IBM Security
Libro blanco de Liderazgo conceptual

Movilice sus apps y el contenido corporativo

Facilite una colaboración móvil sencilla y segura para su empresa

IBM

Estrategia móvil para una nueva era

P: ¿Tiene una estrategia móvil sólida?

R: ¿Estrategia móvil?, ¿Que si nuestros empleados pueden acceder al correo electrónico en su dispositivo móvil? Claro que sí.

Si esta es su respuesta, usted no es el único. Para muchas empresas, el correo electrónico sigue siendo la "aplicación preferida" para las comunicaciones de los empleados fuera de la oficina. Y hace solo un par de años esto suponía un enorme avance. Pero, admitámoslo, leer y contestar el correo electrónico fuera de la oficina no es exactamente "trabajar", sino más bien eliminar algunos obstáculos, seguir avanzando y mantener las apariencias. En el mundo actual, la colaboración móvil tiene un enorme potencial para posibilitar una productividad real y facilitar el trabajo prácticamente a tiempo real, pero muchas empresas apenas han rozado la superficie y aún necesitan aceptar, planificar e implementar una estrategia móvil sólida que les ofrezca todo el poder de la movilidad, con un acceso sencillo y seguro a los recursos empresariales.

En este documento hablaremos sobre cómo se pueden supervisar continuamente ordenadores portátiles y de sobremesa, y otros dispositivos terminales.

En este libro blanco aprenderá a:

- Habilitar un acceso móvil seguro a los datos corporativos sin necesidad de VPN en el dispositivo
- Movilizar SharePoint, el recurso compartido de archivos de Windows y todos sus sitios de intranet
- Proteger los datos corporativos confidenciales con sólidas políticas de seguridad y controles DLP
- Facilitar el acceso móvil sin cambios en su red ni en la configuración de seguridad de su firewall
- Permitir a los usuarios colaborar desde cualquier lugar utilizando sus dispositivos personales

Siga leyendo para obtener más información sobre cómo facilitar a sus empleados acceso a los recursos situados detrás del firewall sin poner en peligro los datos de su empresa mediante políticas de autorización, cifrado y contenedorización.

Acceso sencillo con seguridad

Veamos un sencillo problema: construir una casa perfectamente segura capaz de proteger todos sus preciados bienes. ¿Cómo enfocaría la cuestión? Puede construir un edificio sin ventanas ni puertas: sin ningún punto de entrada o salida. La seguridad sería total, pero no sería un edificio útil para vivir en él. O bien puede prever ventanas y puertas con cerraduras y sistemas de seguridad de primera calidad y disfrutar en la práctica del mismo nivel de seguridad, pero con la posibilidad de entrar, salir, recibir invitados y tomar el aire sin arriesgarse a perder sus preciadas posesiones.

Su estrategia móvil puede ser como una casa sin ventanas ni puertas. O puede ser una casa con ventanas y puertas sin cierres. Su misión es proteger su contenido corporativo, pero también tiene que ponerlo a disposición de los usuarios para que puedan ser productivos. Desde listas de contactos de clientes hasta datos de pacientes, información financiera o archivos de recursos humanos, aplicaciones corporativas o actas del consejo de administración, la información a la que quieren acceder sus empleados crece a diario, y bloquear el acceso ya no es una opción factible. Usted necesita ventanas y puertas, y un sistema de seguridad que le garantice que solo puedan entrar personas autorizadas.

¿Qué sucede si un usuario trae al trabajo su smartphone o tablet personal y descarga los contactos de ventas en el dispositivo? ¿Y si envía por correo electrónico informes financieros sujetos a derechos de propiedad a su dirección de correo electrónico particular para poder trabajar por la noche mientras duermen sus hijos? ¿Y si se trata de un proveedor? Usted desea compartir sus contenidos y sus apps para colaborar de forma más eficiente, pero ¿qué sucede cuando finaliza el proyecto?

Este tipo de situaciones se producen a diario. Las personas buscan formas de obtener la información que necesitan, pero pondrán en riesgo la información corporativa si usted no les ofrece una forma más segura, fiable y sencilla de conseguir lo que necesitan.

Consideraciones sobre el contenido

El contenido de negocio se almacena en redes empresariales en lugares como recursos compartidos de archivos de Windows, SharePoint, sitios de intranet y apps en web. La información que necesitan las personas para colaborar con sus compañeros, socios y clientes y hacer su trabajo está contenida en unidades de disco internas y almacenes de datos, bases de conocimiento, wikis internas, ERP, SCM, HRM, CRM y otros sistemas o procesos de gestión.

La pregunta pasa a ser: ¿cómo construir a partir de esta premisa pensando en el trabajador móvil de hoy en día que precisa acceso durante sus desplazamientos, muchas veces desde dispositivos que no son propiedad de la empresa?

A la hora de proteger sus datos y las redes internas, recursos compartidos de archivos y otros sistemas que los albergan, en su estrategia móvil posiblemente deberá tener en consideración lo siguiente. Algunos de estos puntos pueden parecer evidentes, pero vale la pena destacarlos.

1. Los usuarios deben poder acceder al contenido bajo demanda mediante un enfoque “push” o “pull”
2. Cada usuario debe tener acceso solo al contenido que precise en función del contexto y de la identidad
3. Los datos deberán ser actualizables y sincronizarse entre dispositivos a lo largo del tiempo
4. El proceso de acceder a los datos no debe ser complicado para el usuario
5. Mantener la seguridad no debe resultar costoso, aunque se trate de una gran inversión
6. Mantener la seguridad no debe consumir mucho tiempo de TI
7. Los datos en movimiento deben estar cifrados y protegidos
8. Los datos no podrán salir de la organización sin autorización
9. Los datos creados y almacenados en apps deberán estar protegidos
10. Los dispositivos personales no son propiedad de la organización, por lo que el control tiene ciertos límites

Uno de los principales objetivos de cualquier legislación sobre ciberseguridad ha de ser permitir a los responsables de seguridad actuar rápidamente para proteger sus sistemas con la misma rapidez que los atacantes.

Tecnologías actuales

Examinemos las tecnologías utilizadas en la actualidad y algunos de los problemas inherentes a la seguridad y la productividad.

Correo electrónico

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

No está diseñado para la colaboración. El correo electrónico admite comunicación de persona a persona o de una persona a muchas, pero no las interacciones entre muchas personas que sus usuarios precisan para ser realmente productivos. Esto da lugar a que se creen silos aislados entre grupos que deberían trabajar en colaboración.

La información enviada por correo electrónico puede quedar obsoleta con facilidad; por ejemplo, una persona recibe una hoja de cálculo y sigue trabajando en ella, sin advertir que existe otra versión más actualizada.

El principal problema es que en ocasiones, los datos se cortan, pegan y reenvían a lugares donde no deberían llegar.

VPN

Iniciar sesión en una VPN es una forma habitual de facilitar el acceso a una ubicación protegida por firewall.

Pero obligar a los usuarios a iniciar sesión para poder acceder repercute negativamente en su experiencia. Si pueden elegir entre un contenido más reciente pero de difícil acceso o un contenido menos reciente pero fácil de acceder, como los datos anexos al correo electrónico, muchas personas elijen la ruta más sencilla.

Las VPN precisan licencias por dispositivo, por lo que los costes pueden aumentar con el tiempo. Además, hay estudios que indican que el uso de una VPN puede agotar la batería del dispositivo más rápidamente.

Los dispositivos móviles utilizan tecnología inalámbrica para conectarse, por lo que usted requerirá un sistema de cifrado. Sin embargo, hay que tener presente el problema del acceso en itinerancia. Generalmente, las soluciones que utilizan cifrado de alto nivel tienden a sufrir fallos de comunicación cuando el usuario pasa de un punto de acceso a otro. Afortunadamente, hay soluciones para abordar este problema.

Virtualización de escritorios

Algunas aplicaciones le permiten presentar un escritorio en dispositivos móviles. Todos los elementos accesibles desde el escritorio estarán disponibles también en su smartphone o tablet. Sin embargo, esto suele resultar caro y la experiencia del usuario no ser demasiado satisfactoria. Mediante este enfoque, la disponibilidad y el rendimiento dependen en gran medida de la conectividad de la red. Además, el tamaño de la pantalla y la resolución plantean un problema adicional, especialmente en smartphones con pantallas y espacios de trabajo reducidos. Las aplicaciones optimizadas para un entorno de escritorio pueden ser accesibles en un dispositivo móvil mediante esta virtualización, pero eso no significa que vayan a ser realmente utilizables.

Otro punto que ha de tener en consideración el departamento de TI es que el servidor y los recursos de la red deben tener capacidad para admitir la conexión simultanea de numerosos dispositivos a la red.

Recursos compartidos de archivos de terceros

Los recursos de terceros para compartir archivos le permiten mantener contenidos colaterales en la nube. El principal problema en este caso es la falta de control. El contenido puede enviarse a cualquier persona, todo el mundo tiene acceso al contenido y puede haber problemas de control de versiones.

También existen problemas de experiencia del usuario. A los usuarios no les gusta tener que aprender a utilizar un nuevo programa solo para acceder al contenido que precisan, y hay que tener el cuenta el tiempo de aprendizaje necesario.

Además, los recursos compartidos de archivos pueden resultar caros: a medida que se añaden usuarios es preciso aumentar el número de licencias, y es posible que no pueda aprovechar otras inversiones ya realizadas, como apps y almacenes de contenidos.

Apps de terceros y apps a medida

Si recurre a una empresa externa para desarrollar sus apps, dependerá de ese proveedor. Es posible que la app no integre medidas de prevención de filtración de datos (DLP).

Usted puede intentar desarrollar sus propias aplicaciones, pero en este caso necesitará también personal específico para atenderlas y realizar todos los cambios necesarios para nuevos tipos de dispositivos, actualizaciones de los sistemas operativos, etc.

Muchos expertos en seguridad, altos cargos de agencias de ciberseguridad del gobierno federal e importantes congresistas de Estados Unidos están luchando para que se preste más atención a la supervisión continua, con herramientas de monitorización automatizada, y a una reacción rápida en caso de ataque a sistemas informáticos del gobierno.

La importancia de las políticas

Si tiene intención de permitir a los usuarios acceder a recursos corporativos desde sus dispositivos personales, deberá crear políticas que regulen la forma en que se acceda y se utilicen los datos.

Puede hacer que el usuario tenga que introducir una contraseña para acceder a datos importantes.

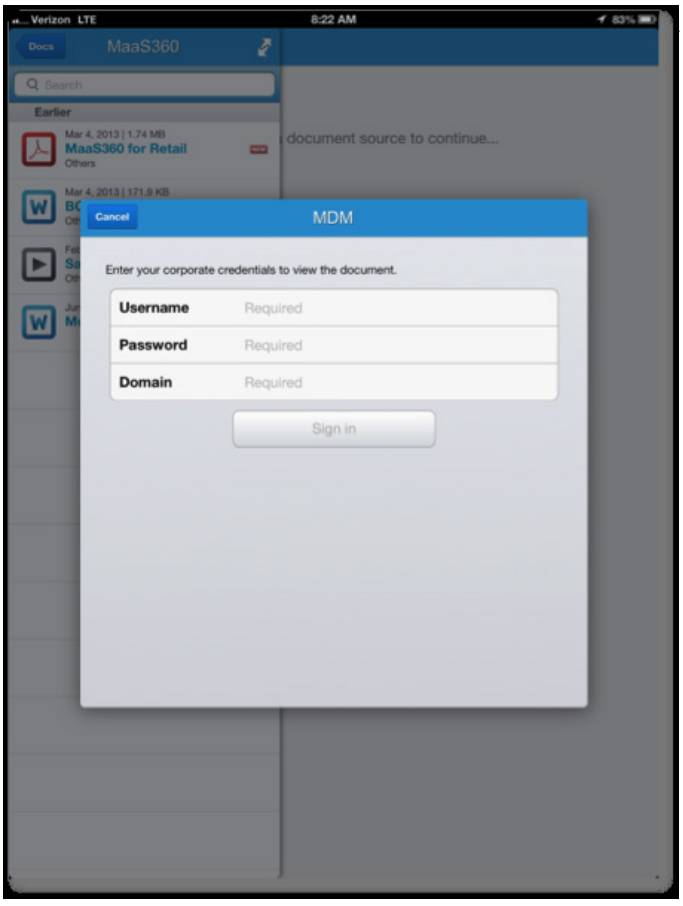

Figura 1: Solicitud de autenticación

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

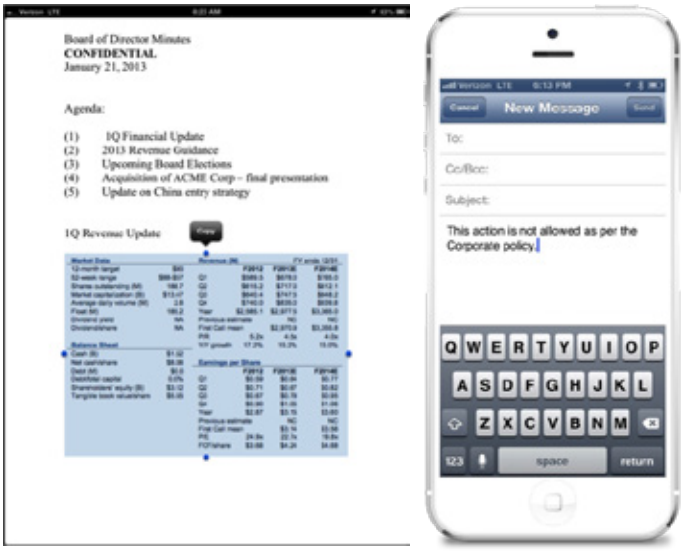

Figura 2: Controles de prevención de filtración de datos, como las restricciones para copiar y pegar

IBM® MaaS360® Productivity Suite

MaaS360 Productivity Suite le ayuda a superar los problemas que plantean las tecnologías actuales e incorpora múltiples maneras de facilitar un acceso seguro y proteger sus datos:

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

MaaS360 utiliza un contenedor con un enfoque de doble identidad: los datos, apps y contenidos específicos de la empresa permanecen en un área protegida del dispositivo. Usted determina los controles que se deben aplicar en el área protegida para que esté seguro el correo, contactos, calendarios, apps (y datos que estas contengan) y documentos y el acceso a páginas web.

Figura 3: MaaS360 Productivity Suite y MaaS360 Content Suite

MaaS360 Productivity Suite utiliza políticas de roles para especificar el nivel de seguridad en todos los dispositivos de un usuario. Estas políticas se crean en el portal de MaaS360 y se implementan en los dispositivos correspondientes de forma inalámbrica, por lo que TI no necesita tener contacto físico con los dispositivos.

Si el dispositivo deja de cumplir los requisitos o si termina el proyecto y la relación con el proveedor, basta con eliminar remotamente el contenedor y todos los datos y apps desaparecen.

El contenedor tiene seguridad integrada e incluye cifrado AES-256 conforme con el estándar FIPS 140-2. Es posible hacer que el usuario tenga que introducir un código de acceso para acceder. También es posible utilizar esta configuración de las políticas para eliminar por completo el contenedor si se viola la seguridad del dispositivo o si el dispositivo no pasa el control de entrada en un periodo de tiempo especificado.

Puede impedir que se muevan, copien o impriman archivos desde el contenedor, así como evitar la importación de archivos.

IBM® MaaS360® Content Suite

MaaS360 Content Suite ofrece un contenedor cifrado y herramientas de productividad para distribuir, ver, crear, editar y compartir documentos en dispositivos móviles, para que las empresas tengan el control que precisan y los empleados consigan el acceso que demandan:

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

MaaS360 Mobile Content Management proporciona un contenedor móvil para documentos que permite la colaboración en contenidos con sólidas prestaciones de gestión del ciclo de vida para distribuir, actualizar, administrar y proteger documentos. Los administradores de TI pueden establecer restricciones de autenticación, copiado/pegado o solo visualización. Los usuarios pueden acceder a contenidos corporativos distribuidos y repositorios de archivos como SharePoint, Box y Google Drive.

MaaS360 Mobile Document Editor está diseñado para evitar filtraciones de datos corporativos, pero permite a los usuarios crear, editar y guardar. Los usuarios pueden colaborar en archivos de Word, Excel, PowerPoint y de texto en dispositivos móviles durante sus desplazamientos.

MaaS360 Mobile Document Sync permite a los usuarios sincronizar fácilmente contenidos entre dispositivos móviles gestionados para seguir creando o editando sus archivos sin interrupciones. TI puede aplicar políticas a los contenidos, como restricción del copiado/pegado y bloquear la apertura o uso compartido en apps no gestionadas. Estos controles pueden aplicarse a todos los documentos, a un grupo de ellos o a documentos individuales, proporcionándole la flexibilidad que usted necesita para proteger sus valiosos datos corporativos.

Los casos de uso compartido de contenidos protegidos son numerosos en prácticamente todo tipo de organizaciones, tanto en ventas, marketing, operaciones o finanzas:

- Ver y compartir cambios de última hora en una presentación de ventas justo antes de reunirse con el cliente
- Colaborar en los datos últimos financieros de una hoja de cálculo antes de embarcar en un vuelo

- Buscar ideas para mensajes de marketing y compartirlas con los compañeros desde una cafetería
- Distribuir documentos financieros trimestrales entre los miembros del consejo de administración y hacer que los documentos dejen de estar disponibles tras la reunión
- Compartir materiales de productos casi en tiempo real con los equipos de ventas para que no necesiten revolver papeles para encontrar las hojas de especificaciones más recientes o información comercial reservada
- Asegurarse de que las tablets de una cadena de establecimientos minoristas dispongan de la información más actualizada sobre productos e inventario

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite es un componente clave para contribuir a que todo esto sea posible. Protege los datos enviados y recibidos ofreciendo un acceso seguro e ininterrumpido a sus contenidos corporativos y su intranet desde dispositivos móviles.

- Facilite acceso móvil sencillo y seguro a los datos, sin VPN en el dispositivo; no es preciso iniciar sesión en la VPN cada vez que se desea información
- Movilice SharePoint, recursos compartidos de archivos de Windows, sitios de intranet y apps web
- Proteja los datos con políticas de seguridad robustas y controles DLP
- No se precisan cambios en la configuración de seguridad del firewall ni de la red

Figura 4: Flujos de datos con MaaS360 Gateway

Puede configurar opciones de políticas para gestionar la interacción de MaaS360 Productivity Suite con los dispositivos de sus usuarios. Por ejemplo, puede especificar URL a wikis corporativas, sistemas de seguimiento de errores de programación o carpetas corporativas accesibles mediante MaaS360 Gateway y aparecerán como favoritos en MaaS360 Secure Mobile Browser. También puede especificar si se precisa autenticación para acceder a estas ubicaciones.

MaaS360 Gateway determina los recursos corporativos que verán los usuarios cuando accedan al contenedor de datos en sus dispositivos.

Probar antes de comprar

MaaS360 es fácil y rápido de probar, y el tiempo dedicado a configurar MaaS360 para sus necesidades será tiempo bien invertido. Cuando haya decidido que MaaS360 es la solución adecuada para su organización, el entorno de prueba se convertirá en su entorno activo.

Para hacer una prueba gratuita de MaaS360, haga clic aquí. Puede comenzar inmediatamente, sin complicados procesos de configuración ni cambios en las infraestructuras. ¡Pruebe MaaS360 hoy mismo!

Figura 5: Productos MaaS360

Acerca de IBM MaaS360

IBM MaaS360 es la plataforma de gestión de la movilidad empresarial que permite que los empleados sean productivos y tengan sus datos protegidos mientras trabajan de la forma habitual. Miles de organizaciones depositan su confianza en MaaS360 como base de sus iniciativas de movilidad. MaaS360 proporciona una capacidad de gestión completa con estrictos controles de seguridad en implementaciones móviles para todos los usuarios, dispositivos, apps y contenidos. Para obtener más información acerca de IBM MaaS360 y descargar una versión de prueba de 30 días sin coste alguno, visite www.ibm.com/maas360

Acerca de IBM Security

La plataforma de seguridad de IBM proporciona la inteligencia de seguridad necesaria para ofrecer a las organizaciones una ayuda holística que permite proteger sus datos, aplicaciones e infraestructura, y a sus empleados. IBM ofrece soluciones de gestión de acceso e identidad, gestión de la seguridad de la información y los eventos, seguridad de las bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos finales, protección contra intrusiones de última generación y mucho más. IBM dirige una de las organizaciones de suministro, desarrollo e investigación de seguridad más grandes 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-ESES-01