Informe Técnico sobre DeviceLock

Contenido:

¿Por qué DeviceLock?

El control de lo que está siendo cargado o descargado de una red informática empresarial es fundamental para la seguridad IT. Al mismo tiempo, el trabajo se complica cada día más. La popularidad de dispositivos portátiles de almacenamiento USB crece rápidamente y es obviamente una amenaza. Este mercado está creciendo exponencialmente[1], con dispositivos que son cada vez más rápidos, con mayor capacidad y menor tamaño. Además, considere que los dispositivos Bluetooth, para promocionar su facilidad de uso, están diseñados para comunicarse con cualquier cliente Bluetooth dentro de su zona de cobertura; y éstas pueden ser sorpresivamente amplias. Asimismo, hay un mercado demandando mejores accesos de red para dispositivos wireless (inalámbricos), y esta demanda probablemente desestima cualquier objeción relativa a la seguridad.

En el corto plazo, las fuerzas en juego del mercado están ganando a los intereses de seguridad. Esto no significa que las corporaciones no sean conscientes de la creciente vulnerabilidad. Hay casos de personas maliciosas dentro o fuera de la corporación descargando y extrayendo información sensible para propósitos que van desde el espionaje industrial a la extorsión, desde el terrorismo a recibir atención frecuente por parte de la prensa. Por otro lado, las corporaciones sí están haciendo cosas con relación a la seguridad. Las inversiones en firewalls, codificación y otras tecnologías y controles diseñados para proteger de robos los datos de red a través de Internet están ciertamente en crecimiento. Sin embargo, estas medidas ofrecen poca protección para dispositivos y puertos no asegurados a nivel local. No podrían detener a un empleado espía que trajera una unidad USB de 2GB al trabajo, la conectara al puerto USB, y comenzara a descargar datos importantes. Tampoco puede impedir que el empleado descontento use un dispositivo similar para cargar un Troyano u otro programa maligno en la red. Para evitar estos problemas, es necesario que los administradores tengan control sobre quiénes tienen acceso a unidades de medios externos y en el momento que tienen esos accesos.

DeviceLock pertenece a DeviceLock, Inc. provee este nivel de control sobre redes basadas en Microsoft Windows. Es una solución basada en software que permite a los administradores de redes la asignación de permisos para puertos FireWire y USB, adaptadores Bluetooth y WiFi, así como para unidades de disco flexible, unidades CD-ROM, dispositivos de cinta y otros medios extraíbles. Soluciona los problemas de seguridad a nivel físico sin dispositivos de bloqueo reales.

[1] De acuerdo a un estudio de Semico Research Corp, "Will USB Flash Drives Change Our Lives? (las unidad de Almacenamiento USB, ¿Cambiarán nuestras vidas? " se espera que crezca desde los 10 millones de unidades de Almacenamiento USB vendidas en el 2002, a cerca de 50 millones en el 2006.

NetworkLock, una extensión para DeviceLock, permite controlar las comunicaciones de red. Los administradores pueden establecer el acceso de usuarios para los protocolos FTP, HTTP, SMTP y Telnet, programas de mensajería instantánea (ICQ/AOL Instant Messenger, Windows Live Messenger and Windows Messenger, Jabber, IRC, Yahoo! Messenger y Mail.ru Agent), aplicaciones de redes sociales y webmail (Gmail, Hotmail, Yahoo! Mail, mail.ru, web.de, gmx.de; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte y Twitter).

ContentLock, otra extensión para DeviceLock, extrae y filtra el contenido de los datos copiados sobre unidades extraíbles y dispositivos de almacenamiento Plug-n-Play, así como los transmitidos a través de la red. Los administradores pueden crear reglas para especificar qué contenido se debe copiar y transmitir.

¿Qué es tan especial en DeviceLock?

Mediante la provisión de control sobre la red para qué usuarios pueden acceder a puertos y dispositivos sobre una computadora local, DeviceLock cierra un hueco de seguridad potencialmente enorme de una manera simple y económica. Por lo que esto es un gran adelanto sobre no hacer nada. Si comparamos con las soluciones físicas que requieren el almacenamiento y administración de bloqueos de hardware y llaves, éste es mucho más barato y fácil de implementar en una corporación. Comparado con otros procedimientos implementados por el administrador, basados solamente en software para controlar hardware local (tales como cambiar el BIOS) DeviceLock es una solución más elegante, más fácil de escalar.

DeviceLock posee una interfaz de usuario fácil de usar con un sencillo asistente de configuración y múltiples vistas gráficas de la información. Los administradores de red pueden incluso configurar y mantener remotamente el servicio DeviceLock en las estaciones de trabajo. Diseñado para funcionar en Windows NT/2000/XP/Vista/7 y Windows Server 2003/2008, también incluye soporte automatizado para su instalación y desinstalación.

DeviceLock también puede administrarse e implementarse a través de Política de grupos dentro de un dominio de Active Directory. La política de grupos usa servicios de directorio y seguridad de participación de grupos para proporcionar flexibilidad y admitir amplia información de configuración. La configuración de política se crea mediante el módulo Microsoft Management Console (MMC) para política de grupos. Mayor integración en Active Directory supone que la administración y distribución de permisos de DeviceLock resulten más sencillas para redes de gran tamaño y más cómodas para los administradores de sistemas. La integración dentro de Active Directory elimina la necesidad de instalar más aplicaciones de terceros para administración y distribución centralizadas. DeviceLock no necesita tener su propia versión basada en servidor para controlar la red entera, en su lugar usa funciones estándar proporcionadas por Active Directory.

Para soluciones de cifrado estandarizadas vía hardware o software de grandes empresas, como PGP Whole Disk Encryption, TrueCrypt, Windows BitLocker To Go, DriveCrypt y unidades USB Lexar JumpDrive SAFE S3000 y SAFE PSD S1100, DeviceLock permite a los administradores la definición y el control centralizado remoto de las directivas de cifrado, que deben seguir sus empleados al utilizar dispositivos extraíbles para el almacenamiento y recuperación de datos corporativos. Por ejemplo, ciertos empleados o sus grupos pueden tener permitido escribir y leer sólo de unidades flash USB cifradas específicamente, mientras que otros usuarios de redes corporativas pueden tener permiso de “sólo lectura” de dispositivos de almacenamiento extraíbles no cifrados, pero no para escribir en ellos.

Además de proteger los equipos locales y de la red frente a daños en la misma y robo de datos, DeviceLock permite obtener un completo registro de actividad de red, dispositivos y puertos.

La capacidad de emulación de datos opcional de DeviceLock mejora significativamente las funciones del auditor IT corporativo para asegurar que la información sensible no sale de las instalaciones. Captura copias completas de los archivos que se copian a dispositivos extraíbles autorizados, PDA Windows Mobile y Smartphones, que se graban en CD/DVD, se transmiten a

través de la red y se imprimen por usuarios finales autorizados. Las copias de emulación se almacenan en un componente centralizado de un servidor, y en cualquier infraestructura SQL compatible con ODBC preferida por el cliente.

DeviceLock Search Server proporciona la búsqueda de texto completo de datos registrados guardados en DeviceLock Enterprise Server. La funcionalidad de búsqueda con texto completo es especialmente útil en situaciones donde el auditor IT corporativo debe buscar copias de emulación para documentos en función de su contenido. DeviceLock Search Server puede reconocer, indexar, buscar y mostrar automáticamente documentos en muchos formatos, como: Adobe Acrobat (PDF), Ami Pro, Archives (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documentos, hojas de cálculo y presentaciones), Quattro Pro, WordPerfect, WordStar y muchos otros.

¿Quién necesita DeviceLock?

El crecimiento rápido de la base de clientes de DeviceLock incluye a corporaciones que son auditadas por el manejo seguro de datos de sus clientes y corporativos, agencias gubernamentales que manejan información sensible, y empresas de servicios profesionales y otros negocios pequeños y medianos que necesiten controlar el acceso a los dispositivos.

Los siguientes son algunos ejemplos de uso de DeviceLock:

- Controlar qué usuarios o grupos pueden tener acceso a puertos USB, FireWire, infrarrojos, COM y LPT; adaptadores WiFi y Bluetooth; el portapapeles de Windows; cualquier tipo de impresora, incluyendo impresoras virtuales, de red y locales; Windows Mobile, BlackBerry, iPhone, iPod Touch, iPad, y PDA Palm y Smartphones; así como unidades de disco flexible, DVD/CD-ROM y otros dispositivos Plug-and-Play y extraíbles.

- Controlar aquellos usuarios o grupos que tienen acceso a aplicaciones y protocolos de red (FTP, HTTP, SMTP, Telnet, Mensajería instantánea, servicios Webmail y Redes sociales).

- Conceder o denegar el acceso de forma selectiva a información en función de tipos de fichero reales, patrones de expresiones regulares con combinaciones booleanas y condiciones numéricas de criterios de coincidencia y palabras clave.

- Controlar el acceso de forma separada a imágenes que contienen texto (por ejemplo, documentos escaneados, capturas de pantalla de documentos) e imágenes que no contienen texto.

- Controlar el acceso a los dispositivos y protocolos en función de la hora del día y el día de la semana.

- Definir qué tipos de datos (archivos, calendarios, correos electrónicos, tareas, notas, etc.) se pueden sincronizar entre equipos corporativos y dispositivos móviles personales.

- Definir distintas directivas de seguridad online y offline para el mismo usuario o grupos de usuarios.

- Detectar discos PGP, DriveCrypt y TrueCrypt cifrados (unidades flash USB y otros medios extraíbles), unidades flash cifradas Lexar SAFE PSD y Lexar JumpDrive SAFE S3000, así como unidades cifradas BitLocker To Go, y aplicar permisos especiales "cifrados" a las mismas.

- Autorizar tan sólo aquellos dispositivos USB específicos que no se van a bloquear a pesar de cualquier otra configuración.

- Permitir el acceso temporal de usuarios a dispositivos USB cuando no existe conexión de red (los usuarios disponen de los códigos de acceso especiales a través del teléfono que permiten desbloquear temporalmente los dispositivos solicitados y tener acceso).

- Identificar de forma única un disco DVD/CD-ROM por la firma de datos y el acceso autorizado a su contenido, a pesar de que DeviceLock pueda haber bloqueado la unidad DVD/CD-ROM.

- Proteger ante usuarios con privilegios de administrador local para permitirles activar DeviceLock Service o quitarlo de sus equipos, si no se encuentran en la lista de administradores de DeviceLock.

- Búsqueda de texto sobre registros de auditoría y archivos de emulación guardados en la base de datos centralizada.

- Configurar los dispositivos para modo de sólo lectura.

- Proteger los discos del formateo accidental o intencionado.

- Detectar y bloquear keyloggers de hardware (USB y PS/2).

- Distribuir permisos y configuraciones a través de Directivas de grupo en un dominio Active Directory.

- Utilizar el complemento RSoP estándar de Windows para visualizar la directiva DeviceLock vigente en ese momento, así como predecir qué directiva sería aplicada en una determinada situación.

- Controlar todo de forma remota utilizando la consola de administración centralizada.

- Obtener un registro completo de actividad de red, dispositivos y puertos, incluyendo cargas y descargas por nombres de fichero y usuarios en el Registro de eventos de Windows estándar.

- Reflejar todos los datos (emulación) copiados a dispositivos de almacenamiento externos (extraíbles, discos flexibles y DVD/CD-ROM) iPhone, iPod, iPad o PDA Palm OS y Smartphones, transferidos a través de puertos COM y LPT, e incluso impresos.

- Guardar los datos de emulación en un componente centralizado de un servidor existente y cualquier infraestructura SQL compatible con ODBC.

- Monitorizar equipos remotos en tiempo real, verificar el estado de DeviceLock Service (en ejecución o no), su integridad y la consistencia de directivas.

- Generar un informe con los permisos y ajustes establecidos.

- Crear informes gráficos basados en los registros (auditoría y emulación) guardados en el servidor.

- Generar un informe con los dispositivos PCMCIA, FireWire y USB conectados actualmente a los equipos, y aquellos que estuvieron conectados.

- Crear un paquete MSI personalizado para DeviceLock Service con directivas predefinidas.

¿Cómo funciona DeviceLock?

DeviceLock funciona en cualquier equipo que utilice Windows NT 4.0/2000/XP/Vista/7 o Windows Server 2003/2008. Es compatible con plataformas de 32-bit y 64-bit.

DeviceLock consta de tres partes: el agente, el servidor y la consola de administración:

1. DeviceLock Service (el agente) es el núcleo de DeviceLock. DeviceLock Service se instala en cada cliente, se ejecuta automáticamente, y proporciona protección de dispositivos y de redes en el equipo cliente mientras permanece invisible para los usuarios locales del equipo.

2. DeviceLock Enterprise Server es el componente opcional para recopilación y almacenamiento centralizados de datos de emulación y registros de auditoría. DeviceLock Enterprise Server utiliza MS SQL Server para guardar sus datos.

   DeviceLock Content Security Server también es el componente opcional que incluye DeviceLock Search Server para búsqueda instantánea de texto sobre archivos de emulación y otros logs guardados en DeviceLock Enterprise Server.

3. La consola de administración es la interfaz de control utilizada por los administradores del sistema para administrar de forma remota cada sistema que cuenta con DeviceLock Service. DeviceLock incluye tres consolas de administración distintas: La Consola de administración de DeviceLock (el complemento MMC), DeviceLock Enterprise Manager y DeviceLock Group Policy Manager (integrada en Windows Group Policy Editor).

¿Quién ha desarrollado DeviceLock?

DeviceLock ha sido desarrollado por DeviceLock, Inc. Desde sus comienzos en 1996, DeviceLock, Inc. (anteriormente SmartLine Inc) ha estado suministrando soluciones de seguridad en la información y administración de redes a organizaciones que confían en la tecnología de Microsoft Windows. La experiencia probada de DeviceLock con las tecnologías de control de acceso ayuda a los clientes a mejorar la seguridad, productividad y disponibilidad de los sistemas. Los profesionales IT eligen soluciones de DeviceLock, Inc. para administrar, auditar y proteger estos sistemas críticos. Nuestros clientes incluyen a BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, y varias agencias y departamentos gubernamentales estatales y federales. DeviceLock, Inc. es una organización internacional con oficinas en San Ramon (California), Londres (Reino Unido), Ratingen (Alemania), Moscú (Rusia) y Milán (Italia).

¿Dónde puede obtener el software DeviceLock?

Está disponible una versión de demostración completa y gratuita descargándola desde:

www.devicelock.com/es/dl/download.html

Soporte técnico de DeviceLock

El soporte técnico para clientes de DeviceLock está disponible enviando un correo electrónico (e-mail) a support@devicelock.com. Dispone de un sitio web que también ofrece gran cantidad de información de ayuda incluyendo problemas conocidos y preguntas frecuentes:

www.devicelock.com/es/support.html

También puede dirigirse a nuestro equipo de soporte técnico en: +1-925-231-0042. El horario de ayuda telefónica es de lunes a viernes, de 8 a.m. a 5 p.m. hora del pacífico.

Precio de DeviceLock

DeviceLock cuesta € 40 (Euros) para una licencia básica de usuario. Hay descuentos disponibles para licencias de usuarios múltiples y para Instituciones Educativas. Para los precios de licencias de usuarios múltiples, consulte: www.devicelock.com/es/dl/register.html

Si desea utilizar las capacidades de NetworkLock y ContentLock, debe adquirir licencias de NetworkLock y ContentLock además de las licencias básicas de DeviceLock.

Procedimientos para comprar y registrarse

Hay varios métodos disponibles para pedir o registrar DeviceLock:

En el sitio web seguro (con tarjeta de crédito)
Por teléfono (con tarjeta de crédito)
Por Fax (con tarjeta de crédito)
Por correo (con cheque)
Por pedidos

Para más información sobre cómo hacer un pedido, consulte:
www.devicelock.com/es/dl/register.html

Información de contacto

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany
TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy
TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK
TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA
TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

Sales@devicelock.com
Support@devicelock.com

www.devicelock.com/es

