Livre blanc technique

# HP Sure Start

Réparation et protection automatiques du BIOS

Mai 2018

# Sommaire



# Introduction

HP Sure Start est capable de détecter, d'arrêter et de récupérer automatiquement après une attaque ou une corruption du BIOS. Ce dispositif agit sans intervention informatique et présente peu voire aucune perte de productivité pour l'utilisateur. À chaque fois que l'ordinateur démarre, HP Sure Start valide automatiquement l'intégrité du code du BIOS afin de s'assurer que le PC est à l'abri des attaques malveillantes. Une fois l'ordinateur opérationnel, le système de détection des intrusions en fonctionnement (Runtime Intrusion Detection) surveille en permanence la mémoire. Si une attaque se produit, le PC est capable de s'auto-réparer en utilisant une « copie de référence » isolée du BIOS en moins d'une minute.

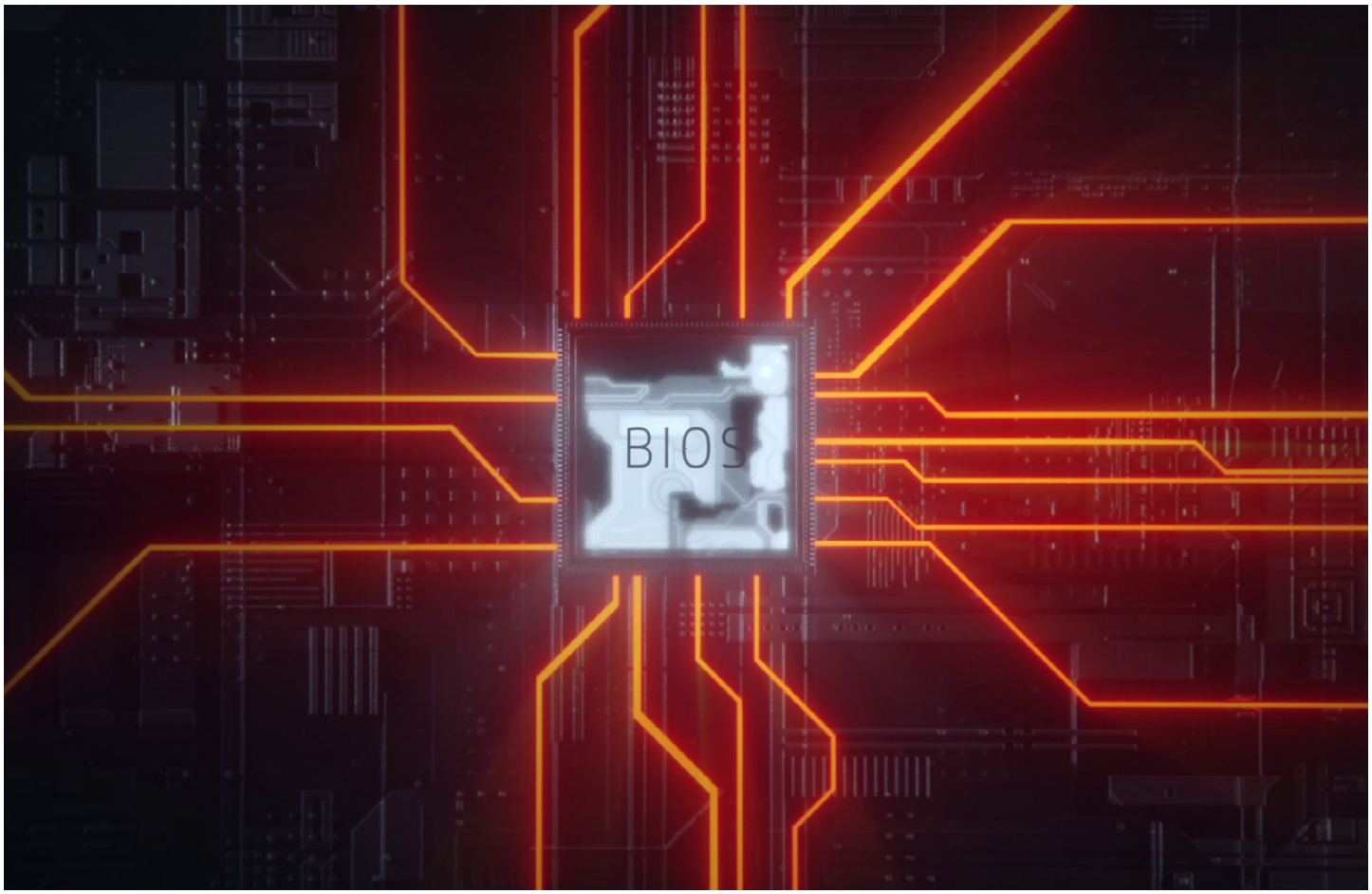
## Pourquoi une protection du BIOS est-elle importante ?

**À mesure que notre monde devient toujours plus connecté, les cyberattaques ciblent de plus en plus le matériel ou le micrologiciel des appareils clients, avec une sophistication toujours plus poussée. Mais si les outils et techniques permettant d'attaquer le micrologiciel étaient auparavant considérés comme théoriques et à la disposition des États-nations uniquement, il est à présent avéré qu'ils existent et se trouvent déjà à disposition dans le domaine public.**

Le micrologiciel de l'appareil (ou BIOS) représente une cible attractive pour les pirates, car les gains potentiels d'une violation réussie pourraient leur offrir :

- Persistance : Le micrologiciel se situe dans une mémoire non volatile du circuit imprimé et ne peut être supprimé simplement en effaçant le disque dur.
- Contrôle : Le micrologiciel exécute le niveau de privilèges le plus élevé en dehors du domaine de l'OS, ce qui permet d'installer un malware indépendant de l'OS.
- Discrétion : Le micrologiciel occupe une zone de la mémoire qui est complètement inaccessible au système d'exploitation et logiciel du système. Puisqu'il ne peut pas être scanné par un antivirus, il peut rester caché indéfiniment.
- Difficulté de récupération : L'ensemble de ces aspects font qu'il est extrêmement difficile de récupérer de ce type d'infection sans recourir à un service incluant un remplacement de la carte mère.

La solution idéale pour protéger les appareils contre ce type d'attaque est conçue à partir du matériel et fait appel aux principes de « cyber-résilience ». Selon ces principes, il est extrêmement difficile, voire impossible, de prévoir et de prévenir toutes les attaques possibles. La bonne solution consiste donc non seulement à fournir une protection renforcée du micrologiciel, mais également à intégrer une capacité générée par le matériel à détecter une attaque et à s'en remettre.



# HP Sure Start offre une protection exceptionnelle du micrologiciel

**HP Sure Start représente l'approche unique et révolutionnaire de HP pour fournir une résilience et une protection avancées du micrologiciel pour les PC HP. Ce dispositif utilise la mise en application matérielle via le HP Endpoint Security Controller (HP ESC) pour offrir une protection du BIOS bien au-delà des normes de l'industrie et s'assurer que le système démarre uniquement un BIOS HP authentique. De plus, si HP Sure Start détecte une falsification du BIOS, du micrologiciel ou du code du BIOS en System Management Mode (SMM) en fonctionnement, il est en mesure de récupérer grâce à une copie de sauvegarde protégée.**

### Résumé des fonctionnalités HP Sure Start

- Protection contre la falsification et mise en application de l'authenticité du micrologiciel de la plateforme centrale HP – mise en application matérielle du HP Endpoint Security Controller pour l'amorçage du système, afin de ne charger que le BIOS HP et le micrologiciel HP véritables et sans modification
- Conformité et surveillance de l'état du BIOS – Enregistrement des événements liés à l'état du micrologiciel via le HP Endpoint Security Controller isolé ; présentation de l'état du micrologiciel de la plateforme ainsi que toute anomalie pouvant indiquer des attaques contrecarrées
- Auto-réparation – Réparation automatique du BIOS HP et de toute corruption du micrologiciel HP à l'aide de la copie de sauvegarde isolée du BIOS et du micrologiciel HP du HP Endpoint Security Controller
- Protection des paramètres du BIOS – Étend la protection du code de BIOS par le HP Endpoint Security Controller afin d'intégrer une sauvegarde du HP ESC et vérification de l'intégrité de tous les réglages du BIOS configurés par les utilisateurs ou administrateurs
- Runtime Intrusion Detection (Détection des intrusions en fonctionnement) – Surveillance permanente du code BIOS critique dans la mémoire en fonctionnement (SMM) lorsque l'OS est en cours d'exécution
- Protection des clés d'amorçage sécurisées – Protection véritablement améliorée des bases de données et clés stockées par le BIOS et essentielles à l'intégrité de la fonctionnalité d'amorçage sécurisée du BIOS par rapport à une mise en œuvre du BIOS selon le standard UEFI
- Espace de stockage protégé – HP Sure Start utilise des méthodes de chiffrement solides pour enregistrer les paramètres du BIOS, les identifiants utilisateur et d'autres paramètres avec le HP Endpoint Security Controller au niveau matériel afin de fournir une protection de l'intégrité, une détection des falsifications et une protection confidentielle des données
- Protection du micrologiciel Intel® Management Engine – Récupération et protection améliorées du micrologiciel Intel Management Engine
- Facilité de gestion – Les administrateurs peuvent gérer les capacités HP Sure Start avec le module Manageability Integration Kit (MIK) pour Microsoft® System Center Configuration Manager (SCCM)

Pour obtenir un résumé des capacités ajoutées à chaque génération de HP Sure Start, consultez l'annexe A en page 11.

### Certification de sécurité tierce

Le HP Endpoint Security Controller situé au niveau matériel et utilisé dans HP Sure Start a subi une évaluation de sécurité par un tiers. Celle-ci a permis de démontrer sa capacité à fournir une mise en application matérielle n'autorisant que le micrologiciel agréé à démarrer sur le PC cible.[1]

La garantie qu'une solution de sécurité fonctionne comme prévu est essentielle dans toute décision d'achat liée à des produits de sécurité. Et puisque sa réputation en termes de qualité en dépend, HP a demandé à un laboratoire indépendant et accrédité de contrôler et de tester le fonctionnement interne du HP Endpoint Security Controller, afin de confirmer que le système fonctionne tel que cela est indiqué dans les critères, la méthodologie et les processus accessibles au public.

### Design cyber-résilient

HP Sure Start fournit non seulement une protection améliorée du BIOS au-delà des normes du secteur, mais il est également conçu à partir du matériel afin d'offrir une cyber-résilience inégalée de la plateforme. Il garantit ainsi la récupération du BIOS, même en cas de faille ou d'attaque destructrice. Les PC professionnels HP équipés de HP Sure Start dépassent ainsi les directives de résilience du micrologiciel de plateforme du National Institute of Standards Technology (NIST) (publication spéciale 800-193, version préliminaire), qui est l'un des principaux efforts déployés par le secteur public pour formaliser les exigences relatives aux plateformes cyber-résilientes.

### Les modèles HP dotés de HP Sure Start

HP a présenté Sure Start en 2014. Depuis lors, HP n'a eu de cesse d'améliorer Sure Start et de développer le nombre de produits qui l'intègrent. HP Sure Start est présent sur toute la gamme de produits Elite 2018, y compris les tablettes, notebooks, ordinateurs de bureau et tout-en-un. HP Sure Start Gen4 est disponible sur les produits HP Elite et HP Pro 600 équipés de processeurs Intel 8ème génération ou AMD®.

# Capacités et aperçu architectural

HP Sure Start comprend deux composants architecturaux majeurs :

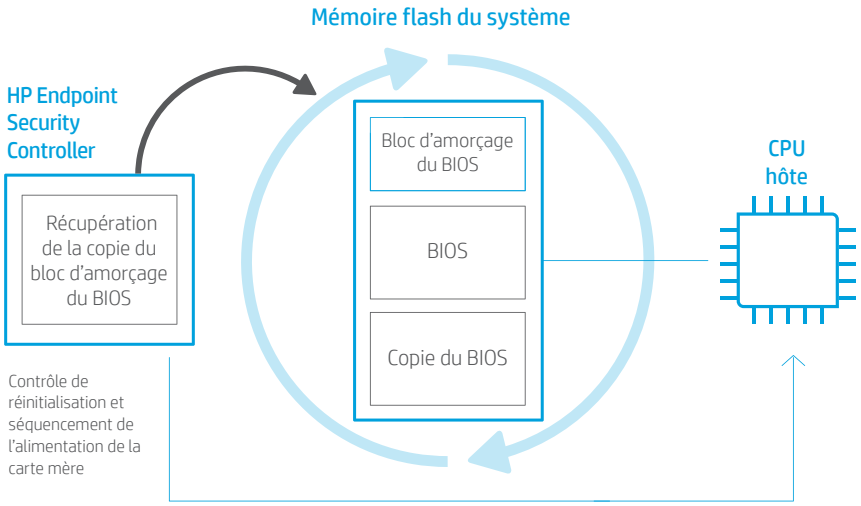
- **HP Endpoint Security Controller** qui exécute le micrologiciel HP Sure Start
- **BIOS HP Sure Start** qui fonctionne en coordination avec le HP Endpoint Security Controller au niveau micrologiciel et matériel

## Vérification de l'intégrité du micrologiciel - le cœur de HP Sure Start

Le HP Endpoint Security Controller (HP ESC) représente le premier dispositif du système à exécuter le micrologiciel au démarrage. Il est activé bien avant le démarrage du système. Parmi les activités du HP ESC se trouvent, sans s'y limiter, la surveillance du bouton d'activation du système et le séquencement de l'alimentation au démarrage de l'exécution du CPU hôte, lorsque l'utilisateur appuie sur le bouton de démarrage.

Après la mise sous tension initiale de la plateforme (avant que le système ne soit lancé), le HP ESC valide l'authenticité du code HP sur son propre micrologiciel avant le chargement et l'exécution du code. Le HP ESC matériel utilise des méthodes de chiffrement solides et conformes aux normes de l'industrie pour réaliser la vérification de l'intégrité. Cette méthode fait usage d'une clé publique RSA HP 2048-bit, contenue dans la mémoire interne permanente en lecture seule. Ainsi, le HP ESC représente la « racine de confiance » matérielle intégrée de la plateforme, utilisée afin de valider son micrologiciel ainsi que le BIOS HP avant leur exécution. Cette « racine de confiance » matérielle assure une protection contre les attaques du micrologiciel, quelle que soit la méthode d'exécution, et constitue la base sur laquelle repose la sécurité de la plateforme HP.

**Figure 1.** Processus de vérification de l'intégrité du micrologiciel.




La figure 1 illustre le processus de vérification de l'intégrité du micrologiciel. Une fois que le HP ESC authentifie et lance l'exécution du micrologiciel HP Sure Start, celui-ci utilise les mêmes opérations de chiffrement puissantes pour vérifier l'intégrité du bloc d'amorçage du BIOS dans la mémoire flash du système. Si le HP ESC trouve un bit invalide, il remplace les contenus de la mémoire flash du système par sa propre copie du bloc d'amorçage du BIOS HP, enregistré dans une mémoire non volatile isolée dédiée au HP ESC.

Le design de HP Sure Start permet de garantir que l'ensemble du code du micrologiciel et du BIOS exécuté sur le HP ESC et le CPU hôte est le code HP conçu pour se trouver sur l'appareil.

*Remarque : La vérification de l'intégrité du bloc d'amorçage dans la mémoire flash du système et toute récupération requise réalisée par le HP ESC se déroulent pendant que le CPU hôte est désactivé. De ce fait, du point de vue de l'utilisateur, l'opération toute entière a lieu alors que le système est encore éteint, en veille ou en veille prolongée.*

Le bloc d'amorçage du BIOS dans la mémoire flash du système représente la base du BIOS HP. Le HP ESC au niveau matériel permet de s'assurer que le bloc d'amorçage du BIOS est le premier code que le CPU exécute après une réinitialisation. Une fois que le HP ESC détermine que le bloc d'amorçage du BIOS contient un code HP authentique, il permet au système de démarrer normalement.

Le HP ESC vérifie également l'intégrité du code du bloc d'amorçage dans la mémoire flash du système à chaque fois que le système est éteint ou mis en mode veille/veille prolongée.

Dans la mesure où le CPU est désactivé dans chacun de ces états et qu'il est nécessaire pour réexécuter le code du bloc d'amorçage du BIOS à relancer, il est essentiel de revérifier l'intégrité du bloc d'amorçage du BIOS à chaque fois afin de contrôler la présence d'éventuelles falsifications.

Par ailleurs, dans le cas des modèles HP Intel, HP Sure Start vérifie régulièrement (toutes les 15 minutes) l'intégrité du bloc d'amorçage du BIOS dans la mémoire flash du système alors que celui-ci fonctionne.[2]

## Intégrité des données uniques de la machine

Le HP ESC et le BIOS fonctionnent ensemble afin de fournir une protection avancée des variables critiques configurées en usine et uniques pour chaque machine. Ces variables sont conçues pour rester constantes tout au long de la vie d'une plateforme spécifique. En usine, une copie de sauvegarde de ces données variables est enregistrée dans la mémoire non volatile du HP ESC. La sauvegarde est mise à disposition du composant du BIOS HP Sure Start en lecture seule, afin de réaliser une vérification de l'intégrité des données à chaque démarrage. Si l'un des réglages de la mémoire flash partagée a changé par rapport aux paramètres d'usine, les composants du BIOS HP Sure Start restaureront automatiquement les données dans la mémoire flash du système à partir de la copie de sauvegarde fournie par le HP ESC.

## Zone du descripteur

Dans les modèles HP Intel, HP Sure Start protège la zone du descripteur de la mémoire flash. La zone du descripteur, unique dans l'architecture Intel, contient des paramètres de configuration importants qui sont testés par le circuit logique Intel Core™ lors de la réinitialisation et utilisés par la suite pour le configurer. La zone du descripteur comprend également un cloisonnement des informations pour la mémoire flash du système qui est utilisée par le circuit logique Intel Core, afin de déterminer l'emplacement du BIOS dans la mémoire flash et donc le lieu où le CPU récupère le code pour l'exécution à partir de la réinitialisation. HP Sure Start surveille l'intégrité de cette zone et rétablit sa configuration prévue en cas de falsification ou de corruption.

## Protection du contrôleur réseau

Par ailleurs, dans le cas des modèles HP Intel, HP Sure Start protège les paramètres du network controller (NIC) qui se trouvent avec la mémoire flash du système. Certains clients de HP présentent des cas d'utilisation qui nécessitent des modifications justifiées des paramètres du NIC configurés en usine. De ce fait, HP Sure Start n'empêche pas les modifications des paramètres du NIC par défaut. Le système fournit à la place une fonctionnalité qui, lorsqu'elle est activée, avertit l'utilisateur que les paramètres du NIC ont changé. De plus, HP Sure Start offre une méthode permettant de restaurer les paramètres du NIC aux valeurs d'usine. Parmi les paramètres protégés se trouvent l'adresse MAC, les réglages Pre-boot eXecution Environment (PXE) et le remote initial program load (RPL). Cette restauration est possible par le biais d'une copie de sauvegarde en lecture seule protégée par le HP ESC.

## Protection du réglage du BIOS

Comme cela a été mentionné précédemment, HP Sure Start vérifie l'intégrité et l'authenticité du code BIOS HP. Dans la mesure où ce code reste statique une fois créé par HP, des signatures numériques peuvent être utilisées pour confirmer chacun des attributs du code. Toutefois, la nature dynamique et configurable par l'utilisateur des paramètres du BIOS crée des enjeux supplémentaires en vue de protéger ces derniers. Les signatures numériques ne peuvent être générées par HP et utilisées par le HP Sure Start ESC au niveau matériel afin de vérifier les paramètres.

La protection des paramètres du BIOS HP Sure Start offre la possibilité de configurer le système de manière à ce que le HP ESC matériel soit utilisé pour sauvegarder et vérifier l'intégrité de l'ensemble des paramètres du BIOS configurés par l'utilisateur.

Lorsque cette fonctionnalité est activée sur la plateforme, l'ensemble des réglages de politique utilisés par le BIOS sont ensuite sauvegardés et un contrôle de l'intégrité est réalisé à chaque démarrage afin de s'assurer qu'aucun des paramètres de politique du BIOS n'a été modifié. Si un changement est détecté, le système utilise la sauvegarde conservée dans le lieu de stockage protégé de HP Sure Start pour revenir automatiquement aux paramètres définis par l'utilisateur.

La fonctionnalité de protection des paramètres du BIOS de HP Sure Start génère des événements sur le ESC HP Sure Start au niveau matériel, dans le cas où une tentative de modification des paramètres du BIOS serait détectée. L'événement est consigné dans le journal d'audit de HP Sure Start et l'utilisateur local reçoit une notification du BIOS pendant le démarrage.

## Espace de stockage protégé HP Sure Start

Le stockage protégé ancré dans le HP Endpoint Security Controller au niveau matériel offre le meilleur niveau de protection pour les paramètres et données du micrologiciel/BIOS protégés par HP Sure Start. Le stockage protégé HP Sure Start est conçu pour fournir à la fois confidentialité, intégrité et détection des falsifications, même dans des scénarios d'attaque physique lorsqu'un pirate décompose le système et établit une connexion directe avec l'appareil de stockage non volatile sur le circuit imprimé.

### Intégrité des données

L'intégrité des données dynamiques enregistrées dans la mémoire non volatile par le micrologiciel et utilisées pour contrôler l'état des différentes capacités est essentielle pour la sécurité globale de toute la plateforme. Les données dynamiques comprennent l'ensemble des paramètres du BIOS qui peuvent être modifiés par l'utilisateur final ou l'administrateur de l'appareil. Parmi les exemples se trouvent (sans s'y limiter) les options de démarrage telles que la fonctionnalité d'amorçage sécurisé, le mot de passe administrateur du BIOS et les politiques liées, le contrôle de l'état du module de plateforme vérifiée, ainsi que les paramètres de la politique HP Sure Start.

Toute attaque réussie, qui parviendrait à franchir les restrictions d'accès existantes destinées à éviter les modifications non autorisées de ces paramètres, pourrait anéantir la sécurité de la plateforme. Imaginez par exemple un scénario dans lequel un pirate réalise une modification non autorisée au niveau de l'état de démarrage sécurisé afin de le désactiver sans être repéré. Dans cette situation, la plateforme démarrerait le kit source du pirate avant que l'OS ne démarre et sans que l'utilisateur ne s'en rende compte.

Le BIOS conforme au standard UEFI (Unified Extensible Firmware Interface, interface micrologicielle extensible unifiée) met en œuvre des restrictions d'accès qui devraient éviter toute modification non autorisée de ces variables. HP respecte ces directives, tout comme le reste du secteur des PC.

Toutefois, étant donné les risques liés à une violation de ces mécanismes pour la plateforme, HP Sure Start offre des défenses secondaires qui s'avèrent au final plus fiables que la norme de base de l'industrie.

Les paramètres du BIOS et autres données dynamiques utilisés par le micrologiciel pour contrôler l'état protégé par HP Sure Start sont enregistrés dans la mémoire non volatile isolée du HP Endpoint Security Controller, qui n'est pas directement accessible au logiciel exécutant le CPU hôte.

De plus, le HP ESC crée et ajoute des mesures d'intégrité uniques à chaque fois qu'un élément de données est enregistré dans cet emplacement de mémoire non volatile. Les mesures d'intégrité sont basées sur un algorithme cryptographique solide (code d'authentification par message haché utilisant une fonction de hachage SHA-256) qui est ancré à un secret contenu dans le HP ESC. Le secret est propre à chaque HP ESC, de manière à ce que chaque contrôleur génère une mesure d'intégrité unique avec un élément identique.

Lorsque l'élément de données est récupéré dans la mémoire non volatile, le HP ESC recalcule les mesures d'intégrité de cet élément de données et les compare à celles ajoutées aux données. Toute modification non autorisée des données dans l'emplacement de mémoire non volatile entraîne une inadéquation. Grâce à cette approche, le HP ESC peut détecter une falsification des éléments de données enregistrés dans l'emplacement de mémoire non volatile.

### Confidentialité des données

Il est essentiel de préserver la confidentialité pour la majeure partie des éléments de données enregistrés par la plateforme. Parmi les exemples se trouvent les hachages du mot de passe administrateur du BIOS, les identifiants utilisateur et les secrets parfois enregistrés par le micrologiciel pour le compte de l'utilisateur, dans le cas de fonctionnalités basées sur le micrologiciel telles que HP Sure Run et HP Sure Recovery.

La protection de ces secrets est difficile avec les approche de BIOS selon l'UEFI, standard de l'industrie, dans la mesure où le stockage non volatile est généralement lisible par le logiciel exécuté sur le processeur hôte. Le stockage protégé de HP Sure Start est conçu pour fournir une protection supérieure à ces données confidentielles par rapport à une exécution du BIOS selon le standard UEFI.

En plus d'un enregistrement isolé et distinct, l'approche HP Sure Start consiste à tirer profit du bloc matériel Advanced Encryption Standard (AES) contenu dans le HP ESC pour réaliser un chiffrement AES-256 de tous les éléments de données confidentielles enregistrés dans la mémoire non volatile HP Sure Start, en plus des mesures d'intégrité des données pour ces éléments. La clé de chiffrement est unique pour chaque HP ESC et ne quitte jamais ce contrôleur. Ainsi, les données chiffrées par un composant HP ESC individuel ne peuvent être déchiffrées que par ce même HP ESC.

## Protection des clés d'amorçage sécurisées

HP Sure Start fournit une protection renforcée des bases de données des clés d'amorçage sécurisées par UEFI enregistrées par le micrologiciel par rapport à une mise en œuvre d'amorçage sécurisé par le standard UEFI. Ces variables sont essentielles pour assurer le bon fonctionnement de la fonctionnalité d'amorçage sécurisé par le standard UEFI, qui vérifie l'intégrité et l'authenticité du chargeur d'amorçage de l'OS avant de lui permettre de démarrer.

HP Sure Start protège les bases de données des clés d'amorçage sécurisées par le standard UEFI en conservant une copie de référence dans le stockage protégé HP Sure Start. Toute modification autorisée par l'OS des bases de données des clés d'amorçage sécurisées par le standard UEFI lors de l'exécution sont surveillées par HP Sure Start et appliquées à la copie de référence par le HP ESC. HP Sure Start utilise ensuite la copie de référence du stockage protégé HP Sure Start pour identifier et rejeter toute modification non autorisée apportée aux bases de données des clés d'amorçage sécurisées par le standard UEFI.

Cette capacité, activée par défaut, concerne les bases de données suivantes :

- Signature database (db)
- Revoked signatures database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) mise à jour de façon dynamique lors de l'exécution par l'OS

## Runtime Intrusion Detection (RTID)

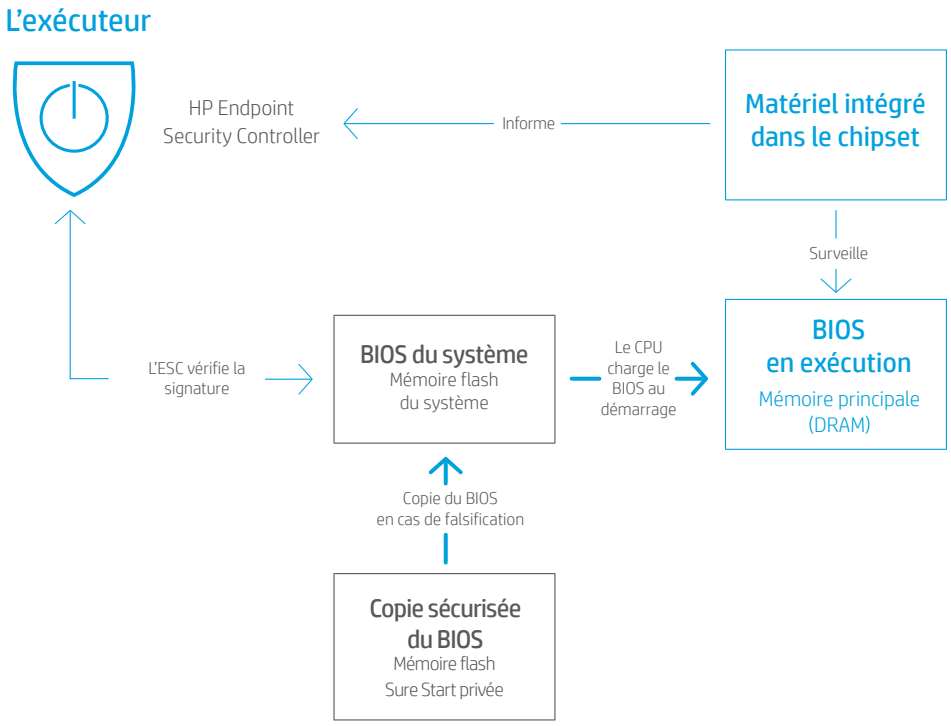
À chaque démarrage, le code du BIOS lance l'exécution de la mémoire flash à une adresse fixe. Il s'agit du code d'amorçage du BIOS, qui offre les capacités « pré-OS » requises avant le démarrage de l'OS. Toutefois, une partie du BIOS restant dans la mémoire DRAM est nécessaire afin de fournir des fonctionnalités avancées de gestion de l'alimentation, des services relatifs à l'OS ainsi que d'autres fonctions indépendantes de l'OS pendant que l'OS est en cours d'exécution. Ce code de BIOS, appelé code System Management Mode (SMM), se trouve dans une zone spécifique de la mémoire DRAM, inaccessible pour l'OS. Nous appelons également ce code le code du BIOS « Runtime » (en exécution) dans le contexte de la fonctionnalité Runtime Intrusion Detection de HP Sure Start. (Pour plus d'informations sur le SMM et son fonctionnement, consultez l'annexe B en page 12).

L'intégrité du code du SMM est essentielle pour assurer la sécurité de l'appareil client. HP Sure Start s'assure que le code du BIOS du SMM HP est intact au démarrage de l'OS. Runtime Intrusion Detection offre des mécanismes permettant de s'assurer que le code du BIOS du SMM reste intact lorsque l'OS est en cours d'exécution, en ajoutant de nouvelles capacités de protection et/ou en fournissant un moyen de détecter une attaque contre ce code.

### Architecture de Runtime Intrusion Detection

La fonctionnalité RTID utilise un matériel spécialisé dans le chipset de la plateforme afin de détecter les anomalies dans le BIOS « Runtime » du SMM HP. Toute détection d'anomalie envoie une notification au HP Endpoint Security Controller, qui peut mettre en œuvre l'action selon la politique configurée indépendamment du CPU.

**Figure 2.** Runtime Intrusion Detection utilise un matériel spécialisé intégré au chipset de la plateforme pour surveiller le code du SMM et repérer d'éventuels changements.



# Notifications de l'utilisateur, journaux d'événements et gestion des politiques

## Notifications de l'utilisateur final HP Sure Start

Dans des conditions de fonctionnement normales, HP Sure Start reste invisible pour l'utilisateur. Les opérations de récupération sont automatiques et utilisent les réglages par défaut, sans qu'aucune interaction ne soit généralement requise de la part de l'utilisateur final ou de l'équipe informatique afin de gérer la récupération, même quand HP Sure Start détecte un problème.

Les utilisateurs peuvent voir des notifications de fonctionnement si un problème d'intégrité du BIOS est détecté via les fonctionnalités HP Sure Start Dynamic Protection ou Runtime Intrusion Detection alors que l'OS est en cours d'exécution. En cas d'événement important ou si une action est réalisée, HP Sure Start affiche un message d'avertissement par le biais de notifications Windows® lors du démarrage suivant. Le logiciel HP Notifications est requis pour permettre d'afficher ces notifications Windows.

## Journaux d'événements HP Sure Start

Le HP Endpoint Security Controller enregistre les événements importants liés aux données et au code du BIOS/micrologiciel surveillés par HP Sure Start. Ces événements sont enregistrés dans l'emplacement de mémoire non volatile de Sure Start. Ils sont copiés à partir du HP ESC vers le Windows Event Viewer lorsque le logiciel de notifications HP (HP Notifications Software) est installé, afin de simplifier l'accès à ces événements par l'utilisateur local ainsi que l'agent d'applicabilité choisi par le client.

Les événement suivants déclenchent le HP Notifications Software. Celui-ci rassemble tous les événements du sous-système HP Sure Start et veille à ce que le Windows Event Viewer soit à jour et comporte tous les événements qui ne sont pas déjà signalés ici :

- Démarrage Windows
- Récupération Windows depuis le mode veille/veille prolongée
- HP Sure Start avec notifications des événements en fonctionnement Dynamic Protection
- HP Sure Start Runtime Intrusion Detection (RTID)

Le HP Notifications Software répertorie les événements HP Sure Start au sein d'un journal d'événements d'application « HP Sure Start » unique. Seuls les événements HP Sure Start y sont consignés. Le chemin du Windows Event Viewer vers les événements HP Sure Start est le suivant : System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

Les catégories de niveau du Windows Event Viewer liées aux événements HP Sure Start sont définies dans le tableau ci-dessous.

Les événements sont répertoriés dans le Windows Event Viewer dans l'ordre où ils ont été générés par HP Sure Start. L'événement le plus ancien du sous-système HP Sure Start est ajouté au Windows Event Viewer en premier, et l'événement le plus récent est ajouté en dernier.

L'horodatage pour chaque entrée du Windows Event Viewer est l'heure à laquelle elle a été ajoutée à ce journal, et NON l'heure à laquelle l'événement est survenu. Chaque entrée Sure Start dans le Windows Event Viewer comprend des données détaillées dans la section Détails sur l'événement, y compris l'horodatage de l'événement réel.

*Remarque : les événements restent dans le HP Endpoint Security Controller, même lorsqu'ils ont été copiés dans Windows Event Viewer. Si le Windows Event Viewer est vidé, l'application HP Notifications Software remplacera toutes les entrées HP Sure Start au prochain événement qui le déclenche afin de vérifier les journaux d'événement de HP Sure Start.*

Types d'événements Windows Event Viewer HP Sure Start

| Niveau de l'événement | Définition |
|---|---|
| Info | Événements auxquels on peut s'attendre pendant le cours normal des opérations (par ex. mise à jour du BIOS). |
| Avertissement | Événements inattendus, qui se sont produits mais ont été entièrement traités par HP Sure Start et ne requièrent aucune action de la part de l'utilisateur/admin pour assurer le bon fonctionnement de la plateforme. Ces événements sont des opérations anormales que l'utilisateur/admin doit parfois étudier de plus près, en particulier s'ils surviennent sur plusieurs machines. |
| Erreur | Événements qui requièrent une action de la part de l'admin/du service HP sur les plateformes pour en assurer la récupération. |

## Contrôles de politique HP Sure Start

Fourni prêt à l'emploi, le BIOS du système HP active et optimise les politiques HP Sure Start pour les utilisateurs de base. Dans la mesure où HP Sure Start est activé par défaut, il n'est pas nécessaire pour ces derniers de modifier les paramètres à protéger avec HP Sure Start. Pour les utilisateurs avancés, le BIOS du système fournit un certain niveau de contrôle en ce qui concerne le comportement de HP Sure Start. Il faut pour cela utiliser les réglages de politique dans les paramètres du BIOS (F10). À moins d'indications spécifiques, ces réglages et fonctions se trouvent dans Security/BIOS Sure Start.

*Remarque : les politiques sont enregistrées dans la mémoire non volatile du HP ESC, qui n'est pas directement accessible par le CPU hôte. Par conséquent, un redémarrage est nécessaire avant l'application des paramètres Sure Start.*

Les paramètres et fonctions HP Sure Start suivants sont disponibles :

- Vérification du bloc d'amorçage à chaque démarrage
- Politique de récupération des données du BIOS
- Restauration de la configuration du contrôleur réseau (Intel uniquement)
- Notification de modification de la configuration du contrôleur réseau (Intel uniquement)
- Scan dynamique en fonctionnement du bloc d'amorçage (Intel uniquement)
- Protection des paramètres du BIOS HP Sure Start
- Protection des clés d'amorçage sécurisées HP Sure Start
- Détection et prévention améliorées des intrusions sur le micrologiciel HP en fonctionnement (Intel uniquement)
- Détection des intrusions sur le micrologiciel HP en fonctionnement (AMD uniquement)
- Politique relative aux événements de sécurité HP Sure Start
- Notification d'amorçage en cas d'événement de sécurité HP Sure Start
- Verrouillage de la version du BIOS
- Sauvegarde/restauration du MBR du disque dur système
- Sauvegarde/restauration du GPT du disque dur système
- Politique de récupération (MBR/GPT) de la zone d'amorçage

### Vérification du bloc d'amorçage à chaque démarrage

HP Sure Start vérifie toujours l'intégrité du bloc d'amorçage du BIOS dans la mémoire flash du système avant de sortir de la veille, de la veille prolongée ou de l'arrêt. Lorsqu'il est **activé**, HP Sure Start vérifie également l'intégrité du bloc d'amorçage à chaque démarrage à chaud (redémarrage Windows). Le compromis à prendre en compte est un temps de redémarrage plus rapide par rapport à un niveau de sécurité plus important. Le réglage par défaut de cette fonctionnalité est **désactivé**.

### Politique de récupération des données du BIOS

Lorsqu'il est configuré en mode **automatique**, HP Sure Start répare automatiquement le BIOS ou les données uniques de la machine lorsque cela est nécessaire. Lorsqu'il est configuré en mode **manuel**, HP Sure Start nécessite une séquence de touches spéciale pour lancer la réparation. En cas de problème avec le code du bloc d'amorçage, le système refuse de démarrer et une séquence clignotante spécifique défile sur la LED système. En cas de problème avec les données uniques de la machine, le système affiche un message à l'écran. La séquence de touches requises ainsi que la séquence clignotante varient selon le type de système : notebook, ordinateur de bureau ou tablette. Le mode manuel est utile dans la mesure où les utilisateurs peuvent réaliser des recherches sur les contenus dans la mémoire flash du système avant la réparation. Les utilisateurs généraux ne sont toutefois pas encouragés à utiliser le mode manuel. Le réglage par défaut de cette fonctionnalité est **automatique**.

### Restauration de la configuration du contrôleur réseau (Intel uniquement)

Cette commande est uniquement disponible sur les systèmes Intel. Lorsqu'elle est sélectionnée, HP Sure Start restaure immédiatement les paramètres par défaut de la configuration du contrôleur réseau.

### Invite de modification de la configuration du contrôleur réseau (Intel uniquement)

Ce réglage est uniquement disponible sur les systèmes Intel. HP fournit une configuration du contrôleur réseau définie en usine, intégrant l'adresse MAC. Lorsque ce réglage est configuré en mode **activé**, le système surveille l'état de la configuration du contrôleur réseau et notifie l'utilisateur en cas de changement dans l'état configuré par défaut. Le réglage par défaut de cette fonctionnalité est **désactivé**.

### Scan dynamique en fonctionnement du bloc d'amorçage (Intel uniquement)

Ce réglage est uniquement disponible sur les systèmes Intel. Lorsque le réglage par défaut est **activé**, HP Sure Start vérifie régulièrement l'intégrité du bloc d'amorçage du BIOS pendant que l'OS est en cours d'exécution. Lorsqu'il est **désactivé**, HP Sure Start ne vérifie l'intégrité qu'avant un démarrage ou une sortie de veille/veille prolongée.

### Protection des paramètres du BIOS HP Sure Start

La politique de protection des paramètres du BIOS est **désactivée** par défaut. Afin d'activer cette fonctionnalité, le propriétaire/l'administrateur de l'appareil client doit en premier lieu configurer l'ensemble des politiques de BIOS selon les réglages qui lui conviennent. Le propriétaire/l'administrateur doit également configurer un mot de passe administrateur de configuration du BIOS afin d'utiliser la protection des paramètres du BIOS de HP Sure Start.

Une fois cela effectué, la politique de protection des paramètres du BIOS devrait afficher « activé ». À ce moment, une copie de sauvegarde de l'ensemble des paramètres du BIOS est créée dans l'emplacement de stockage protégé de HP Sure Start. Par la suite, aucun des paramètres du BIOS ne peut être modifié au niveau local ou à distance. À chaque démarrage, les paramètres de la politique du BIOS sont vérifiés selon l'état souhaité et, en cas de divergence, les paramètres du BIOS sont restaurés à partir de l'emplacement de stockage protégé de HP Sure Start.

Pour modifier un paramètre de BIOS, le mot de passe administrateur du BIOS doit être fourni et la protection des paramètres du BIOS doit ensuite être désactivée. C'est seulement à ce moment-là que les paramètres du BIOS pourront être modifiés.

### Protection des clés d'amorçage sécurisées HP Sure Start

Lorsque ce réglage est configuré par défaut en mode **activé**, HP Sure Start fournit une protection renforcée des clés et bases de données d'amorçage sécurisées utilisées par le BIOS afin de vérifier l'intégrité et l'authenticité du chargeur d'amorçage de l'OS avant le lancement de celui-ci au démarrage. Lorsqu'il est configuré en mode **désactivé**, seule une protection variable d'amorçage sécurisé selon le standard UEFI est utilisée et aucune copie de sauvegarde n'est conservée par le sous-système HP Sure Start.

### Détection et prévention améliorées des intrusions sur le micrologiciel HP en fonctionnement (Intel uniquement) et détection des intrusions sur le micrologiciel HP en fonctionnement (AMD uniquement)

La fonctionnalité RTID est **activée** par défaut sur toutes les plateformes envoyées par l'usine HP. Il n'est pas nécessaire que le client final/l'administrateur active ou « déploie » la fonctionnalité pour profiter du RTID HP Sure Start.

Cette fonctionnalité peut également être configurée en mode **désactivé** par le propriétaire/l'administrateur de la plateforme.

### Politique relative aux événements de sécurité HP Sure Start

Ce réglage de la politique du BIOS permet de contrôler les actions réalisées lorsque HP Sure Start détecte une attaque ou une tentative d'attaque pendant l'exécution de l'OS. Il existe trois configurations possibles pour cette politique :

- **Enregistrement de l'événement dans le journal uniquement** : lorsque ce réglage est sélectionné, le HP ESC consigne les événements de détection. Ceux-ci peuvent être affichés via le chemin Applications and Services Logs/HP Sure Start de Microsoft Windows Event Viewer.[3]
- **Enregistrement de l'événement dans le journal et notification de l'utilisateur** : il s'agit du réglage par défaut. Lorsqu'il est sélectionné, le HP ESC consigne les événements de détection. Ceux-ci peuvent être affichés via le chemin Applications and Services Logs/HP Sure Start de Microsoft Windows Event Viewer. De plus, l'utilisateur est notifié de la survenue de l'événement sur Windows.[4]
- **Enregistrement de l'événement dans le journal et arrêt du système** : lorsque ce réglage est sélectionné, le HP ESC consigne les événements de détection. Ceux-ci peuvent être affichés via le chemin Applications and Services Logs/HP Sure Start de Microsoft Windows Event Viewer. De plus, l'utilisateur est informé sur Windows de la survenue de l'événement, ainsi que de l'imminence de l'arrêt du système.

### Notification d'amorçage en cas d'événement de sécurité HP Sure Start

Le réglage de la politique du BIOS permet de contrôler si les avertissements et messages d'erreur de HP Sure Start qui sont affichés au démarrage du système nécessitent une validation de l'erreur par l'utilisateur local avant que le démarrage ne continue. Lorsque le réglage est en mode **Require Acknowledgement (validation requise)** par défaut, le système s'interrompt et affiche le message d'erreur. L'utilisateur local doit alors appuyer sur une touche pour continuer le démarrage. Si le réglage est en mode **Time out after 15 seconds (expiration après 15 secondes)**, le message est affiché mais le processus de démarrage continue automatiquement après 15 secondes d'affichage du message.

### Verrouillage de la version du BIOS

Dans la configuration du BIOS (F10), cette fonctionnalité est située dans Main/Update System BIOS.

Lorsque cette fonctionnalité est **désactivée**, vous pouvez actualiser le BIOS avec n'importe quel processus pris en charge. Lorsque le HP ESC détecte une mise à jour valide du bloc d'amorçage dans la mémoire flash du système, il actualise la copie de sauvegarde du bloc d'amorçage.

Lorsque cette fonctionnalité est **activée**, l'ensemble des outils de mise à jour du BIOS refusent de mettre à jour le BIOS. De plus, HP Sure Start protège le BIOS contre toute tentative de modification de la version du BIOS en supprimant la mémoire flash du système par le biais d'une méthode non autorisée. Le HP ESC enregistre la version verrouillée du BIOS. Lorsque le HP ESC détecte que le BIOS de la mémoire flash du système a changé, il remplace le bloc d'amorçage du BIOS avec sa propre copie du bloc d'amorçage. La copie du bloc d'amorçage du HP ESC exécute et récupère le reste de la version correcte du BIOS. Le réglage par défaut de cette fonctionnalité est **désactivé**.

### Sauvegarde/restauration du MBR du disque dur système et sauvegarde/restauration du GPT du disque dur système

Dans le réglage du BIOS (F10), cette fonctionnalité est située dans Security/Hard Drive Utilities. Seule l'une de ces capacités est disponible, en fonction du type de partitionnement du lecteur principal (GPT ou MBR) détecté par HP Sure Start.

Lorsque cette fonctionnalité est **activée**, HP Sure Start conserve une copie de sauvegarde protégée de la table de partition MBR/GPT du lecteur principal et compare la copie de sauvegarde au lecteur principal à chaque démarrage. Si une différence est détectée, l'utilisateur est notifié et peut choisir de revenir à l'état d'origine par le biais de la copie ou d'actualiser la copie de sauvegarde protégée avec les modifications. La **politique de récupération (MBR/GPT) de la zone d'amorçage** peut être utilisée en option afin de supprimer la décision de l'utilisateur en ce qui concerne l'action réalisée dans le cas d'une divergence détectée par HP Sure Start.

Lorsque cette fonctionnalité est **désactivée** (par défaut), aucune protection MBR/GPT n'est fournie par HP Sure Start.

### Politique de récupération (MBR/GPT) de la zone d'amorçage

Lorsque cette fonctionnalité est réglée sur **Local User Control (contrôle par l'utilisateur local)** (par défaut), l'utilisateur est notifié de l'action à réaliser lorsque HP Sure Start détecte un changement dans la table de partitionnement MBR/GPT. Lorsque cette fonctionnalité est réglée sur **Recover in the event of corruption (restauration en cas de corruption)**, HP Sure Start restaure automatiquement le MBR/GPT à l'état sauvegardé à chaque fois que des différences sont rencontrées.

## Gestion à distance des contrôles de politique HP Sure Start

Les politiques de HP Sure Start sont fournies prêtes à l'emploi et optimisées pour les utilisateurs généraux. Dans la mesure où HP Sure Start est activé par défaut, l'administrateur à distance n'a pas besoin de réaliser une action quelle qu'elle soit pour activer (ou « déployer ») HP Sure Start. Si l'administrateur à distance souhaite modifier les paramètres de la politique HP Sure Start, des scripts d'utilitaire de configuration du BIOS HP ou d'interfaces de programmation Windows Management Instrumentation (WMI), identiques à ceux employés pour gérer d'autres politiques BIOS de plateforme, peuvent être utilisés pour gérer les politiques de HP Sure Start. De plus, les administrateurs peuvent gérer à distance les capacités de HP Sure Start grâce au module Manageability Integration Kit (MIK) pour Microsoft System Center Configuration Manager (SCCM).

En outre, les administrateurs peuvent gérer à distance les capacités de HP Sure Start et afficher les événements HP Sure Start grâce au module Manageability Integration Kit (MIK) pour Microsoft System Center Configuration Manager (SCCM).

## Conclusion

HP Sure Start offre des avantages essentiels :

- **Une productivité continue** : HP Sure Start préserve la continuité des activités en cas d'attaque ou de corruption accidentelle en supprimant le temps d'arrêt lié à une intervention de maintenance/du service informatique.
- **Des coûts réduits** : La capacité de HP Sure Start à se remettre automatiquement réduit le nombre d'appels passés au centre d'assistance informatique et améliore la productivité, ce qui entraîne au bout du compte une baisse des frais de maintenance pour la plateforme.
- **La tranquillité d'esprit** : HP Sure Start propose plusieurs fonctionnalités de sécurité qui fonctionnent sur un large éventail de plateformes matérielles et logicielles.

Protégez le micrologiciel essentiel de votre BIOS contre les malwares grâce au système de réparation automatique et de détection des intrusions leader de l'industrie HP Sure Start, exclusivement disponible sur les PC Elite sélectionnés.

## Annexe A - HP Sure Start, de génération en génération

HP a présenté Sure Start en 2014. Depuis lors, HP n'a eu de cesse d'améliorer Sure Start et de développer le nombre de produits qui l'intègrent. Le tableau ci-dessous offre un résumé des capacités qui ont été ajoutées à chaque génération.

| Génération | Date de commercialisation | Capacités ajoutées |
|---|---|---|
| HP Sure Start | 2014 | • Mise en application de l'authenticité du BIOS et du micrologiciel avec une capacité d'auto-réparation<br>• Conformité et surveillance du micrologiciel |
| HP Sure Start avec Dynamic Protection | 2015 | • Assistance via Windows Event Viewer<br>• Dynamic Protection (pour les produits Intel sélectionnés) |
| HP Sure Start Gen3 (produits Intel sélectionnés)[5]<br>HP Sure Start avec Runtime Intrusion Detection (produits AMD sélectionnés)[6] | 2017 | • Runtime Intrusion Detection<br>• Protection des paramètres du BIOS<br>• Module Manageability Integration Kit (MIK) pour Microsoft SCCM |
| HP Sure Start Gen4[7] | 2018 | • Stockage protégé - méthodes de chiffrement solides pour enregistrer les paramètres du BIOS, les identifiants utilisateur et d'autres réglages dans le HP Endpoint Security Controller au niveau matériel afin de fournir une protection de l'intégrité, une détection des falsifications et une protection confidentielle des données<br>• Protection des bases de données d'amorçage sécurisées - protection renforcée des bases de données et clés enregistrées par le BIOS, essentielles pour l'intégrité de la fonctionnalité d'amorçage sécurisé de l'OS par rapport à une mise en œuvre du BIOS selon le standard UEFI<br>• Sur les plateformes Intel, récupération et protection renforcées du micrologiciel Intel Management Engine<br>• Certification de sécurité tierce du HP Endpoint Security Controller - tests réalisés par un laboratoire indépendant et accrédité afin de confirmer que la fonctionnalité centrale du HP Endpoint Security Controller matériel fonctionne tel que cela est indiqué dans les critères, la méthodologie et les processus accessibles au public.[1]<br>• Les PC professionnels HP dotés de HP Sure Start dépassent les directives de résilience du micrologiciel de plateforme du NIST (publication spéciale 800-193, version préliminaire). |

## Annexe B - Aperçu du System Management Mode (SMM)

Le System Management Mode (SMM) est une approche répondant aux normes de l'industrie, utilisée pour les fonctionnalités avancées de gestion de l'alimentation de PC et d'autres fonctions indépendantes de l'OS pendant que l'OS est en cours d'exécution. Si les conditions et la mise en œuvre du SMM sont spécifiques aux architectures x86, de nombreuses architectures informatiques modernes utilisent un concept architectural similaire.

Le SMM est configuré par le BIOS au moment du démarrage. Le code du SMM est transcrit dans la mémoire principale (DRAM), puis le BIOS utilise des registres de configuration (verrouillable) spéciaux dans le chipset afin de bloquer l'accès à cette zone lorsque le microprocesseur ne fonctionne pas dans un contexte de SMM. Pendant l'exécution, toute entrée dans le mode SMM est liée à un événement. Le chipset est programmé pour reconnaître de nombreux types d'événements et délais. Et lorsque de tels événements se produisent, le chipset matériel invoque le port d'entrée System Management Interrupt (SMI). Lors de la prochaine limite d'instruction, le microprocesseur enregistre son état global et entre en mode SMM.

Lorsque le microprocesseur entre en mode SMM, il invoque un port de sortie matériel, SMI Active (SMIACT). Ce port indique au chipset matériel que le microprocesseur entre en mode SMM. Un SMI peut être invoqué à tout moment, pendant tous les modes de fonctionnement, à l'exception du SMM lui-même. Le chipset matériel reconnaît le signal du SMIACT et redirige l'ensemble des cycles de mémoire ultérieurs vers une zone protégée de la mémoire (parfois appelée zone SMRAM), réservée spécialement au SMM. Dès qu'il a reçu l'entrée SMI et invoqué la sortie SMIACT, le microprocesseur commence à enregistrer son état interne global dans cette zone de mémoire protégée.

Une fois que l'état du microprocesseur a été enregistré dans la mémoire SMRAM, le code spécifique du gestionnaire SMM qui se trouve également dans la SMRAM (placé là par le BIOS du système au moment du démarrage) lance l'exécution d'un mode de fonctionnement SMM spécial. Lorsqu'ils fonctionnent dans ces modes, la plupart des mécanismes d'isolement de la mémoire et du matériel sont suspendus, et le microprocesseur peut accéder à pratiquement toutes les ressources de la plateforme afin de réaliser les tâches requises. Le code du SMM effectue la tâche requise, puis le microprocesseur revient à son mode de fonctionnement précédent. À ce moment, le code du SMM exécute l'instruction Retour du System Management Mode (RSM) pour sortir du mode SMM. L'instruction RSM entraîne la restauration par le microprocesseur de ses données d'état internes précédentes à partir de la copie enregistrée dans la SMRAM au moment de l'entrée en mode SMM. Lorsque le RSM est terminé, l'état complet du microprocesseur a été restauré à l'état dans lequel il se trouvait juste avant l'événement de SMI, et le programme précédent (OS, applications, hyperviseur, etc.) reprend l'exécution là où il en était resté.

[1] Le matériel du contrôleur HP Sure Start a été certifié conforme au cadre de certification de la Certification de Sécurité de Premier Niveau (CSPN).

[2] HP Sure Start avec Dynamic Protection est disponible sur les produits HP Elite équipés de processeurs Intel Core 6ème génération et supérieurs.

[3] HP Notification Software est requis pour afficher les événements HP Sure Start dans le Windows Event Viewer.

[4] HP Notification Software est requis pour recevoir les notifications.

[5] HP Sure Start Gen3 est disponible sur les produits HP Elite équipés de processeurs Intel Core 7ème génération et supérieurs.

[6] HP Sure Start avec Runtime Intrusion Detection est disponible sur les produits HP Elite équipés de processeurs Intel Core 7ème génération et supérieurs.

[7] HP Sure Start Gen4 est disponible sur les produits HP Elite et HP Pro 600 équipés de processeurs Intel Core 8ème génération ou AMD.

**Découvrez-en plus**
hp.com/go/computersecurity



4AA7-3172FRFR, Mai 2018