

Vodafone Secure Device Manager



Principales tendencias que están cambiando la forma de trabajar



...y representan nuevos retos para el éxito de las empresas en el mundo conectado actual

La globalización y la flexibilidad laboral están cambiando las formas de trabajar



Prácticas BYOD



Transformación
digital de los
puestos de trabajo



Seguridad móvil



Los desafíos del mundo real a los que se enfrenta el cliente Empresas

¿Hacia dónde se dirige el mercado?

No quiero comprar tecnología que se quede obsoleta al cabo de un año.

Gestión demasiado complicada

Necesito que me garanticen que todos los datos de la compañía están seguros y pueden gestionarse fácilmente a lo largo de múltiples plataformas OS.

¿De qué forma puedo gestionar la política BYOD?

Quiero que mis empleados sean lo más productivos posible permitiéndoles el uso de sus propios dispositivos.

Necesito gestionar los costes

- Plazos y recursos
- Posibles brechas de seguridad



Para hacer frente a estos problemas, es imprescindible contar con una solución que ofrezca una visibilidad y un control total de los dispositivos de los empleados que se conectan a los sistemas corporativos o contienen información de la empresa:

- Solución de seguridad agnóstica para la mayoría de los sistemas operativos
- Solución de seguridad para plataformas mixtas
- Costes predecibles y bajo CapEx
- Flexibilidad para cambiar
- Solución gestionada, alojada y soportada técnicamente por Vodafone
- Conectividad fija y móvil segura
- Aumento de la productividad de los trabajadores en movilidad





**¿Qué puede ofrecer
VSDM?**



Vodafone Secure Device Manager (VSDM) – Funcionalidades



Mobile Device Management

Configuración de dispositivos, seguridad y gestión de procedimientos, función de bloqueo y borrado.

- iOS
- Android
- Windows Mobile and Phone
- Symbian
- BlackBerry



Mobile Email Management

Permite que los empleados se conecten al correo electrónico corporativo y garantiza que dichas conexiones son seguras y están gestionadas.
(a través de SEG/PowerShell/Google)



Mobile Content Management

El control de acceso a SharePoint y al almacenamiento en la nube dependerá de la situación en la que se encuentre el dispositivo y de una visualización offline segura.



Mobile Application Management

Distribuye, protege y realiza un seguimiento de las aplicaciones móviles de toda la flota de smartphones.



Mobile Security

Navegador web seguro configurado de forma centralizada
Acceso a los recursos corporativos a través de la intranet
(con Content Locker y MAG)



BYOD o CYOD

Separa las aplicaciones, datos y información personal del contenido corporativo.





Mobile Device Management

Gestión integral y segura de dispositivos móviles



- Administración de distintas flotas de dispositivos desde una única consola
- Integra con la infraestructura corporativa existente
- Aplica las políticas de seguridad de TI a los despliegues móviles
- Ofrece acceso SEGURO a los servicios y recursos CORPORATIVOS
- Configura las opciones y los procedimientos de los dispositivos a través de perfiles
- Conoce la ubicación de tus terminales
- Asigna perfiles de acuerdo a los dispositivos, la titularidad de los mismos o a los grupos
- Visualiza y genera informes sobre todos los activos y procedimientos móviles
- Genera Condiciones de uso conforme a la titularidad del dispositivo
- Proporciona soporte a los dispositivos propiedad de los empleados, a los corporativos y a los compartidos
- Gestión de dispositivos robustos o rugged





Mobile Email Management

Asume el control del acceso al correo electrónico y configura cuentas de email en los dispositivos

- Integración con las infraestructuras de correo electrónico de la compañía
- Encipta los adjuntos del correo electrónico para evitar la pérdida de datos
- Configuración automática de opciones y credenciales
- Impide que aplicaciones de terceros puedan copiar/pegar datos
- Define las políticas y medidas que garantizan el cumplimiento normativo del correo electrónico
- Borra los contenidos adjuntos de los dispositivos que están comprometidos
- Bloquea el acceso al correo corporativo en base al fabricante, modelo o SO
- Controla y monitoriza los datos corporativos sensibles en los dispositivos personales de los empleados
- Instala, elimina y gestiona certificados de correo electrónico





Mobile Content Management



Cifra, distribuye y comparte información con total seguridad a nivel de toda la compañía

- Intercambia documentos corporativos a través de Secure Content Locker™ (SCL)
- Protege los contenidos sensibles en un contenedor corporativo y promueve prácticas de colaboración seguras
- Integración empresarial en instalación o en repositorios Cloud Content
- Aplica la autenticación multifactor
- Gestiona los permisos de acceso de los usuarios y los privilegios de archivos
- Delega el control de administración a grupos internos
- Lleva un seguimiento de las versiones, actualización y uso de los documentos
- Integra los contenidos generados por los usuarios en el Portal de Autoservicio





Mobile Application Management

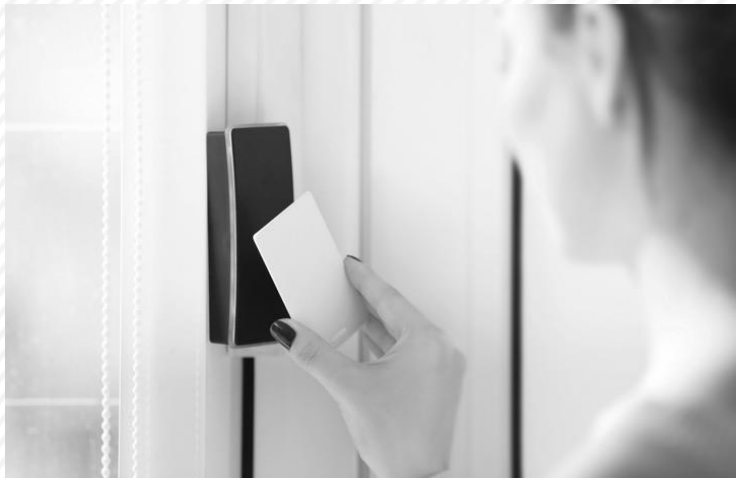
Distribuye y administra aplicaciones de empresa públicas o adquiridas

- Integración con App Store, Google Play y Microsoft Store
- Ofrece un catálogo coherente de aplicaciones para móviles, tablets y ordenadores portátiles
- Crea un Catálogo de aplicaciones corporativas a medida
- Despliega aplicaciones por usuario, función del dispositivo o grupo smart
- Obliga al cumplimiento con listas blancas y negras de aplicaciones.
- Lleva un seguimiento del inventario, versiones y cumplimiento de las aplicaciones
- Despliega aplicaciones y actualizaciones internas de forma inalámbrica.
- Ofrece autenticación SSO para acceder a las aplicaciones corporativas
- Se integra con servicios de análisis de reputación de aplicaciones externas





Mobile Security



Protege los datos corporativos y controla el acceso de empleados a los sistemas de la empresa

- Ofrece autenticación de doble factor
- Establece controles de acceso a la red
- Aplica políticas de seguridad coherentes
- Separa los datos corporativos y personales
- Encripta datos corporativos de naturaleza sensible
- Aplica normativas de cumplimiento y actuaciones de escalado
- Gestiona el acceso de los usuarios a los recursos corporativos
- Lleva a cabo borrados de datos de dispositivos y aplicaciones en remoto
- Soporta certificados PKI internos y certificados de terceros

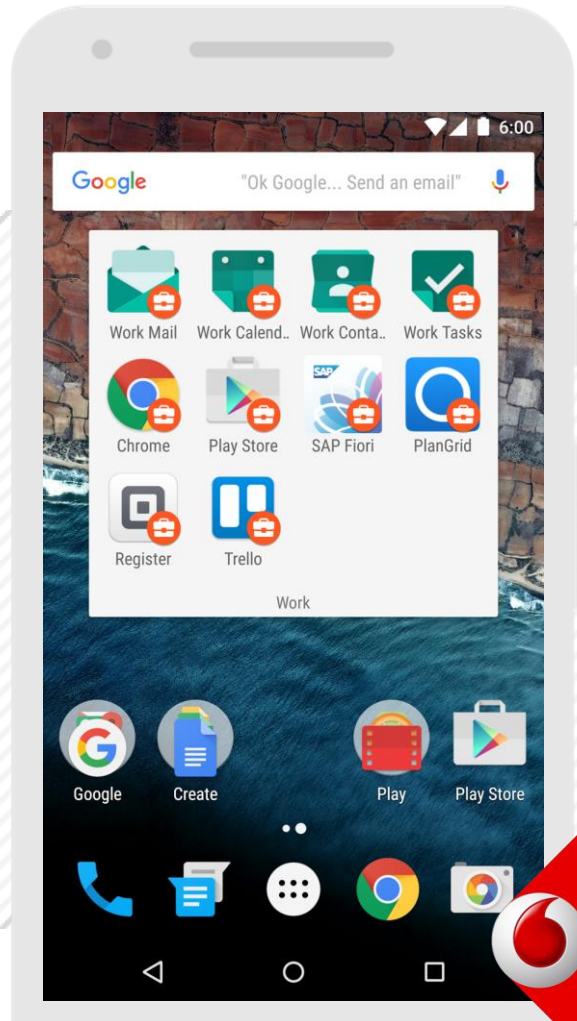


BYOD/CYOD

Gestiona la distribución y control de las aplicaciones en los terminales de tu empresa.

Cambia de las aplicaciones Corporativas a las Personales con tan solo un click.

La empresa solo tiene acceso a los datos corporativos, no a los personales.

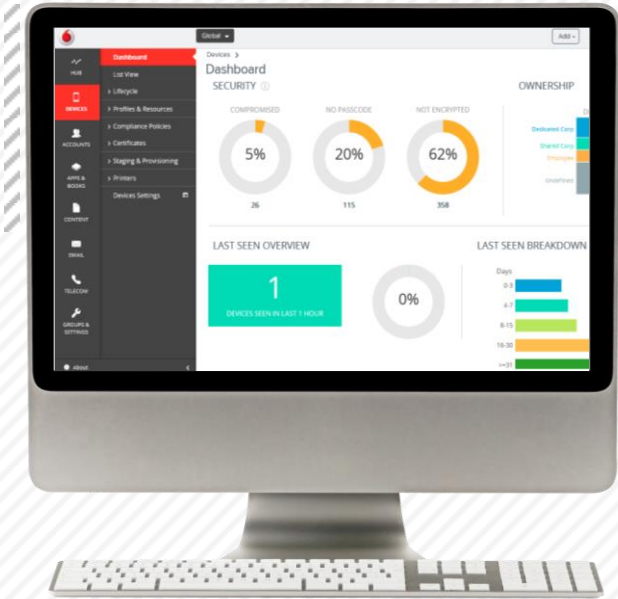


2

**Nuestro portal de
administración**



Aumenta la productividad y reduce los tiempos de respuesta



Rápido acceso a información de negocio crítica

Interfaz de usuario intuitiva basada en navegador

Vistas flexibles

Herramientas de filtrado rápido

Personalización de menús/preferencias

Almacenamiento de consultas y búsquedas habituales

Fácil para detectar problemas de incumplimiento o seguridad y tomar medidas

Integración con los sistemas corporativos a través de cloud connector

Arquitectura escalable y multiempresa

Una interfaz segura, flexible y fácil de utilizar



Rápido acceso a información de negocio crítica

Acceso de seguridad según posición jerárquica

Estructura flexible: acceso por compañía, división y región

Rápida implantación y control gradual para una fácil customización

Acceso seguro para dispositivos de terceros y proveedores de aplicaciones



4

Resumen



¿Para qué necesitan los clientes Vodafone Secure Device Manager?

Visibilidad y control absolutos de todos los dispositivos móviles

- Control y aprovechamiento de las plataformas móviles
- Administración y gestión de aplicaciones
- Cumplimiento de las normativas sobre seguridad y privacidad
- Protección de los datos corporativos
- Preservar la experiencia de usuario
- Evitar la pérdida de datos



Gracias

