

Pour mieux isoler le SMM, AMD propose un module de sécurité intitulé AMD SMM Supervisor, qui s'exécute immédiatement avant le transfert du contrôle au gestionnaire SMI, suite à une interruption SMI. AMD SMM Supervisor se trouve dans le bloc de service AMD DRTM et sert à :

- interdire au SMM de modifier la mémoire du système d'exploitation ou de l'hyperviseur, sauf pour un petit tampon de communication entre ceux-ci ;
- empêcher le SMM d'introduire un nouveau code SMM lors de l'exécution ;
- empêcher le SMM d'accéder au DMA, aux E/S ou aux registres capables de compromettre l'hyperviseur ou le système d'exploitation.

PROTECTION DE DMA

Grâce à la technologie de remappage de DMA, les plateformes AMD prennent en charge la protection de l'accès direct à la mémoire (DMA) dans les environnements de pré-démarrage et de système d'exploitation via les technologies sécurisées d'AMD telles que Input Output Memory Management Unit (IOMMU).

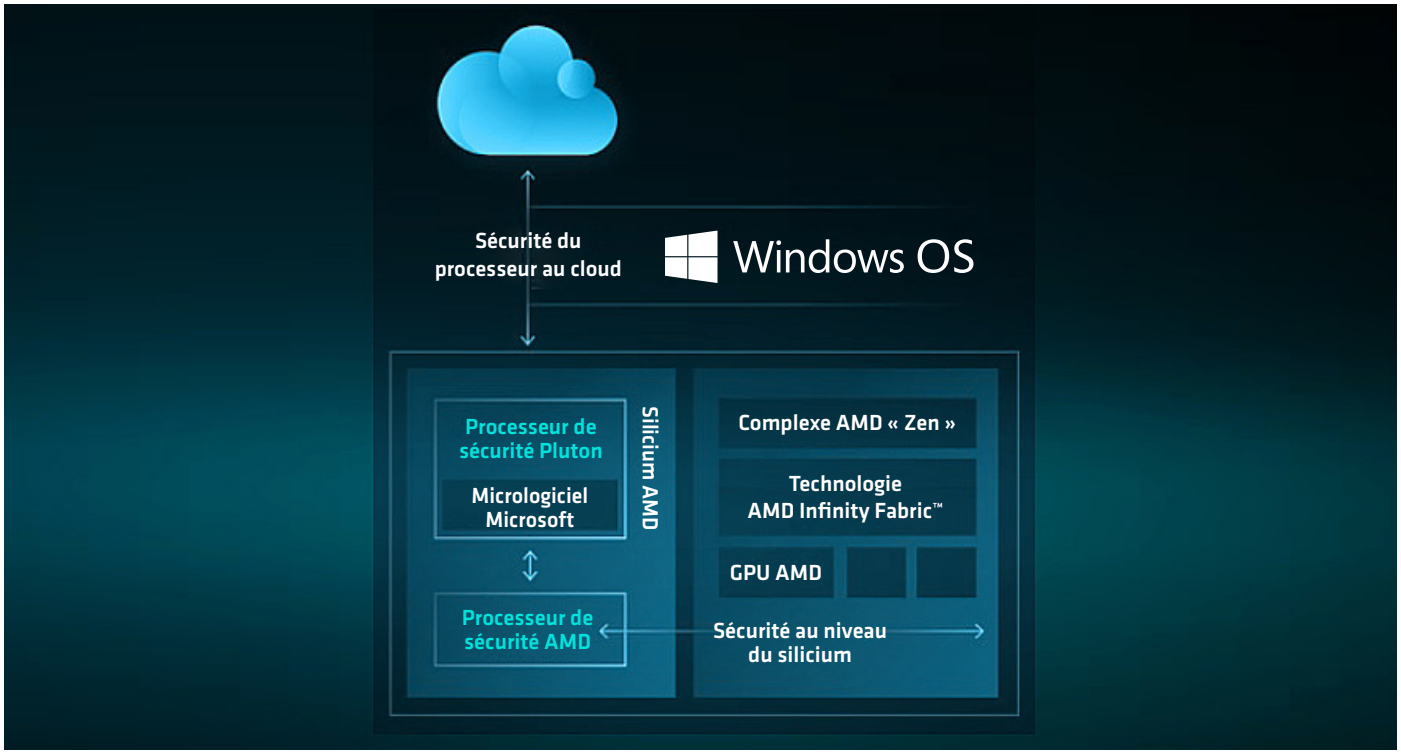
- La protection de DMA permet d'éviter les éventuelles attaques ciblant le micrologiciel de la plateforme, lorsque des agresseurs utilisent des appareils connectés pour viser un accès direct à la mémoire.
- L'accès DMA offre un accès direct à l'espace d'adresse de mémoire physique des appareils pour en améliorer les performances. Toutefois, il simplifie également l'injection de malware dans le système à l'insu du système d'exploitation.

Pour éviter de telles attaques, AMD a conçu une architecture de sécurité destinée à gérer et contrôler l'accès DMA de l'appareil, via l'IOMMU, au niveau du micrologiciel précédant le système d'exploitation. L'architecture de sécurité DMA transfère la responsabilité des paramètres de protection de la mémoire système, du micrologiciel à l'OS, une fois que le chargeur de démarrage du système d'exploitation a été établi en mémoire. La protection de DMA à l'aide de l'IOMMU s'applique à chaque démarrage, jusqu'à ce que le système d'exploitation assume lui-même le contrôle de l'IOMMU.

PROCESSEUR DE SÉCURITÉ MICROSOFT PLUTON[8]

Conçu par Microsoft et développé par des partenaires silicium, Microsoft Pluton est un processeur de cryptographie sécurisé intégré au CPU qui assure la sécurité au cœur du système afin de garantir l'intégrité du code et la protection la plus récente grâce aux mises à jour fournies par Microsoft via Windows Update.

Figure 6. Présentation de l'architecture de sécurité Microsoft Pluton.



Pluton protège les informations d'identification, identités, données personnelles et clés de cryptage. Les informations sont beaucoup plus difficiles à supprimer, même si un attaquant installe un malware ou prend le contrôle physique complet du PC.

Microsoft Pluton est conçu pour fournir les fonctionnalités d'un Trusted Platform Module (TPM) tout en proposant d'autres fonctionnalités de sécurité, au-delà de ce qui est possible avec la spécification TPM 2.0. Il permet d'accroître les fonctionnalités du micrologiciel Pluton et du système d'exploitation au fil du temps via Windows Update.

AMD Secure Processor 2.0 (ASP 2.0) et le processeur de sécurité Microsoft Pluton coexistent sur la puce client AMD et communiquent afin de protéger l'intégrité de l'appareil. Microsoft Pluton contribue à protéger les systèmes PC Windows en agissant comme une racine de confiance hardware intégrée pour l'écosystème Windows, tandis qu'ASP 2.0 agit comme une racine de confiance hardware au niveau du silicium, ce qui contribue à assurer l'intégrité en authentifiant le micrologiciel initial chargé sur les plateformes.

MISE À JOUR DES PLATEFORMES

Les processeurs AMD PRO offrent des défenses de sécurité en temps réel contre les attaquants qui tentent d'accéder au système, ainsi qu'un mécanisme de mise à jour robuste. Cela permet aux organisations de mettre à jour leurs plateformes et de rectifier les vulnérabilités créées par des bugs matériels ou logiciels.

AMD travaille en étroite collaboration avec les OEM pour fournir une architecture de mise à jour de plateforme renforcée, conforme aux meilleures pratiques et pouvant être intégrée aux solutions de mise à jour de plateforme des OEM. Les processeurs AMD PRO disposent en outre d'une fonctionnalité Firmware Anti-Rollback (FAR), qui empêche la rétrogradation du micrologiciel d'AMD Secure Processor 2.0 (ASP 2.0) grâce à une politique basée sur le hardware. Enfin, les processeurs AMD PRO contiennent également une architecture de récupération sécurisée, « A/B Recovery », qui peut s'intégrer à une solution OEM afin de permettre la récupération en cas de panne critique.

ACCÉLÉRATEUR CRYPTOGRAPHIQUE

Les opérations cryptographiques sont désormais importantes dans le cadre de la protection des données et des communications. Aussi cruciales soient-elles, elles exigent par ailleurs énormément de ressources de calcul. AMD fournit de nouvelles instructions optimisées au niveau du silicium pour contribuer à réduire les coûts associés aux calculs de l'algorithme cryptographique.

Les architectures AMD « Zen 2 » et supérieures ont ajouté la prise en charge du cryptage AES vectorisé pour 256 bits (vAES256) et intègrent des intrinsèques AES au niveau x86, permettant aux applications utilisateur de bénéficier de performances et d'une efficacité cryptographiques améliorées.

CERTIFICATION FIPS 140-3 NIVEAU 1

Compte tenu de la nature sensible des données que les organismes gouvernementaux gèrent et des services essentiels qu'ils fournissent, la sécurité des terminaux est une préoccupation majeure lors de l'achat de PC portables pour les administrations. Un hardware obsolète dépourvu de fonctionnalités de sécurité modernes peut entraîner des coûts élevés liés à la perte de données et aux interruptions de service.

Les Federal Information Processing Standards (FIPS) des États-Unis sont un ensemble de normes annoncées publiquement que le National Institute of Standards and Technology (NIST) a développées pour les systèmes informatiques des organismes gouvernementaux non militaires et de leurs sous-traitants. Les normes FIPS définissent les exigences en matière de sécurité et d'interopérabilité des ordinateurs.

Les processeurs AMD PRO incluent la certification de sécurité **FIPS 140-3 Niveau 1**.

Figure 7. Programme de validation d'algorithme cryptographique pour les processeurs AMD Ryzen™ PRO Série 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

Le module FIPS est une combinaison de hardware, de software et/ou de micrologiciels prenant en charge les fonctionnalités de sécurité à certifier. Bien que les normes FIPS aient été développées pour être utilisées par le gouvernement fédéral, de nombreux acteurs du secteur privé les adoptent volontairement, notamment les institutions financières et les fournisseurs de cloud. De plus, leur utilisation s'étend au-delà de l'Amérique du Nord, y compris aux processeurs informatiques destinés aux partenaires européens de l'OTAN.

CLOUD BARE METAL RECOVERY

Cloud Bare Metal Recovery offre un mécanisme sécurisé de restauration à distance des systèmes, réduisant les temps d'arrêt et assurant la continuité des activités en cas de panne matérielle ou logicielle critique. Cette fonctionnalité s'active avant le démarrage du système d'exploitation pour permettre la restauration du système via le cloud sans nécessiter l'envoi de l'appareil pour réparation.

En s'intégrant à l'architecture de sécurité AMD PRO, Cloud Bare Metal Recovery renforce l'initialisation et la restauration au niveau du hardware afin de prévenir toute altération ou exploitation malveillante pendant le processus de restauration.

SUPPLY CHAIN SECURITY (DEVICE IDENTITY)

La sécurité Supply Chain Security, assurée par AMD Device Identity, authentifie le hardware AMD tout au long de son cycle de vie, de la fabrication au déploiement et au-delà. Cette fonctionnalité permet de garantir la traçabilité et la protection contre les composants contrefaits ou altérés, garantissant ainsi aux entreprises l'intégrité de leur hardware.

AMD Device Identity fournit une vérification cryptographique de l'authenticité du silicium AMD, afin que seul le hardware authentique soit intégré aux systèmes d'entreprise. Cela permet de se protéger contre les attaques visant la chaîne logistique et qui pourraient compromettre le micrologiciel ou le hardware avant le déploiement.

WATCHDOG TIMER

Watchdog Timer améliore la fiabilité du système en détectant et en atténuant les processus bloqués ou qui ne répondent pas au niveau hardware. Cette fonctionnalité renforce la tolérance aux pannes, ce qui permet aux systèmes de rester opérationnels et de se rétablir efficacement en cas de problèmes.

Intégré à l'architecture de sécurité AMD PRO, Watchdog Timer fonctionne avec le démarrage sécurisé et d'autres fonctionnalités de base pour fournir une détection fiable des pannes pendant les opérations de pré-démarrage et d'exécution. Cette fonctionnalité renforce la résilience du système dans les environnements critiques et réduit le risque d'interruption de service causée par des pannes logicielles ou matérielles.

POINTS FORTS DE LA SOLUTION

COUCHE DE SÉCURITÉ	FONCTION-NALITÉS	AVANTAGES
SYSTÈME	FONCTION-NALITÉS DE SÉCURITÉ DES OEM	Collaboration étroite entre le développeur de système d'exploitation, le fournisseur de hardware et les partenaires OEM pour compléter et activer les fonctionnalités de sécurité d'entreprise OEM.
SÉCURITÉ DU SYSTÈME D'EXPLOITATION	WINDOWS 11 SECURITY	Prise en charge complète de l'initiative PC à cœur sécurisé, de la protection hardware de la pile, de la protection avancée contre les menaces, de l'identification améliorée, de BitLocker et plus encore.
HARDWARE ET MICROLOGICIEL	AMD SECURE PROCESSOR 2.0	Un processeur de sécurité dédié qui valide le code avant de l'exécuter pour garantir l'intégrité des données et des applications.
	DÉMARRAGE SÉCURISÉ DE PLATEFORME AMD	Protection au démarrage qui permet d'empêcher les software non autorisés et malveillants de prendre le contrôle des fonctions vitales du système.
	AMD MEMORY GUARD	Offre un cryptage en temps réel de la mémoire système qui permet de vous défendre contre les attaques physiques en cas de perte ou de vol de votre PC portable.
	AMD SHADOW STACK	Approche robuste de la sécurité pour assurer une meilleure protection contre les attaques du flux de contrôle en vérifiant la pile de programmation normale par rapport à une copie stockée sur le hardware et en activant la protection hardware de la pile de Microsoft dans la sécurité Windows 11®.
	PROCESSEUR DE SÉCURITÉ MICROSOFT PLUTON	Une technologie de sécurité du processeur au cloud conçue et mise à jour par Microsoft, qui renforce la sécurité au cœur des PC Windows 11 avec une protection continue des informations d'identification, des identités, des données personnelles et du cryptage.
	AMD FIRMWARE TPM	Un TPM sous forme de micrologiciel qui garantit l'authenticité de la plateforme et permet de s'assurer qu'il n'y a aucun signe de failles de sécurité.
	CERTIFICATION DU MODULE FIPS 140-3 NIVEAU 1	Norme de cryptage gouvernementale adoptée par le secteur privé comme meilleure pratique pour valider la sécurité du hardware cryptographique.
	AMD SECURE PROCESSOR 2.0	Constitue une racine de confiance hardware, validant le micrologiciel initial et protégeant la plateforme contre le code non autorisé.
	CLOUD BARE METAL RECOVERY	Permet une récupération sécurisée du système via le cloud sans avoir à expédier d'appareils, pour minimiser les temps d'arrêt en cas de panne critique.

RÉCAPITULATIF

Les technologies AMD PRO offrent une base complète pour répondre aux exigences en constante évolution des entreprises modernes. En intégrant une sécurité avancée, une gérabilité fluide et une fiabilité adaptée aux entreprises dans chaque processeur AMD Ryzen™ PRO, AMD permet aux entreprises de protéger leurs données, de rationaliser leurs opérations informatiques et de garantir une productivité supérieure dans divers environnements de travail.

À mesure que les organisations adoptent des opérations hybrides et intègrent des workflows basés sur l'IA, AMD s'engage toujours à stimuler l'innovation. À chaque génération, les technologies AMD PRO repoussent les limites de la sécurité, des performances et de la gérabilité afin d'aider les entreprises à faire face aux défis d'aujourd'hui et à se préparer aux opportunités de demain.

CLAUSE DE NON-RESPONSABILITÉ

Les informations contenues dans le présent document ne sont fournies qu'à titre indicatif et peuvent être modifiées sans préavis. Bien que toutes les précautions aient été prises dans la préparation du présent document, il pourrait cependant contenir des inexactitudes techniques, des omissions et des erreurs typographiques. AMD n'a aucune obligation de mettre à jour ou de corriger ces informations. Par ailleurs, les PRODUITS AMD peuvent contenir des défauts, ou « errata », susceptibles d'amener le processeur à s'écarter des spécifications publiées. AMD identifiera de tels défauts de temps à autre, sans préavis, sans que cela constitue pour autant une obligation de le faire. Advanced Micro Devices, Inc. n'émet aucune déclaration ni garantie concernant l'exactitude ou le caractère complet du contenu du présent document, et n'assume aucune responsabilité que ce soit, notamment de garantie implicite de non-violation, de qualité marchande ou d'adaptation à des usages particuliers lors de l'utilisation ou du fonctionnement de composants hardware, software ou d'autres produits AMD présentés ici. Aucune licence, notamment implicite ou découlant d'une question déjà tranchée, n'est accordée par le présent document pour quelque droit de propriété intellectuelle que ce soit. Les conditions et limitations applicables à l'achat ou à l'utilisation de produits AMD sont définies dans un accord signé entre les parties, ou dans les conditions générales de vente d'AMD.

NOTES DE BAS DE PAGE

1. Le cryptage intégral de la mémoire système avec AMD Memory Guard est inclus dans les processeurs AMD Ryzen PRO, AMD Ryzen Threadripper PRO et AMD Athlon PRO. Activation nécessaire par l'OEM. Vérifiez auprès du fabricant de votre système avant l'achat. GD-206.
2. En activant le démarrage sécurisé de plateforme AMD, un OEM permet à son code BIOS doté d'une signature cryptographique de s'exécuter uniquement sur les plateformes dotées d'une carte mère compatible avec cette fonctionnalité. Des fusibles de mémoire morte programmable au sein du processeur associent le processeur à la clé de signature du code du micrologiciel de l'OEM. À partir de là, ce processeur peut uniquement être utilisé avec des cartes mères dotées de la même clé de signature. GD-192.
3. Par rapport à Intel vPro, la gérabilité AMD PRO met en œuvre davantage de profils DASH Management Initiative pour prendre en charge la gestion multifournisseur des systèmes de bureau et portables. KRKP-7
4. Par rapport à Intel vPro, la gérabilité AMD PRO met en œuvre une version plus récente du protocole TLS (Transport Layer Security) qui offrait des niveaux de sécurité plus élevés et une latence plus faible (TLS 1.3 par rapport à TLS 1.2) KRKP-8
5. Rapport Principled Tech - https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. AMD Secure Processor est un processeur de sécurité sur puce dédié et intégré à chaque SoC (système sur puce) et ASIC (Application Specific Integrated Circuit) conçu par AMD. Il permet un démarrage sécurisé avec racine de confiance ancrée au niveau matériel, initialise le SoC via un flux d'amorçage sécurisé et établit un environnement d'exécution de confiance isolé. GD-72.
7. Le cryptage intégral de la mémoire système avec AMD Memory Guard est inclus dans les processeurs AMD Ryzen PRO, AMD Ryzen Threadripper PRO et AMD Athlon PRO. Activation nécessaire par l'OEM. Vérifiez auprès du fabricant de votre système avant l'achat. GD-206
8. Microsoft Pluton est une technologie détenue par Microsoft et concédée sous licence à AMD. Microsoft Pluton est une marque déposée de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. En savoir plus sur https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/. Le processeur de sécurité Microsoft Pluton nécessite une activation OEM. Vérifiez auprès de l'OEM avant l'achat. AMD n'a pas vérifié les déclarations tierces. GD-202.
9. AMD Secure Processor est un processeur de sécurité sur puce dédié et intégré à chaque SoC (système sur puce) et ASIC (Application Specific Integrated Circuit) conçu par AMD. Il permet un démarrage sécurisé avec racine de confiance ancrée au niveau matériel, initialise le SoC via un flux d'amorçage sécurisé et établit un environnement d'exécution de confiance isolé. GD-72.