

Ivanti Unified Endpoint Management

El reto

El teletrabajo es una realidad. Para progresar en esta nueva normalidad (y no solo resistirla), las empresas necesitan acceder de forma segura y gestionar fácilmente los datos empresariales en cualquier punto final utilizado por sus empleados, proveedores y trabajadores de primera línea.

El lugar de trabajo digital moderno actual implica el uso de varios puntos finales, como Android, iOS, macOS y Windows 10. Para algunas empresas, este ámbito podría incluir también otros dispositivos inmersivos y resistentes como HoloLens, Oculus, Zebra y otros.

Las necesidades son evidentes: gestionar la privacidad y el cumplimiento de la normativa, minimizando el riesgo y protegiendo la experiencia del usuario. Esto significa separar y proteger las aplicaciones corporativas de las aplicaciones personales de los dispositivos de los usuarios. Todo ello es posible lograrlo de forma sencilla y segura con una solución de Unified Endpoint Management (UEM).

Proteja su lugar de trabajo “en cualquier parte” con la primera plataforma de seguridad de extremo a extremo y de Zero Trust Security

Ivanti UEM cuenta con la primera plataforma de seguridad de extremo a extremo y de Zero Trust para acceder y proteger los datos de forma segura en todo el lugar de trabajo en cualquier lugar.

Esta plataforma valida cada dispositivo para garantizar que solo los usuarios, dispositivos, aplicaciones y servicios autorizados puedan acceder a los recursos empresariales. Este proceso sin fisuras ofrece seguridad a la vez que preserva la experiencia del usuario en cualquier punto final.

Las empresas que se consolidan en el teletrabajo lo hacen con la seguridad móvil de la empresa como eje central. Es un gran reto, no obstante, Ivanti UEM se lo pone fácil. Y a medida que sus necesidades cambian, nuestra UEM se adapta a su empresa.

Desarrolle su sistema con tecnologías que permiten eliminar las contraseñas (zero sign-on (ZSO)), garantizar la autenticación de los usuarios (multi-factor authentication (MFA)) y detectar y mitigar las amenazas a la seguridad de los puntos finales (mobile threat defense (MTD)).

Seguridad integral

Proteja, gestione y supervise cualquier dispositivo móvil u ordenador corporativo o personal que acceda a datos críticos para la empresa. UEM cuenta con la visibilidad y los controles de TI para que sea simple.

Tanto si se trata de dispositivos propios, como si son de la empresa o de ambos, UEM garantiza la seguridad en una amplia gama de puntos finales y gestiona todo el ciclo de vida de estos, incluyendo:

- Incorporación automatizada.
- Configuración y aplicación de normas.

- Distribución y gestión de aplicaciones.
- Gestión y supervisión de la seguridad.
Desactivación y retirada.

UEM se basa en una estructura de eficacia probada, segura, escalable y preparada para la empresa, con opciones de despliegue flexibles que dan prioridad a la experiencia del usuario, al tiempo que mantienen los más altos estándares de seguridad.

Sentry actúa como una pasarela de correo electrónico y contenidos en línea que gestiona, codifica y asegura el tráfico entre el dispositivo móvil y los sistemas empresariales internos. Tunnel es una solución de VPN para aplicaciones multi-OS que permite a las empresas autorizar aplicaciones móviles específicas para acceder a los recursos corporativos detrás del cortafuegos sin requerir ninguna interacción del usuario.

Gestione y expanda su negocio con confianza y seguridad con el móvil y la nube

Control de la organización y de los usuarios. Con UEM, las empresas implementan estrategias de movilidad y seguridad a medida para satisfacer las necesidades del negocio al ritmo de esta. Los datos de los usuarios permanecen confidenciales y los datos corporativos están protegidos, dando a los usuarios y a los administradores el control de su información.

Libertad de elección. Ivanti UEM es agnóstico en cuanto a sistemas operativos y dispositivos. Los

administradores pueden elegir la implementación en la nube o en las instalaciones en función de su presupuesto. Y los empleados pueden utilizar sus puntos finales preferidos para trabajar.

Adopción impulsada por la experiencia. La facilidad de uso equivale a mayor adopción. Y una mayor adopción significa acelerar la productividad y el crecimiento.

UEM ayuda a los departamentos de TI a impulsar la adopción de las aplicaciones de productividad en el

trabajo mediante una experiencia de usuario nativa. Esto simplifica el cumplimiento de la normativa y al mismo tiempo disminuye las amenazas a la seguridad y la TI ocultos.

Resistencia empresarial. Extremadamente seguro. Super discreto. La seguridad invisible y automatizada garantiza el cumplimiento de la normativa y permite que su negocio siga adelante.

Principales casos de uso

- **Garantizar la privacidad y el cumplimiento de las empresas encargadas de proteger los datos sensibles.** Proteja los datos empresariales en cualquier punto final, separando los datos empresariales de los personales.
- **Permitir la gestión de múltiples dispositivos, multi-OS y multi-app desde una única plataforma.** En un entorno de varios dispositivos con diversos sistemas operativos y aplicaciones, la gestión unificada es una prioridad.
- **Capacitar a los trabajadores de primera línea.** Ayude a los trabajadores de campo, de flotas y móviles de la sanidad, el transporte, la fabricación y otros sectores que dependen de dispositivos robustos o dispositivos en modo quiosco.

- **Proporcionar al usuario final una mayor capacidad de elección y una experiencia de uso sin fisuras.** Para garantizar la productividad y el cumplimiento de los usuarios, la elección del dispositivo y la experiencia del usuario son imprescindibles. Ivanti UEM proporciona una incorporación simplificada y una experiencia superior en el dispositivo.

Normas y certificaciones de seguridad

- Common Criteria Certification
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- SOC 2 Type II
- CCN (España)
- SOC 2 Type II
- CCN (España)

Gestión unificada de puntos finales de Ivanti

Gestión y seguridad de los dispositivos	Secure UEM	Secure UEM Premium
<p>Seguridad y gestión. Proteja y gestione los puntos finales con sistemas operativos iOS, macOS, iPadOS, Android y Windows 10. Disponible en las instalaciones y como servicio en la nube.</p>	✓	✓
<p>Gestión de aplicaciones móviles (MAM). Proteja las aplicaciones empresariales con AppStation en los dispositivos de empleados y proveedores sin necesidad de gestionar los dispositivos.</p>	✓	✓
<p>Fácil incorporación. Aproveche servicios como Apple Business Manager (ABM), Google Enrollment y Windows AutoPilot para ofrecer a los usuarios una inscripción automática de dispositivos.</p>	✓	✓
<p>Pasarela de correo electrónica segura. Pasarela de correo electrónico segura. Sentry es una pasarela en línea que gestiona, codifica y asegura el tráfico entre el punto final móvil y los sistemas empresariales internos.</p>	✓	✓
<p>Distribución y configuración de la aplicación. Apps@Work es una tienda de aplicaciones empresariales que, junto con el Programa de Compras por Volumen (VPP) de Apple, facilita la distribución segura de aplicaciones móviles. Además, funciones como iOS Managed Apps y Android Enterprise permiten una fácil configuración de los ajustes a nivel de aplicación y políticas de seguridad.</p>	✓	✓
Conectividad segura	Secure UEM	Secure UEM Premium
<p>VPN por aplicación. Tunnel es una solución VPN multi-OS que permite a las empresas autorizar aplicaciones móviles específicas para acceder a los recursos corporativos detrás del firewall sin requerir ninguna interacción del usuario.</p>		✓
Acceso condicional	Secure UEM	Secure UEM Premium
<p>Motor de confianza. Combina varias señales como el usuario, el dispositivo, la app, la red, la región geográfica y más para proporcionar un control de acceso adaptativo.</p>		✓
<p>Autenticación de usuarios sin contraseña. La autenticación multifactorial sin contraseña utiliza el dispositivo como identidad para una única aplicación en la nube o en las instalaciones.</p>		✓

Gestión unificada de puntos finales de Ivanti (continuación)

Ampliar las operaciones de TI	Secure UEM	Secure UEM Premium
<p>Herramientas de servicio de asistencia. Help@Work permite al departamento de TI ver y controlar de forma remota la pantalla de un usuario, con su permiso, para ayudar a solucionar los problemas de forma eficiente.</p>	✓	✓
<p>Informes. Obtenga visibilidad y control detallados de todos los dispositivos gestionados mediante informes personalizados y acciones de corrección automatizadas.</p>	✓	✓
Asegurar la productividad	Secure UEM	Secure UEM Premium
<p>Aplicación segura de correo electrónico y gestión de información personal (PIM). Email+ es una aplicación PIM segura y multiplataforma para iOS y Android. Los controles de seguridad incluyen cifrado de grado gubernamental, autenticación basada en certificados, S/MIME, cifrado a nivel de aplicaciones y refuerzo del código de acceso.</p>		✓
<p>Navegación segura por la red. Web@Work permite una navegación segura por la web al proteger tanto los datos en movimiento como los datos en reposo. Los marcadores personalizados y el túnel seguro garantizan a los usuarios un acceso rápido y seguro a la información empresarial.</p>		✓
<p>Colaboración segura de contenidos. Docs@Work permite a los usuarios acceder, crear, editar, marcar y compartir contenidos de forma segura desde repositorios como SharePoint, Box, Google Drive y otros.</p>		✓
<p>Contenedores para aplicaciones móviles. Instale el SDK de AppConnect o la aplicación wrapper para proporcionar una capa adicional de seguridad a sus aplicaciones móviles internas, o elija entre nuestro ecosistema de aplicaciones integradas en AppConnect.</p>		✓
<p>Credenciales derivadas. Apoyar la autenticación de dos factores utilizando tarjetas de acceso común (CAC) y la verificación de la identidad personal (PIV).</p>		✓

Sobre Ivanti

Ivanti hace posible el lugar de trabajo en cualquier lugar. En el teletrabajo, los empleados utilizan una gran cantidad de dispositivos para acceder a las redes de TI, las aplicaciones y los datos para seguir siendo productivos mientras trabajan desde “cualquier parte”. La plataforma de automatización de Ivanti conecta las soluciones líderes del sector de gestión unificada de puntos finales, seguridad de confianza cero y gestión de servicios empresariales, proporcionando un único panel de control para que las empresas puedan aprovisionar y proteger por sí mismas sus dispositivos, así como prestar un servicio a los usuarios finales. Más de 40.000 clientes, entre los que se encuentran 78 de las 100 empresas de la lista Fortune, han elegido Ivanti para descubrir, aprovisionar, configurar y proteger a sus activos de TI desde el centro de datos hasta la nube y el borde, y ofrecer excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, visite [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the left side of the contact information, with a red-to-orange gradient.

[ivanti.lat](https://www.ivanti.lat)

+57 315 5718981

contact-latam@ivanti.com

[ivanti.es](https://www.ivanti.es)

+34 91 049 66 76

contact@ivanti.es