IBM Security
Documento técnico de líderes de pensamiento

Movilice su contenido y aplicaciones corporativas

Habilite una colaboración simple y protegida para la empresa

IBM

Estrategia móvil para una nueva era

P: ¿Tiene una estrategia móvil robusta?

R: ¿Estrategia móvil? ¿Quiere decir si nuestros empleados pueden tener acceso al correo electrónico en sus dispositivos móviles? Sí, nosotros tenemos eso.

Si esta es su respuesta, sepa que no es el único. Muchas compañías todavía confían en que el correo electrónico es la "aplicación elegida" que habilita a los empleados a comunicarse fuera de la oficina. Y esto era una verdad absoluta hasta hace apenas un par de años. Sin embargo, reconozcámoslo, revisar el correo electrónico y responderlo fuera de la oficina, no es exactamente "trabajar", sino apenas eliminar unos pocos obstáculos, movilizar algunas cosas y mantener las apariencias. En el mundo actual, la colaboración móvil tiene muchísimo más potencial para desbloquear la verdadera productividad y facilitar el trabajo real en tiempo casi real, pero muchas compañías solo han arañado la superficie y todavía tienen que adoptar, planear e implementar una estrategia móvil robusta que aproveche el poder de la movilidad con acceso simple y protegido a los recursos empresariales.

En este documento comentaremos de qué manera se puede aplicar el monitoreo continuo a las computadoras portátiles, computadoras de escritorio y otros dispositivos de punto final.

En este artículo, usted aprenderá cómo:

- Proporcionar acceso móvil protegido a los datos corporativos sin tener VPN en el dispositivo
- Conferir movilidad a SharePoint, Windows File Share y todos sus sitios intranet
- Proteger datos corporativos sensibles con políticas de seguridad robustas y controles de DLP
- Proporcionar acceso sin requerir cambios a la configuración de seguridad de su red o cortafuegos
- Permitir a los usuarios colaborar sobre la marcha desde sus dispositivos personales

Siga leyendo para obtener más información sobre cómo brindar a sus empleados acceso a recursos ubicados detrás del cortafuegos a la vez de proteger su información con políticas de autorización, cifrado y protección en contenedor.

Acceso simple con seguridad

Veamos un desafío simple: Construir una casa perfectamente segura que pueda proteger todos sus inapreciables objetos de valor. ¿Cómo puede resolverlo? Usted puede construir una casa sin ventanas ni puertas: ningún punto de entrada o de salida. Probablemente, esto podría ser perfectamente seguro pero no muy útil para vivir. O bien podría construir la casa con ventanas y puertas que tengan cerraduras y sistemas de seguridad de máxima calidad para protegerlas y así disponer del mismo nivel de seguridad, pero poder entrar, salir, recibir a visitantes y dejar entrar aire fresco sin arriesgarse a perder sus preciosas pertenencias.

Su estrategia móvil bien podría ser igual a una casa sin ventanas ni puertas. O bien, podría ser una casa con ventanas y puertas que no tengan cerraduras. Usted tiene la responsabilidad de proteger su contenido corporativo, pero también tiene que ponerlo a disposición de los usuarios para que puedan ser productivos. Desde las listas de contactos con los clientes hasta la información sobre pacientes, desde información financiera hasta los archivos de Recursos Humanos, desde aplicaciones corporativas hasta las actas de directorio: la información a la que desean acceder los empleados crece diariamente, y bloquear el acceso a ella deja de ser una opción factible. Usted necesita algunas ventanas y puertas, y un sistema de seguridad que ayude a asegurar que solo podrán entrar aquellos que sean autorizados.

¿Qué sucede si un usuario trae un teléfono inteligente personal o tableta al trabajo y descarga contactos de ventas al dispositivo? ¿Qué sucede si envían por correo electrónico sus informes financieros registrados a la dirección de correo electrónico de su casa para poder trabajar a la noche, luego de que los niños se acuesten? ¿Y qué ocurriría con un proveedor? Seguramente querrá compartir su contenido y aplicaciones con él para colaborar más eficientemente, ¿pero qué sucederá cuando el proyecto esté terminado?

Estas situaciones se producen diariamente. Las personas encuentran maneras de obtener la información que necesitan, poniendo en riesgo la información corporativa, a menos que usted les facilite una manera más segura, confiable y simple para que obtengan lo que necesitan.

Consideraciones sobre contenidos

Los contenidos empresariales se almacenan en las redes corporativas en lugares como compartición de archivos de Windows, SharePoint, sitios de intranet y aplicaciones web. Las personas de información que necesitan colaborar con colegas, asociados y clientes para hacer sus trabajos se ven atrapadas en discos internos y depósitos de información, bases de conocimiento, wikis internos, ERP, SCM, HRM, CRM y otros sistemas o procesos de administración.

Entonces la pregunta es, ¿cómo se aprovecha todo eso para el moderno trabajador móvil que necesita acceso sobre la marcha, muchas veces desde dispositivos que no son propiedad de la empresa?

Mientras protege su información y las redes internas, comparticiones de archivos y otros sistemas que la contienen, es posible que le convenga pensar sobre las siguientes consideraciones como parte de su estrategia móvil. Algunas pueden parecer obvias, pero vale la pena tenerlas en cuenta.

1. El contenido debe ser accesible para los usuarios bajo demanda mediante un enfoque de transmisión o descarga forzadas
2. Cada usuario debe tener acceso solo al contenido que necesite, con base en el contexto y la identidad
3. Se debe poder actualizar y sincronizar la información en todos los dispositivos a lo largo del tiempo
4. El proceso de acceder a la información no debe ser pesado para el usuario
5. El mantenimiento de la seguridad no debe ser costoso, aunque es una gran inversión
6. El mantenimiento de la seguridad no debe consumir tiempo de TI
7. La información en movimiento debe ser cifrada y protegida
8. No se debe permitir que los datos salgan de la organización sin autorización
9. La información creada y almacenada en las aplicaciones debe ser protegida
10. Como los dispositivos personales no son propiedad de la organización, hay un límite a lo que usted puede controlar.

Uno de los objetivos más importantes de cualquier legislación federal sobre seguridad cibernética debe ser habilitar a los defensores a actuar con la misma rapidez para proteger a sus sistemas que la que emplean los atacantes.

Tecnologías actuales

Demos un vistazo a las tecnologías que se usan hoy en día y algunos de los problemas inherentes a la habilitación de la seguridad y productividad.

Correo electrónico

El correo electrónico es la aplicación elegida para la colaboración, pero solo es una herramienta entre muchas otras.

No está diseñado para colaboración. El correo electrónico soporta la comunicación uno a uno o uno a muchos, en lugar de las interacciones muchos a muchos que sus usuarios necesitan para ser verdaderamente productivos. Esto favorece el desarrollo de "silos" entre grupos que deberían estar trabajando juntos.

La información enviada por correo electrónico puede convertirse en obsoleta fácilmente: las personas reciben una hoja de cálculo y siguen trabajando con ella, sin advertir que ha sido reemplazada por algo más actualizado.

El principal problema es que la información se puede cortar, pegar y reenviar a lugares adonde usted no querría que llegara.

VPN

Iniciar sesión con una VPN es una opción común cuando se desea obtener acceso eludiendo a un cortafuegos.

Desafortunadamente, forzar a los usuarios a iniciar sesión para tener acceso degrada la experiencia del usuario. Si se les da a elegir entre contenido nuevo pero de difícil acceso y contenido obsoleto al que se puede acceder fácilmente y que proviene de viejos adjuntos de correo electrónico, las personas pueden optar por el camino más simple.

Las VPN requieren licencias por dispositivo, por lo que sus costos pueden incrementarse a lo largo del tiempo. Además, está comprobado que usar una VPN en el dispositivo puede agotar la batería del mismo más rápidamente.

Como los dispositivos móviles usan tecnología inalámbrica para conectarse, usted necesitará cifrado. Sin embargo, está la cuestión del acceso durante el "roaming" (itinerancia). Típicamente, las soluciones que dependen de cifrado de más alto nivel tienen el potencial de quebrarse cuando los usuarios se trasladan entre puntos de acceso. Afortunadamente, hay algunas soluciones que abordan ese aspecto.

Virtualización del escritorio

Algunas aplicaciones le permiten exhibir un escritorio en los dispositivos móviles. Todos los elementos accesibles desde el escritorio deberían estar disponibles también en su teléfono inteligente o tableta. Sin embargo, por lo general es costoso y la experiencia del usuario puede no ser satisfactoria. Con este enfoque, la disponibilidad y el rendimiento dependen en gran medida de la conectividad de la red. Además, los problemas de tamaño y definición de la pantalla plantean otro reto, especialmente en los teléfonos inteligentes que tienen pantallas y espacios de trabajo pequeños. Las aplicaciones optimizadas para un entorno de escritorio pueden ser accesibles desde un dispositivo móvil mediante la virtualización del escritorio, pero eso no significa necesariamente que puedan utilizarse.

Otra consideración que TI debe tener en cuenta es que los recursos de servidores y red deben tener la capacidad de soportar numerosos dispositivos que se conecten a su red simultáneamente.

Comparticiones de archivos de terceros

Las comparticiones de archivos de terceros le permiten guardar información colateral en la nube. Uno de los grandes problemas aquí es que usted no tiene ningún control. El contenido puede ser enviado a cualquiera, puede ser visto por cualquiera y usted puede tener problemas de control de versiones.

También puede haber problemas en la experiencia de los usuarios. A los usuarios no les gusta verse forzados a aprender nuevo software solo para tener acceso al contenido que necesitan y usted debe contabilizar el tiempo que les tomará el aprendizaje.

Las comparticiones de archivos de terceros también pueden ser costosas: a medida que agrega usuarios necesitará agregar licencias, y es posible que no pueda usar sus inversiones existentes, como tiendas de aplicaciones y contenidos.

Aplicaciones de terceros y personalizadas

Si usted recurre a un tercero desarrollador para sus aplicaciones, estará dependiendo de su proveedor. Es posible que no se incluya la Prevención contra filtraciones de información (DLP) en la aplicación.

Usted puede tratar de desarrollar sus propias aplicaciones, pero entonces necesitará personal para respaldarlas e incorporar los cambios que se requieran por nuevos tipos de dispositivos, actualizaciones del sistema operativo, etc.

Muchos expertos en seguridad, principales funcionarios de seguridad cibernética del gobierno federal y legisladores líderes están presionando por aplicar más énfasis sobre el monitoreo continuo, herramientas de monitoreo automatizadas y rápida reacción ante los ataques a los sistemas tecnológicos de información gubernamental.

La importancia de las políticas

Si tiene la intención de permitir que los usuarios tengan acceso a los recursos corporativos desde sus dispositivos personales, necesitará crear políticas para regular cómo se accede a su información y cómo se la usa.

Puede exigir que un usuario introduzca una contraseña antes de acceder a información importante.

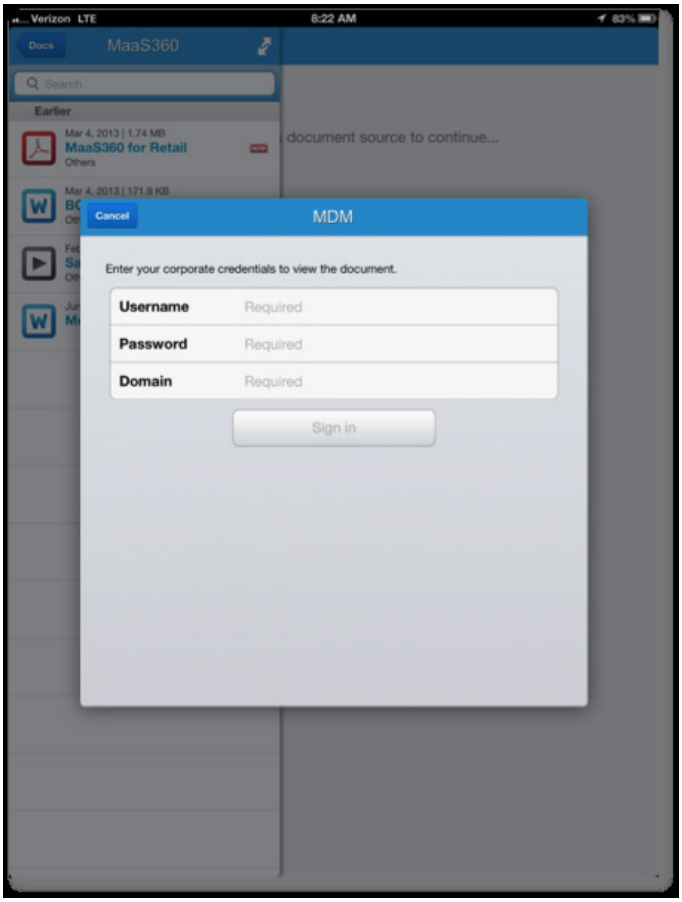

Figura 1: Una solicitud de autentificación

También puede restringir la función de cortar y pegar texto de un documento.

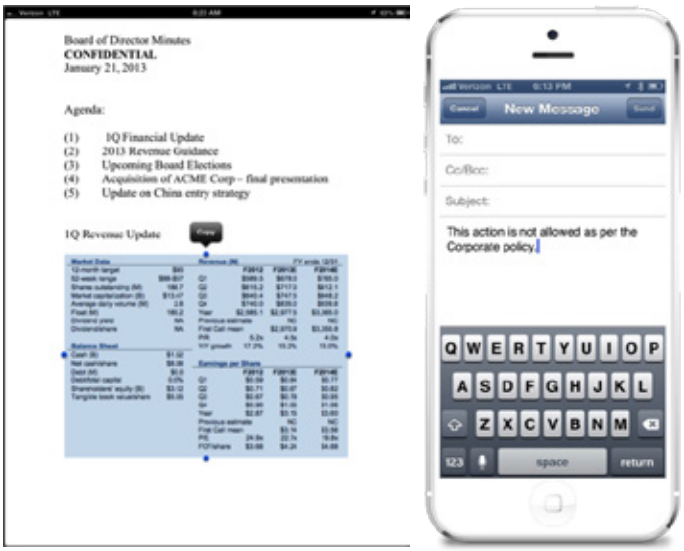

Figura 2: Controles de prevención contra filtraciones de información tales como restricciones de copiar y pegar

IBM® MaaS360® Productivity Suite

La Productivity Suite de MaaS360 le ayudará a superar los retos planteados por las tecnologías actuales y está diseñada con múltiples maneras de permitir acceso seguro y de proteger su información en reposo:

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 usa un contenedor como parte de un enfoque de persona dual: la información, las aplicaciones y el contenido que son específicos de la compañía permanecen en un área protegida del dispositivo. Usted determina los controles que se imponen a esa área protegida de manera que el correo, los contactos, los calendarios, las aplicaciones (y la información de éstas), los documentos y el acceso a la página web puedan ser protegidos.

Figura 3: Productivity Suite y Content Suite de MaaS360

La Productivity Suite de MaaS360 usa políticas de personalidad para especificar seguridad en todos los dispositivos de un usuario. Estas políticas son creadas en el portal de MaaS360 y distribuidas a los dispositivos inscriptos a distancia, de manera que TI no necesita tener contacto físico con los dispositivos.

Cuando el dispositivo infringe el cumplimiento, o cuando el proyecto se termina y el proveedor parte, usted simplemente elimina el contenedor a distancia y la información y las aplicaciones desaparecerán.

El contenedor tiene la seguridad incorporada. Incluye cifrado AES-256, que cumple con FIPS 140-2. Usted puede exigir a los usuarios que introduzcan una clave de acceso cuando deseen tener acceso. También puede usar estos ajustes de políticas para eliminar totalmente el contenedor si los dispositivos son liberados o se les desbloquea el "root", o si los dispositivos no han iniciado sesión luego de un período determinado.

También puede evitar que los archivos sean desplazados, copiados o impresos desde el contenedor y puede evitar que se importen archivos al interior del mismo.

IBM® MaaS360® Content Suite

La Content Suite de MaaS360 proporciona un contenedor cifrado y herramientas de productividad para distribuir, visualizar, crear, editar y compartir documentos en dispositivos móviles, brindando a las organizaciones el control que necesitan y a los empleados el acceso que demandan.

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

El Mobile Content Management de MaaS360 proporciona un contenedor de documentos móvil para colaboración de contenidos con un robusto conjunto de capacidades de administración de ciclo vital para distribuir, actualizar, administrar y proteger documentos. Los administradores de TI pueden imponer restricciones de autentificación, copiar/pegar y solo lectura. Los usuarios pueden acceder a contenido distribuido por la empresa y a depósitos de archivos tales como SharePoint, Box y Google Drive.

El Mobile Document Editor de MaaS360 se ha diseñado para prevenir filtraciones de información corporativa a la vez de permitir a los usuarios crear, editar y guardar. Los usuarios pueden colaborar en archivos Word, Excel, PowerPoint y de texto en los dispositivos móviles mientras están desplazándose.

Mobile Document Sync de MaaS360 habilita a los usuarios a sincronizar fácilmente el contenido a través de dispositivos móviles administrados para continuar creando o editando sus archivos sin interrupción. TI puede aplicar políticas de contenido tales como restringir la función copiar/pegar y bloquear la apertura de los documentos o su compartición en aplicaciones no administradas. Estos controles pueden aplicarse a todos los documentos, a un grupo de ellos o a documentos individuales, lo que le brinda la flexibilidad que usted necesita para proteger valiosa información corporativa.

Los casos prácticos de uso compartido seguro para su organización son interminables, ya sea en los departamentos de Ventas, Marketing, Operaciones o Finanzas:

- Vea y comparta cambios de última hora a una presentación de ventas sobre la marcha, justo antes de una reunión con el cliente
- Trabaje en colaboración sobre los últimos resultados financieros en una hoja de cálculo, antes de tomar un avión

- Participe en una tormenta de ideas de mensajes de marketing y compártalos con sus colegas en una cafetería
- Distribuya documentos financieros trimestrales al Directorio y configure el documento para que caduque después de la reunión
- Comparta materiales de productos en tiempo casi real con los equipos de ventas de modo que no tengan que rebuscar para encontrar la información de la competencia o las hojas de especificaciones más recientes
- Asegúrese de que las tabletas en las tiendas minoristas tengan la información de productos e inventario más actualizada

IBM® MaaS360® Gateway Suite

La Gateway Suite de MaaS360 es un componente clave para hacer que todo esto sea posible. Protege a la información en movimiento brindando acceso sin problemas y protegido a su contenido e intranet corporativos desde dispositivos móviles.

- Provea acceso móvil simple y protegido a la información sin una VPN en el dispositivo; no es necesario iniciar sesión en la VPN cada vez que desee información
- Movilice SharePoint, Windows File Shares, sitios intranet y aplicaciones web
- Proteja la información con políticas de seguridad robustas y controles de DLP
- No se requieren cambios en las configuraciones de seguridad de su red o cortafuegos

Figura 4: La información fluye con Gateway de MaaS360

Puede configurar opciones de políticas para administrar la manera en que la Productivity Suite de MaaS360 interactúa con los dispositivos de sus usuarios. Por ejemplo, puede especificar URL a las wikis corporativas, sistemas de rastreo de fallas, etc. o carpetas corporativas accesibles a través de la Gateway de MaaS360, y aparecerán como marcadores en el Secure Mobile Browser de MaaS360. También puede especificar si se requiere autentificación para acceder a estas ubicaciones.

La Gateway de MaaS360 determina cuáles serán los recursos corporativos que los usuarios verán cuando accedan al contenedor de información en sus dispositivos.

Pruebe antes de comprar

Es fácil y rápido probar MaaS360, y además, el tiempo que invierta en configurar MaaS360 de acuerdo a sus necesidades está bien invertido. Una vez que decida que MaaS360 es la solución correcta para su organización, ¡su entorno de prueba se convertirá en su entorno real!

Para obtener una prueba sin costo de MaaS360, por favor haga clic aquí. Puede comenzar ya mismo: no hay un proceso de preparación complicado ni es necesario cambiar la infraestructura. ¡Pruebe MaaS360 hoy mismo!

Figura 5: Productos MaaS360

Acerca de IBM MaaS360

IBM MaaS360 es la plataforma de administración de movilidad empresarial para habilitar la productividad y la protección de datos para la manera de trabajar de las personas. Miles de organizaciones confían en MaaS360 como cimiento de sus iniciativas de movilidad. MaaS360 brinda administración total con sólidos controles de seguridad a través de usuarios, dispositivos, aplicaciones y contenidos para respaldar cualquier implementación móvil. Para obtener más información acerca de IBM MaaS360 e iniciar una prueba durante 30 días sin costo alguno, visite www.ibm.com/maas360

Acerca de IBM Security

La plataforma de seguridad de IBM brinda la inteligencia de seguridad para ayudar a las organizaciones a proteger holísticamente a sus personas, datos, aplicaciones e infraestructura. IBM ofrece soluciones para administración de identidades y acceso, información de seguridad y administración de eventos, seguridad de bases de datos, desarrollo de aplicaciones, administración de riesgos, administración de puntos finales, protección contra intrusión de última generación y mucho más. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo. Para obtener más información, visite www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en los Estados Unidos de América
Marzo de 2016

Por favor, recicle

WGW03111-COES-01