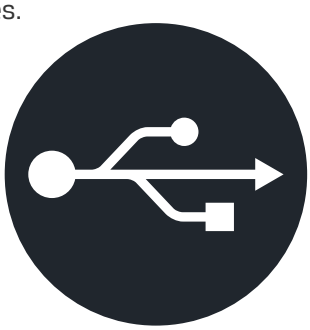
Cómo permitir acceso al dispositivo USB

sin comprometer la seguridad de punto final (Endpoint Security)

Introducción

En enero de 1996, la especificación oficial USB 1.0 al momento de su lanzamiento anunciaba una nueva era de uniformidad, conveniencia y versatilidad tanto para los proveedores de dispositivos periféricos como para los usuarios finales. 27 años después, mantiene la compatibilidad con versiones anteriores con cada actualización, y USB sigue siendo la piedra angular de la interfaz de hardware de la computadora desde los servidores hasta los teléfonos inteligentes.



La simplicidad plug-and-play de USB y las velocidades cada vez mayores han hecho que el almacenamiento portátil USB evolucione como uno de los grandes ganadores. Sin embargo, esta conveniencia es poco favorable cuando se trata de seguridad de datos. En el mundo actual, sin el uso de herramientas adecuadas, como la protección de terminales en las computadoras huésped y las prácticas adecuadas de seguridad de datos, los usuarios con una actitud descuidada en el uso de almacenamiento USB portátil se exponen a sí mismos y a otros a posibles filtraciones de datos que podrían ser costosas para el usuario final e incluso pueden comprometer a toda una organización o gobierno.

Además de proteger el entorno del huésped, la unidad USB también debe protegerse con contraseña y encriptada por hardware en el mismo dispositivo. Esto ofrece la defensa más sólida contra la intrusión. Repasaremos algunas de las mejores prácticas para utilizar las unidades USB de forma más segura junto con una mirada más profunda a las unidades USB en general.

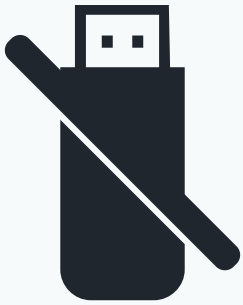
Si bien un enfoque combinado es ideal, es la solidez del encriptado y los componentes del hardware de la propia unidad USB los que son de suma importancia. Estos benefician a sectores que van desde el financiero hasta la salud, manufactura y ejército. También juegan un papel en el trabajo remoto cuando el acceso a la red no está disponible, es vulnerable o no es práctico.

Las unidades USB encriptadas por hardware están disponibles con diferentes grados de certificación, al tiempo que brindan una variedad de funciones de seguridad. Al examinar sus atributos y oportunidades de personalización, su conveniencia como soluciones independientes es un ejemplo a seguir al asegurar su lugar en todas las formas de entornos sensibles.

Autoridad de puertos: El almacenamiento USB combinado con el software de prevención de pérdida de datos en la administración de Endpoint

Durante décadas, las aplicaciones antivirus y antimalware han ofrecido protección al nivel más fundamental – escanear automáticamente las descargas y los dispositivos adjuntos e informar o actuar sobre el contenido sospechoso. La protección del software antivirus de última generación (NGAV) lleva esto un paso más allá. En lugar de depender únicamente de una base de datos de firmas de virus continuamente actualizada, NGAV agrega funciones de detección de comportamiento y aprendizaje automático (Machine Learning) que pueden identificar y mitigar amenazas desconocidas.

Sin embargo, no es la única arma en el arsenal, y para aquellos que desean protección a prueba de balas de los periféricos y más, el software Endpoint Management Data Loss Prevention (DLP) o de prevención de pérdida de datos en la administración de Endpoint, proporciona los medios para denegar cualquier tipo de acceso a puertos USB y otros puntos de acceso.



La actitud de 'Block All Ports (bloquear todos los puertos) hacia la seguridad ciertamente puede eliminar el riesgo y, en algunas circunstancias, puede ser deseable, pero tal política a menudo puede resultar un instrumento muy directo con consecuencias indeseables.

Sin embargo, algunos administradores de TI prefieren rechazar las solicitudes para abrir puertos USB en las máquinas de los usuarios, ya que hacerlo en estos puntos finales (endpoints) permitirán el acceso directo a través del firewall empresarial. Esta precaución es comprensible, pero cuando se trata de habilitar el acceso para el almacenamiento USB, el aprovisionamiento de este privilegio no tiene por qué ser un gran dolor de cabeza para la seguridad si se cumplen ciertos requisitos previos.

Un requisito esencial es un conjunto de aplicaciones de gestión de endpoints que incluya análisis de detección de amenazas en soluciones antivirus/antimalware, así como supervisión y gestión centralizadas de todos los endpoints de los usuarios.

En general, este enfoque directo y sencillo aparece en varias formas en soluciones unificadas de proveedores populares como McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection y WinMagic SecureDoc, por nombrar algunos.

Mejoras en la lista blanca (whitelist)

Cuando se trata de proteger las unidades de almacenamiento USB, el método implementado depende del nivel de protección requerido. Un enfoque simple pero efectivo es incluir en la lista blanca los dispositivos de almacenamiento USB utilizando sus respectivos valores de Identificador de proveedor (VID) e Identificador de producto (PID). Una cosa a saber de todos los periféricos USB es que los fabricantes tienen cada uno un VID único, pero el PID cambia para cada producto nuevo que se lanza.

Para las listas blancas, usar únicamente el VID del fabricante sería demasiado amplio para ser seguro, ya que se permitirían todas las unidades USB que este haya producido. El PID ofrece más depuración y exige que solo un modelo específico tenga acceso al sistema huésped.

Si bien esto es una mejora, todavía no es ideal. Los dispositivos de almacenamiento USB son muy populares, ya que permite a los usuarios adquirir dispositivos propios que coincidan con los modelos autorizados. Teniendo esto en cuenta, Kingston Technology ofrece una solución a medida para reforzar la seguridad de las unidades de almacenamiento USB.

Disponibles a través de su programa de personalización, los perfiles PID específicos para una organización se pueden crear y aplicar a una variedad de unidades de memoria flash USB encriptadas de Kingston. Las empresas que implementan dispositivos con un identificador de producto personalizado no solo se benefician de una lista blanca simplificada, sino de una seguridad considerablemente mejor. Sin un PID personalizado que coincida, se denegará el acceso incluso a dispositivos aparentemente idénticos adquiridos de forma independiente por los empleados.

Si bien el uso de PID personalizados permitirá a los administradores de TI poner en funcionamiento nuevas unidades de almacenamiento USB rápida y fácilmente, una alternativa más granular es utilizar números de serie de dispositivos

individuales que se encuentran en la mayoría de las unidades USB encriptadas de Kingston. Este acuerdo requiere que cada número de serie único de cada dispositivo se registre en la suite de administración de endpoint. Inicialmente, esto implicará la tramitación por parte del personal de IT, y Kingston puede proporcionar una lista de números de serie con cada pedido – estos siempre son alfanuméricos y no secuenciales. La elección de este método permite políticas mucho más flexibles basadas en la propiedad del dispositivo individual con la ventaja de un rastreo preciso de la procedencia de los dispositivos que puede ser invaluable en escenarios de IT forense. Algunos dispositivos Kingston incluyen un número de serie y un código de barras en la carcasa para el escaneo electrónico, y otros dispositivos se pueden personalizar para agregar un código de barras y un número de serie en la carcasa para empresas; estos elementos se pueden utilizar para el seguimiento de dispositivos.

De forma predeterminada, los sistemas de administración de punto final proporcionan acceso a VID/PID para el bloqueo de puertos y la creación de listas blancas. Lo que ofrece Kingston es una forma más versátil de aprovechar estas funciones para permitir políticas más flexibles e imaginativas que faciliten el uso de dispositivos de almacenamiento USB. Al establecer un método de identificación apropiado, una postura general de "Bloquear todos los puertos (Block All Ports) no solo es demasiado simplista, sino que se vuelve innecesaria.

Soluciones seguras y compatibles para usuarios remotos

Cuando se trata de seguridad, agregar los dispositivos de la lista blanca solo se ocupa de la mitad del problema, o para decirlo de otra manera, la mitad de la solución.

La conveniencia y simplicidad de las unidades de almacenamiento USB las hace indispensables en muchas empresas e instituciones donde la portabilidad es la clave para experimentar transferencias de datos sin fricciones. En la mayoría de los entornos, por razones de cumplimiento y una buena higiene de IT, es necesario equipar al personal con unidades USB encriptadas para tales tareas. Al utilizar una combinación de protección con contraseña y encriptado del dispositivo, el almacenamiento portátil cuenta con salvaguardas para evitar el acceso a datos confidenciales en caso de pérdida, robo o abandono de un dispositivo en una situación potencialmente vulnerable.

Esta no es una solución única para todo, ya que las técnicas de encriptado varían y las diferencias más significativas salen a la luz al comparar soluciones de encriptado por software y hardware. Entonces, ¿cuál es mejor? Depende de sus necesidades, pero una pregunta más diligente sería preguntar: "¿Cuál es más seguro?"

El encriptado por software es esencialmente una opción económica que satisfará a algunos sectores con operaciones a menor escala. También se adaptaría a las empresas cuyas transferencias de datos no se consideran sensibles y cuyas preocupaciones tienen más que ver con el cumplimiento de las políticas.

Sin embargo, el modus operandi del encriptado por software es también su talón de Aquiles, ya que requiere aplicaciones orientadas al cliente que dependen de una computadora para realizar las tareas de encriptado. Por lo tanto, por asociación, una unidad de almacenamiento encriptada por software es tan segura como la computadora huésped.

La exposición a las vulnerabilidades también aumenta ya que los piratas informáticos con acceso a la memoria de la computadora pueden "olfatear" las claves de cifrado/descifrado. Los datos en el dispositivo también pueden estar sujetos a ataques de fuerza bruta, ya que la protección de acceso con contraseña no es necesaria si se puede acceder y copiar los archivos encriptados.

Recuerde, es probable que el encriptado basado en software necesite actualizaciones de software de vez en cuando, lo que puede complicar la implementación al crear una carga adicional para el personal de IT. Lo peor de todo es que los empleados frustrados que tienen problemas con la portabilidad del dispositivo entre plataformas pueden eliminar por completo el encriptado por software. Los usuarios del dispositivo pueden copiar los datos del dispositivo encriptado a una computadora, formatear el dispositivo a un dispositivo no encriptado y luego volver a copiar los datos en el dispositivo. En este punto, los datos no estarían seguros y serían totalmente vulnerables a una filtración. Para fines de cumplimiento con las leyes y regulaciones de privacidad de datos, esto es inaceptable ya que la seguridad de la unidad USB se puede desactivar de manera efectiva.

Encriptado en chip: la solución dura y rápida

Por el contrario, una unidad USB encriptada por hardware funciona de forma independiente de la computadora, ya que cuenta con un procesador exclusivo integrado en el dispositivo que gestiona el encriptado. Tiene un proceso de encriptado siempre activo con protección contra ataques de contraseña por fuerza bruta; los datos encriptados no son accesibles y no se pueden copiar.

Las unidades USB encriptadas por hardware de grado militar y empresarial de Kingston utilizan encriptado AES de 256 bits en modo XTS. Una técnica de encriptado aprobada a nivel mundial, el AES de 256 bits proporciona protecciones de datos rigurosas. Al utilizar dos claves separadas en diferentes etapas del proceso de cifrado/descifrado, el modo XTS tiene un efecto similar al de encriptar los datos dos veces.

En uso, la clave del encriptado se deriva del generador de números aleatorios del controlador del dispositivo que se desbloquea con la contraseña del usuario. A medida que la autenticación se lleva a cabo dentro del hardware encriptado del dispositivo, 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.

Uno de los beneficios más inmediatos del encriptado por hardware es que el rendimiento del dispositivo es significativamente mejor que el de un dispositivo encriptado por software, ya que no hay que descargar las tareas de encriptación en la computadora huésped. Todo ocurre dentro del dispositivo.

Las unidades USB con encriptado por hardware, como el Kingston IronKey D500S, son dispositivos protegidos con contraseña que están encriptados desde su fabricación. En uso, solo el volumen de inicio protegido contra escritura es visible para empezar, ya que contiene la aplicación utilizada para autenticar la contraseña y desbloquear el volumen principal de almacenamiento encriptado. Este procedimiento evita la instalación de cualquier tipo de controlador o software en la PC huésped.

Además, las unidades USB encriptadas por hardware de Kingston cuentan con controladores de firmware firmados digitalmente que evitan cualquier manipulación del firmware dentro del dispositivo. Tener esta capa adicional de seguridad brinda protección contra ataques como BadUSB que explotan una vulnerabilidad inherente en el firmware del dispositivo USB. Esto puede dar lugar a que se ejecuten comandos de forma encubierta o código malicioso en el equipo huésped.

Por supuesto, un enfoque de "Bloquear todos los puertos" limitaría el riesgo delas amenazas de BadUSB, pero ¿por qué sacrificar la productividad con prácticas tan obsoletas? Como se destacó anteriormente, se puede mantener un entorno seguro junto con el uso de dispositivos de almacenamiento portátiles si se implementan procedimientos simples de adquisición e implementación al introducir unidades USB encriptadas por hardware.

Trabajo remoto seguro y complaciente

Para los trabajadores remotos, estar lejos de las protecciones del entorno laboral seguro de una organización exige una estrategia actualizada , así como una nueva mirada a las prioridades.

Cuando se trata de un plan de seguridad remota, ¿existe algún beneficio al bloquear los puertos USB en la computadora portátil de sus empleados solo para que se conecten a través de Internet para acceder a un servidor para cargar o recuperar documentos? Por el camino las conexiones de Internet abiertas, como puntos de acceso Wi-Fi inseguros o que no son de confianza, puede ser todo lo que se encuentre disponible y esto introduce una amplia variedad de peligros que aumentan enormemente la posibilidad de una infracción. Amenazas como la interceptación de datos y la

vigilancia mediante suplantación de identidad, los ataques Man-In-the-Middle (MitM) y la información clandestina de la red son solo algunos de los métodos de piratería cada vez más sofisticados disponibles para los ciberdelincuentes. Incluso las VPN se han visto comprometidas.

La conexión de red de una organización a Internet es solo otro punto final, y su exposición inherente la convierte en un punto de entrada extremadamente vulnerable y específico. Abrirlo al acceso remoto conlleva sus propios riesgos de seguridad, especialmente cuando se trata de datos confidenciales.

Confiar a los trabajadores remotos con unidades USB protegidas por contraseña y encriptadas por hardware elimina eficazmente las posibles vulnerabilidades de la red. Sin embargo, hacer tales cambios requiere un examen más detenido de los dispositivos USB disponibles y cómo estos satisfacen las demandas de cada entorno de trabajo remoto. No se trata simplemente de tomar una decisión sobre la capacidad del dispositivo, o si debe registrar su número de serie. Se trata de la construcción física del propio dispositivo.

Medidas de seguridad a prueba de manipulaciones: Las opciones sólidas

La mayor preocupación aquí es si una unidad USB encriptada por hardware es a prueba de manipulaciones o no. La seguridad de un dispositivo ante tal interferencia se refleja en estándares como FIPS 140-3, que tiene varios niveles que examinan la resistencia de la construcción física de un dispositivo sin utilizar métodos criptográficos.

La certificación FIPS-197 sólo observa los atributos del encriptado por hardware y dispositivos como las series IronKey Vault Privacy 50 y el SSD externo Vault Privacy 80, que son modelos orientados a la empresa en los que los requisitos de seguridad de los datos no son de nivel militar. Estas unidades son menos costosas pero carecen de protección contra la manipulación física de los dispositivos.

Con la certificación FIPS 140-3 Nivel 3 (pendiente), los métodos implementados para exponer la manipulación de dispositivos se clasifican como de grado militar. Kingston suministra estos dispositivos FIPS 140-3 Nivel 3 a empresas, gobiernos y al ejército en todo el mundo.

Utilizando epoxi internamente para recubrir todos los circuitos de accionamiento necesarios para la seguridad y pegando los componentes internos a la carcasa se crea otro muro de defensa. Cualquier intento de abrir la carcasa de metal será extremadamente difícil y hace que los chips internos y otros componentes se rompan y que eventualmente la unidad deje de funcionar. Con este epoxi duro y opaco en su lugar, la manipulación de componentes vitales se convierte en una tarea casi imposible. Dispositivos como el Kingston IronKey D500S y S1000 contienen esta medida de seguridad adicional.

Estas protecciones para los dispositivos no se limitan a medidas físicas únicamente, y el Kingston IronKey S100 lleva la protección contra manipulaciones a otro nivel. El criptochip interno del IronKey S1000 puede detectar cualquier tipo de manipulación física y dejará la unidad inutilizable tan pronto como se encienda el dispositivo. Confiar en dispositivos de almacenamiento USB encriptados por hardware para acceder y transferir archivos confidenciales es un movimiento pragmático que facilita las operaciones remotas sin problemas y garantiza de manera efectiva la seguridad.

Asegúrese de investigar el hardware de los dispositivos USB y las funciones de seguridad para ver si está a la altura de sus necesidades específicas y su caso de uso. Cada dispositivo USB debe revisarse caso por caso con acreditaciones confiables que ayuden a guiar estas decisiones. Independientemente de las prioridades, Kingston ofrece una gama de soluciones de unidades USB encriptadas por hardware y opciones de personalización a precios asequibles que abordan todo tipo de entornos: desde el cumplimiento general hasta las especificaciones militares más estrictas.

Seguridad primero: Sin redes, sin problemas

Hoy en día, la oficina no tiene fronteras y, a medida que el trabajo desde casa continúa floreciendo, ha puesto en relieve los problemas de vulnerabilidad del acceso remoto para muchas empresas. Muchos están experimentando estos desafíos por primera vez y buscan formas más seguras de adaptarse a esta tendencia que va en aumento.

Para satisfacer estas necesidades en una amplia gama de industrias, los dispositivos de almacenamiento USB encriptados por hardware ya están bien consolidados y brindan una solución segura en donde la transferencia de datos a través de redes puede ser poco práctica o indeseable por varias razones.

En finanzas, los reguladores solicitan con frecuencia datos para verificar la conducta y el cumplimiento de una empresa. El riesgo de exposición es demasiado grande para contemplar el uso de una red para transferir documentos confidenciales que contienen detalles precisos de inversiones, mercado de operaciones y otras actividades bancarias confidenciales. La solución simple y efectiva es entregar esta información en una unidad USB encriptada por hardware.

El uso de unidades USB seguras para transferir archivos en áreas de la salud es algo cotidiano. Esto también es para la conveniencia de los médicos o consultores que deseen analizar archivos, consultarlos para investigación o presentar ejemplos de casos a estudiantes de medicina. También hay necesidades más prácticas cuando se trata de sistemas patentados, como dispositivos de imágenes médicas, donde el acceso a la red está ausente o es inseguro. Al utilizar unidades USB encriptadas por hardware compatibles, los archivos se pueden transferir fácilmente para su uso en otro lugar.

Qué hacer y qué no hacer

✓ **Utilice dispositivos seguros y compatibles** y revise las especificaciones para adquirir dispositivos que se adapten a las necesidades de cada implementación.

✗ **No autorice una política aleatoria o de "Traiga su propio dispositivo" (BYOD) persona** – para cualquier empresa, perder dispositivos no encriptados es un precio demasiado alto en términos de daños económicos y de reputación.

✓ **Implemente una suite de administración de punto final** y use unidades USB encriptadas por hardware que ofrecen características distintivas de listas blancas.

✗ **No deje nada al azar.** Evalúe adecuadamente los requisitos para entornos de trabajo locales y remotos.

✓ **Eduque al persona** sobre cuestiones de seguridad. Es de su propio interés que la empresa permanezca protegida contra las violaciones de seguridad.

✗ **No haga que la seguridad sea tan desagradable** que los usuarios busquen maneras que puedan llevar a al uso de soluciones dudosas de IT. El hecho de que siempre se haya aplicado una política general no significa que se adapte a todos los escenarios. El lugar de trabajo está cambiando y, eligiendo las soluciones adecuadas, se pueden desarrollar y aplicar nuevas políticas.

En este caso, el Kingston IronKey Keypad 200 (KP200) es la solución ideal. Como una unidad independiente del sistema operativo, no hay un volumen de inicio para ingresar la contraseña, sino que cuenta con un teclado alfanumérico que desbloquea el dispositivo para su uso en cualquier plataforma. Como una navaja suiza de dispositivos USB encriptados por hardware, su uso se extiende a la manufactura; transferir de forma segura aplicaciones creadas en el mundo de la investigación y el desarrollo de IT a maquinaria controlada por plataformas de tecnología operativa (OT). Para operaciones de plataforma mixta que también cuentan con Linux, el KP200 es una de las soluciones seguras disponibles más sencillas.

Las unidades de almacenamiento USB encriptadas por hardware también tienen un papel vital a desempeñar en la aplicación de la ley. Protegen y transfieren de forma segura archivos de casos, imágenes y otras pruebas a agentes de campo, equipos de investigación y equipos forenses. Kingston ofrece un beneficio adicional, ya que puede proporcionar dispositivos con el número de serie interno impreso en la carcasa externa junto con un código de barras. La emisión y catalogación de unidades se vuelve simple y fácil de rastrear. Es tan fácil como registrar manualmente un número de serie o tan rápido como escanear un código de barras, la auditoría y la administración del inventario no podrían ser más fáciles. Es una función estándar en los dispositivos Kingston IronKey D300S, D300SM y S1000B/E, pero también está disponible para otros modelos encriptados por hardware como parte del programa de personalización de Kingston.

Movilidad de almacenamiento y seguridad: A la vanguardia

La protección por contraseña, el encriptado por hardware, las protecciones a prueba de manipulaciones, las listas blancas granulares de puntos finales, la certificación FIPS 140-3 nivel 3 de grado militar (pendiente), y el registro a simple vista son características estándar de las unidades USB de Kingston que se pueden implementar sin demora.

Estas sólidas defensas de seguridad garantizan que la unidad USB y sus datos permanezcan seguros en su entorno huésped. Si bien las especificaciones son impresionantes en papel, elegir un modelo al azar sin ninguna investigación no proporcionará necesariamente un emparejamiento ideal para algunas organizaciones con requisitos más exigentes.

Como fabricante independiente, Kingston ofrece una amplia gama de opciones para satisfacer las necesidades del cliente. A través del programa de personalización de Kingston, se encuentran disponibles soluciones avanzadas que están diseñadas para brindar una experiencia de usuario perfecta.

La personalización segura va más allá de proporcionar a una organización su propio PID USB para la lista blanca. El perfil de seguridad de la aplicación de inicio también se puede personalizar utilizando quince preferencias diferentes, desde los datos de contacto y de la empresa, hasta habilitar pistas de contraseña y determinar el número máximo de intentos de contraseña. Externamente, la marca de la empresa (co-logo) está disponible, así como una gama de colores para dispositivos específicos. Con un pedido mínimo de cincuenta unidades, todas estas funciones proporcionan una ruta de integración sin esfuerzo para la implementación de los dispositivos.

Si aún no se dispone de una aplicación de gestión de puntos finales adecuada para el almacenamiento USB seguro, existe una solución de administración disponible para las organizaciones que deseen gestionar su flota de unidades Kingston, que incluye opciones para restablecer las contraseñas de forma remota.

La ubicuidad y la conveniencia del USB han hecho que sobreviva a una variedad de tecnologías prometedoras y, para muchas tareas, la inmediatez y conveniencia del almacenamiento USB perdura. Los dispositivos USB protegidos, siempre seguros y fácilmente disponibles ofrecen una solución simple que se puede apreciar fácilmente.

¿Por qué preocuparse por las filtraciones de datos en la red en entornos remotos? Con las unidades USB de almacenamiento encriptadas por hardware de Kingston, la respuesta está en la palma de su mano.

Para obtener más información sobre cómo Kingston puede ayudarlo visite kingston.com/ironkey o si tiene preguntas más específicas, consulte a uno de nuestros Expertos en encriptado USB.

#KingstonIsWithYou #KingstonIronkey