DOCUMENTO TÉCNICO: FEBRERO DE 2017

CINCO PASOS CRUCIALES PARA MODERNIZAR SU ENTORNO DE WINDOWS

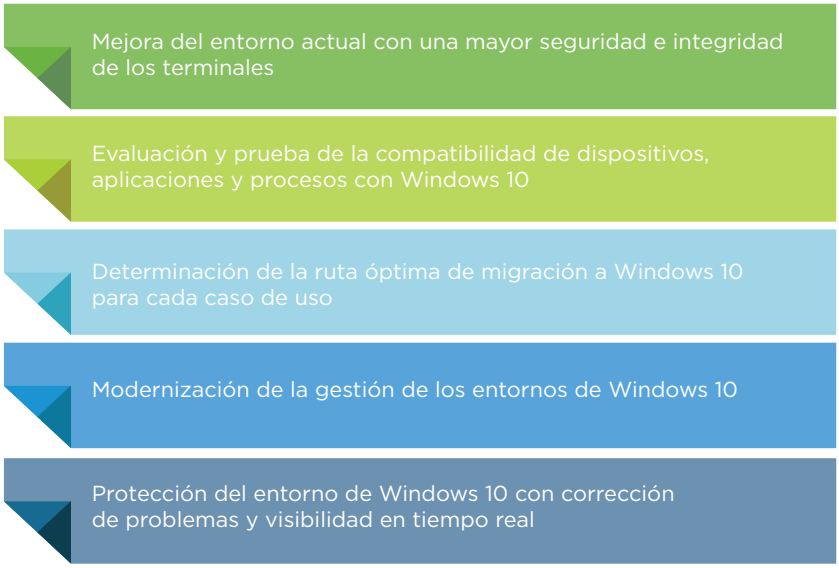
Guía para sacar el máximo partido de sus inversiones existentes en Windows y facilitar su transición a Windows 10 para implementaciones físicas y virtuales.

vmware®

El mundo funciona con Windows

Existen más de 1500 millones de dispositivos que ejecutan Windows*. En los últimos 30 años, la mayoría de las organizaciones de todo el mundo han adoptado Windows como estándar y han realizado inversiones significativas en sus entornos de Microsoft, en conceptos como licencias, configuración, servicios profesionales e infraestructura para Active Directory, Microsoft Exchange, gestión del ciclo de vida del PC, etc. Microsoft también continúa desarrollando soluciones para ayudar a las organizaciones a realizar la transición a la cloud con productos como Microsoft Office 365 y Azure Active Directory, y con la creación de un moderno marco de gestión de la cloud móvil en Windows 10.

Al mismo tiempo, de manera generalizada los departamentos de TI reciben una presión constante para reducir los costes, a la vez que, de algún modo, refuerzan la seguridad y aumentan la productividad de los empleados con la tecnología más avanzada. Windows 10 presenta una experiencia mejor para los usuarios y oportunidades para que los equipos de TI adopten un enfoque de gestión y seguridad radicalmente diferente que alivie sus cargas. Sin embargo, para optimizar y aprovechar realmente al máximo su entorno de Windows, las organizaciones necesitan implementar las medidas siguientes:



En este documento, se explican los cinco pasos que pueden dar las organizaciones para optimizar sus inversiones existentes en Windows y se describe cómo pueden adoptar soluciones modernas de gestión y seguridad en su transición hacia Windows 10.

Paso 1: Ajustar el entorno de Windows para dotarlo de un mayor recorrido

Los propietarios responsables de automóviles realizan ajustes para inspeccionar, reparar o sustituir bujías, filtros de aire y otras piezas que no funcionan a pleno rendimiento. A veces se utilizan soluciones complementarias, como cambiar a un aceite de larga duración o usar un aditivo para el combustible que sirva para eliminar la acumulación de carbonilla en los conductos de combustible. Al hacerlo, obtienen un vehículo más eficiente y de mayor duración.

¿Cuándo fue la última vez que ajustó su entorno de Windows? El primer paso para conseguir un entorno de Windows moderno es mejorar los procesos, la tecnología y los informes existentes para facilitar su trabajo y el de sus usuarios finales. ¿Sabe cuántas máquinas de su flota han implementado con éxito el parche que envió el martes pasado? ¿Sabe cuántos usuarios ejecutan una aplicación que carece de una actualización esencial de seguridad? ¿Ha estudiado las innovaciones en el campo de los teléfonos móviles y las tabletas que podrían facilitar su trabajo con los ordenadores?

- ¿Cuándo fue la última vez que ajustó su entorno de Windows?
- ¿Sabe cuántas máquinas de su flota han implementado con éxito el parche que envió el martes pasado?
- ¿Sabe cuántos usuarios ejecutan una aplicación que carece de una actualización esencial de seguridad?
- ¿Ha estudiado las innovaciones en el campo de los teléfonos móviles y las tabletas que podrían facilitar su trabajo con los ordenadores?

Los comentarios que escuchamos de los clientes son siempre los mismos. Los usuarios quieren ser productivos en cualquier lugar y con cualquier dispositivo. Suelen acceder a los recursos corporativos desde fuera de la red con diversos tipos de dispositivos, lo que aumenta el número de vectores de amenazas para la organización. El departamento de TI necesita visibilidad en tiempo real del entorno de Windows para saber qué dispositivos no están actualizados con los parches más recientes y cuáles ejecutan aplicaciones sin firmar o versiones antiguas de dependencias de aplicaciones (como Java o .NET) que exponen el dispositivo y la red corporativa a posibles ataques. Necesita tener la capacidad de realizar acciones basadas en esa información, como implementar un parche, eliminar un proceso no autorizado o realizar un borrado remoto de un dispositivo que plantea una amenaza de seguridad.

Visibilidad y seguridad del entorno en tiempo real

Imagine que pudiera tener visibilidad completa de todos sus terminales en 15 segundos o menos. Imagine que escribe una pregunta sencilla en inglés como lo haría en Google para consultar todo su entorno, que obtiene los resultados en segundos (incluso para millones de terminales) y que es capaz de recopilar información importante y actuar sobre ella al momento. Ahora es posible. VMware® funciona con las versiones de escritorio y de servidor de Windows 7, 8.1 y 10, ya sean virtuales o físicas, y le permite:

- Identificar y controlar los puntos de acceso no gestionados
- Detectar amenazas avanzadas en millones de terminales en unos segundos
- Corregir rápidamente las deficiencias de los terminales comprometidos según las necesidades
- Restaurar una imagen maestra en los terminales de Windows comprometidos

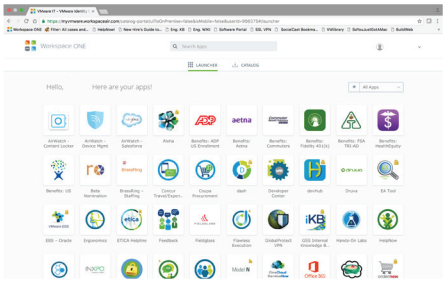
La plataforma se extiende por toda la organización para proteger los terminales, ofrecer visibilidad del inventario de software activo y la utilización de recursos detallada al personal de operaciones de TI, y distribuir aplicaciones y parches según las necesidades. A medida que los clientes planifican el paso a Windows 10, VMware les permite obtener información acerca del entorno existente para solucionar cualquier problema y agilizar la transición a dicho sistema.

VMware también proporciona a los clientes una forma moderna de proteger y gestionar dispositivos móviles, terminales de Windows y servidores. La integración con el ecosistema de VMware se traduce en una mayor conformidad, una contención de amenazas más rápida y acciones de corrección personalizables que se ajustan a los niveles de amenaza mediante políticas de configuración y gestión dinámicas.

Por ejemplo, puede utilizar VMware para ejecutar consultas con el fin de detectar terminales que no cumplen los requisitos de conformidad y, a continuación, poner en cuarentena esos dispositivos. Una vez que la amenaza está controlada, VMware puede informar a los usuarios finales sobre la vulneración de la conformidad y los administradores de TI pueden implementar la corrección necesaria para que los terminales la recuperen.

Configuración inalámbrica y catálogo de aplicaciones consolidado

¿Recuerda la última vez que recibió una llamada telefónica de un ejecutivo que estaba de viaje y que había «perdido» su portátil? Con suerte, tendría activado el cifrado de BitLocker ya que, de lo contrario, la información confidencial de la empresa podría haberse filtrado y no habría nada que hacer para evitarlo. Sin embargo, si hubiera implementado la gestión unificada de terminales (UEM), podría haber realizado un borrado remoto para evitar la pérdida de datos.



Las soluciones de gestión de la movilidad empresarial (EMM) dan a las organizaciones la capacidad de configurar una red Wi-Fi, configurar una red VPN, acceder a una tienda de aplicaciones empresariales consolidada y realizar un borrado remoto en iOS, Android y otros sistemas operativos móviles. Al implementar soluciones de EMM compatibles con los entornos tradicionales de Windows, las organizaciones pueden complementar las herramientas de gestión del ciclo de vida del PC empleando las mismas funcionalidades de los sistemas operativos móviles para ofrecer a los usuarios una experiencia mejor, aumentar la seguridad y ahorrar tiempo al equipo de TI.

Soporte para trabajadores remotos e implementación de aplicaciones mediante la virtualización

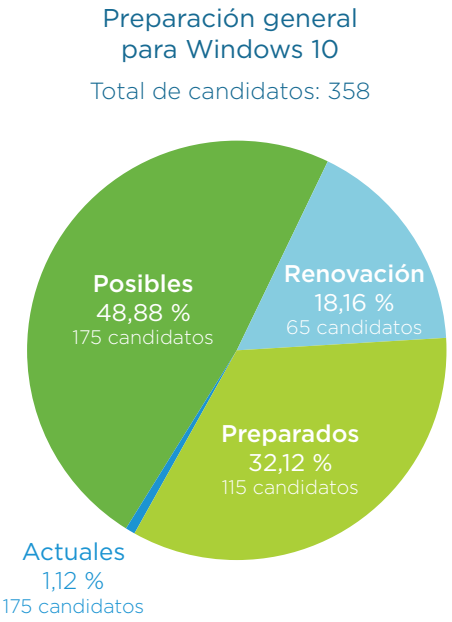
¿Cuándo fue la última vez que evaluó las necesidades y los casos de uso de los usuarios finales? Es posible que tenga algunos grupos de usuarios de escritorios virtuales para los escenarios más comunes, como centros de llamadas y desarrolladores remotos, pero ¿ha pensado en otras formas de extender los recursos a sus empleados, trabajadores externos y partners? Con la virtualización de escritorios y aplicaciones, puede proporcionar recursos que los usuarios necesitan para trabajar en su dispositivo personal o en cualquier dispositivo. Algunas de sus aplicaciones pueden requerir un sistema operativo, un navegador o una versión de un complemento en concreto, por lo que se deben virtualizar para que puedan ejecutarse de forma independiente del sistema operativo de los usuarios.

VMware le permite implementar escritorios virtuales de forma centralizada según las necesidades, adoptar el uso de dispositivos personales en el trabajo y eliminar el tiempo de inactividad debido a terminales perdidos o dañados, así como mejorar la seguridad al mantener los datos seguros y protegidos en el centro de datos y mejorar los resultados al evitar actualizaciones de hardware o al reducir los costes de los terminales. De este modo, se obtiene una estrategia en materia de informática para el usuario final simplificada, segura y escalable.

Descubra un nuevo universo en su transición a Windows 10

Se ha dicho que si Henry Ford hubiera preguntado a sus clientes que querían, habrían respondido: caballos más rápidos. El automóvil de Ford cambió el transporte abordando el problema de una forma totalmente distinta. Del mismo modo, Windows 10 representa un cambio drástico con respecto a sus predecesores a la hora de redefinir el modo en que el departamento de TI gestiona todo el ciclo de vida de ordenadores, teléfonos móviles, tabletas y de cualquier otro terminal que ejecute el último sistema operativo de Microsoft.

Antes del lanzamiento de Windows 10, los departamentos de TI tenían que enfocar el entorno como si se tratase de una visita a un centro comercial: juntar tecnologías dispares que no funcionan bien juntas para abordar diversos desafíos relacionados con la configuración, la distribución de software, la aplicación de parches, los programas maliciosos y la seguridad.



Con Windows 10, Microsoft ha introducido una posibilidad nueva que funciona como un sitio de comercio electrónico: es cómodo, la tecnología funciona bien en conjunto y crea nuevas oportunidades que no existían antes. Tras hablar con cientos de clientes que han migrado a Windows 10 o están diseñando sus implementaciones, hemos descubierto que, después de mejorar la seguridad de los entornos actuales, existen otros cuatro pasos fundamentales en la transición hacia una implementación correcta de Windows 10:

Evaluación ▶ Migración ▶ Gestión ▶ Protección

Paso 2: Evaluar el entorno actual para eliminar las conjeturas relacionadas con las implementaciones físicas y virtuales

Muchas organizaciones tienen dificultades para saber por dónde comenzar la transición hacia Windows 10: desde saber cuáles de sus máquinas pueden ejecutar Windows 10 hasta qué casos de uso podrían ser más adecuados para la virtualización de escritorios, pasando por muchas otras. Con la herramienta de evaluación de escritorios adecuada, las organizaciones pueden recibir recomendaciones inteligentes sobre qué máquinas y casos de uso son más adecuados para una migración física in situ a Windows 10 y cuáles son más adecuados para ejecutar un escritorio virtual local o desde la cloud. Esto le proporciona información de referencia sobre su entorno para determinar cómo debe abordar la migración a Windows 10. Para obtener más información sobre la herramienta de evaluación, visite assessment.vmware.com.

Al igual que con las actualizaciones anteriores a versiones nuevas de Windows, los administradores de TI responsables de los entornos de escritorios virtuales o físicos tendrán que probar las aplicaciones para detectar cualquier problema de compatibilidad antes de migrar su flota a Windows 10. Si las aplicaciones no se ejecutan en Windows 10, el departamento de TI puede implementarlas como aplicaciones virtuales para que sigan funcionando después de la migración a Windows 10 y los usuarios puedan seguir haciendo su trabajo. Las aplicaciones heredadas como Internet Explorer 6 son un ejemplo de esto.

Paso 3: Determinar el plan de migración para las máquinas virtuales y físicas

Según Microsoft, el 96 por ciento de las empresas están poniendo en marcha proyectos piloto de Windows 10. Sin embargo, muchas todavía están diseñando sus planes para la migración. Hay varias preguntas que hacemos a los clientes como punto de referencia para guiar su transición hacia Windows 10:

- ¿Tiene previsto adoptar Windows 10 durante los próximos tres o cuatro años a medida que vaya renovando sus PC?
- ¿Está planificando hacer una migración de todas las máquinas actuales in situ o mediante imágenes personalizadas?
- ¿Tiene previsto virtualizar los terminales que no son compatibles con Windows 10?
- ¿Tiene en su empresa casos de uso para los que los escritorios y las aplicaciones virtuales resultan eficientes?
- ¿Está planificando una combinación de todo lo anterior?

Cada organización tiene que determinar la vía de migración que mejor se adapta a sus necesidades, pero estas son algunas de las maneras en que las ayudamos a enfocar su vía de migración:

Renovación

Durante el proceso de renovación de dispositivos que tendrá lugar los próximos tres o cuatro años, las organizaciones efectuarán la transición a Windows 10 y gestionarán cualquier dispositivo nuevo con el moderno marco de gestión unificada de terminales (UEM) que les permite optimizar los procesos de TI, reducir los costes de gestión y ofrecer una experiencia de usuario final excelente.

Migración

- In situ: las organizaciones utilizan las herramientas de migración in situ para migrar las máquinas desde versiones anteriores del sistema operativo hasta la imagen base de Windows 10 y aprovisionan las políticas y aplicaciones recomendadas por la empresa utilizando la solución UEM.
- Imagen personalizada: en lugar de la imagen base del sistema operativo, las organizaciones también pueden migrar a una imagen recomendada por la empresa con aplicaciones y datos personalizados y realizar automáticamente el registro en la gestión mediante UEM.

Virtualización

- Las aplicaciones y los escritorios virtuales se actualizan de forma centralizada y se entregan a los usuarios finales en sus dispositivos. Esto permite abordar varios casos de uso, como por ejemplo:
  - Las máquinas actuales que no son compatibles con Windows 10 reciben un escritorio virtual
  - Las organizaciones valoran los escritorios virtuales para una situación en la que haya ordenadores portátiles propiedad de los empleados
  - Las aplicaciones esenciales que no son compatibles con Windows 10 se virtualizan
  - Las organizaciones crean un aislamiento de Internet o de datos para implementaciones sensibles en cuanto a la seguridad

Paso 4: Evaluar UEM para las máquinas físicas en el nuevo marco de Windows

Los procesos tradicionales de creación de la imagen, configuración e instalación de un PC físico pueden llevar varias horas. Con el tiempo, los residuos de las aplicaciones y del registro entorpecen el rendimiento del sistema causando discrepancias entre imágenes, lo que produce problemas de rendimiento para el usuario final y a menudo requiere que el equipo de TI pase varias horas creando de nuevo las imágenes de los dispositivos y molestando a los usuarios.

La mayoría de las organizaciones utilizan las herramientas de gestión del ciclo de vida del PC con cientos de GPO, scripts personalizados y otras herramientas improvisadas para gestionar su entorno de Windows. Lamentablemente, las herramientas de PCLM heredadas tienen varias limitaciones, como la incapacidad de realizar acciones en dispositivos situados fuera del dominio y de la red de la empresa, el mantenimiento de una infraestructura costosa y los procesos laboriosos tales como la creación de imágenes y otros.

Lo bueno de los teléfonos móviles modernos es que se puede entrar en una tienda, comprar un dispositivo, introducir las credenciales y, a continuación, acceder automáticamente a todas las aplicaciones y servicios propios, de forma inalámbrica y en cuestión de minutos. ¿Por qué los usuarios de PC no pueden tener la misma experiencia de usuario? Con Windows 10 sí que es posible. Cuando se utiliza Windows 10 junto con una solución UEM, las organizaciones disponen de una nueva forma de gestionar su flota de ordenadores de escritorio y ofrecer una experiencia de usuario similar a la que se obtiene con los teléfonos móviles y las tabletas. Solo tiene que introducir su correo electrónico del trabajo y su contraseña, y el dispositivo se configurará en minutos de forma inalámbrica con todas las aplicaciones, políticas corporativas y servicios necesarios para realizar el trabajo. Este nuevo enfoque redefine la forma en que el equipo de TI gestiona todo el ciclo de vida de los ordenadores, teléfonos móviles, tabletas y cualquier otro terminal de forma uniforme y desde una consola unificada.

Moderna gestión y seguridad de Windows que dan prioridad a la cloud

Ya no es necesario emplear horas en crear una imagen de cada máquina. Ya no habrá mas ciclos regulares de aplicación de parches ni será imposible realizar acciones con usuarios situados fuera de la empresa. Al implementar UEM en equipos con Windows 10, el departamento de TI tiene más tiempo para centrarse en el soporte de la empresa y tiene un entorno mucho más seguro. Los usuarios obtienen un catálogo de aplicaciones unificado en su ordenador con Windows 10, su tableta y su teléfono móvil, y tienen un portal de autoservicio para abordar problemas comunes en lugar de consumir el tiempo del equipo de TI.

Paso 5: Reforzar la seguridad mediante la visibilidad del entorno en tiempo real

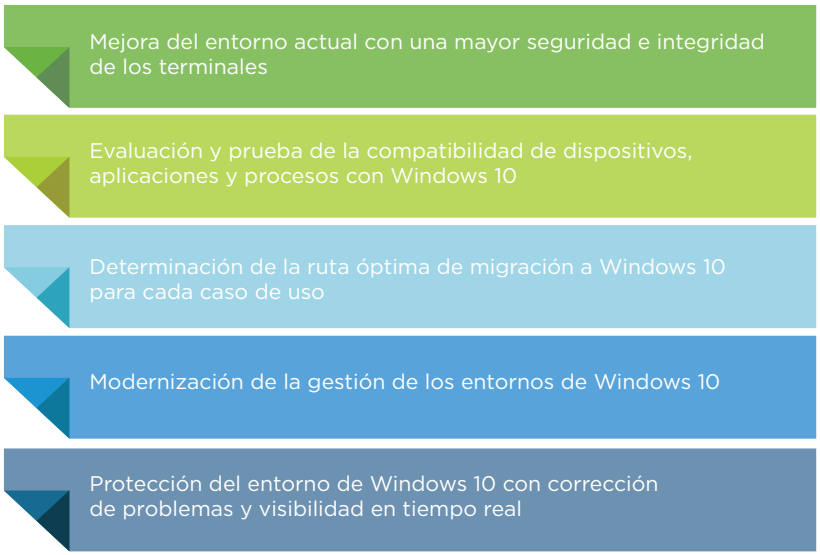
Andrew Grove, cofundador y antiguo director ejecutivo de Intel Corporation, vivió de acuerdo con un lema sencillo: Solo sobreviven los paranoicos. Este mismo principio que guió el éxito de Intel debe ser el mantra de todos los que trabajan en TI. En el pasado, las organizaciones tenían un entorno operativo estándar: un único tipo de dispositivo que ejecutaba un sistema operativo con un conjunto de aplicaciones aprobadas previamente en una red específica. Ahora, el departamento de TI debe gestionar diversos tipos de sistemas operativos que se ejecutan en todo tipo de dispositivos con combinaciones únicas de aplicaciones que funcionan dentro o fuera de la red de la empresa.

Ante la necesidad de gestionar este entorno operativo dinámico y combatir una creciente gama de ciberataques, el departamento de TI se ha visto obligado a adoptar un modelo de confianza cero para proteger los datos corporativos. VMware permite que el departamento de TI pueda reforzar el sistema operativo permitiendo las autenticaciones sin contraseña, evitando el uso de aplicaciones no autorizadas y sin firmar, supervisando los dispositivos con vulnerabilidades y realizando acciones de corrección automatizadas sin necesidad de tiques de incidencias de TI. Estas acciones pueden ser, por ejemplo, restringir al instante el acceso a los recursos del trabajo cuando se determina que un sistema operativo está en peligro o incluso enviar un comando de borrado a distancia cuando un dispositivo se pierde o ha sido robado. VMware también ofrece las prestaciones mencionadas anteriormente relacionadas con la visibilidad en tiempo real y la seguridad de los dispositivos que ejecutan Windows 10.

Para obtener más información sobre cómo VMware puede ayudar a modernizar su entorno de Windows y sacar más provecho de sus inversiones en productos de Microsoft, visite www.WindowsUEM.com/es

Obtenga más valor de su entorno

Solo hemos dado una idea superficial de lo que es posible hacer con VMware para obtener más valor de sus inversiones en Microsoft. Cuando se plantee complementar su entorno actual con funciones adicionales y cuando realice la transición a Windows 10, tenga en cuenta este breve resumen de las cinco formas principales en las que VMware puede respaldar sus iniciativas:



Además de realizar las implementaciones de Windows, también puede que invierta en otros productos de Microsoft, como Office 365, Azure Active Directory, etc. Las soluciones de informática de usuario final de VMware pueden permitirle implementar y configurar con mayor facilidad aplicaciones y servicios de Office y conectar sus credenciales y políticas de Active Directory para obtener la identidad federada y el inicio de sesión único en sus aplicaciones.

1500 millones de dispositivos: http://www.computerworld.com/article/2919104/windows-pcs/where-will-microsoft-find-1-billion-devices-for-windows-10.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel +34 914125000 Fax +34 914125001 www.vmware.es