



HP WOLF SECURITY

INFORME TÉCNICO DE HP WOLF SECURITY FOR BUSINESS

PILA DE SEGURIDAD DE HP PARA ORDENADORES
COMERCIALES

INFORME TÉCNICO

DESDE EL MOMENTO EN QUE EL ORDENADOR SE ENCIENDE,

los productos de seguridad del portfolio de HP Wolf Security for Business trabajan juntos en segundo plano para proteger los equipos de tu negocio.

ÍNDICE

| | |
|---|---|
| INTRODUCCIÓN..... | 2 |
| COMPONENTES DE HP WOLF SECURITY FOR BUSINESS ¹ | 2 |
| CONTROLADOR HP ENDPOINT SECURITY | 2 |
| HP BIOSPHERE GEN6 ² | 3 |
| HP SURE START GEN6 ³ | 3 |
| HP SURE RUN GEN4 ⁴ | 3 |
| HP SURE RECOVER GEN4 ⁵ | 4 |
| HP CLIENT SECURITY MANAGER GEN7 ⁷ | 4 |
| HP SURE ADMIN ⁸ | 4 |
| HP SPAREKEY | 4 |
| UNIDADES AUTOCIFRADAS CERTIFICADAS | 5 |
| HP SECURE ERASE ⁹ | 5 |
| HP SURE CLICK ¹⁰ | 5 |
| HP SURE SENSE ¹¹ | 5 |
| HP SURE VIEW ¹² | 6 |
| HP TAMPER LOCK ¹³ | 6 |
| CONCLUSIÓN..... | 6 |

INTRODUCCIÓN

En el cambiante panorama actual, la mayoría de las personas trabajan desde casa y la seguridad de los ordenadores se encuentra en riesgo. Los ordenadores empresariales se utilizan fuera del entorno seguro de la oficina y la seguridad tradicional basada en la red no puede satisfacer las necesidades de seguridad por sí sola. En estos tiempos de cambio, los dispositivos son la primera línea de defensa, de modo que la seguridad para ordenadores basada en el hardware es más necesaria que nunca. Mientras el panorama digital sigue cambiando y los riesgos para la seguridad evolucionan, las soluciones de seguridad integradas en los ordenadores empresariales HP están diseñadas para proteger tu empresa. Desde el momento en que el ordenador se enciende, los productos de seguridad del portfolio de HP Wolf Security for Business trabajan juntos en segundo plano para proteger los equipos de tu negocio.

COMPONENTES DE HP WOLF SECURITY FOR BUSINESS¹

| | | DISPOSITIVO | IDENTIDAD | DATOS |
|-----------------------------------|---------------|----------------------------------|-----------|------------------------------------|
| | | HP Image Assistant | | |
| PROTECCIÓN REFORZADA POR HARDWARE | ENCIMA DEL SO | | | HP Sure View |
| | DENTRO DEL SO | | | HP Sure Click |
| | | | | HP Sure Sense |
| | DEBAJO DEL SO | HP Sure Run | | |
| | | HP Sure Start | | |
| | | HP Sure Recover | | HP Secure Erase |
| | | HP Tamper Lock | | Unidades autocifradas certificadas |
| | | HP Sure Admin | | |
| HP BIOSphere | | | | |
| | | HP Client Security Manager | | |
| | | Controlador HP Endpoint Security | | |

CONTROLADOR HP ENDPOINT SECURITY

El controlador HP Endpoint Security es el componente de hardware que constituye la base de la arquitectura de seguridad de los ordenadores empresariales HP. Este microcontrolador de hardware aislado físicamente y protegido criptográficamente debajo del SO crea la raíz de confianza de hardware que permite soluciones de seguridad reforzadas por hardware, de recuperación automática y gestionables, como HP BIOSphere Sure Start, HP Sure Run y HP Sure Recover.

HP BIOSPHERE GEN6²

Con más de una década de liderazgo en materia de seguridad de la BIOS, el firmware para ordenadores de HP BIOSphere automatiza la protección de la BIOS y mejora la capacidad de gestión. La BIOS es una serie de instrucciones de arranque que se utilizan para cargar los componentes de hardware críticos e iniciar el firmware. HP BIOSphere crea un ecosistema de protección alrededor de la BIOS debajo del SO para ayudar a defender tu equipo. Con protecciones automatizadas, medidas de seguridad personalizables y una capacidad de gestión sencilla, HP BIOSphere protege tu ordenador de ataques sin interrumpir la productividad del empleado.

HP SURE START GEN6³

Desde el momento en que el ordenador se enciende, HP Sure Start trabaja debajo del SO para proteger el dispositivo al comunicarse con HP BIOSphere para confirmar que la BIOS permanece intacta. Si se detecta una manipulación de la BIOS, HP Sure Start, junto con el controlador HP Security, reemplaza la BIOS por una versión limpia y arranca el equipo con una BIOS limpia y totalmente funcional. HP Sure Start sigue inspeccionando constantemente la BIOS del sistema y se recupera de forma automática en caso de que la BIOS esté dañada por malware, rootkits o corrupción. Al garantizar que solo se ejecuta el código de la BIOS de confianza, HP Sure Start protege el ordenador en su nivel más fundamental.

Novedad de la Gen6:

- Ahora está disponible en una gama más amplia, desde la serie ProBook 400 hasta la serie EliteBook 1000, incluidos los ordenadores AMD.
- La tecnología Smart Flash mejora el tiempo de recuperación en un 91 % al borrar y preprogramar cualquier bloque de 4 kb que no esté como debería.
- La detección de intrusiones en tiempo de ejecución del controlador Endpoint Security ofrece compatibilidad con una unidad de protección de memoria (MPU, por sus siglas en inglés) dentro de dicho controlador. Para ello, este detecta y bloquea cualquier ejecución de código fraudulenta.
- Protege de los ataques DMA previos al arranque en ranuras internas con visual en la parte inferior de los ordenadores Intel.

HP SURE RUN GEN4⁴

HP Sure Run protege el dispositivo debajo del SO al utilizar una protección reforzada por hardware para mantener los procesos críticos en funcionamiento, incluso si el malware trata de cerrarlos. Con el respaldo del controlador HP Endpoint Security, HP Sure Run supervisa los procesos clave, avisa a los usuarios y al personal de IT de cualquier cambio y reinicia de forma automática los procesos clave en caso de que se detengan. HP Sure Run, al ser la solución de persistencia de aplicaciones reforzada por hardware de HP, posee la capacidad de mantener comunicaciones con el hardware de aplicación de políticas mientras se ejecuta el SO. HP Sure Run supervisa continuamente la presencia de servicios y aplicaciones críticas, incluso si el agente de HP Sure Run en el SO es atacado o eliminado. Para garantizar la integridad del SO, HP Sure Run interactúa con el controlador HP Endpoint Security a nivel de hardware debajo del SO. Se incluye sin cargo adicional en productos HP seleccionados. Entre las funciones introducidas en HP Sure Run Gen3 se incluyen: Dynamic Persistence, que reinstala automáticamente el agente en caso de que se detenga, y Kill Prevention, que detiene los efectos secundarios del malware.

HP SURE RECOVER GEN4⁵

HP Sure Recover, que se integra en el hardware y el firmware del sistema, protege el dispositivo al permitir que los usuarios restauren sus máquinas de forma rápida y segura a la imagen más reciente utilizando solo una conexión de red. Con la creación de nuevas imágenes integrada de HP Sure Recover⁶, el usuario puede instalar el sistema operativo y los controladores desde un dispositivo de almacenamiento local dedicado sin intervención del personal de IT. HP Sure Recover aumenta la resiliencia y reduce el tiempo de inactividad al mínimo por medio de una solución de recuperación automatizada del sistema operativo que se integra en el hardware y el firmware de los ordenadores HP. HP Sure Recover te permite recuperar rápidamente el sistema operativo, siempre que sea necesario, durante todo el ciclo de vida del ordenador. HP Sure Recover funciona con éxito incluso si la unidad principal se ha borrado por completo. HP Sure Recover permite al personal de IT programar la creación de nuevas imágenes para toda la flota. Entre las funciones introducidas en HP Sure Recover Gen3 se incluyen: Recuperación basada en la red de la nube mediante Wi-Fi y recuperación eficiente con pausa, reanudación y reintento.

Novedad de la Gen4:

- Preparado para imagen corporativa

HP CLIENT SECURITY MANAGER GEN7⁷

HP Client Security Manager provee la fuerza de la autenticación de seguridad basada en hardware para apoyar los esfuerzos de protección de los usuarios y profesionales de IT mediante la configuración y el control de una serie de funciones de seguridad integradas en los ordenadores HP dentro del SO, incluido HP Sure Run y HP Sure Recover.

HP SURE ADMIN⁸

Con una herramienta opcional de gestión de la BIOS que no requiere contraseña de HP Sure Admin, los profesionales de IT disponen de una vía para alejarse de la gestión de la BIOS basada en contraseña. HP Sure Admin ofrece un enfoque moderno basado en una sólida criptografía de clave pública que se puede utilizar para gestionar de forma segura la configuración de la BIOS de los ordenadores empresariales HP sin necesidad de revelar el secreto de autorización.

Las herramientas de gestión remota de HP Sure Admin ofrecen un método innovador que permite al administrador remoto y al administrador presente localmente gestionar de forma remota la configuración de la BIOS de los ordenadores empresariales HP para atender al usuario con rapidez y seguridad.

HP SPAREKEY

¿Has olvidado tu contraseña de Windows? HP SpareKey trabaja dentro del SO para proteger la identidad, restablecer contraseñas y restaurar el acceso a ordenadores bloqueados sin intervención del personal de IT. Para ello, realiza al usuario una serie de preguntas de seguridad predeterminadas.

UNIDADES AUTOCIFRADAS CERTIFICADAS

Las unidades de disco duro y las unidades de estado sólido autocifradas emplean cifrado basado en hardware para proteger su contenido incluso después de que se extraigan del ordenador. Dado que el proceso de cifrado de datos se basa en hardware, el impacto en el rendimiento es mínimo o nulo.

HP SECURE ERASE⁹

El simple hecho de eliminar archivos de un disco duro no los hace irre recuperables. HP Secure Erase es una función a nivel de BIOS que protege los datos al destruir de forma permanente la información confidencial de las unidades de disco duro y de estado sólido. Esto garantiza que la información eliminada nunca se podrá recuperar ni poner en riesgo.

HP SURE CLICK¹⁰

Los usuarios acceden cada vez más a aplicaciones empresariales y de consumo sobre la marcha, en redes que no son de confianza, y a veces desde sus propios dispositivos personales. Los navegadores web son un vector de ataque principal para malware y otras amenazas en línea. HP Sure Click brinda una solución revolucionaria desarrollada por medio de la colaboración entre HP y Bromium, los pioneros del aislamiento de aplicaciones mediante el uso de una tecnología de microvirtualización patentada. HP Sure Click es una solución de navegación segura reforzada por hardware dentro del SO que aísla el contenido web en una máquina virtual aislada de la CPU, donde el malware no puede afectar a otras pestañas, aplicaciones ni al sistema operativo. Al aislar de manera eficaz la actividad contenida en el navegador, HP Sure Click reduce la capacidad de dañar de un proceso comprometido.

Con HP Sure Click, el dispositivo puede impedir los ataques procedentes del navegador. El malware se bloquea para que no pueda acceder a documentos, intranets de empresas o incluso otros sitios web. A continuación, se borra de forma automática cuando se cierra la pestaña del navegador, de modo que se elimina las costosas reparaciones y tiempos de inactividad. Al brindar una seguridad y una privacidad sin precedentes dentro de una experiencia de usuario rápida, familiar y receptiva, el aislamiento de tareas de HP Sure Click protege a los usuarios mientras trabajan y juegan.

Novedad para 2020:

- Se han añadido los navegadores Firefox y Edge.
- Compatibilidad con UWP/Ingress para aplicaciones de Office y Skype.
- Opción de incorporación automática de sitios de confianza.
- Mejoras en la aplicación, incluyendo modificaciones en los botones de opción.
- Recopilación de datos en la desinstalación.
- Nueva compatibilidad con Windows 10 IoT Enterprise 2016 y 2019 LTSC.

HP SURE SENSE¹¹

Ante el creciente riesgo de que la IA se utilice en ataques de malware, Sure Sense es la solución de HP que emplea IA de aprendizaje profundo con funcionalidades de protección contra malware que se encuentran años luz por delante. HP Sure Sense detecta las amenazas de día cero desconocidas hasta la fecha y protege el ordenador en tiempo real. HP Sure Sense actúa dentro del SO junto con HP Sure Run para mantener los dispositivos protegidos en todo momento, independientemente de si estos se encuentran en línea o no.

El algoritmo de aprendizaje profundo sumamente avanzado de HP Sure Sense escanea cada archivo en el dispositivo y reconoce instintivamente cualquier nueva amenaza, incluso ataques de día cero desconocidos que el software antivirus tradicional basado en firmas podría pasar por alto. El sistema de reconocimiento instintivo de HP Sure Sense solo tiene que actualizarse cuatro veces al año. HP Sure Sense se envía en una lista selecta de ordenadores y también se encuentra disponible como descarga de paquete de software (Softpaq) para que los profesionales de IT puedan añadirlo a la imagen corporativa. Al investigar, reparar y contener la amenaza en menos de un minuto, HP Sure Sense protege en tiempo real frente a ransomware, exploits, spyware y amenazas ejecutables. HP Sure Sense ofrece toda esta potente protección con un uso extraordinariamente ligero de los recursos del sistema de la CPU (1 %).

HP SURE VIEW¹²

Ni siquiera el mejor software de seguridad puede impedir un hackeo visual, es decir, que usuarios no autorizados vean información confidencial en una pantalla no vigilada. HP dispone de una solución para evitar que los datos se vean comprometidos visualmente. Con solo pulsar un botón, HP Sure View protege los datos al activar una pantalla de privacidad integrada que hace que los datos sean visibles solo para el usuario que está sentado directamente frente a ella. Con HP Sure View, los usuarios pueden trabajar con confianza desde cualquier ubicación sin temor a que los datos en pantalla se vean comprometidos por miradas curiosas. No obstante, los usuarios pueden compartir la pantalla con clientes y compañeros con solo pulsar una tecla, que activa y desactiva la función. Con independencia del lugar en el que se utilice el ordenador (en un avión, en un centro de atención médica o en cualquier ubicación remota), HP Sure View dota a los empleados del poder de la privacidad. Con HP Sure View, tu pantalla es tuya y tú eliges si quieres compartir la vista o no.

HP TAMPER LOCK¹³

Debido al intercambio de información de código abierto entre los atacantes, los posibles atacantes disponen ahora con facilidad de instrucciones detalladas sobre cómo realizar ataques. Cada vez es más habitual que los atacantes abran físicamente el chasis de un ordenador y pirateen sus componentes para eliminar las contraseñas de inicio de sesión, modificar el tráfico o detectar pulsaciones de teclas. HP Tamper Lock detecta cuando se ha abierto o manipulado el chasis de un equipo. Posteriormente, genera una solicitud de introducción de contraseña de la BIOS de HP Sure Admin para arrancar el ordenador.

CONCLUSIÓN

Como creador de los ordenadores más seguros del mundo, HP se toma muy en serio la seguridad de los ordenadores empresariales.

HP ha ideado un sólido conjunto de herramientas de seguridad que funcionan de manera coordinada para proteger sin descanso los activos de tus puntos de conexión y tus datos, de modo que puedas centrarte en tu negocio.

Obtén más información acerca de estas [soluciones de seguridad de HP](#) en el HP Security Center, que se encuentra disponible en línea.

INFORME TÉCNICO DE HP WOLF SECURITY FOR BUSINESS

- ¹ HP Wolf Security for Business requiere Windows 10, incluye diversas funciones de seguridad de HP y está disponible en productos HP Pro, Elite y de estaciones de trabajo. Consulta la información detallada del producto para conocer las funciones de seguridad que incluye y los requisitos del SO.
- ² HP BIOSphere Gen6 requiere Windows 10 y está disponible en productos HP Pro y Elite, ordenadores y estaciones de trabajo Z. Las funciones pueden variar dependiendo de la plataforma y de las configuraciones.
- ³ HP Sure Start Gen6 se encuentra disponible en ordenadores HP seleccionados y requiere Windows 10.
- ⁴ HP Sure Run Gen4 se encuentra disponible en ordenadores HP seleccionados y requiere Windows 10.
- ⁵ HP Sure Recover Gen4 se encuentra disponible en ordenadores HP seleccionados y requiere Windows 10 y una conexión de red abierta. Debes realizar copias de seguridad de los archivos importantes, fotos, vídeos, etc., antes de utilizar HP Sure Recover para evitar perder tus datos. La recuperación basada en la red mediante Wi-Fi solo está disponible en ordenadores con el módulo Wi-Fi de Intel.
- ⁶ HP Sure Recover Gen4 con creación de nuevas imágenes integrada es una función opcional que requiere Windows 10 y se debe configurar en el momento de la compra. Para evitar la pérdida de datos, debes realizar copias de seguridad de los datos importantes, archivos, fotografías, vídeos, etc. La recuperación basada en la red mediante Wi-Fi solo está disponible en ordenadores con el módulo Wi-Fi de Intel.
- ⁷ HP Client Security Manager Gen7 requiere Windows y está disponible en productos HP Pro y Elite, ordenadores y estaciones de trabajo Z.
- ⁸ HP Sure Admin requiere Windows 10, HP BIOS y HP Manageability Integration Kit de <http://www.hp.com/go/clientmanagement>, así como la aplicación para móvil HP Sure Admin Local Access Authenticator de la tienda de Android o Apple.
- ⁹ HP Secure Erase - Para los métodos descritos en la publicación especial 800--88, Método de saneamiento «definido», del Instituto Nacional de Estándares y Tecnología. HP Secure Erase no es compatible con plataformas con Intel® Optane™.
- ¹⁰ HP Sure Click requiere Windows 10. Visita https://bit.ly/2PrLT6A_SureClick para obtener información detallada.
- ¹¹ HP Sure Sense está disponible en ordenadores HP seleccionados y no está disponible con Windows 10 Home.
- ¹² La pantalla de privacidad integrada HP Sure View Reflect constituye una función opcional que debe configurarse en el momento de la compra y que está diseñada para funcionar en orientación horizontal.
- ¹³ El cliente o tu administrador deben habilitar HP Tamper Lock.

Regístrate para recibir actualizaciones: hp.com/go/getupdated



© Copyright 2021 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de HP quedan establecidas en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí indicado debe interpretarse como una garantía adicional. HP no se hace responsable de los errores u omisiones de carácter técnico o editorial que puedan existir en este documento.



Microsoft y Windows son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y en otros países. Wi-Fi® es una marca comercial registrada de Wi-Fi Alliance.