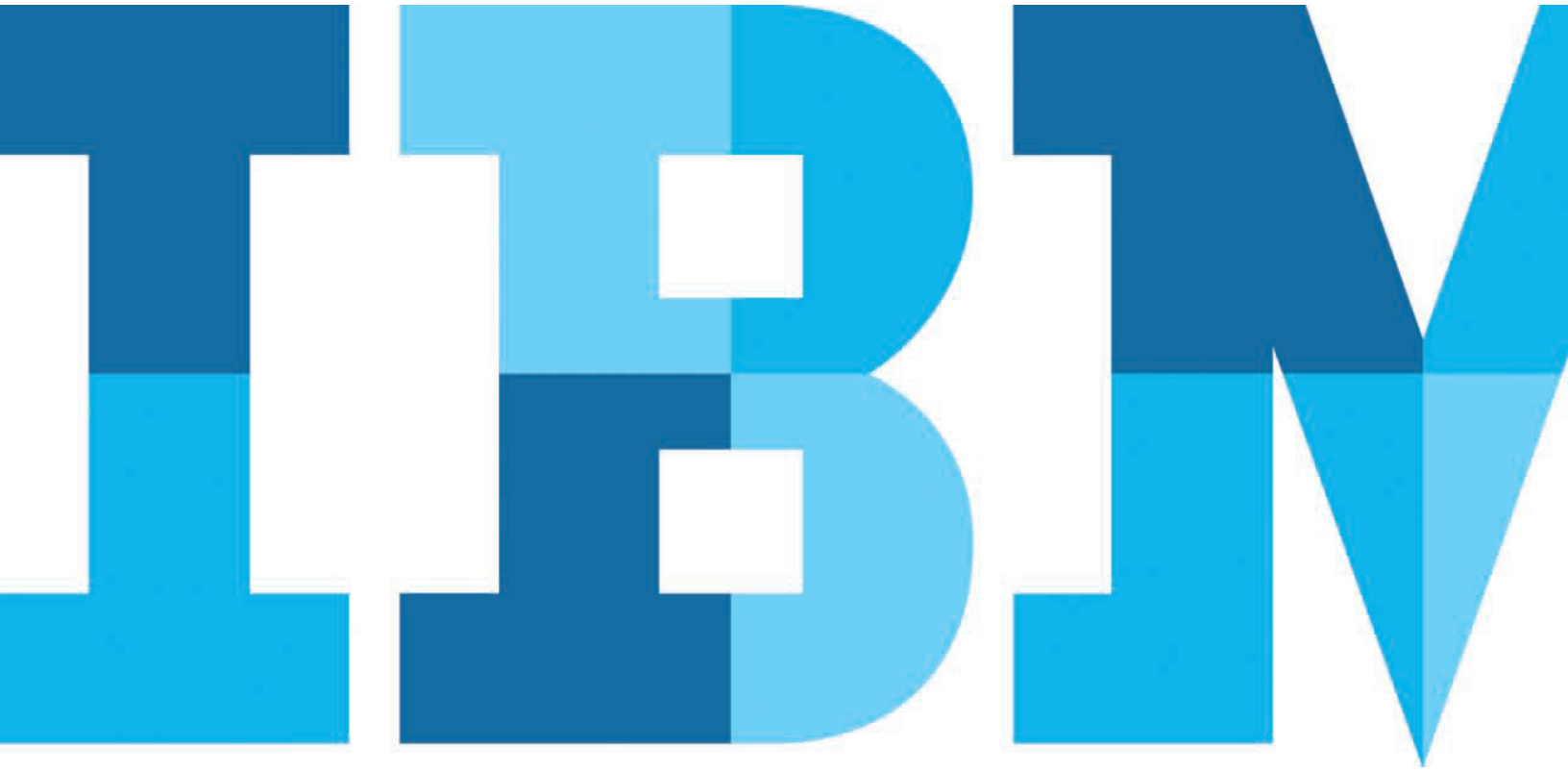
Marzo 2013

El valor de integrar el desarrollo de aplicaciones móviles y la gestión de dispositivos móviles

Cierre la brecha de la seguridad en las fases de desarrollo de aplicaciones móviles integrando poderosas capacidades de gestión de dispositivos móviles.



IBM

Contenido

Introdución

Según las más recientes estimaciones, en el mundo existen casi seis mil millones de suscripciones a dispositivos móviles.[1] No hay duda que el uso de dispositivos móviles está en alza y las organizaciones de TI se suman a la tendencia: no solo adoptan la estrategia de que los empleados traigan sus propios dispositivos (bring-your-own-device, BYOD) a la empresa; sino que también aprovechan el aumento en la demanda de aplicaciones móviles. De hecho, en los últimos tres años se han desarrollado más de 300.000 aplicaciones móviles.[2]

Las ventajas del desarrollo de aplicaciones móviles son muchas: las aplicaciones personalizadas pueden proporcionar formas focalizadas y específicas para cada compañía de mejorar la productividad de negocios y el compromiso, dar servicio al cliente y diferenciarse de la competencia.[3]
Además, algunas organizaciones deciden desarrollar sus propias aplicaciones móviles internas porque no pueden controlar con el nivel necesario, los dispositivos móviles y sus aplicaciones comercialmente disponibles o sistemas operativos (OS) nativos. Si la organización crea sus propias aplicaciones, puede integrar en ellas el diseño de los controles que elija.

Pero ¿cómo puede el sector de TI, que ya enfrenta los desafíos de administrar una Infraestructura cada vez más móvil, con mayor diversidad y complejidad, asegurar la seguridad de los dispositivos y las aplicaciones móviles durante la etapa crítica del desarrollo? Las versiones beta de las aplicaciones móviles en general se distribuyen a los dispositivos de los empleados durante la fase de testeo interno, agregando capas de riesgo y de complejidad al proceso de desarrollo. Es absolutamente necesario mantener la confidencialidad de las aplicaciones beta, tanto para evitar el robo de propiedad intelectual como para evitar que versiones no terminadas, lleguen a manos del público. Sin embargo, al enfrentar estas cuestiones, la mayoría de las organizaciones de TI utilizan herramientas de gestión de dispositivos móviles y de desarrollo de aplicaciones móviles totalmente separadas, lo cual puede exponerlas a importantes brechas en términos de la seguridad de los dispositivos y las aplicaciones.

Este documento informativo analiza los desafíos de administrar los dispositivos móviles y las brechas de seguridad que pueden producirse en el proceso de desarrollo de aplicaciones móviles. Luego considera las ventajas de utilizar tecnologías integradas para el desarrollo de aplicaciones y la gestión de dispositivos móviles, en lugar de soluciones independientes, para abordar los desafíos -y las oportunidades- de la tendencia BYOD y los entornos de desarrollo de aplicaciones móviles.

Abordando los desafíos de la administración de aplicaciones y dispositivos móviles

Mientras que el uso generalizado de los dispositivos móviles en el ámbito empresarial ha permitido nuevos niveles de productividad y flexibilidad en el lugar de trabajo, también ha introducido nuevos cambios y desafíos relacionados con la gestión y seguridad de la Tecnología Informática (TI), lo cual significa romper absolutamente con los paradigmas tradicionales de gestión.

Modelo de gestión tradicional	Nuevo paradigma de gestión de dispositivos
Equipos proporcionados por la empresa	Dispositivos propios de los usuarios (BYOD: traiga su propio dispositivo)
Un reducido grupo de plataformas/modelos con soporte	Muchos fabricantes/modelos diferentes
Actualizaciones iniciadas y administradas por TI	Actualizaciones al sistema operativo y las aplicaciones administradas por operadores móviles, fabricantes de dispositivos y usuarios
Aplicaciones y seguridad estrechamente controladas por TI	Dispositivos móviles controlados por los usuarios

Como resultado de estos cambios –especialmente el uso de dispositivos propiedad de los empleados en lugar de dispositivos provistos por la compañía – es más difícil que nunca para el sector de TI mantener el control de los datos, las aplicaciones y las actualizaciones de la organización. Con el auge de la tendencia BYOD (traiga su propio dispositivo), el poder ahora está en manos del usuario del dispositivo móvil. Esto genera serias preocupaciones en entornos de desarrollo de aplicaciones móviles, donde la seguridad de las aplicaciones empresariales en proceso se encuentra en riesgo.

Limitaciones de tecnologías de sistema operativo nativo

Cualquiera sea el entorno, es difícil para las organizaciones de TI salvaguardar los datos de las aplicaciones empresariales en los dispositivos móviles debido a las limitaciones de gestión que presentan los sistemas operativos nativos tales como Google Android y Apple iOS. Esta situación es muy distinta al modelo de computación tradicional, en el que el sector de TI fácilmente podía borrar los datos corporativos de las computadoras de escritorio cuando un empleado dejaba la organización o no cumplía con la política de la Compañía. Pero el control resulta especialmente crítico en los entornos móviles, donde el riesgo de pérdida de datos de aplicaciones es mayor. Ello se debe a que las tecnologías de sistemas operativos nativos priorizan la experiencia del usuario más que el control del área de TI. Y muchas no permiten que TI borre datos de aplicaciones de los dispositivos móviles. De hecho, estos sistemas operativos nativos a menudo evitan que la aplicación empresarial detecte si el dispositivo móvil en el cual está instalada cumple o no cumple con la normativa.

Esta falta de control deja una marcada brecha de seguridad. ¿Qué sucedería, por ejemplo, si un empleado con múltiples aplicaciones empresariales en un dispositivo Android violara la política corporativa, poniendo los datos de la empresa en riesgo? El área de TI debería denegar temporalmente el acceso o eliminar en forma remota las aplicaciones empresariales del dispositivo, además de eliminar los datos de aplicaciones. Pero como Android OS no permite que el sector de TI fuerce la instalación o desinstalación de aplicaciones o su control remoto, las aplicaciones empresariales quedarían expuestas a un alto riesgo. Y ¿qué sucedería si las aplicaciones en cuestión se encontraran en la fase de prueba para su despliegue? Su lanzamiento anticipado podría tener efectos catastróficos para la organización en términos de pérdidas financieras y de propiedad intelectual.

Limitaciones del uso de herramientas de desarrollo y gestión independientes

En el mundo más inteligente que habitamos, donde empresas cada vez más instrumentadas, interconectadas e inteligentes recopilan, procesan, utilizan y almacenan una cantidad de información sin precedentes, las organizaciones deben invertir en herramientas que aseguren y administren la gama de dispositivos que utilizan los empleados. La correcta solución de gestión de dispositivos móviles puede permitir la administración unificada de todos los dispositivos de la empresa, desde computadoras de escritorio hasta portátiles, Smartphones y más. Sin embargo, cuando se utilizan dispositivos móviles en el proceso de desarrollo –como debe ser, para probar nuevas aplicaciones móviles – se presentan algunos problemas de administración y seguridad. Las aplicaciones en desarrollo pueden quedar expuestas a riesgos porque la mayoría de las soluciones de administración de dispositivos móviles no se integran con plataformas de desarrollo de aplicaciones móviles. Una respuesta común para muchas organizaciones es utilizar herramientas de gestión de dispositivos que sean independientes de las herramientas de desarrollo utilizadas para construir aplicaciones móviles. Pero esta opción deja a las organizaciones la necesidad de encontrar una forma de abordar las brechas de seguridad. Conectar las funciones de desarrollo y gestión puede ayudar a su organización a superar estas limitaciones.

Estos son beneficios claros de la integración del desarrollo de aplicaciones móviles con la gestión de dispositivos móviles.

Integrando tecnologías de desarrollo y gestión móvil

Pueden obtenerse valiosas ventajas si se integra el desarrollo de aplicaciones móviles con la gestión de dispositivos móviles. Las organizaciones pueden proteger mejor sus datos empresariales durante el desarrollo, consolidando la gestión de políticas de aplicaciones móviles en una única infraestructura. Integrar estas herramientas también puede ayudar a optimizar el flujo de trabajo entre los equipos de desarrollo y operaciones.

Consolidar la gestión de políticas de aplicaciones móviles

Integrar las dos tecnologías también puede ayudar a superar muchas limitaciones de gestión de OS nativo. Por un lado, esta integración permite que una aplicación móvil periódicamente "se registre" con la herramienta de gestión de puntos terminales para proporcionar el estado de cumplimiento del usuario y el dispositivo. El departamento de TI luego puede denegar el acceso a las aplicaciones empresariales móviles si el dispositivo no cumple con la política.

Al integrar las herramientas de gestión de puntos terminales y las plataformas de desarrollo de aplicaciones móviles, los administradores pueden manejar políticas de todas las aplicaciones construidas utilizando la plataforma de desarrollo de aplicaciones móviles y probadas con dispositivos móviles. Luego pueden evitar la necesidad de configurar algunas políticas a nivel de dispositivo en la herramienta de administración de puntos terminales y de manejar por separado políticas específicas de aplicaciones utilizando la plataforma de desarrollo de aplicaciones móviles. La integración de la gestión de dispositivos móviles con el desarrollo de aplicaciones móviles también permite a las organizaciones optimizar las políticas entre los entornos de desarrollo y operaciones, ya que los procesos de aprobación de seguridad y cumplimiento obligatorio pueden ser complejos y llevar mucho tiempo.

Por ejemplo, la integración permite que un portafolio de aplicaciones desarrolladas en una plataforma de desarrollo de aplicaciones móviles pase por una lista de verificación uniforme de aprobación y cumplimiento, bajo el control de un grupo de seguridad centralizado, durante la fase de prueba. Además, los desarrolladores de aplicaciones pueden recibir retroalimentación interativa de otras partes interesadas en consideraciones de políticas, cumplimiento y seguridad. El grupo de seguridad luego puede preaprobar estas aplicaciones en la etapa de producción en un marco temporal mucho más corto. Esto, a su vez, puede reducir la duración de los ciclos de lanzamiento de aplicaciones, ya que los grupos de desarrollo se independizan de tener que implementar o exigir políticas de a una aplicación por vez.

Escenario de integración de base móvil: denegar el acceso a aplicaciones

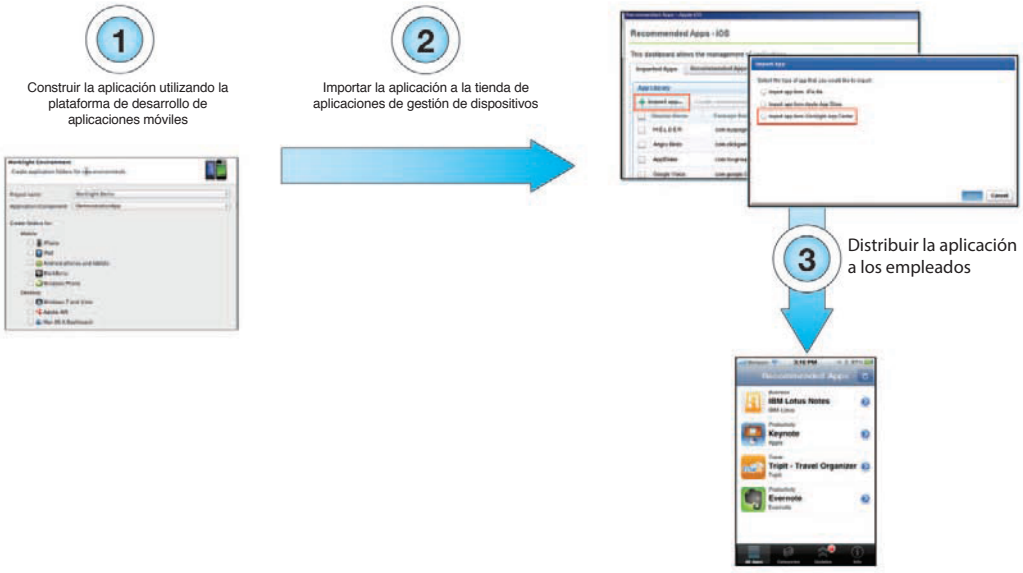
La integración de la plataforma de desarrollo de aplicaciones móviles con la gestión de dispositivos móviles proporciona mayor control de TI, lo cual es necesario para proteger correctamente las aplicaciones móviles durante la fase de prueba del despliegue de aplicaciones.

Optimizar el flujo de trabajo de desarrollo de aplicaciones

La integración de las funciones de desarrollo y gestión también permite optimizar el flujo de trabajo de desarrollo de aplicaciones móviles, lo cual contribuye aún más a la capacidad de una organización de implementar aplicaciones a medida con más rapidez. Puede lograr que las aplicaciones avancen en forma más armónica durante todo el proceso de implementación, desde el desarrollo hasta el aseguramiento de la calidad, hasta los dispositivos móviles de los empleados, para pruebas internas, durante las cuales las aplicaciones se someten a un control estricto, antes de llegar a las manos de los usuarios.

Además, la integración puede proporcionar un grado mayor de seguridad y calidad durante el proceso de desarrollo. Por ejemplo, el uso de una herramienta de gestión con una plataforma de implementación de aplicaciones puede ayudar a los desarrolladores a sentirse más seguros de que están usando la versión correcta de la aplicación, que no ha sido corrompida o manipulada de alguna manera entre las etapas de desarrollo y producción. Da al equipo más control para sacar la aplicación de la prueba para ajustes, actualizarla más tarde o sacarla de circulación, si fuera necesario.

Escenario de integración de base móvil: optimizar el flujo de trabajo de desarrollo de aplicaciones



La solución ideal de gestión de puntos terminales permitiría a los desarrolladores importar y distribuir aplicaciones móviles directamente a través de una tienda de aplicaciones empresariales integrada, mejorando aún más el flujo de trabajo entre los equipos de desarrollo y operaciones.

Eligiendo un sólido cimiento de movilidad de IBM

Usted puede contar con que IBM le proporcionará una estrategia móvil de principio a fin para su organización. IBM ofrece tanto una solución de gestión de puntos terminales líder de la industria como una plataforma robusta de desarrollo de aplicaciones móviles, junto con la capacidad exclusiva de integrar ambas soluciones. IBM® Worklight®, una plataforma de desarrollo de aplicaciones móviles avanzada, abierta, integral y basada en estándares para Smartphones y Tablets, se integra fácilmente con la herramienta de gestión IBM Endpoint Manager for Mobile Devices, que permite la administración unificada de todos los dispositivos empresariales.

Worklight permite a las organizaciones de todos los tamaños desarrollar, conectar, operar y administrar en forma eficiente aplicaciones móviles y omni-canal utilizando una única plataforma integrada. Incluye un entorno de desarrollo integral, middleware de tiempo de ejecución optimizado para el entorno móvil, un centro de aplicaciones empresariales privadas y una consola integral de gestión y análisis, todo con el soporte de mecanismos de seguridad.

Endpoint Manager for Mobile Devices ofrece el control adicional que los desarrolladores necesitan durante el proceso crítico de desarrollo de aplicaciones móviles. Y con un solo clic, las organizaciones pueden pasar las aplicaciones terminadas –desarrolladas utilizando el centro de aplicaciones de la plataforma Worklight – del desarrollo a las operaciones, para su distribución a los usuarios finales a través del Endpoint Manager Enterprise Application Store.

Conclusión

El amplio conjunto de capacidades móviles que ofrece IBM ayuda a las organizaciones a aumentar su eficiencia y obtener una ventaja competitiva. En particular, la capacidad de integrar IBM Endpoint Manager for Mobile Devices e IBM Worklight permite un conjunto avanzado de capacidades de desarrollo, conectividad y gestión de aplicaciones para dar soporte –y protección– a la amplia variedad de tipos de dispositivos y aplicaciones móviles que son cada vez más comunes en las infraestructuras tecnológicas de la actualidad.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
Producido en EEUU
Marzo de 2013

1 “The World in 2011: ITC Facts and Figures,” International Telecommunication
Union (ITU),
http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf
2 “Infografía: 2012 Mobile Growth Statistics,” Trinity Digital Marketing,
July 9, 2012. http://www.digitalbuzzblog.com/infographic-2012-mobile-growth-statistics/
3 Angel, Jessy. “Is Mobile App Development Slated for Future Growth?”
Social Media Today, 18 de octubre de 2012.
http://socialmediatoday.com/jessy-angel/921151/mobile-app-development-slated-further-growth