Las mejores maneras de ampliar la administración de endpoints y la seguridad en los dispositivos móviles

Combinar la protección de endpoints y la Administración de dispositivos móviles (MDM)

Por Dana Ragsdill, gerente de productos, Quest

La administración de endpoints, ¿se extiende a la administración de sus dispositivos móviles, como teléfonos inteligentes y tabletas?

Tiene sentido que los administradores del área de TI piensen en los dispositivos móviles simplemente como otra categoría de endpoints. Al igual que los endpoints tradicionales de equipos, impresoras y dispositivos de red, los dispositivos móviles contienen datos, son vulnerables y los empleados dependen de ellos para terminar sus tareas. Pero aun cuando la mayoría de las empresas dispone de estrategias bien desarrolladas para la administración de endpoints, muchas aún no siguieron el paso lógico de migrar los dispositivos móviles para esta transformación.

En esta documentación se examinan los motivos de la incorporación de la administración de dispositivos móviles (MDM) en la administración de endpoints. Se analiza cómo los administradores del área de TI pueden ejecutar cuatro funciones administrativas: inscribir, realizar inventario, configurar y proteger, para los dispositivos móviles como lo hacen para los dispositivos tradicionales. Los lectores obtendrán un mayor conocimiento de cómo adaptar la administración de dispositivos móviles empresariales en sus estrategias existentes para la administración de endpoints.

ADMINISTRAR ENDPOINTS SIGNIFICA ADMINISTRAR DISPOSITIVOS MÓVILES

El principal argumento para migrar los dispositivos móviles a la administración de endpoints es que estos cumplen un papel fundamental para los empleados a la hora de terminar sus tareas. Eso tiene un lado positivo y un lado negativo.

Lado positivo

En las empresas inteligentes, los administradores del área de TI dan soporte a todos los dispositivos con acceso a la red, aun si los empleados tienen su propio dispositivo (BYOD). Cuando se trata de aumentar la productividad de los empleados en los dispositivos móviles, soportan las innovaciones, como la comunicación VoIP, las aplicaciones de almacenamiento en la nube, la flexibilidad del lugar de trabajo y las aplicaciones esenciales de software de la empresa. En un estudio se señala una brecha del 16 % en la productividad (que asciende a más de seis horas por semana) entre los empleados “pioneros” que usan mucho la tecnología móvil y aquellos que la usan poco.[1]

Figura 1: La administración de dispositivos móviles se extiende a la administración de endpoints.

Entonces, no sorprende que el 72 % de los profesionales en seguridad cibernética informen que la pérdida de datos es su principal preocupación en relación con BYOD.

Lado negativo

Pero ese camino hacia una mayor productividad no está completamente bordeado de rosas. Sin dudas, los dispositivos móviles son un punto de entrada para las amenazas de seguridad, lo que significa que la seguridad de los endpoints tiene que cubrir la seguridad de los dispositivos móviles. Nokia informa que, en general, las tasas de infección de dispositivos móviles creció un 63 % del primer semestre al segundo semestre de 2016, y la tasa de infección para teléfonos inteligentes en particular creció un 83 % en ese período.[2]

Entonces, no sorprende que el 72 % de los profesionales en seguridad cibernética informen que la pérdida de datos es su principal preocupación en relación con BYOD.[3] Cualquier dispositivo móvil lo suficientemente grande como para ser útil es lo suficientemente pequeño como para perderse o que lo roben con facilidad y, a pesar de las medidas contra robos integradas en los teléfonos inteligentes, los dispositivos siguen siendo irresistiblemente tentadores para los ladrones. Un dispositivo robado sin protección puede convertirse rápidamente en una puerta trasera para una red.

Si bien el simple volumen de los dispositivos móviles es abrumador, Gartner calcula que, en el año 2017, se enviarán alrededor de 1900 millones en todo el mundo[4], el mayor impacto en el área de TI es que los dispositivos móviles aportan más complejidad a la empresa. Los entornos heterogéneos del área de TI se están ampliando en todos los tipos de dispositivos y sistemas operativos. Además de las plataformas tradicionales de Chrome OS, Linux, macOS y Windows están iOS, Android y otros sistemas operativos móviles con aplicaciones y arquitectura asociadas. A su vez, pueden conducir a múltiples consolas y diferentes vistas de endpoints que tienen acceso a los recursos de red.

[1] *"Mobility, performance and engagement," The Economist, mayo de 2016, http://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf*

[2] *"Nokia Threat Intelligence Report," 2017, https://pages.nokia.com/8859.Threat.Intelligence.Report.html*

[3] *"BYOD and Mobile Security – 2016 Spotlight Report," Crowd Research Partners, marzo de 2016, http://crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf*

[4] *"Gartner Forecasts Flat Worldwide Device Shipments Until 2018," Gartner, enero de 2017, http://www.gartner.com/newsroom/id/3560517*

Quest

Cuando el movimiento para dar soporte a los dispositivos móviles genera un alboroto en cuanto a su administración sencilla y segura, el lado negativo puede opacar el lado positivo. La productividad puede aumentar para los usuarios a medida que se desploma para los administradores.

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES: CUATRO CONSIDERACIONES PRINCIPALES

La ampliación adecuada de la administración de endpoints para incluir dispositivos móviles conlleva cuatro funciones administrativas:

1. Inscribir
2. Realizar inventario
3. Configurar
4. Asegurar

En el caso de los dispositivos móviles, se aplican diferentes consideraciones y prácticas a cada una de estas funciones.

Inscribir

Primero, a diferencia de los endpoints habituales de los equipos y otros dispositivos conectados a la red, el área de TI sabe que los teléfonos inteligentes y las tabletas no ejecutan agentes. Entonces, ¿de qué manera el área de TI puede garantizar que el hardware y el software que se usan para administrar los endpoints puedan ubicar dispositivos móviles y conectarse a ellos?

La manera más simple es con una aplicación creada para el respectivo sistema operativo. Si la empresa proporciona el dispositivo, puede instalar la aplicación antes de ofrecérsela al usuario. En el caso de BYOD, el usuario debería poder instalar la aplicación sencillamente desde una tienda de aplicaciones o portal interno. En cualquiera de los casos, la inscripción uniforme y sin problemas es lo suficientemente importante a fin de garantizar que los usuarios no tengan excusas para no instalar la aplicación y que el área de TI no necesite intervenir para cada instalación.

Realizar inventario

Una vez inscritos los dispositivos, los administradores deberían poder ver e informar sobre cada dispositivo móvil conectado a la red.

En muchos entornos, los inventarios de endpoints pueden no incluir dispositivos móviles (en especial, los dispositivos de uso propio), por lo que los administradores están en desventaja de varias maneras:

- Los dispositivos móviles podrían estar accediendo a las redes inalámbricas o recursos corporativos. Cada administrador desearía la capacidad para determinar esto, y la visualización de los dispositivos en el inventario es una manera rápida y eficaz de hacerlo.
- Cada empresa debería poder responder de manera rápida y satisfactoria la pregunta “¿Cuántos dispositivos móviles tenemos y quiénes los tienen?”. Un inventario de endpoints que incluya todos los dispositivos móviles que se poseen es útil para llevar un registro.
- En el inventario completo de endpoints no solo se muestran las características tradicionales, como fabricación, modelo, versión de sistema operativo y estado de actualización, sino también los atributos específicos del dispositivo móvil, como IMEI, estado de protección y si el dispositivo se descifró.

La recopilación de esta información en un informe es fundamental ya que los administradores intentan determinar qué plataformas requieren soporte, qué dispositivos móviles no cumplen con las normas y si alguno de ellos es vulnerable.

Configurar

La administración de endpoints incluye poder configurar los dispositivos en la red. Aun en el entorno heterogéneo de múltiples sistemas operativos y propiedad mixta, los administradores en empresas inteligentes mantienen tanta homogeneidad como les sea posible dentro de las plataformas (versión de sistema operativo, parches) y en todas las plataformas (aplicaciones empresariales) por diversos motivos:

- La capacidad para configurar ayuda a los administradores a instalar certificados para acceder a los recursos corporativos.
- Los administradores pueden instalar y mantener de manera uniforme las aplicaciones o las que los empleados necesitan para hacer su trabajo.
- Pueden configurar parámetros básicos para el acceso a la red, el correo electrónico y las listas de direcciones globales.
- Las políticas rigen el acceso sobre la base de los atributos del empleado y deben aplicarse en todos los dispositivos.
- Las plataformas y las aplicaciones están programadas para obtener actualizaciones continuas que bloqueen las vulnerabilidades.
- Los administradores deberían poder establecer planes automatizados que se implementen siempre que los atributos o las circunstancias cambien, sin tener que tocar cada dispositivo.

El principal objetivo de la configuración es administrar los dispositivos móviles como otro tipo de endpoints, independientemente del fabricante.

Asegurar

Ningún dispositivo debería estar conectado a una red a menos que sea segura. Las mismas características de administración de endpoints que aplican las políticas de seguridad, como la solicitud de un código de acceso, deberían extenderse a cualquier dispositivo móvil que necesite obtener acceso a los recursos corporativos.

> Cada empresa debe poder responder a la pregunta “¿Cuántos dispositivos móviles tenemos y quiénes los tienen?”.

Claro, algunas políticas solo funcionan con dispositivos móviles de propiedad de la empresa. Los usuarios tienen menos probabilidades de permitir la instalación de software innecesario en un dispositivo propio y están menos inclinados a arriesgar el acceso corporativo a los datos personales del dispositivo. Pero, si las circunstancias lo permiten, los administradores deben mantener el privilegio de bloquear un dispositivo, limpiarlo de manera remota, ubicar un dispositivo perdido y restablecerlo a la configuración de fábrica, a fin de proteger los datos y los activos de la empresa. La administración de endpoints debe permitir que MDM esté a ese nivel.

Los administradores deben mantener el privilegio de bloquear un dispositivo, limpiarlo de manera remota, ubicar un dispositivo perdido y restablecerlo a la configuración de fábrica, a fin de proteger los datos y los activos de la empresa.

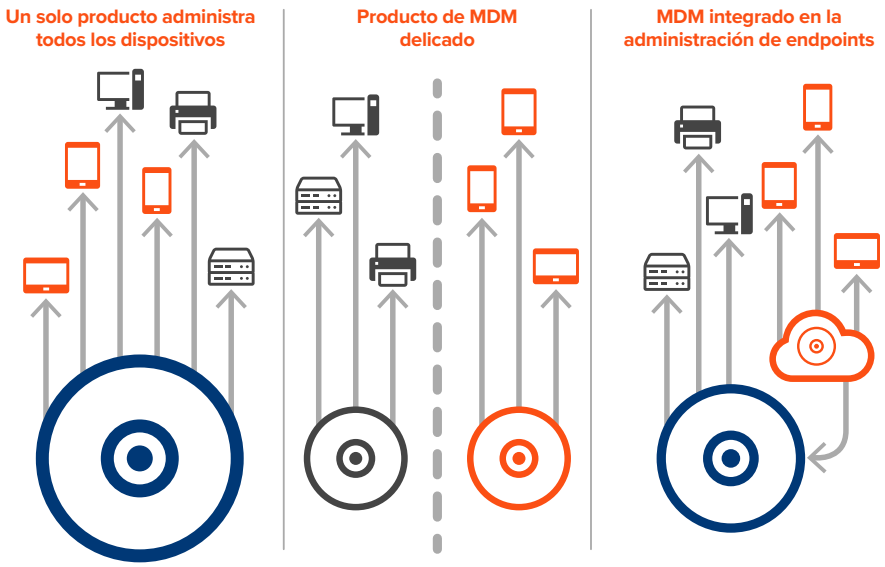

Figura 2: Tres opciones para la administración de MDM

ADAPTAR LA MDM A LA ADMINISTRACIÓN DE ENDPOINTS EXISTENTE

Dada la necesidad de ampliar la administración de endpoints a la MDM, las empresas están frente a tres opciones:

1. La opción ideal sería un solo producto para administrar todos los dispositivos en cualquier parte de la red. Los dispositivos de este tipo son raros, grandes, complejos e incómodos.
2. En el otro extremo del espectro se encuentra la opción menos deseable de un producto de MDM específico. Inscribiría, realizaría inventario, configuraría y protegería todos los dispositivos móviles perfectamente, pero los administraría específicamente como dispositivos móviles y no de manera amplia como endpoints, y estaría integrado y separado del sistema de administración de endpoints existente.
3. El medio ideal es un producto diseñado para integrarse en un sistema de administración de endpoints tradicional que adapte la MDM a la administración de endpoints completa.

En la tercera opción, el nivel más bajo de integración permitiría el inventario desde una sola consola. El siguiente nivel permitiría el inventario y el control de los dispositivos desde una sola consola. El mayor nivel de integración permitiría a la empresa adquirir cualquier cantidad de dispositivos móviles necesaria para administrar de manera separada de los dispositivos tradicionales. Pero, permitiría el conjunto completo de funciones de inscripción, inventario, configuración y protección mediante una única consola, lo que aumentaría la productividad de los administradores del área de TI.

El nivel más alto se aplica a todos los endpoints: equipos, equipos portátiles, teléfonos inteligentes, tabletas, servidores, impresoras y dispositivos de red. La administración de endpoints completa bloquea las vulnerabilidades que ponen en peligro la seguridad y preocupan a los administradores del área de TI.

ACERCA DE CLOUD MOBILE DEVICE MANAGER DE KACE

ConCloud Mobile Device Manager de KACE, los administradores del área de TI pueden proteger su red de las amenazas de BYOD y seguridad móvil. Pueden inscribir, realizar inventario, configurar y proteger los dispositivos móviles en la mayoría de las plataformas comunes. El producto alojado en SaaS permite a los administradores realizar inventario, administrar contraseñas y ubicar, borrar y restablecer dispositivos móviles de manera sencilla.

Cloud Mobile Device Manager de KACE, que está integrado en el Dispositivo de administración de sistemas KACE, ofrece un inventario integral de todos los endpoints de la red, tradicionales y móviles, desde una única consola. Esto ayuda a los clientes a migrar sin problemas a una administración de endpoints unificada de todos los dispositivos utilizados por los empleados.

ACERCA DE QUEST

Quest ayuda a nuestros clientes con la reducción de las tediosas tareas de administración, a fin de que usted pueda centrarse en la innovación necesaria para que su empresa crezca. Las soluciones de Quest® son escalables, rentables y simples de usar, y proporcionan eficiencia y productividad inigualables. Además de la invitación de Quest para que la comunidad global participe de esta innovación y de nuestro firme compromiso para garantizar la satisfacción del cliente, Quest continuará con la aceleración de la entrega de las soluciones más integrales para la administración de la nube de Azure, SaaS, seguridad, movilidad del personal e información impulsada por datos.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Visite nuestro sitio web (https://www.quest.com/mx-es) para obtener información sobre nuestras oficinas regionales e internacionales.