MaaS360®
by Fiberlink, an IBM company

Seguridad de datos móviles

En busca del equilibrio

Seguridad de datos móviles: En busca del equilibrio

Tabla de contenidos

MaaS360®
by Fiberlink, an IBM company

Equilibre la tolerancia de riesgos relacionados con la protección de los datos confidenciales de su empresa con el ofrecimiento de una experiencia de usuario productiva y sencilla.

Seguridad de datos móviles: En busca del equilibrio

Los términos *Prevención de fuga de datos (DLP)* y *Contenedor* empiezan a predominar en las conversaciones sobre administración de dispositivos móviles. En los últimos años se han realizado grandes avances en cuanto a las herramientas y las soluciones que ofrecen funciones de administración y seguridad para los dispositivos móviles, tanto para los corporativos como para los personales.

Aunque estas soluciones satisfacen la necesidad de proteger el dispositivo, tienen deficiencias en los aspectos de seguridad más sofisticados, comunes en los ordenadores portátiles y las implementaciones de redes distribuidas. En concreto, carecen de los controles integrales de DLP, habituales en las soluciones de administración de los ordenadores portátiles.

La prudencia aboga por buscar formas de complementar su solución de administración de dispositivos móviles (MDM) con controles de seguridad adicionales más sólidos para ayudar a proteger y asegurar los datos sensibles y que no se distribuyan a terceras personas sin autorización, ya sea de forma involuntaria o malintencionada.

Sepa cuáles son sus objetivos

A medida que investigue en el ámbito tecnológico, descubrirá que hay enfoques diferentes. Estos enfoques tienen distintos pros y contras; sin embargo, lo primero es saber cuáles son sus objetivos. Tiene que equilibrar la tolerancia de riesgos relacionados con la protección de los datos confidenciales de su empresa con el ofrecimiento de una experiencia de usuario productiva y sencilla mientras desarrolla sus objetivos y define un perfil de enfoque. Asegúrese de tener en cuenta lo siguiente:

Detener a las amenazas dentro de la propia empresa: Una política de código de acceso y el cifrado de los dispositivos no detendrá a un usuario no autorizado en su intento de copiar datos. El control de lo anterior entra dentro del ámbito del DLP. Puede que su organización ya haya realizado considerables inversiones para controlar el movimiento de los datos confidenciales que se escapan a su alcance y sus perímetros de software de los ordenadores portátiles y de sobremesa. En ese caso, busque capacidades que amplíen el DLP hasta sus dispositivos móviles implantados. Su política y sus objetivos deben ser coherentes con todos los tipos de dispositivos de la organización.

Detener a las amenazas procedentes de fuera de la empresa: La comunidad de proveedores de MDM ha hecho una gran labor ofreciendo herramientas que protegen los datos de los dispositivos móviles. Con aplicar códigos de acceso y el cifrado, y siendo capaz de borrar el contenido del dispositivo, tiene el 90 % de la batalla ganado. Sin embargo, sigue habiendo dificultades considerables para ser capaces de aplicar y verificar estos controles de forma constante y fiable, especialmente en las muchas variantes de la plataforma Android. Esta fragmentación añade la dimensión de la diversidad de dispositivos cuando no todos ellos pueden protegerse de forma razonable.

Soporte del programa de dispositivos personales amplio y flexible: La diversidad de los dispositivos es un factor importantísimo de su enfoque y su estrategia. Después de todo, que los empleados aporten sus dispositivos personales (BYOD) no es sinónimo de traer aquellos que el departamento informático autoriza, lo que que acabaría con el espíritu del programa. Aunque contar con un programa y un proceso de certificación de dispositivos puede proporcionar cierta estructura, un programa de dispositivos personales BYOD completamente abierto precisará ayuda en el frente tecnológico para mantener un nivel mínimo de seguridad de los datos.

La persona dual es la administración de dos entornos de usuario independientes para separar las experiencias y los datos laborales de los personales en un dispositivo móvil.

Persona dual: Es en este punto donde el debate se desvía de la seguridad y entra en la funcionalidad y el deseo de dar cabida a un programa flexible de dispositivos personales. Para muchas organizaciones, no hay políticas, ni necesidad de contar con ellas, para tener unos controles de DLP sólidos. Simplemente quieren aislar los datos personales del usuario sin dejar de controlar los datos corporativos. Si piensa un poco en sus objetivos, puede que llegue a la conclusión de que la solución de persona dual es la adecuada para su organización. Básicamente, el sistema de persona dual consiste en la administración de dos entornos de usuario independientes para separar las experiencias y los datos laborales de los personales en un dispositivo móvil.

Otros factores: Como en todo, las soluciones tienen un precio. Básicamente tiene que plantearse cómo la escalará, de qué forma hará que sea resistente y cuánto le costará. Debe tener en cuenta la experiencia del usuario y asegurarse de que implementa algo que los usuarios aceptarán y adoptarán. Ahora vive en democracia, no en la autocracia informática de antaño.

Elija el enfoque

Ahora que ya ha cuantificado sus objetivos, sopesemos los enfoques disponibles.

Contenedor: El término "contenedor" parece ser el más utilizado para describir las soluciones que ofrecen una aplicación de trabajo y una zona de datos independientes. El término "aislamiento de procesos" también se utiliza frecuentemente. Puede que también escuche "persona dual", término que se usa para describir este tipo de solución. No obstante, persona dual debe considerarse como objetivo en lugar de solución (es decir, implementar una solución de contenedor para llegar a la persona dual).

Considere este enfoque como una zona completamente separada y "aislada", donde se desarrollan ciertas actividades y donde el movimiento de los datos se limita a la zona de aislamiento de procesos. Como toda la actividad laboral se realiza en esta zona aislada, el usuario no puede usar el cliente de correo electrónico nativo. En lugar de ello, tendrá que usar la funcionalidad de correo electrónico, el calendario y los contactos que proporciona el software que hay dentro del contenedor. Esto puede ocasionar cierta insatisfacción del usuario, aunque si está correctamente implementado, puede proporcionar una experiencia de usuario impecable. Es importante ayudar a su base de usuarios a comprender la importancia que ofrece la solución para que la organización logre sus objetivos de seguridad de los datos.

Vaciado: Se trata de una solución que intercepta el flujo de correo electrónico, separa el contenido relevante (como los documentos adjuntos, el texto, etc.) y hace que esté disponible para su visualización o manipulación en una aplicación independiente donde se pueda controlar el flujo de datos. En el caso del correo electrónico, el usuario interactúa con el cliente nativo hasta que haya algo a lo que tengan que acceder y que se haya eliminado (separado) del flujo de correo electrónico. El contenido eliminado se puede almacenar en el servidor que realizó el "vaciado" o en el terminal móvil modificado para abrirlo solamente en una aplicación segura.

MaaS360®
by Fiberlink, an IBM company

Si su organización se centra en impedir que un usuario no autorizado propague datos confidenciales desde un dispositivo móvil, tanto las soluciones de contenedor, como de virtualización o separación de los documentos adjuntos del correo electrónico podrían resultar bastante eficaces.

Gracias a una solución de vaciado, la experiencia del usuario se puede desarticular. El usuario recibiría un mensaje de correo electrónico sin texto ni documentos adjuntos (muchas soluciones no separan el texto por este motivo) y sería necesario iniciar otra aplicación para acceder de forma segura al texto y a los documentos adjuntos.

Virtualización: Concretamente, a lo que nos referimos aquí es a la tecnología en la que una parte del software, denominada "hipervisor", implementa una "máquina virtual" en el software del dispositivo móvil (no en un servidor remoto). En este tipo de soluciones, el dispositivo virtual estaría totalmente bajo el control y la administración de la empresa. Todas las aplicaciones y los datos corporativos residirían en la máquina virtual del dispositivo móvil; por lo tanto, el movimiento de datos entre el dispositivo virtual y el físico estaría muy controlado. Básicamente esto es lo mismo que la Infraestructura de escritorio virtual (VDI) para PC y portátiles y, además, viene con muchas de las mismas dificultades de implementación y administración.

La tecnología alberga ciertas esperanzas, dado que todas las funciones del hardware y el software del dispositivo tienen la posibilidad de virtualizarse y controlarse, hasta la conectividad de red y las funciones del hardware. Por ejemplo, la tarjeta SIM puede virtualizarse y modificarse virtualmente cuando cambia de red (los operadores de telefonía odiarán esta capacidad). En realidad, hasta que los dispositivos móviles no admitan la virtualización del hardware, de forma similar a como lo hace Intel VT y AMD-V en PC, la adopción masiva está todavía muy lejos, especialmente en el caso de iOS.

Nada de lo anterior: Cuando haya pasado el tiempo, puede ser este el punto en el que acaben muchas empresas. Si no se dedica a los servicios sanitarios o financieros, no tiene requisitos normativos como PCI o HIPAA, o ha determinado sus necesidades específicas de seguridad móvil e implementado una estrategia de administración de dispositivos y aplicaciones sensible, el coste adicional y la complejidad para sus usuarios y su equipo informático podría no estar justificados.

Realice la selección en función de las prioridades

Ahora esquematicemos todo en función de sus prioridades.

Prioridad: Amenaza del personal de la propia empresa – Si su organización se centra en impedir que un usuario no autorizado propague datos confidenciales desde un dispositivo móvil, tanto las soluciones de contenedor, como de virtualización o separación de los documentos adjuntos del correo electrónico podrían resultar bastante eficaces. Todas ellas pueden proteger el texto y los documentos adjuntos y, sin embargo, ofrecer experiencias fundamentalmente diferentes en el proceso, como se indica anteriormente. (En el caso del vaciado, seleccione cuidadosamente un producto que ofrezca la separación tanto de texto como de documentos adjuntos). Si no hay flexibilidad ni tolerancia ante la fuga de datos desde el correo electrónico, la solución de contenedor cuenta con ciertas ventajas, ya que proporciona una mejor experiencia de usuario y, además, es un poco menos compleja de configurar y administrar. En teoría, la virtualización sería una opción viable para abordar la amenaza que representa el propio personal de la empresa, pero tiene dificultades de implementación y administración.

Prioridad: Amenaza de otras personas ajenas a la empresa – La amenaza que suponen las personas ajenas queda bastante bien cubierta si adopta un enfoque responsable en cuanto a los dispositivos que permite conectar al sistema de correo electrónico. Si emplea la solución MDM (porque tiene una, ¿verdad?) para restringir las conexiones a los dispositivos de confianza compatibles con una política de código de acceso y con el cifrado y cuyo contenido se puede borrar de forma remota; de esta forma, los datos que se pueden fugar y los daños relacionados causados por un dispositivo robado o perdido son mínimos, por no decir nulos. Puede ahorrarse el coste adicional y la complejidad de las soluciones DLP si su prioridad es la amenaza de las personas ajenas. Tapar el hueco de la fuga de datos móviles solo es eficaz si también tiene los demás huecos cubiertos.

Una solución de contenedor que ofrece una zona segura para que residan los datos corporativos dentro de un dispositivo inseguro es una alternativa a tener que actualizar dispositivos sin certificar o no aptos que los usuarios aportan al programa.

Prioridad: Soporte del programa de dispositivos personales BYOD – Un paso prudente al implementar un programa de dispositivos personales BYOD es contar con un proceso de certificación de dispositivos y crear una lista de dispositivos admitidos que pueda ofrecer un nivel de seguridad básico. Si ya ha aplicado uno, se dará cuenta de inmediato de que hay una gran divergencia en el nivel de soporte para las funciones de seguridad esenciales entre las diferentes variantes de Android. En una situación ideal, que los empleados traigan sus dispositivos personales significaría exactamente lo anterior, además de adaptar una amplia variedad de dispositivos.

Una solución de contenedor, que ofrece una zona segura para que residan los datos corporativos dentro de un dispositivo inseguro, es una alternativa a tener que actualizar dispositivos sin certificar o no aptos que los usuarios aportan al programa. Las soluciones de vaciado pueden ofrecer una ventaja parecida, siempre que admitan la separación y la protección del texto y los documentos adjuntos del correo electrónico y estén configurados para tal fin. La virtualización no ayudaría a dar soporte a un amplio perfil de dispositivos personales dada la cantidad limitada de dispositivos que pueden permitir la ejecución de un hipervisor.

Prioridad: Persona dual – Otro motivo atractivo para implementar una solución de contenedor o vaciado de documentos adjuntos no está meramente relacionado con la seguridad. A medida que proliferan los dispositivos particulares en la empresa, se hace inevitable la mezcla de datos corporativos y personales, independientemente de los esfuerzos por impedirlo. Otro motivo clave es pasar a un enfoque más amable y discreto al manejar datos corporativos en estos dispositivos.

En lugar de limitarse a informar a los usuarios de que el contenido de sus dispositivos se borrará por completo en caso de que les roben el terminal o lo pierdan, o bien dejen de trabajar en la empresa, puede darles la opción de usar una solución de contenedor o vaciado. De este modo, tienen la posibilidad de borrar solamente los datos corporativos de forma confidencial y sin afectar a los datos personales que el usuario pueda haber almacenado en el dispositivo. La opción del contenedor logra este objetivo de forma más eficaz y, en un entorno de incentivos y amenazas, puede tratarse del mejor incentivo de entre los que elegir. Los usuarios se vuelcan en su personaje "laboral" y están satisfechos de saber que el equipo informático no se inmiscuirá en su contenido personal.

El enfoque de vaciado tampoco es apto para lograr el objetivo de la persona dual porque no hay una separación clara entre los datos personales y los corporativos, dado que el cliente de correo electrónico nativo sigue usándose para actividades tanto personales como laborales.

La virtualización ofrece grandes expectativas también, pero está tan limitada en cuanto a soporte de dispositivos que no es una alternativa práctica en este punto del programa de dispositivos personales.

Busque antes de dar el salto

En resumen, investigue antes de precipitarse. Defina sus objetivos, comprenda a sus usuarios e infórmese de qué tecnologías están a su disposición y cómo influirán en el entorno y los usuarios. Y lo que es más importante, infórmese antes de decidirse por un proveedor. Mientras interactúe con los proveedores y las pruebas de sus soluciones, busque alternativas que se adapten al panorama móvil que tan rápidamente evoluciona y vuelva a evaluar sus objetivos de vez en cuando.

Para obtener más información

Si desea obtener más información sobre nuestra tecnología y nuestros servicios, visite www.maaS360.com.

1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Teléfono 215.664.1600 | **Fax** 215.664.1601 | sales@fiberlink.com

WP_201304_0046