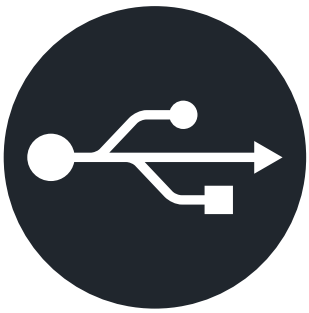
Cómo permitir el acceso a unidades USB

sin comprometer la protección de los puntos de conexión

Introducción

En enero de 1996, la presentación oficial de la especificación USB 1.0 anunció una nueva era de uniformidad, conveniencia y versatilidad tanto para los proveedores como para los usuarios finales de dispositivos periféricos. Han transcurrido 27 años y mantiene su retrocompatibilidad con cada revisión. USB persiste como piedra angular de las interfaces de hardware informáticas desde servidores hasta teléfonos inteligentes.



La sencillez de la conexión instantánea y las crecientes velocidades han posibilitado que el almacenamiento portátil en USB evolucione como uno de los grandes triunfadores. No obstante, este nivel de comodidad tiene su contrapartida en cuanto a la seguridad de los datos. En el mundo actual, si no se utilizan las herramientas adecuadas —como la protección de los puntos de conexión en ordenadores host y las prácticas de seguridad adecuadas—, los usuarios con actitudes descuidadas hacia el uso de almacenamiento USB portátil se exponen, y exponen a los demás, a posibles vulneraciones de datos que pueden resultar costosas para el usuario final, e incluso pueden comprometer a toda una organización o a un gobierno.

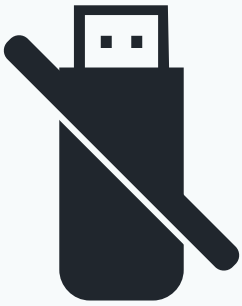
Además de proteger al entorno anfitrión, las unidades USB podrían protegerse mediante el uso de contraseñas y el cifrado por hardware integrado en el dispositivo. Esto constituye la defensa más sólida contra las intrusiones. Vamos a ver algunas buenas prácticas para utilizar las unidades USB de manera más segura y, además, analizaremos a fondo las unidades USB en general.

Aunque lo ideal es un concepto combinado, lo más importante es la solidez del cifrado y de los componentes de hardware de la propia unidad USB. Esto beneficia a diversos sectores, desde el financiero y el sanitario hasta el industrial y el militar. Además, juegan un importante papel en el teletrabajo cuando el acceso a las redes no está disponible, es vulnerable o resulta poco práctico.

Las unidades USB de hardware cifrado se presentan en diferentes categorías de homologación y ofrecen diversas características de seguridad. Examinando sus atributos y opciones de personalización podemos adaptarlas como soluciones independientes, protegiéndolas en todos sus aspectos dentro de entornos sensibles.

Autoridad de puerto: confluencia del almacenamiento en USB con el software de prevención de pérdida de datos del Administrador de puntos de conexión

Durante décadas, las aplicaciones antivirus y antimalware han ofrecido protección en el nivel más fundamental: exploran automáticamente las descargas y dispositivos conectados, e informan —o directamente actúan— sobre cualquier contenido sospechoso. La protección que ofrece el software antivirus de nueva generación (NGAV) va un paso más adelante. En lugar de basarse exclusivamente en una base de datos continuamente actualizada de firmas de virus, los NGAV incorporan funciones de aprendizaje automático y detección de patrones de comportamiento, capaces de identificar y mitigar amenazas desconocidas.



No obstante, no son la única arma del arsenal. Y para quienes deseen protección a prueba de balas para periféricos de usuario y otros, el software de prevención de pérdida de datos (DLP) de gestión de puntos de conexión ofrece los medios para denegar cualquier tipo de acceso a los puertos de USB y otros puntos de acceso.

La táctica de protección de "Bloquear todos los puertos" elimina, sin duda, los riesgos. Y en algunas circunstancias incluso es deseable. No obstante, esta metodología suele ser un instrumento demasiado contundente de consecuencias indeseables.

No obstante, algunos administradores de TI prefieren rechazar propuestas de apertura de puertos de USB en los equipos de los usuarios, ya que al hacerlo esos puntos de conexión permitirán el acceso directo a través de los cortafuegos. Dicha prudencia es comprensible, pero a la hora de habilitar el acceso para el almacenamiento en USB, la atribución de este privilegio no tendría que ser un problema de seguridad masivo si se observasen ciertos prerrequisitos.

Un requisito esencial es un paquete de aplicaciones de administración de puntos de conexión que incorpore la detección de amenazas de soluciones antivirus/antimalware junto con una monitorización y gestión centralizadas de todos los puntos de conexión de los usuarios.

En general, este método aparece de diversas maneras en las soluciones unificadas más populares de los principales proveedores, como McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection y WinMagic SecureDoc, por citar solo unas pocas.

Sofisticación en la inclusión en la lista blanca

A la hora de proteger los dispositivos de almacenamiento USB, el método implementado dependerá del nivel de protección requerido. Una norma sencilla, aunque eficaz, es incluir dispositivos de almacenamiento USB en la lista blanca utilizando sus respectivos valores de Identificador de proveedor (VID) e Identificador de producto (PID). Un común denominador de todos los periféricos USB es que cada fabricante tiene un VID único, pero que los PID cambian con cada nuevo producto que aparece.

A efectos de inclusión en las listas blancas, usar solamente el VID del fabricante podría ser demasiado generalizado como para resultar seguro, por cuanto permitiría todos y cada uno de los dispositivos USB jamás producidos. El PID permite afinar mejor la puntería, y exige que se permita acceso al sistema host a un modelo específico solamente.

Aunque se trata de una mejora, todavía no es lo ideal. Los dispositivos de almacenamiento USB son enormemente populares, puesto que permiten a los usuarios emplear sus propios dispositivos compatibles con los modelos autorizados. Teniendo todo esto en cuenta, Kingston Technology ofrece una solución a medida para reforzar la seguridad de los dispositivos de almacenamiento USB.

Disponibles a través de su programa de personalización, es posible crear perfiles de PID a la medida de cada organización y aplicarlos a diversas unidades Flash USB cifradas de Kingston. Las organizaciones que implementan dispositivos que incorporan un identificador de producto a la medida no solamente se benefician de simplificar la elaboración de sus listas blancas, sino también de una mayor protección. Si no se ajustan a los PID personalizados, se denegará el acceso a los dispositivos adquiridos particularmente por los empleados, aunque aparentemente sean idénticos.

Mientras que el uso de PID personalizados permitirá a los administradores de TI incorporar rápida y fácilmente nuevos

dispositivos USB, una alternativa más granular es emplear los números de serie individuales de los dispositivos que llevan la mayoría de las unidades USB cifradas de Kingston. Para esto se requiere que cada número de serie exclusivo del dispositivo quede registrado en el paquete de administración de puntos de conexión. Inicialmente, esto implicará la necesidad de procesamiento por parte del personal de TI, y Kingston puede facilitar una lista de números de serie con cada pedido: siempre son alfanuméricos y nunca secuenciales. La elección de este método posibilita políticas muchísimo más flexibles basadas en la propiedad de cada unidad individual, con la ventaja añadida de un trazado exacto de la proveniencia de los dispositivos, un elemento fundamental en los escenarios de informática forense. Algunas unidades de Kingston incluyen un número de serie y un código de barras en la carcasa para su escaneo electrónico. Otras pueden personalizarse para agregar un código de barras y un número de serie para las organizaciones. Estos elementos se emplean para llevar un seguimiento de las unidades.

De manera predeterminada, los sistemas de administración de puntos de conexión permiten el acceso a los VID/PID tanto para el bloqueo de puertos como para la inclusión en las listas blancas. Lo que Kingston ofrece es un método más versátil para aprovechar estas funciones y posibilitar políticas más prácticas e imaginativas que faciliten el uso de los dispositivos de almacenamiento USB. Una vez establecido un método de identificación adecuado, el mandato generalizado de "Bloquear todos los puertos" no solo resulta excesivamente simplista, sino que supone innecesario.

Soluciones seguras y compatibles para usuarios remotos

A la hora de proteger, incluir los dispositivos en listas blancas resuelve solo la mitad del problema. O, por decirlo de otra manera, es una media solución.

La conveniencia y simplicidad de los dispositivos de almacenamiento USB los hace indispensables en numerosas empresas e instituciones en las que la portabilidad es fundamental para experimentar transferencias de datos sin obstáculos. En la mayoría de los entornos, por motivos de cumplimiento normativo y de higiene informática, es necesario equipar al personal con unidades USB cifradas para realizar dichas tareas. Utilizando una combinación de protección por contraseña y cifrado de los dispositivos, se incorporan al almacenamiento portátil medidas que impiden el acceso a datos sensibles en caso de que la unidad se extravíe, sea robada o quede expuesta a una situación potencialmente vulnerable.

No se trata de una solución "de talla única", ya que las técnicas de cifrado varían y las diferencias más significativas salen a la luz cuando comparamos entre soluciones de cifrado de software y de hardware. ¿Y cuál es mejor? Pues dependerá de sus necesidades. No obstante, la pregunta más sensata a formular tendría que ser "¿Cuál es más segura?"

Esencialmente, el cifrado del software es una opción económica, que satisfará a algunos sectores por su menor cantidad de operaciones. También es adecuado para entidades cuyas transferencias de datos no se consideran sensibles y cuya preocupación está más centrada en el cumplimiento de políticas.

No obstante, el modus operandi del cifrado del software es también su talón de Aquiles, ya que requiere que sean las aplicaciones de cara al cliente basadas en un ordenador las que efectúen las tareas de cifrado. En consecuencia, por asociación, un dispositivo de almacenamiento de software cifrado será igual de seguro que el ordenador host.

Además, la exposición a las amenazas se ve incrementada porque los hackers con acceso a la memoria de los ordenadores pueden "oler" las claves de cifrado/descifrado. Por otra parte, los datos de la unidad pueden ser objeto de ataques de fuerza bruta, ya que no se necesita protección por contraseña si es posible acceder a los archivos cifrados, y copiarlos.

Debe recordarse que el cifrado basado en software posiblemente requiera periódicamente actualizaciones, susceptibles de complicar la implementación al generar una carga de trabajo adicional sobre el personal de TI. Lo peor de todo es que el cifrado del software puede ser totalmente eliminado por empleados frustrados que tengan problemas con la portabilidad de las unidades entre las plataformas. Los usuarios de las unidades pueden copiar los datos de la unidad cifrada en un ordenador, reformatear la unidad convirtiéndola en no cifrada y, a continuación, copiar en ella los datos. En esta situación, los datos quedarían desprotegidos y totalmente expuestos a una vulneración. A efectos de cumplimiento de las leyes y normas de privacidad de los datos, es inadmisible que la protección de las unidades USB pueda ser totalmente desactivada.

Cifrado en los chips: la solución difícil y rápida

Por contraste, las unidades USB de hardware cifrado funcionan independientemente del ordenador, ya que incorporan un procesador dedicado en su interior que gestiona el cifrado. Tiene un proceso de cifrado siempre activado con protección contra ataques de contraseñas de fuerza bruta. Los datos cifrados no son accesibles y no pueden copiarse.

Las unidades USB de hardware cifrado de Kingston de calidad empresarial y calidad militar utilizan el cifrado AES de 256 bits en modo XTS. Técnica de cifrado globalmente reconocida, la AES de 256 bits incorpora rigurosas salvaguardas de datos. Al utilizar dos claves separadas en diferentes fases del proceso de cifrado/descifrado, el modo XTS tiene un efecto similar al de cifrar los datos dos veces.

Cuando está en uso, la clave de cifrado se deriva del generador de números aleatorios del controlador de la unidad, desbloqueado con la contraseña del usuario. Como la autenticación tiene lugar dentro del hardware cifrado de la unidad, las claves de cifrado y otras funciones de seguridad críticas están protegidas contra amenazas comunes, como BadUSB, ataques de arranque en frío, código malicioso y ataques de fuerza bruta.

Una de las ventajas más evidentes del cifrado del hardware es que el funcionamiento de la unidad es significativamente mejor que el de las unidades de software cifrado, ya que las tareas de cifrado no se descargan al ordenador host. Todo tiene lugar dentro de la unidad.

Las unidades USB de hardware cifrado, como la IronKey D500S de Kingston, son dispositivos protegidos por contraseña que se entregan cifrados de fábrica. Durante el uso, para empezar solamente es visible el iniciador de volumen protegido contra escritura, ya que contiene la aplicación empleada para autenticar la contraseña y desbloquear el volumen de almacenamiento principal cifrado. Este procedimiento evita la necesidad de instalar cualquier tipo de controlador o software en el ordenador host.

Además, las unidades USB Kingston de hardware cifrado incorporan un firmware de firma digital, que impiden la manipulación del firmware contenido en el dispositivo. Esta capa adicional de seguridad protege contra ataques como BadUSB, que aprovechan una vulnerabilidad inherente del firmware del dispositivo USB. Esto podría conllevar la ejecución encubierta de comandos, o bien la ejecución de código malicioso, en el equipo anfitrión.

Obviamente, una política de "Bloquear todos los puertos" limitaría el riesgo de ataques de BadUSB, pero ¿por qué sacrificar la productividad con métodos tan obsoletos? Como ya se ha indicado, es posible mantener un entorno seguro sin renunciar al uso de dispositivos de almacenamiento portátil si se implementan procedimientos de compra e implementación sencillos para introducir unidades USB de hardware cifrado.

Teletrabajo seguro y compatible

Para los trabajadores remotos, estar apartados de las protecciones del entorno de trabajo seguro de sus organizaciones requiere de una revisión de las estrategias, así como de una nueva evaluación de las prioridades.

A la hora de preparar un plan de seguridad remota, ¿existe alguna ventaja en bloquear los puertos USB de los portátiles de los empleados solamente para que se conecten, a través de Internet, a un servidor para cargar o recuperar documentos? Para quienes trabajan a distancia o sobre la marcha, es posible que lo único disponible sea una conexión abierta a Internet, igual de insegura o carente de confianza como un punto de acceso wifi. Esto supone una amplia variedad de peligros que incrementan

enormemente las posibilidades de una vulneración. Las amenazas tales como la interceptación de datos o la vigilancia a través de suplantaciones, ataques de intermediario y escuchas furtivas en las redes son solo algunos de los cada vez más sofisticados métodos de pirateo que utilizan los ciberdelincuentes. Incluso las VPN se han visto expuestas.

La conexión de red de una organización a Internet no es más que otro punto de conexión, y su exposición inherente los convierte en puntos de entrada extremadamente vulnerables y preferidos. Su apertura al acceso remoto implica sus propios riesgos de seguridad, en especial en lo que respecta a los datos sensibles.

Suministrar a los teletrabajadores unidades USB protegidas por contraseña y con hardware cifrado elimina eficazmente estas potenciales vulnerabilidades de redes. No obstante, para ello se requerirá una evaluación exhaustiva de las unidades USB disponibles actualmente y en qué medida se ajustan a las demandas de cada entorno de teletrabajo. No se trata de algo tan sencillo como elegir en función a la capacidad de las unidades, o si deberían registrarse o no sus números de serie. Esto tiene que ver con la estructura física del propio dispositivo.

Protecciones inviolables: las opciones sólidas

El principal asunto es si las unidades USB de hardware cifrado son o no a prueba de manipulaciones. Cuán segura es una unidad a dichas interferencias se refleja en normas como FIPS 140-3, que incorpora diversos niveles que examinan la resiliencia de la estructura física de las unidades sin emplear métodos criptográficos.

La homologación FIPS-197 observa solamente los atributos de cifrado del hardware y dispositivos tales como el IronKey Vault Privacy 50 de Kingston y el SSD externo Vault Privacy 80, modelos orientados hacia la empresa cuyos requisitos de seguridad no alcanzan el grado militar. Estas unidades son más económicas, pero carecen de protección contra la manipulación física.

En la certificación FIPS 140-3 de Nivel 3 (pendiente), los métodos implementados para exponer las manipulaciones de los dispositivos se consideran de grado militar. Kingston suministra estas unidades FIPS 140-3 de Nivel 3 a empresas, administraciones públicas y organismos militares de todo el mundo.

Se utiliza la resina epóxida para revestir los circuitos de la unidad, y se encolan los componentes internos a la carcasa para crear otro muro de defensa. Todo intento de abrir la carcasa metálica resultaría extremadamente difícil y provocaría que los chips internos y demás componentes eventualmente se rompieran, provocando que la unidad resultase inservible. Gracias al uso de esta resina opaca y dura, manipular los componentes vitales se convierte en tarea prácticamente imposible. Dispositivos como el IronKey D500S y el S1000 de Kingston incluyen esta medida de seguridad adicional.

Estas protecciones de dispositivos no están limitadas solo a medidas físicas y la unidad IronKey S1000 de Kingston eleva la inviolabilidad a un nivel superior. El chip criptográfico interno de la unidad IronKey S1000 puede detectar cualquier manipulación física, y dejará inservible la unidad en cuanto esta se conecte. Emplear dispositivos de almacenamiento USB de hardware cifrado para acceder a archivos sensibles y transferirlos es una decisión pragmática que facilita las operaciones remotas y garantiza efectivamente la seguridad de campo.

Asegúrese de estudiar las características de seguridad y del hardware de las unidades USB para confirmar que son adecuadas para sus necesidades específicas y condiciones de uso. Cada unidad USB debe evaluarse caso por caso, recurriéndose a acreditaciones de confianza para ayudar a orientar estas decisiones. Sean cuales fueren las prioridades, Kingston ofrece una variedad de soluciones de unidades USB de hardware cifrado, así como opciones de personalización, a precios asequibles y a la medida de todo tipo de entornos: desde cumplimiento normativo en general y hasta las más estrictas especificaciones militares.

La seguridad es lo primero: sin redes, sin problemas

Hoy en día, la oficina no tiene fronteras y el trabajo desde casa sigue floreciendo. Para muchas organizaciones, esta situación ha puesto en el centro de atención los problemas de vulnerabilidad del acceso remoto. Muchas están experimentando estas dificultades por primera vez, y buscando métodos más seguros para adaptarse a esta creciente tendencia.

Para atender a estas necesidades en un amplio espectro de sectores, los dispositivos de almacenamiento USB de hardware cifrado ya son una realidad bien consolidada que ofrecen una solución segura para los casos en que la transferencia de datos a través de redes puede ser indeseable o impracticable por diversos motivos.

En el sector financiero, las autoridades reguladoras solicitan frecuentemente datos para verificar el comportamiento y el cumplimiento normativo de las firmas. El riesgo de exposición es demasiado grande como para contemplar el uso de redes para la transferencia de documentos sensibles que contienen detalles precisos de inversiones, operaciones bursátiles y otras actividades bancarias confidenciales. La solución más sencilla y eficaz es proporcionar estos datos en una unidad USB de hardware cifrado.

El uso de unidades USB seguras para transferir archivos en entornos sanitarios es habitual. También resulta conveniente para médicos o especialistas que pueden querer analizar archivos, enviarlos a investigación o presentar casos clínicos a los estudiantes de medicina. Existen también necesidades más prácticas cuando hablamos de sistemas patentados, como los dispositivos médicos para la obtención de imágenes, en que el acceso a las redes es inexistente o inseguro. Utilizando unidades USB de hardware cifrado compatibles, es posible transferir fácilmente los archivos para utilizarlos en otros lugares.

Qué debe y qué no debe hacer

✓ **Utilice unidades seguras y compatibles,** y revise las especificaciones para adquirir dispositivos que se ajusten a las necesidades de cada implementación.

✗ **No autorice políticas aleatorias o que admitan el uso de dispositivos particulares**; para cualquier organización, la pérdida de unidades no cifradas implica pagar un precio demasiado alto, no solo financiero, sino también de daño reputacional.

✓ **Implemente un paquete de administración de puntos de conexión** y utilice unidades USB de hardware cifrado que incorporen funciones diferenciadas de estructuración de listas blancas.

✗ **No deje nada librado al azar.** Evalúe correctamente los requisitos de los entornos locales y de trabajo a distancia.

✓ **Insista en la formación del personal** sobre asuntos de seguridad. Conciéncieles de que es de su interés el que la organización se proteja contra vulneraciones de la seguridad.

✗ **No convierta la protección en algo tan engorroso** que los empleados se salten las normas y empiecen a utilizar soluciones informáticas en la sombra. El hecho de que siempre se haya aplicado una política de talla única no implica que sea adecuada para todos los escenarios. El entorno de trabajo está cambiando, y si se eligen soluciones adecuadas será posible elaborar e implementar nuevas políticas.

En este escenario destaca especialmente el modelo IronKey Keypad 200 (KP200) de Kingston. Al ser un dispositivo independiente de cualquier sistema operativo, no existe ningún iniciador de volumen en el cual introducir la contraseña. En su lugar, cuenta con un teclado alfanumérico que desbloquea el dispositivo para poder utilizarlo en cualquier plataforma. Es una especie de navaja del ejército suizo de las unidades USB de hardware cifrado, y puede utilizarse también entornos industriales. Transfiere de manera segura aplicaciones empleadas en el mundo de la I+D de la informática a maquinaria controlada por plataformas de tecnologías operativas (TO). En plataformas mixtas en las que también se emplea Linux, la unidad KP200 es una de las soluciones seguras más perfectas que existen.

Los dispositivos de almacenamiento USB con hardware cifrado también juegan un papel vital en los entornos policiales o judiciales. Protegen y permiten transferir de manera segura archivos de casos, imágenes y otras pruebas a operadores de campo, departamentos de investigación y equipos forenses. Kingston ofrece una ventaja adicional, por el hecho de poder ofrecer unidades con el número de serie estampado en la carcasa exterior, junto con un código de barras. Los procedimientos de distribución y catalogación de unidades se simplifican, y se facilita su seguimiento. Es tan sencillo como registrar manualmente un número de serie o escanear un código de barras. Las auditorías y gestiones de inventarios no podrían ser más fáciles. Es una característica incorporada de serie en las unidades IronKey D500S, D500SM y S1000B/E de Kingston, aunque también la ofrecemos en otros modelos de hardware cifrado como parte del Programa de Personalización de Kingston.

Movilidad de almacenamiento y seguridad: los últimos avances

La protección con contraseña, el cifrado del hardware, las salvaguardas inviolables, las listas blancas granulares de los puntos de conexión, la homologación FIPS 140-3 de Nivel 3 de grado militar (pendiente) y el registro de unidades sobre la marcha son algunas de las características de serie de las unidades USB de Kingston que permiten implementarlas sin demora.

Estas sólidas protecciones de seguridad garantizan que las unidades USB y sus datos se mantengan protegidos en el entorno anfitrión. Aunque las especificaciones parezcan muy atractivas sobre el papel, elegir aleatoriamente un modelo sin haberlo estudiado no es garantía de encontrar los dispositivos adecuados en el caso de algunas organizaciones con requisitos más rigurosos.

Como fabricante independiente, Kingston ofrece una amplia variedad de opciones para satisfacer las necesidades de sus clientes. A través del Programa de Personalización de Kingston podemos ofrecerle las más avanzadas soluciones, diseñadas para posibilitar una perfecta experiencia de uso.

La personalización va más allá de ofrecer a una organización sus propios PID de USB para incluirlos en la lista de dispositivos admitidos. También puede personalizarse el perfil de seguridad del iniciador de la aplicación utilizando quince opciones diferentes a partir de los datos de contacto y de la organización para habilitar indicios de contraseñas y determinar el número máximo de intentos de introducirlas. Externamente ofrecemos la opción de marca de la organización (logotipo compartido) y diversos colores para unidades específicas. Con un pedido mínimo de cincuenta unidades, todas estas opciones posibilitan una sencilla ruta de integración para la implementación de los dispositivos.

Si todavía no tiene instalada una aplicación de administración de puntos de conexión adecuada para el almacenamiento en USB, ofrecemos una solución para organizaciones que desean gestionar sus unidades Kingston, incluyendo opciones de reconfigurar las contraseñas a distancia.

La ubicuidad y comodidad de las unidades USB les han permitido sobrevivir a muchas tecnologías prometedoras. Para numerosas tareas, la inmediatez y la conveniencia del almacenamiento en USB ha perdurado. Siempre seguras y disponibles, las unidades USB protegidas ofrecen una solución sencilla que sabrá valorar fácilmente.

¿Por qué preocuparse por las vulneraciones de datos de red en entornos remotos? Con los dispositivos de almacenamiento USB de hardware cifrado IronKey de Kingston, tendrá la respuesta en la palma de su mano.

Para obtener más información sobre cómo Kingston puede ayudarle, visite kingston.com/ironkey. Para consultas más específicas, pregunte a alguno de nuestros expertos en unidades USB cifradas.

#KingstonIsWithYou #KingstonIronkey