Libro blanco técnico

HP Sure Start

Protección y reparación automática a nivel BIOS

Mayo de 2018

Contenido

Introducción

El arranque seguro de HP (HP Sure Start) puede detectar, detener y recuperarse de forma automática de un ataque o de corrupción de la BIOS, sin intervención del departamento de TI y con mínima o ninguna interrupción de la productividad del usuario. Cada vez que se suministra energía al PC, HP Sure Start valida automáticamente la integridad del código de la BIOS y asegura que el PC se mantenga a salvo de ataques malintencionados. Una vez que el PC se encuentra operativo, la detección de intrusiones en tiempo de ejecución monitoriza constantemente la memoria. En caso de ataque, el PC puede autorrepararse utilizando una "copia maestra" (golden copy) aislada de la BIOS en menos de un minuto.

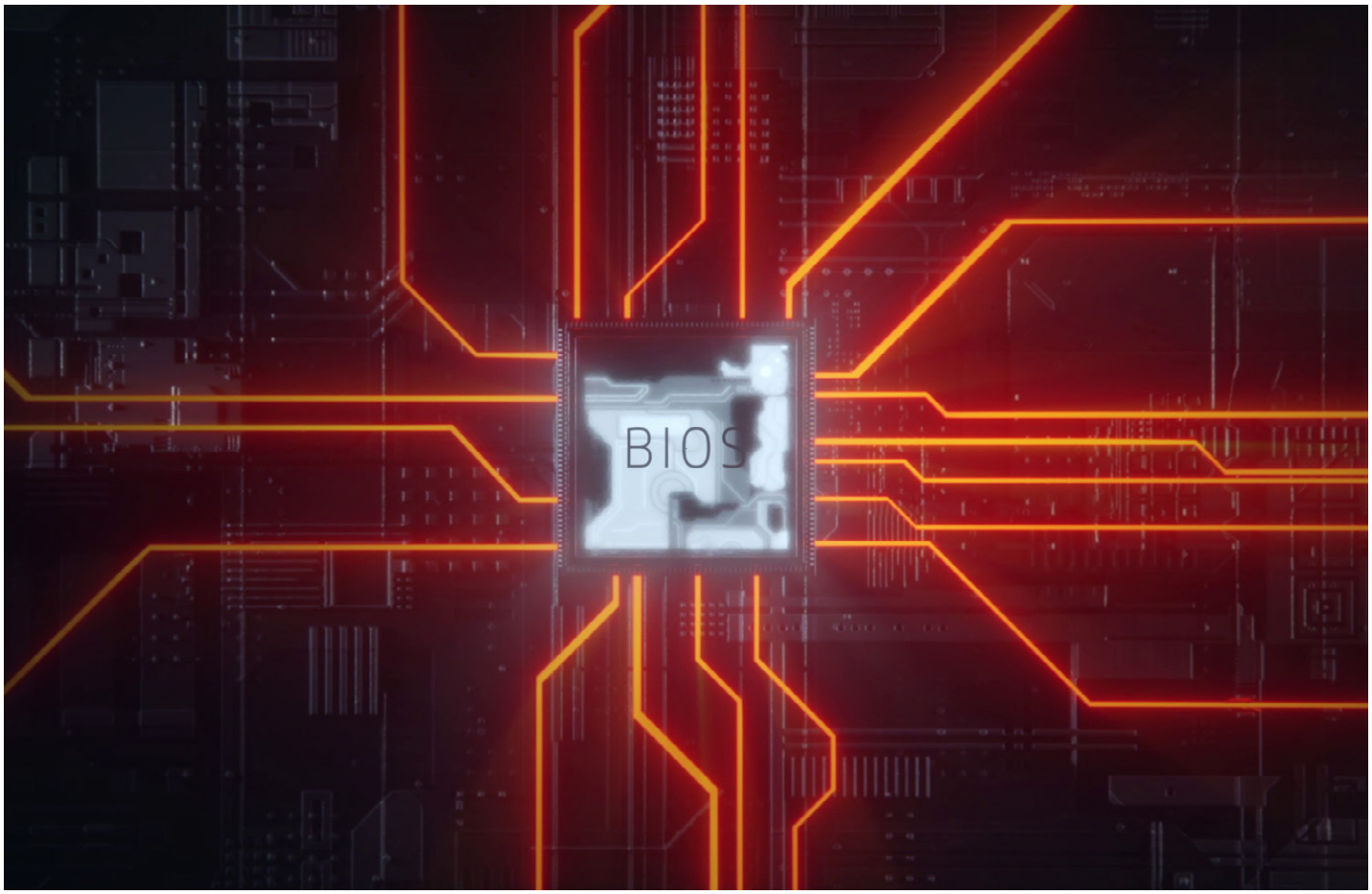
¿Por qué es importante proteger la BIOS?

A medida que nuestro mundo se vuelve más interconectado, los ciberataques se orientan directamente al firmware y el hardware del dispositivo cliente cada vez con mayor frecuencia y sofisticación. Las técnicas y herramientas capaces de atacar el firmware eran antes solo una preocupación teórica, cuando se pensaba que únicamente los estados-nación podrían llegar a disponer de ellas. Pero tales herramientas y técnicas no solo existen hoy día, sino que son incluso del dominio público.

El firmware (o BIOS) del dispositivo es un blanco muy atractivo para un hacker, dadas las ventajas potenciales que podría obtener en caso de penetrar en este componente clave:

- Persistencia: El firmware reside en una memoria no volátil de la tarjeta de circuitos, que no puede eliminarse con solo borrar el disco duro.
- Control: El firmware ejecuta operaciones al más alto nivel de privilegio, es decir, fuera del dominio del SO, lo que permite introducir un malware que sea independiente del SO.
- Sigilo: El firmware ocupa una región de la memoria completamente inaccesible al sistema operativo y al software del sistema; así, al no poder ser escaneado por los antivirus, tiene altas probabilidades de que nunca sea detectado.
- Dificultad de recuperación: Todas estas características hacen que resulte extremadamente difícil recuperarse de esta clase de infección, a menos que se recurra a una operación de servicio que incluya el reemplazo de la tarjeta madre del sistema.

La solución ideal para proteger cualquier dispositivo contra este tipo de ataques es el diseño a partir de la base del hardware utilizando principios de "ciber-resiliencia". Tales principios empiezan por reconocer que es extremadamente difícil, si no imposible, prever y prevenir cualquier posible ataque. La solución ideal, pues, no es solo proporcionar una mejor protección del firmware, sino incluir además la capacidad al nivel más básico del hardware de detectar un ataque exitoso y poder recuperarse de él.



HP Sure Start proporciona la máxima protección del firmware

HP Sure Start es un revolucionario sistema exclusivo de HP que proporciona protección avanzada del firmware y resiliencia para los PC de HP. Para ello, recurre a un hardware reforzado a través del HP Endpoint Security Controller (HP ESC) que protege la BIOS mucho más allá de los estándares de la industria y asegura que el sistema solo pueda arrancar con una BIOS auténtica de HP (Genuine HP BIOS). Además, en caso de que HP Sure Start detecte cualquier interferencia con la BIOS, el firmware, o el código BIOS del System Management Mode (SMM) en tiempo de ejecución, puede efectuar una recuperación a partir de una copia de respaldo (backup) protegida.

Resumen de características de HP Sure Start

- Refuerzo de autenticidad de la plataforma central del firmware HP y protección contra intervenciones – Refuerzo del hardware del controlador HP Endpoint Security Controller de arranque del sistema, de modo que solo puede cargarse el firmware y la BIOS HP auténtica y sin modificaciones
- Monitorización y cumplimiento del estado del firmware – Registro de eventos relacionados con el estado del firmware a través del controlador independiente HP Endpoint Security Controller, que presenta el estado de la plataforma del firmware junto con cualquier anomalía que pudiera indicar un ataque repelido
- Autorreparación automática de corrupción de la BIOS y el firmware HP mediante una copia independiente de seguridad del controlador HP Endpoint Security Controller para la BIOS y el firmware HP
- Protección de la configuración de la BIOS – Extiende la protección del controlador HP Endpoint Security Controller del código BIOS a la comprobación de integridad y seguridad por parte del HP ESC de todos los usuarios y administradores existentes en la configuración de la BIOS
- Detección de intrusiones en tiempo de ejecución – Monitorización continua del código BIOS fundamental de la memoria de ejecución (SMM) mientras opera el SO
- Protección de claves de arranque seguro – Protección óptima de las bases de datos y claves almacenadas en la BIOS, críticas para la integridad de la función de arranque seguro del SO, en comparación con el modelo de implementación estándar UEFI de la BIOS
- Almacenamiento protegido – HP Sure Start emplea robustos métodos de criptografía para almacenar la configuración de la BIOS, las credenciales de usuarios y otras configuraciones del hardware del controlador HP Endpoint Security Controller, proporcionando protección de integridad, detección de intervenciones y protección de la confidencialidad de los datos
- Protección del firmware mediante el motor de gestión Intel® Management Engine – Protección y recuperación mejoradas del firmware Intel Management Engine (motor de gestión Intel)
- Gestionabilidad – Los administradores pueden gestionar las capacidades de HP Sure Start con el complemento (plugin) Manageability Integration Kit (MIK) de Microsoft® System Center Configuration Manager (SCCM)

Puede verse un resumen de las capacidades añadidas en cada generación sucesiva de HP Sure Start, en el Apéndice A, página 11.

Certificación de seguridad independiente

El hardware del controlador HP Endpoint Security Controller utilizado en el sistema HP Sure Start ha superado la evaluación de seguridad de un organismo independiente y obtenido la certificación de que proporciona un hardware reforzado que garantiza que solo el firmware autorizado puede ejecutarse en el PC.[1]

La garantía de que la solución de seguridad funciona según lo indicado constituye un factor crítico en cualquier decisión de compra relativa a productos de seguridad. Debido a que esta es la referencia máxima en términos de calidad, HP ha sometido la funcionalidad interna del controlador HP Endpoint Security Controller a revisión y prueba por parte de un acreditado laboratorio independiente a fin de validar dicho funcionamiento según lo especificado mediante criterios, métodos y procesos públicamente disponibles.

Diseño ciber-resiliente

HP Sure Start no solo proporciona protección mejorada de la BIOS más allá de los estándares vigentes en la industria, sino que su diseño a partir de la base del hardware le aporta a la plataforma una ciber-resiliencia inmejorable que asegura la recuperación de la BIOS aun en el caso de penetración o ataque destructivo del mismo. Los PC comerciales de HP equipados con HP Sure Start exceden las directrices de resiliencia del proyecto de plataforma de firmware del Instituto Nacional de Tecnologías Normativas (National Institute of Standards Technology, NIST) (Publicación Especial 800-193), uno de los mayores esfuerzos realizados por el sector público por formalizar los requisitos para las plataformas ciber-resilientes.

HP Sure Start: modelos compatibles

HP presentó Sure Start en 2014. Desde ese momento, ha estado mejorando Sure Start y ha incrementado el número de productos que lo incorporan. HP Sure Start se ofrece en toda la gama de productos Elite 2018, que incluye tabletas digitales, portátiles, ordenadores de escritorio y dispositivos "todo en uno" (all in one, AIO). HP Sure Start Gen4 está disponible en los productos HP Elite y HP Pro 600 equipados con procesadores Intel o AMD® de 8.ª generación.

Resumen general de arquitectura y capacidades

HP Sure Start consta de dos componentes arquitectónicos principales:

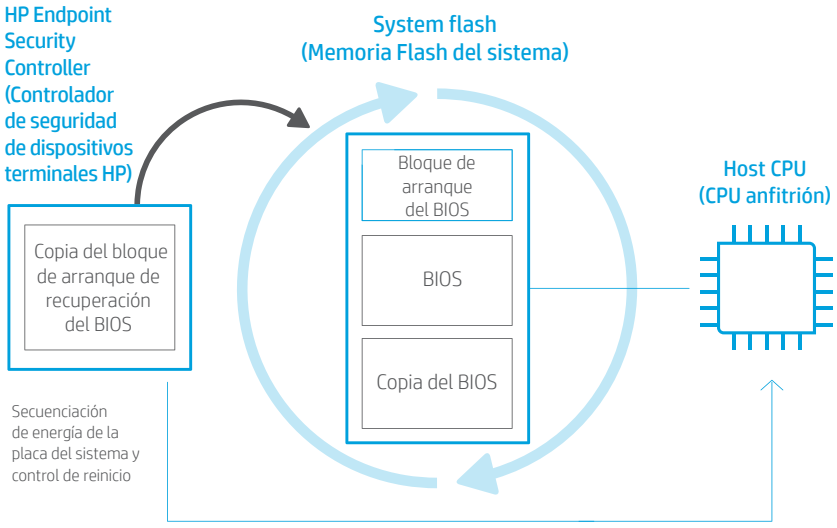
- **HP Endpoint Security Controller**, que ejecuta el firmware de HP Sure Start
- **HP Sure Start BIOS**, que funciona en conjunción con el hardware y firmware del HP Endpoint Security Controller

Verificación de la integridad del firmware – el núcleo de HP Sure Start

El controlador HP Endpoint Security Controller (HP ESC) es el primer dispositivo en ejecutar el firmware al encenderse el sistema, iniciando su actividad mucho antes del arranque del sistema. Las actividades de HP ESC incluyen, entre otras, la monitorización del botón de encendido del sistema y la secuenciación de la puesta en marcha y ejecución de la CPU anfitriona cuando el usuario presiona el botón de encendido.

Al llegar la energía a la plataforma (antes de encenderse el sistema), el HP ESC valida la autenticidad de su propio código HP del firmware antes de cargar y ejecutar el código. El hardware HP ESC emplea robustos métodos criptográficos dentro de los estándares de la industria para realizar la verificación de integridad, consistente en una clave pública RSA de HP de 2048 bits contenida en la memoria interna permanente de solo lectura. De este modo, HP ESC constituye la raíz de confianza (Root of Trust, RoT) incorporada al hardware mismo de la plataforma, que sirve para validar su firmware y la BIOS de HP antes de su ejecución. Este sistema de hardware Root of Trust protege contra ataques de sustitución del firmware sin importar el método de ataque empleado, y compone el cimiento fundacional sobre el que se construye la seguridad de la plataforma HP.

Figura 1. Proceso de verificación de la integridad del firmware.



La Figura 1 ilustra el proceso de verificación de la integridad del firmware. Una vez que HP ESC autentifica y empieza a ejecutar el firmware de HP Sure Start, este firmware utiliza operaciones criptográficas igualmente sólidas para verificar la integridad del bloque de arranque BIOS de la memoria flash del sistema (system flash BIOS boot block). Si se encuentra un solo bit no válido, el HP ESC sustituye el contenido de la memoria flash del sistema por su propia copia del bloque de arranque de la BIOS HP, que está almacenada en una memoria independiente no volátil (non-volatile memory, NVM) exclusiva del HP ESC.

El diseño de HP Sure Start garantiza que toda codificación de firmware y BIOS que se ejecute tanto en el HP ESC como en la CPU anfitriona corresponda con la codificación HP propia del dispositivo.

Nota: Mientras la CPU anfitriona está desactivado se comprueba la integridad del bloque de arranque de la memoria flash, además de cualquier recuperación necesaria por parte del HP ESC. Por ello, desde el punto de vista del usuario, toda la operación se realiza mientras el sistema está todavía apagado, en modo de suspensión o de hibernación.

El bloque de arranque BIOS de la memoria flash es el componente fundamental de la BIOS de HP. El hardware de HP ESC garantiza que el bloque de arranque de la BIOS sea el primer código ejecutado por la CPU al reiniciarse. Una vez que el HP ESC comprueba que el bloque de arranque BIOS contiene el código HP auténtico, permite el arranque del sistema de manera normal.

El HP ESC verifica además la integridad del código del bloque de arranque de la memoria flash cada vez que el sistema se apaga o se pone en modo de suspensión o hibernación. Dado que la CPU se apaga en cualquiera de estos estados y tiene que ejecutar otra vez el código del bloque de arranque BIOS para volver a ponerse en funcionamiento, es crucial volver a comprobar la integridad del bloque de arranque de la BIOS cada vez, para descartar cualquier interferencia.

Además, en los modelos Intel de HP, el sistema HP Sure Start verifica periódicamente (cada 15 minutos) la integridad del bloque de arranque BIOS de la memoria flash mientras el sistema está en funcionamiento.[2]

Integridad de la información exclusiva del equipo

El HP ESC y la BIOS funcionan juntos para proporcionar protección avanzada de las variables críticas preconfiguradas de fábrica de cada equipo que deba mantenerse constante durante toda la vida útil de la plataforma. En la fábrica, se guarda una copia de seguridad de estos datos variables en la memoria de almacenamiento no volátil del HP ESC; dicho respaldo lo utiliza el componente HP Sure Start de la BIOS solo como lectura para comprobar la integridad de los datos en cada proceso de arranque. Si se encuentra cualquier cambio en la memoria flash compartida con respecto a la configuración de fábrica, los componentes HP Sure Start de la BIOS restablecen automáticamente los datos de la memoria flash a partir de la copia de respaldo proporcionada por el HP ESC.

Región del descriptor

En los modelos Intel de HP, el sistema Sure Start protege la región del descriptor de la memoria flash del sistema. Una característica exclusiva de la arquitectura Intel es que la región del descriptor contiene los parámetros de configuración esenciales que proporciona la unidad lógica Intel Core™ al efectuarse el reinicio y que se emplean a continuación para configurar la lógica Core fundamental. La región del descriptor contiene además la información de la partición de la memoria flash que utiliza la unidad lógica de Intel Core para determinar dónde se encuentra la región de la BIOS dentro de la memoria flash, que es donde la CPU proporciona el código de ejecución desde el reinicio. HP Sure Start monitoriza la integridad de esta región y la restaura a la configuración que debe tener, en caso de que se haya producido alguna intervención o corrupción.

Protección del controlador de red

Además, en los modelos Intel de HP, el sistema Sure Start protege la configuración del controlador de red (NIC) que se encuentra en la memoria flash del sistema. Algunos clientes de HP tienen usos específicos que requieren cambios legítimos de la configuración NIC de fábrica, por lo que HP Sure Start no evita de manera predeterminada que se puedan efectuar cambios en la configuración del NIC. Por en contrario, HP Sure Start proporciona esta posibilidad advirtiendo al usuario en caso de que se produzcan cambios en el NIC y, además, HP Sure Start posibilita poder restaurar la configuración del NIC a los valores de fábrica. La protección de la configuración incluye la dirección MAC, la configuración del Pre-boot Execution Environment (PXE) y la carga inicial remota del programa (remote initial program load, RPL). Dicha restauración es posible gracias a la copia de respaldo de solo lectura protegida por el HP ESC.

Protección de la configuración de la BIOS

Como se ha descrito anteriormente, el HP Sure Start verifica la integridad y la autenticidad del código de la BIOS. Dado que este código permanece estático después de su creación por HP, permite el uso de firmas digitales para confirmar ambos atributos del código. No obstante, la naturaleza dinámica de la BIOS, que, además, puede ser configurada por el usuario, plantea dificultades adicionales para poder proteger esta configuración, ya que las firmas digitales no pueden ser generadas por HP ni utilizadas por el hardware ESC del sistema HP Sure Start para su verificación.

Pero la protección de la configuración de la BIOS de HP Sure Start permite configurar el sistema de modo que el hardware HP ESC se utilice para respaldar y verificar la integridad de toda la configuración de la BIOS establecida por el usuario.

Cuando se activa esta función de la plataforma, todas las configuraciones de la directriz utilizada por la BIOS son posteriormente respaldadas, con lo que se puede verificar la integridad en cada arranque para asegurar que no se haya modificado ninguna de las directrices de configuración de la BIOS. Si se encuentra cualquier cambio, el sistema utiliza el respaldo (backup) del almacenamiento protegido de HP Sure Start para restablecer automáticamente la configuración establecida por el usuario.

La función de protección de la configuración de la BIOS de HP Sure Start activa determinados procesos del hardware ESC de HP Sure Start si se detecta cualquier intento de modificar la configuración de la BIOS. Tales procesos se alojan en el registro de auditoría de HP Sure Start, y el usuario local recibe una notificación de la BIOS durante el arranque.

Almacenamiento protegido de HP Sure Start

El almacenamiento protegido enraizado en el hardware del controlador HP Endpoint Security Controller proporciona el más alto nivel de protección de los datos de la BIOS y el firmware, así como de la configuración protegida por HP Sure Start. El almacenamiento protegido de HP Sure Start ha sido diseñado para proporcionar integridad y confidencialidad de los datos, evitando cualquier interferencia aun bajo ataques de naturaleza física orientados a desarmar el sistema y establecer una conexión directa con el dispositivo de almacenaje no volátil de la tarjeta de circuitos.

Integridad de la información

La integridad de la información dinámica almacenada por el firmware en la memoria no volátil, que se usa para controlar el estado de diversas capacidades, es crítica para la posición de seguridad de la totalidad de la plataforma. Dicha información dinámica incluye toda la configuración de la BIOS que puede ser modificada por el usuario final o el administrador del dispositivo. Algunos ejemplos son las opciones de arranque, como la función de arranque seguro, la contraseña BIOS del administrador y las directrices relacionadas, el estado de control del módulo Trusted Platform Module y la configuración de las directrices de HP Sure Start.

Un ataque exitoso que lograra superar las restricciones de acceso existentes para evitar la modificación no autorizada de estas configuraciones podría burlar la seguridad de la plataforma. Como ejemplo, piénsese en un ataque que lograra modificar el estado de arranque seguro de modo que pudiera desactivarse sin ser detectado. En tal caso, la plataforma arrancaría a partir del sistema básico introducido por el hacker antes de iniciarse el SO, sin que el usuario tuviera posibilidad de advertirlo.

La BIOS de interfaz Unified Extensible Firmware Interface (UEFI) estándar de la industria implementa restricciones de acceso destinadas a impedir cualquier modificación no autorizada de estas variables, y HP las incorpora al igual que el resto de fabricantes de PC.

No obstante, dados los riesgos que comporta para la plataforma una posible interferencia de tales mecanismos, HP Sure Start aporta una línea de defensa adicional que es aún más robusta que la estándar existente en el sector.

La configuración de la BIOS y otra información dinámica utilizada por el firmware para controlar el estado protegido por HP Sure Start se almacenan en la memoria independiente no volátil del controlador HP Endpoint Security Controller, la cual no es directamente accesible al software que opera en la CPU anfitriona.

Adicionalmente, el HP ESC crea y agrega medidas de integridad únicas cada vez que se almacena un elemento de información en este almacén de memoria no volátil. Las medidas de integridad se fundamentan en un sólido algoritmo criptográfico (basado en códigos fraccionados de autenticación que utilizan el sistema de fraccionamiento SHA-256) enraizado en un mensaje cifrado contenido en el HP ESC. Dicho mensaje cifrado es único de cada HP ESC, de tal modo que cada controlador genera una medida de integridad exclusiva para cada elemento idéntico.

Al leer posteriormente el elemento de información cifrado en la memoria no volátil, el HP ESC recalcula la medida de integridad de dicho elemento de información y la compara con la medida de integridad que se agregó anteriormente. Cualquier modificación no autorizada de la información almacenada en la memoria arrojaría una diferencia al efectuar esta comparación; de este modo, el HP ESC puede detectar cualquier intromisión en la información contenida en el almacén de memoria no volátil.

Confidencialidad de los datos

La confidencialidad es un factor crítico para muchos de los elementos de información contenidos en la plataforma. Entre estos están los componentes fraccionados de la contraseña BIOS del administrador, las credenciales de los usuarios y otros datos confidenciales almacenados por el firmware con relación al usuario para ciertas funciones del firmware, como los sistemas de operación segura HP Sure Run y recuperación segura HP Sure Recovery.

La protección de la confidencialidad puede verse amenazada si solo se emplean los procedimientos UEFI estándar para la BIOS, ya que el almacenamiento no volátil puede ser leído por un software que opere dentro del procesador anfitrión. En comparación, la protección que ofrece HP Sure Start a la información confidencial almacenada es mucho mayor que la del sistema UEFI estándar para la BIOS.

Además del registro de almacenaje independiente, HP Sure Start hace uso del bloque de hardware de normas avanzadas de cifrado (Advanced Encryption Standard, AES) del controlador HP ESC para cifrar mediante el procedimiento AES-256 todos los elementos de información confidencial contenidos en la memoria no volátil de HP Sure Start, a lo que hay que sumar las medidas de integridad de la información aplicadas a dichos elementos. La clave de cifrado empleada es única para cada controlador HP ESC y nunca sale del mismo, por lo que la información codificada por cada componente del HP ESC solo puede ser descodificada por ese mismo HP ESC.

Protección de claves de arranque seguro

HP Sure Start proporciona protección mejorada de las bases de datos claves de arranque seguro UEFI almacenadas por el firmware, en comparación con el sistema de arranque seguro UEFI estándar. Esas variables son críticas para la correcta operación de la función de arranque seguro UEFI que verifica la integridad y la autenticidad del gestor de arranque del SO antes de iniciar el mismo.

HP Sure Start protege las bases de datos claves del arranque seguro UEFI manteniendo una copia maestra en el almacenamiento protegido de HP Sure Start para detectar cualquier modificación no autorizada de dichas bases de datos por el SO durante el tiempo de ejecución y aplicar la copia maestra del controlador HP ESC. De este modo, HP Sure Start utiliza dicha copia maestra de su almacenamiento protegido para identificar y rechazar cualquier cambio no autorizado de las bases de datos claves del arranque seguro UEFI estándar.

Esta capacidad, que se activa de forma predeterminada, cubre las siguientes bases de datos:

- Base de datos de firmas (db)
- Base de datos de firmas revocadas (dbx)
- Clave de acceso Key Enrollment Key (KEK)
- Clave de plataforma Platform Key (PEK), actualizada dinámicamente por el SO en tiempo de ejecución

Detección de intrusión en tiempo de ejecución Runtime Intrusion Detection (RTID)

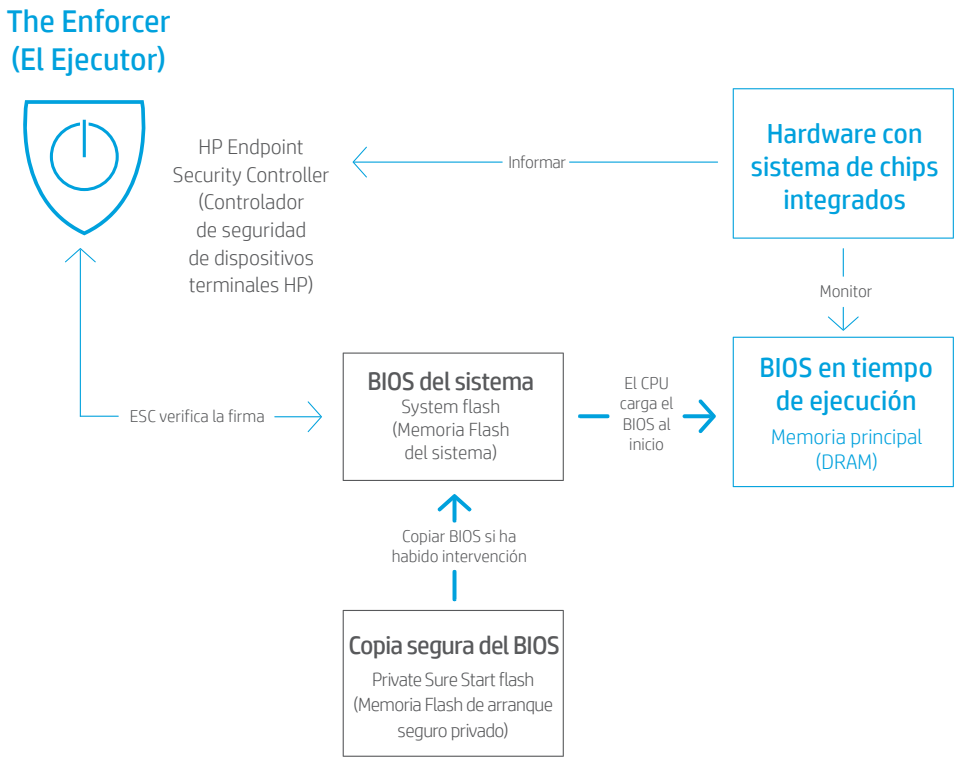
En cada arranque, el código de la BIOS inicia la ejecución de la memoria flash en una dirección fija. Esto se conoce como código de arranque de la BIOS, y ofrece capacidades "previas al SO" (Pre-OS) necesarias antes del inicio del SO. Hay, sin embargo, una parte de la BIOS que permanece en la memoria DRAM y que se necesita para emplear funciones avanzadas de gestión de energía, servicios del SO, y otras funciones independientes del SO mientras este está en operación. Este código BIOS, conocido como código del modo de gestión del sistema, System Management Mode (SMM), reside en un área especial de la DRAM que permanece oculta del SO. Ese código también se llama código BIOS de "tiempo de ejecución" (Runtime) en el contexto de la función RTID de HP Sure Start. (Para más detalles sobre el SMM y cómo funciona, véase el Apéndice B, página 12).

La integridad del código SMM es crítica para la posición de seguridad del dispositivo cliente. HP Sure Start comprueba que el código HP SMM BIOS esté intacto al iniciarse el SO. El sistema RTID provee los mecanismos para garantizar que el código SMM BIOS permanezca intacto mientras se ejecuta el SO, añadiendo nuevas capacidades de protección a la vez que aportando una manera de detectar cualquier ataque a este código.

Arquitectura del sistema RTID

La función RTID utiliza hardware especializado de la plataforma de microcircuitos para detectar anomalías del HP SMM BIOS en tiempo de ejecución. La detección de cualquier anomalía genera una notificación al controlador HP Endpoint Security Controller, que puede realizar la acción configurada en la directiva de forma independiente a la CPU.

Figura 2. El sistema Runtime Intrusion Detection hace uso de hardware especializado incorporado en la plataforma de microcircuitos para monitorizar si ha habido cualquier cambio en el código SMM.



Notificaciones al usuario, registro de eventos y gestión de directrices

Notificaciones al usuario final de HP Sure Start

En condiciones normales de funcionamiento, HP Sure Start es invisible para el usuario. Las operaciones de recuperación se realizan de forma automática con la configuración predeterminada, sin que se necesite la intervención del usuario o de TI para la recuperación en caso de que HP Sure Start identifique algún problema.

El usuario podría ver la notificación en tiempo de ejecución en caso de que se detectara un problema de integridad de la BIOS mediante las funciones HP Sure Start Dynamic Protection o Runtime Intrusion Detection mientras el SO está en funcionamiento. Si se detectara algún evento significativo o se realizara alguna acción de importancia, la próxima vez que arranque el sistema HP Sure Start mostrará un mensaje de advertencia mediante el sistema de avisos de Windows®.

Se necesita el software de notificaciones de HP para poder ver estos avisos de Windows.

Registro de eventos de HP Sure Start

El controlador HP Endpoint Security Controller registra los eventos críticos relacionados con el código de la BIOS y el firmware y la información monitorizada por HP Sure Start. Estos eventos se guardan en el almacenamiento de memoria no volátil de Sure Start, y se copian desde el HP ESC al Windows Event Viewer (visor de eventos de Windows) si está instalado el software de notificaciones HP Notifications, para facilitar el acceso a los mismos por parte del usuario local o del agente de gestionabilidad del usuario.

Los eventos siguientes activan el software HP Notifications para que recoja todos los eventos del subsistema HP Sure Start y actualizar el Windows Event Viewer con aquellos eventos que no hayan aparecido todavía:

- Arranque de Windows
- Salida de Windows de suspensión/hibernación
- HP Sure Start con notificación de eventos de protección dinámica en tiempo de ejecución
- Detección de intrusión en tiempo de ejecución (RTID) de HP Sure Start

El software de HP Notifications efectúa el registro de eventos específicos de la aplicación HP Sure Start. En este registro solo se incluyen los eventos de HP Sure Start. La ruta del Windows Event Viewer a los eventos de HP Sure Start es la siguiente: System Tools (Herramientas del Sistema)/Event Viewer (Visor de Eventos)/ Applications and Services Logs (Registros de Aplicaciones y Servicios)/ HP Sure Start.

Las categorías a nivel del Windows Event Viewer relacionadas con los eventos de HP Sure Start se definen en la siguiente tabla.

Los eventos aparecen en el Windows Event Viewer en el orden en que son generados por HP Sure Start. El evento más antiguo del subsistema HP Sure Start aparece primero en el Windows Event Viewer, y el más reciente se añade en último lugar.

El registro horario de cada entrada del Windows Event Viewer es la hora a la que se añadió al registro, NO la hora en la que sucedió. Cada entrada del Windows Event Viewer de Sure Start contiene información detallada del evento, incluyendo el registro horario de la ocurrencia del evento.

Nota: Los eventos se mantienen en el controlador HP Endpoint Security Controller aun después de haber sido copiados al Windows Event Viewer Si se borra el Windows Event Viewer, la aplicación del software HP Notifications reemplaza todas las entradas de HP Sure Start al producirse el siguiente evento que activa la lectura del registro de eventos de HP Sure Start.

Tipos de eventos en el Windows Event Viewer (Visor de Eventos de Windows) de HP Sure Start

Nivel de evento	Definición
Información	Eventos que se espera que ocurran durante el curso normal de las operaciones (p. ej., actualización de la BIOS).
Advertencia	Los eventos inesperados que se hayan producido pero de los que haya habido recuperación total por HP Sure Start sin requerir ninguna acción del usuario ni el administrador del sistema para la plena operabilidad de la plataforma. Tales eventos son operaciones anómalas que el usuario o el administrador debería investigar más a fondo, especialmente si existe una tendencia a los mismos en diversos dispositivos.
Error	Eventos que requieren la intervención del administrador o del servicio HP para la recuperación total de la plataforma.

Control de las directrices de HP Sure Start

Al iniciarse el dispositivo por primera vez, la BIOS del sisitema de HP activa y optimiza las directrices de HP Sure Start para un usuario normal. Dado que HP Sure Start se activa de forma predeterminada, el usuario normal no tiene necesidad de modificar la configuración para tener la protección de HP Sure Start. Para los usuarios avanzados, la BIOS del sistema ofrece cierto control del comportamiento de HP Sure Start, ya que se pueden configurar las directrices en la configuración de la BIOS (F10).

Si no se indica otra cosa, esta configuración y las funciones se encuentran bajo la BIOS o Seguridad de Sure Start.

Nota: Las directrices se almacenan en la memoria no volátil del controlador HP ESC no directamente accesible por la CPU anfitriona, por lo que hay que efectuar un reinicio para que la configuración de Sure Start tenga efecto.

Se encuentran disponibles las siguientes funciones y configuraciones de HP Sure Start:

- Verificación del bloque de arranque para cada arranque
- Directrices de recuperación de datos de la BIOS
- Restauración de la configuración del controlador de red (solo Intel)
- Aviso de cambio en la configuración del controlador de red (solo Intel)
- Escaneo dinámico en tiempo de ejecución del bloque de arranque (solo Intel)
- Protección de la configuración de la BIOS de HP Sure Start
- Protección de las claves de arranque seguro de HP Sure Start
- Prevención y detección de intrusión mejoradas en tiempo de ejecución del firmware de HP (solo Intel)
- Detección de intrusión en tiempo de ejecución del firmware de HP (solo AMD)
- Directrices de eventos de seguridad de HP Sure Start
- Notificación de arranque de evento de seguridad de HP Sure Start
- Bloqueo de la versión de la BIOS
- Almacenamiento/restauración MBR del disco duro del sistema
- Almacenamiento/restauración GPT del disco duro del sistema
- Directrices de recuperación (MBR/GPT) del sector de arranque

Verificación del bloque de arranque para cada arranque

HP Sure Start siempre verifica la integridad del bloque de arranque BIOS de la memoria flash antes de que el sistema salga del modo de suspensión o hibernación, o al iniciarse. Al **activar** esta función, HP Sure Start verifica también la integridad del bloque de arranque para cada arranque en caliente (reinicio de Windows). El tiempo de reinicio será algo más lento, a cambio de mayor seguridad. La configuración predeterminada de esta función es **desactivada**.

Directrices de recuperación de datos de la BIOS

Al configurar esta función en **Automática**, HP Sure Start repara automáticamente la BIOS o los datos exclusivos del equipo cada vez que es necesario. Si se configura como **Manual**, HP Sure Start necesitará de una secuencia especial de claves para efectuar la reparación. En caso de problemas con el código del bloque de arranque, el sistema no arrancará y el sistema LED emitirá una secuencia de señales característica. En caso de problemas con los datos exclusivos del equipo, el sistema mostrará un mensaje en la pantalla. La secuencia de claves requerida, así como la secuencia de señales, dependerán de si el sistema es un portátil, un ordenador de escritorio o una tableta. El modo manual es útil para los usuarios que puedan realizar el análisis forense del contenido de la memoria flash del sistema antes de hacer la reparación. No se recomienda el modo manual para los usuarios normales. La configuración predeterminada de esta función es **Automática**.

Restauración de la configuración del controlador de red (solo Intel)

Este control está disponible solo en sistemas Intel. Al seleccionarse esta función, HP Sure Start restablece inmediatamente el controlador de red a la configuración de fábrica.

Aviso de cambio en la configuración del controlador de red (solo Intel)

Esta configuración solo está disponible en sistemas Intel. HP proporciona una configuración del controlador de red predeterminada de fábrica que incluye la dirección MAC. Cuando se **activa** esta función, el sistema monitoriza el estado de la configuración del controlador de red y avisa al usuario en caso de cualquier cambio en el estado predeterminado de fábrica. La configuración predeterminada de esta función es **desactivada**.

Escaneo dinámico en tiempo de ejecución del bloque de arranque (solo Intel)

Esta configuración solo está disponible en sistemas Intel. Con la configuración predeterminada en estado **activado**, HP Sure Start verifica periódicamente la integridad del bloque de arranque BIOS mientras el SO está en funcionamiento. En posición **desactivada**, HP Sure Start verifica la integridad solo antes del arranque o de que el sistema salga del modo de suspensión o hibernación.

Protección de la configuración de la BIOS de HP Sure Start

La configuración predeterminada de la directriz de protección de la BIOS es **desactivada**. Para activar esta función, el propietario/administrador del dispositivo cliente debe configurar primero todas las directrices de la BIOS de la manera que prefiera. El propietario/administrador deberá configurar también la contraseña BIOS del administrador para poder hacer uso de la protección de configuración de la BIOS de HP Sure Start.

Una vez realizado esto, deberá cambiar la directriz de protección de la configuración de la BIOS a “activada”. En este momento, se creará una copia de seguridad (backup) de toda la configuración de la BIOS en el almacenamiento protegido de HP Sure Start. Posteriormente a ello, no se podrá modificar ninguna configuración de la BIOS de forma local ni remota. En cada arranque, se verificará que la directriz de la BIOS se encuentre en el estado prefijado y, de haber alguna discrepancia, se restaurará la configuración de la BIOS a partir del almacenamiento protegido de HP Sure Start.

Para modificar la configuración de la BIOS, deberá proporcionarse la contraseña BIOS del administrador y desactivarse después la protección de la configuración de la BIOS para poder hacer los cambios en la BIOS.

Protección de claves de arranque seguro de HP Sure Start

Con esta función predeterminada de fábrica como **activada**, HP Sure Start proporciona protección mejorada de las bases de datos y claves de arranque seguro que utiliza la BIOS para verificar la integridad y autenticidad del gestor de arranque del SO antes de efectuar el arranque. Si se coloca en función **desactivada**, solo se empleará la protección variable de arranque seguro UEFI estándar, y el subsistema HP Sure Start no guardará copia de seguridad (backup).

Prevención y detección de intrusión mejoradas en tiempo de ejecución del firmware de HP (solo Intel) y Detección de intrusión en tiempo de ejecución del firmware de HP (solo AMD)

La función RTID viene **activada** de forma predeterminada para todas las plataformas que salen de la fábrica HP, por lo que no es necesario que el cliente final o el administrador la active ni la ponga "en operación" para aprovechar las ventajas de la RTID de HP Sure Start.

No obstante, si se desea, esta función puede ser **desactivada** por el propietario o administrador de la plataforma.

Directrices para incidencias de seguridad de HP Sure Start

Esta configuración de directrices de la BIOS controla la acción que se debe efectuar cuando HP Sure Start detecta un ataque o intento de ataque mientras el SO está en funcionamiento. Hay tres configuraciones posibles de estas directrices:

- **Registro de incidencias únicamente**: Si se selecciona esta opción, el controlador HP ESC registra los casos de detección, que pueden verse en los registros de aplicaciones y servicios o la ruta de HP Sure Start al Windows Event Viewer (Visor de Eventos) de Microsoft Windows.[3]
- **Registro de incidencias y notificación al usuario**: Esta es la configuración predeterminada. Si se selecciona esta opción, el controlador HP ESC registra los casos de detección, que pueden verse en los registros de aplicaciones y servicios o la ruta de HP Sure Start al Windows Event Viewer (Visor de Eventos) de Microsoft Windows. Además, también se avisa al usuario desde Windows de la incidencia. [4]
- **Registro de incidencias y desconexión del sistema**: Si se selecciona esta opción, el controlador HP ESC registra los casos de detección, que pueden verse en los registros de aplicaciones y servicios o la ruta de HP Sure Start al Windows Event Viewer (Visor de Eventos) de Microsoft Windows. Además, también se avisa al usuario desde Windows de la incidencia y de que el cierre del sistema es inminente.

Notificación de arranque de evento de seguridad de HP Sure Start

Esta configuración de directrices de la BIOS controla si las advertencias y mensajes de error de HP Sure Start que aparecen cuando arranca el sistema requieren que el usuario local acuse recibo del error antes de proseguir con el proceso de arranque. Con la configuración predeterminada **Requerir reconocimiento**, el sistema se detiene mostrando el mensaje de error, y el usuario local debe pulsar una tecla para proseguir el proceso de arranque. Si se cambia la configuración a **Detención durante 15 segundos**, el mensaje se muestra igualmente pero el proceso de arranque continúa automáticamente al cabo de 15 segundos.

Bloqueo de la versión de la BIOS

En la configuración BIOS (F10), esta función se encuentra en Main/Update System BIOS (BIOS del sistema principal/actualización).

Si se pone en **desactivada**, se podrá actualizar la BIOS mediante cualquier proceso compatible. Si el controlador HP ESC detecta una actualización válida del bloque de arranque en la memoria flash del sistema, actualiza la copia de seguridad (backup) del bloque de arranque.

Si se pone esta configuración como **activada**, ninguna herramienta de actualización de la BIOS de HP actualizará la BIOS. Además, HP Sure Start protege la BIOS de cualquier intento de cambiar la versión de la misma eliminando la memoria flash del sistema por algún método no autorizado. El HP ESC registra la versión bloqueada de la BIOS. Si el controlador HP ESC detecta algún cambio en la BIOS de la memoria flash del sistema, sobrescribe el bloque de arranque de la BIOS a partir de la copia efectuada por el HP ESC. La copia del bloque de arranque efectuada por el HP ESC ejecuta y recupera la restante versión correcta de la BIOS. La configuración predeterminada de esta función es **desactivada**.

Almacenamiento/restauración MBR del disco duro del sistema y Almacenamiento/restauración GPT del disco duro del sistema

En la configuración BIOS (F10), esta función se encuentra en Security/Hard Drive Utilities (Seguridad/Utilidades del disco duro). Solo hay una de estas capacidades disponible, dependiendo del tipo de partición del disco primario (GPT o MBR) que detecte HP Sure Start.

En la posición **activada**, HP Sure Start mantiene una copia de seguridad (backup) protegida de la tabla de partición MBR/GPT del disco primario, y la compara con la primaria de cada arranque. Si se detecta una diferencia, el usuario recibe un aviso y puede decidir entre hacer una recuperación al estado original a partir de la copia, o actualizar la copia protegida según los cambios. Opcionalmente, pueden usarse las **directrices de recuperación (MBR/GPT) del sector de arranque** para eliminar la decisión del usuario respecto a la acción a efectuar en caso de que el sistema HP Sure Start encontrara una discrepancia.

Con esta configuración **desactivada** (de forma predeterminada), HP Sure Start no proporciona la protección MBR/GPT.

Directrices de recuperación (MBR/GPT) del sector de arranque

Con la configuración de **Control local del usuario** (de forma predeterminada) el usuario recibe el aviso para que tome una decisión en caso de que HP Sure Start detecte algún cambio en la tabla de partición MBR/GPT. Si la posición es **Recuperar en caso de corrupción**, HP Sure Start restaura automáticamente el sistema MBR/GPT al estado almacenado cada vez que se encuentre una diferencia.

Gestión remota de los controles de directrices de HP Sure Start

Al iniciarse el dispositivo por primera vez, las directrices de HP Sure Start se optimizan para el usuario normal. Dado que HP Sure Start se activa de forma predeterminada, el administrador remoto no tiene necesidad de activar HP Sure Start ni ponerlo "en operación". En caso de que el administrador remoto quisiera modificar la configuración de las directrices de HP Sure Start, los mismos comandos API de Windows Management Instrumentation (WMI) (instrumentación de gestión de Windows) o de la HP BIOS Configuration Utility (utilidad de configuración) que se emplean para gestionar otras directrices de la plataforma BIOS pueden utilizarse para gestionar las directrices de HP Sure Start. Además, el administrador puede gestionar de forma remota las capacidades de HP Sure Start mediante el complemento (plugin) de integración de gestionabilidad Manageability Integration Kit (MIK) para el gestor de configuración Microsoft System Center Configuration Manager (SCCM).

O, si lo prefiere, el administrador puede gestionar de forma remota las capacidades de HP Sure Start y ver los eventos de HP Sure Start con el complemento (plugin) Manageability Integration Kit (MIK) para Microsoft System Center Configuration Manager (SCCM).

Conclusión

HP Sure Start proporciona los siguientes beneficios claves:

- **Productividad ininterrumpida** – HP Sure Start mantiene la continuidad del negocio en caso de ataque informático o corrupción accidental, eliminando pérdidas de tiempo mientras se espera el servicio de TI.
- **Reducción de costes** – La capacidad de recuperación automática de HP Sure Start reduce las llamadas al servicio de asistencia de TI y mejora la productividad, lo que en última instancia reduce los costes de mantenimiento de la plataforma.
- **Tranquilidad** – HP Sure Start posee múltiples funciones de seguridad en una extensa variedad de plataformas de software y hardware.

Proteja el componente crítico de la BIOS y el firmware de ataques de malware, con el sistema líder de la industria en detección de intrusiones al firmware y reparación automática que le ofrece HP Sure Start, disponible de forma exclusiva en ciertos ordenadores HP Elite.

Apéndice A – HP Sure Start, de Gen a Gen

HP presentó Sure Start en 2014. Desde ese momento, ha estado mejorando Sure Start y ha incrementado el número de productos que lo emplean. La siguiente tabla presenta un resumen de las capacidades que se han ido añadiendo en cada generación.

Generación	Fecha de lanzamiento	Capacidades añadidas
HP Sure Start	2014	• Validación de la autenticidad del firmware y la BIOS, con capacidad de autorreparación • Monitorización y cumplimiento del firmware
HP Sure Start con protección dinámica	2015	• Compatibilidad del visor de eventos Windows Event Viewer • Protección dinámica (en productos Intel selectos)
HP Sure Start Gen3 (productos Intel selectos)[5] HP Sure Start con detección de intrusión en tiempo de ejecución Runtime Intrusion Detection (productos AMD selectos)[6]	2017	• Runtime Intrusion Detection • Protección de la configuración de la BIOS • Complemento (plugin) Manageability Integration Kit (MIK) para Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Almacenamiento protegido: métodos criptográficos robustos de almacenaje de la configuración de la BIOS, credenciales de usuario y otras configuraciones en el hardware del controlador HP Endpoint Security Controller para proporcionar protección de la integridad, detección de intervenciones y protección de la confidencialidad de la información • Protección de la base de datos del sistema de arranque seguro: protección mejorada de las bases de datos y claves almacenadas por la BIOS que son críticas para la integridad de la función de arranque seguro del SO en comparación con la protección UEFI estándar de la BIOS • En las plataformas Intel, protección y recuperación mejoradas del firmware del motor de gestión Management Engine Intel • Certificación de seguridad independiente del controlador HP Endpoint Security Controller: pruebas efectuadas por un acreditado laboratorio independiente para la validación del funcionamiento del núcleo del hardware HP ESC según lo especificado mediante criterios, métodos y procesos públicamente disponibles[1] • Los PC comerciales de HP equipados con HP Sure Start exceden las directrices de resiliencia del proyecto de plataforma de firmware del NIST (Publicación Especial 800-193)

Apéndice B – Resumen general del System Management Mode (SMM)

El System Management Mode (SMM) es un sistema estándar de la industria para funciones avanzadas de gestión de energía en ordenadores y otras funciones independientes del SO mientras este está en funcionamiento. Aunque las características y la implementación del SMM son específicas de las arquitecturas x86, muchas otras arquitecturas de computación modernas utilizan un concepto similar.

El SMM se configura por la BIOS en el momento de efectuar el arranque. El código SMM se registra en la memoria principal DRAM, tras lo cual la BIOS emplea unos registros de configuración especiales (bloqueables) del conjunto de microcircuitos para bloquear el acceso a esta área cuando el microprocesador no está operando en un contexto SMM. En tiempo de ejecución, la entrada al SMM se efectúa en función de eventos. El conjunto de microcircuitos está programado para reconocer una diversidad de eventos y límites de tiempo. Al producirse uno de tales eventos, el hardware del conjunto de microcircuitos valida el PIN de entrada del System Management Interrupt (SMI). En el límite de la instrucción siguiente, el microprocesador registra la totalidad del estado y entra al SMM.

Al efectuar la entrada al SMM, el microprocesador valida el PIN de salida del hardware, SMI Active (SMIACT). Este PIN avisa al hardware del conjunto de microcircuitos que el microprocesador está entrando al SMM. El SMI puede ser validado en cualquier momento durante cualquier proceso en modo de operación, pero no por el propio SMM. El hardware del conjunto de microcircuitos reconoce la señal SMIACT y redirige todos los ciclos de memoria subsiguientes a un área protegida de la memoria (a veces llamada área SMRAM), reservada específicamente para el SMM. Inmediatamente después de recibir la entrada SMI y validar la salida SMIACT, el microprocesador empieza a registrar la totalidad de su estado interno en esta área protegida de la memoria.

Una vez que el estado del microprocesador está almacenado en la memoria SMRAM, el código de manipulación especial SMM que también reside en la SMRAM (porque fue colocado allí por la BIOS del sistema en el momento del arranque) empieza a funcionar en un modo de operación especial SMM. Mientras opera en este modo, se suspenden la mayor parte de los mecanismos de aislamiento de memoria y de hardware, por lo que el microprocesador puede acceder prácticamente a todos los recursos de la plataforma para activarla a fin de que realice las tareas requeridas. El código SMM completa la tarea requerida, tras lo cual el microprocesador vuelve al modo de operación anterior. En ese momento, el código SMM ejecuta la instrucción de retorno del System Management Mode (RSM) para salir del SMM. La instrucción RSM hace que el microprocesador recupere los datos anteriores del estado interno a partir de la copia almacenada en SMRAM cuando entró en la SMM. Al completar la instrucción RSM, el estado completo del microprocesador se habrá restaurado al estado inmediatamente anterior al evento SMI, y el programa anterior (SO, aplicaciones, hipervisor, etc.) retoma la ejecución exactamente donde había quedado.

[1] El hardware del controlador HP Sure Start ha sido certificado dentro del marco de certificación CSPN.

[2] HP Sure Start con protección dinámica está disponible en los productos HP Elite equipados con procesadores Intel Core de 6.ª generación o superior.

[3] El software HP Notifications debe estar instalado para poder ver los eventos de HP Sure Start en el Windows Event Viewer (visor de eventos de Windows).

[4] El software HP Notifications debe estar instalado para poder recibir notificaciones.

[5] HP Sure Start Gen3 está disponible en los productos HP Elite equipados con procesadores Intel de 7.ª generación.

[6] HP Sure Start con Runtime Intrusion Detection está disponible en los productos HP Elite equipados con procesadores AMD de 7.ª generación.

[7] HP Sure Start Gen4 está disponible en los productos HP Elite y HP Pro 600 equipados con procesadores Intel o AMD de 8.ª generación.

Para más información, visite
hp.com/go/computersecurity

4AA7-3172ESE, Mayo de 2018