RESUMEN EJECUTIVO

Modernizar la gestión y la seguridad de Windows 10 mediante la gestión unificada de terminales de VMware AirWatch

Necesidades en constante evolución del lugar de trabajo moderno

LA EVOLUCIÓN de los empleados de hoy en día los hace más móviles y autosuficientes que nunca. El uso de dispositivos móviles es cada vez mayor, y los empleados se sirven de una serie de aplicaciones, dispositivos y servicios basados en la cloud. Cada vez son más los que eligen realizar tareas tanto personales como profesionales en el mismo dispositivo, y esperan capacidad de elección y autoservicio, además de privacidad. El hecho de que el departamento de TI no responda a estas expectativas da lugar a una experiencia de uso deficiente que desmotiva a los empleados y fomenta el creciente uso de soluciones de TI en la sombra.

Además, la propia organización de TI queda en su mayoría dividida en silos entre los ámbitos de la gestión de escritorios y los dispositivos móviles. Los equipos de TI han abordado la gestión de dispositivos móviles con modernas soluciones de gestión de la movilidad empresarial (EMM). Sin embargo, los dispositivos de escritorio se han gestionado por separado hasta ahora mediante herramientas tradicionales de gestión del ciclo de vida del PC (PCLM).

Este modelo de gestión fragmentada no cumple de forma suficiente las expectativas de seguridad y costes del departamento de TI. Dado que los usuarios ya no están limitados a un espacio físico, y que las herramientas de PCLM tradicionales requieren que los dispositivos se incorporen a la red y el dominio corporativos para recibir políticas de TI y actualizaciones de parches del sistema operativo, se incrementan tanto el riesgo de incumplimiento como las posibles vías de ataque a la seguridad.

La respuesta a estas demandas de los empleados modernos empieza con la eliminación de los silos de gestión y la consecución de un enfoque de gestión uniforme y centrado en el usuario en todos los terminales. Según Chris Silver, analista de Gartner, «El futuro de la gestión de terminales reside en la consolidación de herramientas de gestión que sirvan para los PC tradicionales y los dispositivos móviles, con el desarrollo entre ambos un marco de gestión común».

La introducción de los protocolos de gestión de dispositivos móviles en Windows 10 ofrece al departamento de TI la oportunidad de unir los equipos de gestión de TI y consolidar las herramientas, reducir los costes, aumentar la eficiencia y reforzar la seguridad de la empresa. Ahora, la empresa puede optimizar la gestión de los dispositivos de usuario gracias a la implementación de una solución de gestión unificada de terminales (UEM) para gestionar tanto los escritorios como los dispositivos móviles.

LIMITACIONES DEL ENFOQUE DE GESTIÓN TRADICIONAL DE LOS PC

El objetivo principal de las organizaciones de TI debe ser proporcionar experiencias satisfactorias a los usuarios finales para que sean más eficaces y productivos. Sin embargo, las experiencias de usuario en relación con los dispositivos móviles y los PC son polos opuestos en muchos aspectos. Mientras que el proceso de implementar y configurar un dispositivo móvil es ya un proceso eficiente y en autoservicio, la implementación de un equipo de escritorio o portátil puede llevar varias semanas, además de las incontables horas de creación de imágenes, configuración y mantenimiento.

Los usuarios sienten cada vez más frustración ante el hecho de que la gestión y la configuración de los dispositivos móviles se vea optimizada mientras que la configuración de los PC sigue siendo un proceso lento y restrictivo

¿Qué es lo que debe cambiar?

1 El sistema operativo

Lo primero que debe evolucionar es el sistema operativo Windows, que tiene que adaptarse a los requisitos de los empleados actuales. Windows 10 presenta un sistema operativo centrado en el usuario con características que permiten la elección, privacidad y movilidad de los usuarios. Más significativa es la introducción de un enfoque fundamentalmente diferente para la seguridad y la gestión del sistema operativo, que esté más en consonancia con las soluciones modernas de EMM. El conjunto unificado de protocolos de gestión en PC, tabletas y teléfonos de Windows 10 permite que ahora el equipo de TI pueda consolidar las herramientas de gestión, aprovisionar dispositivos de forma inmediata y distribuir políticas y aplicaciones por vía inalámbrica para que los usuarios puedan empezar a trabajar al instante.

2 Las herramientas de gestión

Las herramientas tradicionales de gestión de PC no pueden abordar con eficacia los requisitos de los empleados de hoy en día, que esperan poder trabajar en cualquier lugar, en cualquier momento y desde cualquier dispositivo. Cuando acceden a las aplicaciones y los datos corporativos, los usuarios esperan obtener una experiencia similar en todos sus dispositivos. Satisfacer estas expectativas es cada vez más complicado para aquellos equipos de TI que siguen haciendo uso de herramientas tradicionales para gestionar los PC, ya que estas son:

- **Costosas**: los enfoques de gestión de PC tradicionales sobrecargan el servidor y son laboriosos; requieren varias soluciones de software y se basan en complejos métodos de gestión de imágenes y configuración. La gestión de los paquetes de software y los parches del sistema operativo es un proceso tedioso, y los equipos de TI se enfrentan a la necesidad de desarrollar y mantener competencias internas en los silos de gestión de escritorios y dispositivos móviles.

- **Poco seguras**: se gestionan principalmente mediante objetos de política de grupo (GPO), que solo son viables para dispositivos conectados a la red o al dominio. Con este enfoque, completar las políticas de seguridad, los parches del sistema operativo y las actualizaciones de aplicaciones podría llevar semanas o incluso meses, lo que puede exponer a la empresa a mayores riesgos de seguridad. Debido a que se siguen apareciendo a diario nuevas vías de ataque, resulta cada vez más difícil para los equipos de TI obtener una visibilidad adecuada del estado y la conformidad de los terminales.

- **Restrictivas**: los enfoques tradicionales resultan muy frustrantes para los usuarios, ya que restringen el control que estos tienen sobre sus dispositivos. Para aumentar la seguridad, el departamento de TI debe limitar los tipos de dispositivos y bloquear el sistema operativo únicamente con aplicaciones y actualizaciones de confianza. Esto ofrece poco margen para la personalización, y los usuarios disponen de pocas funciones de autoservicio, o incluso ninguna. Estas restricciones dan lugar a un alto grado de interacción por parte del equipo de TI y a un mayor número de llamadas al servicio de soporte técnico, incluso para tareas sencillas como instalar una aplicación en el dispositivo.

EL COMIENZO DE LA GESTIÓN UNIFICADA DE TERMINALES

La introducción de las API de gestión de la movilidad en Windows 10 cambia drásticamente el modo en que las organizaciones gestionan sus terminales de PC. Sin embargo, a diferencia de iOS y Android, los PC presentan varios desafíos únicos, como:

- La necesidad de admitir scripts y GPO complejos
- El empaquetado y la distribución de aplicaciones clásicas de Windows (Win32)
- La comprobación de los parches del sistema operativo antes de que estén disponibles para los usuarios
- El inmenso tamaño de esas aplicaciones y actualizaciones, que provoca restricciones en la red

Las organizaciones necesitan una plataforma de gestión unificada de terminales que combine, por un lado, la eficiencia del equipo de TI y el usuario final que se da con la EMM en los dispositivos móviles, y por otro, los requisitos detallados de la gestión de PC tradicional.

La gestión unificada de terminales de VMware AirWatch incorpora un conjunto completo de funciones de Windows 10 que permiten la implementación del sistema operativo, la configuración, la distribución de aplicaciones (incluidas las aplicaciones Win32) y actualizaciones, y la seguridad integral. La adopción de un enfoque moderno que dé prioridad a la cloud reduce los costes y la carga de trabajo del equipo de TI, y facilita una implementación y gestión de Windows 10 más sencillas y seguras. Esto permite a las organizaciones:

- Pasar de un proceso costoso de creación de imágenes a un modelo de implementación más sencillo
- Admitir la aplicación de parches del sistema operativo y la distribución de software para dispositivos situados fuera del dominio y en cualquier red
- Proporcionar a los usuarios acceso en régimen de autoservicio y capacidad de elección de características, dispositivos y aplicaciones
- Establecer la coexistencia de datos personales y empresariales en los dispositivos
- Posibilitar una visibilidad, seguridad y conformidad instantáneas para todos los terminales, tanto dentro como fuera de la red

Con la gestión unificada de terminales de AirWatch, la gestión de Windows también se puede adaptar a cualquier caso de uso, como:

- Implementar Windows 10 para trabajadores remotos
- Incorporar equipos personales de los empleados

La UEM de AirWatch ofrece una gestión de dispositivos más sencilla, más segura y más rentable

- Llevar a cabo implementaciones corporativas en todas las sucursales
- Gestionar un terminal especial para la unidad de negocio

IMPLEMENTAR UNA GESTIÓN Y UNA SEGURIDAD DE WINDOWS QUE DAN PRIORIDAD A LA CLOUD

MDM para Windows

AirWatch admite flujos de trabajo de registro de dispositivos uniformes y adecuados para diversos casos de uso, como dispositivos propiedad de la empresa o personales, conectados a un dominio, nuevos o existentes. Con AirWatch, un dispositivo de OEM genérico puede transformarse totalmente para prepararlo para un estado de confianza de manera inmediata, sin la necesidad de crear imágenes, lo que ahorra tiempo y dinero al departamento de TI. Además de los flujos de trabajo aptos para el entorno de TI, AirWatch también ofrece a los usuarios finales una integración intuitiva y de autoservicio de los dispositivos.

Para los usuarios o trabajadores externos que utilizan dispositivos personales en el trabajo, AirWatch también ofrece un registro reforzado en la gestión basado en la confidencialidad de las aplicaciones y los requisitos de seguridad. Por ejemplo, el acceso a las aplicaciones de productividad básicas puede concederse a través de un catálogo de aplicaciones de la empresa personalizado en función de la identidad y los derechos del usuario; sin embargo, el acceso a las aplicaciones que contengan datos confidenciales de la empresa solo será posible si el dispositivo se gestiona por completo con AirWatch.

AirWatch puede gestionar dispositivos Windows integrados por medio de este moderno marco de cloud móvil, así como configurar políticas al instante de forma inalámbrica. Con cada actualización de Windows 10, Microsoft amplía de forma constante el conjunto de protocolos de gestión común disponible para los proveedores de EMM. Esto hace que la gestión se asemeje más a los perfiles de usuario y los ajustes que vemos hoy en día en los dispositivos móviles. Por ejemplo, el uso obligatorio de códigos de acceso, la configuración del correo electrónico, la habilitación del acceso a las redes wifi y VPN corporativas y la imposición de restricciones para dispositivos y aplicaciones tienen como objetivo simplificar la configuración del sistema operativo y mejorar la seguridad.

Gestión de la configuración

Al gestionar ordenadores con Windows, el equipo de TI se enfrenta a menudo a requisitos de automatización complejos, que implican la distribución de scripts complejos, políticas de GPO y otros ajustes de la gestión de PC tradicional. Por ejemplo, puede haber empresas que quieran incluir la imagen de su marca en los escritorios con un fondo de pantalla personalizado, eliminar las aplicaciones preinstaladas y definir las políticas de cortafuegos y antivirus. Las prestaciones de gestión de la configuración en AirWatch permiten al departamento de TI crear «productos» que incluyan estos archivos, aplicaciones o ajustes personalizados. Dichos productos se pueden distribuir a los dispositivos de forma instantánea a través de cualquier red; también pueden asociarse a una secuencia de tareas y condiciones de instalación más compleja.

Gestión de parches del sistema operativo

Con Windows Update como servicio, Microsoft está impulsando las actualizaciones acumuladas del sistema operativo de forma inalámbrica. Las actualizaciones que han pasado por un amplio ciclo de pruebas están disponibles como una sección de mantenimiento preparada para la empresa. A pesar de las ventajas que supone este modelo de distribución en la cloud y de prestación de servicios, los equipos de TI todavía temen perder el control sobre:

- Las actualizaciones que se distribuyen

Wifi | VPN | Certificados | Correo electrónico | Códigos de acceso | Conformidad y restricciones | Cifrado | Cortafuegos y antivirus | Gestión de licencias del SO

AirWatch simplifica la configuración y la gestión de dispositivos de manera inalámbrica

- La posibilidad de que el sistema operativo deje de funcionar correctamente, al no haber comprobado minuciosamente las actualizaciones a nivel interno
- Las restricciones de la red, ya que las actualizaciones ahora ocupan un tamaño de varios gigabytes

AirWatch permite al equipo de TI implementar o aplazar las actualizaciones y los parches del sistema operativo en función de la prioridad del dispositivo y los periodos de mantenimiento deseados. Permite que el entorno de TI pueda aprobar de forma automática o desautorizar determinados grupos de actualizaciones, como las de aplicaciones, desarrolladores, seguridad, etc., según la susceptibilidad de los usuarios con respecto a las actualizaciones de funciones y seguridad. Gracias al almacenamiento en caché de igual a igual, AirWatch permite optimizar la distribución de actualizaciones y evita la congestión de la red. El departamento de TI puede recibir un inventario detallado y llevar a cabo una auditoría de conformidad de actualizaciones individuales de Windows, además de superar los desafíos relacionados con la aplicación de parches fuera de la red.

Distribución de software

Con Universal Windows Platform (UWP), Microsoft ha unificado la experiencia de las aplicaciones en todos los dispositivos con Windows 10. Ahora, las aplicaciones de UWP públicas se pueden distribuir a través de Windows Store (con una experiencia en tienda similar a la de otras plataformas de sistemas operativos móviles) o a través de una tienda para empresas interna personalizada para una organización. AirWatch se integra con Windows Store y Windows Store para empresas para optimizar la distribución de estas aplicaciones modernas.

No obstante, la mayor parte del software para empresas de Windows todavía se compone de aplicaciones clásicas Win32 de gran tamaño y cuyo empaquetamiento, implementación y mantenimiento pueden resultar complejos. Este hecho hace de la distribución de software uno de los mayores desafíos a la hora de gestionar Windows con soluciones de EMM. AirWatch aborda este desafío acortando las distancias de la gestión del ciclo de vida entre las aplicaciones UWP y Win32.

Con AirWatch, el departamento de TI puede consolidar la gestión de aplicaciones móviles y la experiencia de implementación del software Win32 tradicional en una única consola de administración. Los administradores pueden gestionar parches de aplicaciones de terceros, distribuir dependencias e incluso definir condiciones o contingencias para la instalación de aplicaciones.

Con App Stacks, AirWatch introduce un nuevo enfoque de distribución de software que supera los desafíos del empaquetado de aplicaciones y las instalaciones poco fiables. El equipo de TI también puede implementar aplicaciones Win32 con mayor rapidez en cualquier dispositivo Windows, de una forma tan fiable y sencilla como la implementación de aplicaciones móviles. Para el usuario final, AirWatch ofrece un catálogo de autoservicio y una experiencia de inicio de sesión único uniforme en todas las aplicaciones Windows, incluidas las aplicaciones nativas, SaaS y remotas.

Estado y seguridad del cliente

La nueva era de desafíos de ciberseguridad actual también requiere una seguridad integral. AirWatch genera confianza entre los usuarios, refuerza la defensa del sistema operativo frente a nuevas amenazas y separa los datos personales y empresariales para proteger los datos en reposo, en uso y en tránsito de la empresa.

- **Confianza entre los usuarios**: incluso las contraseñas más seguras

Prestaciones de la gestión de aplicaciones Win32

pueden resultar vulnerables y ser objeto de robo mediante diferentes procedimientos, como la suplantación de identidad, el registro de pulsaciones de teclas o los programas maliciosos. AirWatch se integra con las funciones de identificación de Windows 10 para definir políticas que permitan la autenticación sin contraseña, utilizando gestos o un PIN. Las organizaciones pueden habilitar la autenticación multifactor de forma predefinida para ayudar a protegerse de los ataques de tipo «pass-the-hash».

- **Refuerzo del sistema operativo**: AirWatch permite al equipo de TI tomar medidas de seguridad proactivas al evitar que se descarguen o ejecuten aplicaciones que no sean de confianza o no estén autorizadas. AirWatch comprueba la integridad y la conformidad del dispositivo en tiempo real y bloquea automáticamente el acceso a las aplicaciones y servicios de la empresa a cualquier dispositivo que no cumpla con las políticas.
- **Protección de datos**: la prevención de la pérdida de datos se ha convertido en una de las principales prioridades hoy en día, ya que los dispositivos son cada vez más móviles, lo que aumenta la probabilidad de que alguien los robe o se pierdan. Además, los usuarios realizan con frecuencia tareas personales y empresariales en los mismos dispositivos. AirWatch establece políticas para cifrar los datos, permite a los administradores y a los usuarios finales borrar de forma remota el dispositivo si lo pierden o alguien lo roba, y garantiza la separación de los datos personales y empresariales aprovechando las funciones de contenedorización nativas del sistema operativo Windows.

La UEM de AirWatch ayuda a las empresas a aplicar una gestión de la seguridad integral de forma rentable.

PROTEGER CUALQUIER TERMINAL DESDE UNA ÚNICA PLATAFORMA

Por razones de diseño, la UEM debe ser independiente a la plataforma, proporcionando una solución única que permita gestionar todos los dispositivos y sistemas operativos que se emplean en cualquier caso de uso en una empresa. Esto garantiza que los usuarios finales tengan una experiencia uniforme con independencia del dispositivo que utilicen para acceder al entorno corporativo.

La UEM de AirWatch ofrece un enfoque holístico centrado en el usuario para gestionar y proteger cualquier terminal desde una única plataforma. Admite la implementación global en distintas divisiones, regiones y departamentos dentro de una única consola gracias a una arquitectura multicliente. La UEM de AirWatch se integra con los sistemas de la empresa para sacar el mayor partido a las inversiones existentes en infraestructura y extender esos servicios a todos los terminales.

Con la UEM de VMware AirWatch, el equipo de TI puede automatizar los procesos a través de motores de políticas dinámicos e inteligentes en las plataformas de Windows 10. Esto alivia las tareas de TI manuales y posibilita las funciones de autoservicio, reduciendo así los costes de soporte.

¿Está preparado para replantearse la gestión de sus terminales? Le invitamos a registrar hasta un máximo de 100 dispositivos en un periodo de prueba gratuito de 30 días. Para obtener más información, visite el sitio web.