ivanti

Unified Endpoint Management para el lugar de trabajo “en cualquier parte”

Índice de contenidos

Introducción

La movilidad y el consumo de las TI se han convertido en una forma de vida en la empresa. En términos más sencillos: los usuarios de hoy en día esperan realizar su trabajo desde cualquier lugar y en cualquier momento utilizando una amplia variedad de dispositivos, desde ordenadores de sobremesa y portátiles hasta tabletas y teléfonos inteligentes. Esto se ha vuelto aún más relevante en el teletrabajo.

En su momento, el trabajo más "serio" se realizaba en ordenadores portátiles y de sobremesa, y los dispositivos móviles se utilizaban solo para el correo electrónico y otros fines limitados en los desplazamientos o en casa. En la actualidad, los usuarios esperan acceder a la misma información, ejecutar muchas de las mismas aplicaciones y servicios, y realizar gran parte del mismo trabajo en cualquier dispositivo, ya sea de la empresa o propio. Las tendencias en el desarrollo de los ordenadores están difuminando las líneas entre lo que es un ordenador y lo que es un dispositivo móvil.

Esta igualdad de dispositivos móviles ha creado un reto importante para la empresa, aunque también existe una oportunidad evidente. En primer lugar, el reto: el departamento de TI debe aplicar políticas para gestionar y proteger las aplicaciones y la información sensible a las que se accede y que se almacenan en cada dispositivo sin comprometer la productividad del usuario, sus preferencias de trabajo móvil y el uso personal del dispositivo. A pesar de las mejores intenciones y esfuerzos, en muchas empresas la gestión de los puntos finales y la seguridad no han seguido el ritmo de la igualdad de los dispositivos.

¿Cuál es el riesgo de no actuar? Las organizaciones de TI se exponen a amenazas y filtraciones de datos. Sin contexto (el empleado, sus dispositivos y su ubicación, zero trust y las experiencias personalizadas de los empleados), el departamento de TI se ve obligado a crear un estado de bloqueo para evitar el riesgo que afecta a la productividad de los empleados.

TI necesita una solución que pueda ajustar la política de seguridad por empleado de forma automática, supervisar la red de forma anticipada y alertar al equipo de TI inmediatamente.

Gestión de dispositivos en la era de las fugas de datos

El enfoque adoptado en la mayoría de las empresas es el siguiente: un sistema de gestión o un conjunto de sistemas de gestión para ordenadores de sobremesa y portátiles, y un sistema de gestión, un proveedor y una estrategia totalmente independientes para los dispositivos móviles, como los smartphones y las tabletas. En muchos casos, hay dos puestos de TI diferentes centrados en los dispositivos móviles y en los sistemas de punto final tradicionales al utilizar diferentes herramientas de gestión.

Este enfoque tiene graves inconvenientes, sobre todo en la era de las cada vez más frecuentes y perjudiciales violaciones de datos. Los dispositivos móviles son propensos a la pérdida y al robo, lo que los expone a que las aplicaciones y los datos de la empresa se vean comprometidos. El malware móvil es una puerta de entrada potencial en la red corporativa. Además de la pérdida, el robo y el malware, la implantación de dos sistemas de gestión diferentes para distintos dispositivos presenta otros graves problemas e implicaciones.

Experiencia común del usuario final

Las aplicaciones y estrategias de gestión independientes dificultan la experiencia de usuario común en todos los dispositivos que los usuarios exigen. La incorporación, el aprovisionamiento y el soporte de múltiples dispositivos puede resultar innecesariamente complejo y lento. Aquí es donde surge la oportunidad.

> Asegure el lugar de trabajo en cualquier lugar con una solución que le permita identificar y gestionar todos los dispositivos de sus empleados desde la nube hasta el borde; implementar un acceso seguro zero trust con automatización contextual; y ofrecer experiencias personalizadas para cada empleado donde quiera que trabaje. El impacto: una mayor productividad con mejor velocidad operativa, coste y calidad de servicio.

Políticas comunes de los usuarios

Proteger la información sensible de la empresa y el acceso a la red requiere elaborar un conjunto estricto de políticas de acceso y seguridad de los usuarios. A medida que aumenta la frecuencia y la sofisticación del uso de los dispositivos móviles, el departamento de TI tiene el reto de elaborar y aplicar un conjunto común de políticas de identidad y acceso y un marco normativo en todos los sistemas de punto final utilizados por cada empleado. El despliegue de un conjunto común de políticas es más complejo cuando se utilizan dos sistemas de gestión completamente independientes. Un enfoque más sencillo es utilizar una única solución de Unified Endpoint Management (UEM). Esto también ayuda a mitigar la complejidad de tener varios equipos involucrados.

Antes, muchas empresas tenían a su personal de TI a cargo de los dispositivos de escritorio y portátiles, mientras que los teléfonos inteligentes los manejaba el personal de telecomunicaciones. Esto significaba que los dos equipos tenían habilidades, prioridades y perspectivas diferentes.

Este tipo de acuerdo incluía brechas invisibles en la creación y despliegue de políticas que dejaban vía libre a los hackers y a las violaciones de datos.

Además, depender de dos plataformas de gestión diferentes con políticas aparentemente idénticas significa que a veces pueden implantarse de forma diferente, lo que provoca brechas ocultas.

Un sistema UEM unificado crea un único conjunto de políticas de acceso y seguridad de los usuarios y las despliega de forma coherente y fluida en todos los dispositivos de los usuarios.

Costes de gestión y recursos

Trabajar con dos plataformas de gestión independientes, con diferentes proveedores, contratos de asistencia e interfaces, requiere más tiempo, formación y recursos que utilizar una única plataforma. La incorporación, los costes de soporte y los requisitos de recursos no solo son mayores, sino que cualquier cambio en el estado o los derechos de acceso del usuario requiere cambios de política en dos sistemas distintos, lo que requiere muchos recursos y es más propenso a errores que el uso de un único sistema de gestión.

Más tiempo y recursos dedicados a la gestión de dispositivos significa también menos tiempo y recursos dedicados a las estrategias tecnológicas que mejoran el negocio. Ante el ritmo del cambio tecnológico y el papel cada vez más importante que este cambio desempeña en la competitividad de las empresas, los departamentos de TI estarán mejor si pueden dedicar el menor tiempo posible a las tareas de gestión del día a día.

El mito de la integración

A medida que las plataformas de gestión de la movilidad empresarial (EMM) han ido adquiriendo mayor protagonismo en la empresa, sus proveedores empiezan a pregonar la integración con las plataformas de gestión de puntos finales de ordenadores de sobremesa y portátiles existentes. Se trata de una tendencia prometedora, aunque la supuesta integración entre sistemas muy diferentes no produce el mismo ahorro y facilidad de uso que un único sistema UEM, la interfaz y la relación con el proveedor. El objetivo de la UEM es implementar un conjunto coherente de políticas y recursos de apoyo para cada usuario en todos sus dispositivos, en lugar de una separación artificial entre sistemas y dispositivos móviles y tradicionales. Este sistema debería ofrecer las siguientes capacidades en todos los dispositivos:

Gestión de puntos finales. Gestión de puntos finales de todos los dispositivos de los usuarios, que incluye la detección y el inventario de dispositivos, el aprovisionamiento del dispositivo (despliegue del sistema operativo/inscripción del dispositivo), (la distribución de software/aplicaciones móviles), la asistencia y el control remoto.

Aplicación de la seguridad que permite reforzar la seguridad operativa con la gestión de parches, la seguridad de los puntos finales, la distribución de software, la actualización y la aplicación de políticas de identidad y acceso. En el caso de los dispositivos móviles, el bloqueo y el borrado remotos tras sospecha de pérdida o robo son capacidades importantes.

Aprovisionamiento, incluyendo la incorporación y la retirada de nuevos dispositivos e imágenes de dispositivos. El autoaprovisionamiento de los usuarios es una capacidad que ofrecen muchas soluciones de MDM y debería ofrecerse también en una solución integral de gestión de puntos finales.

Lo ideal sería que todas estas funciones de seguridad de aplicaciones y datos estuvieran estrechamente integradas en el mismo sistema UEM, de modo que la gestión de los ordenadores portátiles, los PC, los dispositivos móviles, las aplicaciones y la información de los usuarios se llevara a cabo con una sola pantalla y un único conjunto coherente de políticas empresariales que abrieran la puerta a que un único personal pudiera gestionarlo todo.

La solución Ivanti

La solución Ivanti para gestionar los dispositivos de los usuarios elimina la separación artificial entre los sistemas tradicionales de escritorio y portátiles y sus homólogos de dispositivos móviles. Ivanti se centra en la gestión unificada de puntos finales, ofreciendo una única solución de gestión de TI empresarial y un conjunto de políticas para gestionar todo el ciclo de vida de todos los dispositivos de cada usuario de la empresa. Con UEM, el usuario -no el dispositivo- es el centro de atención. Con este enfoque centrado en el usuario, Ivanti ofrece la única solución de gestión integral que proporciona la misma experiencia fluida que los usuarios esperan en todos sus dispositivos. Las capacidades del Endpoint Manager de Ivanti, líder en la industria, son:

Descubrimiento e inventario.
Ivanti descubre e inventa automáticamente todos los PCs gestionados y no gestionados, portátiles, teléfonos inteligentes, tabletas y otros dispositivos móviles conectados a la red, independientemente del sistema operativo. Con Ivanti Cloud Services Appliance, el departamento de TI puede incluso descubrir e identificar dispositivos en ubicaciones remotas y gestionarlos a través de conexiones de bajo ancho de banda, sin necesidad de VPN.

Implantación y distribución de sistemas operativos.
Ivanti simplifica y automatiza la instalación y la implantación de los sistemas operativos Windows y macOS en todos sus sistemas de usuario relevantes, conservando el usuario, las aplicaciones, la configuración y los archivos para restaurarlos en un equipo nuevo o existente.

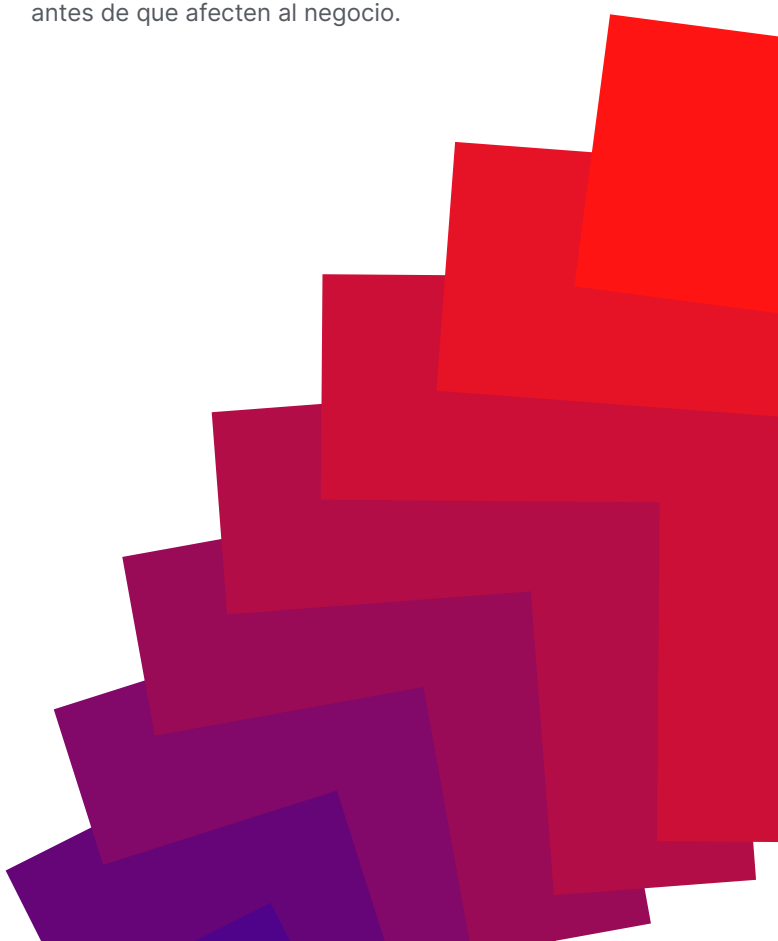
Distribución de software.
Ivanti automatiza la distribución de software a través de todos los dispositivos, desde Windows hasta Mac y dispositivos móviles con iOS y Android. Las tecnologías de distribución empresarial patentadas pueden distribuir grandes paquetes de software a través de miles de dispositivos en minutos con un consumo mínimo de ancho de banda.

Administración sencilla y basada en el usuario.
Permite al departamento de TI aplicar una única configuración de usuario y una única política de seguridad en todos los dispositivos que lleva un usuario.

Con esta capacidad, una sola implementación de políticas puede conectar y aprovisionar un dispositivo de un nuevo empleado en cuestión de minutos.

Gestión de licencias de software.
Estas herramientas ofrecen una auditoría y supervisión automatizada de las licencias de software para ayudar a las organizaciones a comprar solo lo que realmente necesitan, y proporcionan información detallada para ayudar a renegociar los acuerdos de licencia de los proveedores para controlar los costes. El uso inteligente de la gestión de licencias de software permite a las empresas ahorrar miles o incluso cientos de miles de dólares.

Cuadros de mando e informes de sistemas
para obtener visibilidad sobre el funcionamiento de todos los sistemas, incluidos los PC, los Mac, los teléfonos inteligentes y las tabletas. Xtraction puede proporcionar a los directores de informática, jefes de departamento y directores de TI gráficos y cuadros oportunos para presentaciones empresariales que demuestren el valor de las TI y la toma de decisiones. Incluso proporciona herramientas para la elaboración de informes sobre el rendimiento de la inversión (ROI). Ivanti también incluye herramientas completas de supervisión de umbrales y alertas para que el departamento de TI pueda abordar los problemas antes de que afecten al negocio.



Control remoto Ivanti y resolución de problemas.
El departamento de TI es capaz de controlar los dispositivos para solucionar problemas de soporte o transferir archivos entre sistemas cuando sea posible.

Gestión de la energía.
Crear y desplegar políticas de gestión de la energía en la red.

Gestión integral de la movilidad empresarial.
Esto incluye la gestión de aplicaciones móviles, la gestión de dispositivos móviles y las capacidades de gestión de la seguridad móvil, como la localización, el bloqueo y el borrado remotos de dispositivos. Esta capacidad también es capaz de gestionar ordenadores de sobremesa, portátiles y dispositivos híbridos tanto en modo MDM como en un modo completo basado en agentes que permite todas las acciones de gestión.

Espacios de trabajo basados en roles.
Los usuarios pueden acceder a todos los servicios de TI, incluido el servicio de asistencia y las actualizaciones de seguridad de las que dependen y a las que tienen derecho en todos sus dispositivos.

Los módulos opcionales se integran estrechamente con Endpoint Manager para proporcionar gestión de activos; gestión del ciclo de vida del software y el hardware; y gestión de servicios; con procesos para mantener la productividad de los usuarios y la eficiencia de la organización.

Ivanti UEM ayuda a dar soporte a todos los dispositivos que la gente utiliza e incrementa la productividad tanto del usuario como del departamento de TI. Con el enfoque unificado de Ivanti para la gestión de dispositivos y aplicaciones, el departamento de TI de la empresa obtiene una solución que reduce los costes de gestión de los puntos finales y los requisitos de recursos, cubre las brechas en la seguridad de los puntos finales y ofrece una experiencia de usuario impecable.

Ha llegado el momento de aprovechar la TI centrada en el usuario

Hubo un tiempo en que los PC y los portátiles vivían en mundos separados y tenían capacidades diferentes a las de sus dispositivos móviles. En aquella época, tenía cierta lógica desarrollar e implantar sistemas de gestión separados para cada uno de ellos. En el actual lugar de trabajo “en cualquier parte”, los usuarios dependen de todos sus dispositivos para hacer su trabajo. En este entorno, tener dos sistemas de gestión separados crea una carga innecesaria tanto para los usuarios como para el departamento de TI.

La gestión unificada de puntos finales de Ivanti elimina esta carga al centrar la seguridad y la gestión en el usuario, ofreciendo no solo una gestión unificada, sino una experiencia de usuario única y unificada en cualquier dispositivo, en cualquier lugar y en cualquier momento.

ivanti

ivanti.lat
+57 315 5718981
contact-latam@ivanti.com

ivanti.es
+34 91 049 66 76
contact@ivanti.es