Universitat Oberta de Catalunya

uoc.edu

TRABAJO FINAL DE MÁSTER

INTEGRACIÓN SEGURA DEL BYOD

Estudiante: Alba de la Fuente Ramos

Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Seguridad Empresarial

Tutor: Amadeu Albós Raya

Responsable de la asignatura: Victor Garcia Font

Fecha: 04/06/2019

A todos aquellos que me quieren y que siempre han estado a mi lado en todas mis decisiones, triunfos y derrotas. Gracias a la mejor familia, pareja y amigos que podría tener.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Integración segura del BYOD
Nombre del autor:	Alba de la Fuente Ramos
Nombre del consultor/a:	Amadeu Albós Raya
Nombre del PRA:	Victor Garcia Font
Fecha de entrega (mm/aaaa):	04/06/2019
Titulación:	Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del Trabajo Final:	Seguridad Empresarial
Idioma del trabajo:	Castellano
Palabras clave	Seguridad, BYOD, UEM

Resumen

A medida que muchos departamentos de TI luchan por mantenerse al día con los cambios tecnológicos anuales, los empleados de la compañía desean cada vez más usar sus propios dispositivos para acceder a los datos corporativos.
Los dispositivos que son propiedad de los empleados a veces son aprobados por la compañía y son compatibles con dispositivos que son propiedad de la empresa. En otros casos, los dispositivos de propiedad de los empleados forman parte del sistema paralelo conocido como TI instantánea: hardware o software dentro de una empresa que no es compatible con el departamento central de TI de la organización. Ya sea que el hardware y el software de los empleados sean compatibles o no, suponen riesgos para la seguridad de la organización si se conectan a la red corporativa o acceden a los datos corporativos. Para minimizar el riesgo y adaptarse a las tecnologías de consumo, muchas empresas están implementando políticas BYOD (Bring Your Own Device).
Las políticas BYOD permiten a los empleados de la empresa a trabajar en el dispositivo que elijan: accediendo al correo electrónico corporativo en su iPhone o usando un Android para ver documentos de texto de la empresa. El objetivo de las empresas con este sistema es el aumento de la productividad y reducción de costes. Pero si BYOD no se comprende y regula completamente, puede amenazar la seguridad de TI y poner en riesgo los sistemas comerciales sensibles de una empresa.
En este trabajo, se busca profundizar en la integración de seguridad que requieren los sistemas que aceptan las políticas BYOD, analizando los riesgos actuales, estableciendo criterios y diseñando medidas que garanticen la seguridad integral del sistema.
Después de analizar en profundidad las diferentes medidas, se analizará a nivel práctico un sistema del estilo MDM (Mobile Device Management) que se propondrá para aplicar en dispositivos de una empresa con políticas BYOD.

Abstract

While IT departments struggle to keep up with the annual technological changes, the company employees increasingly want to use their own devices to access to corporate data.

Devices owned by employees are usually approved by the company and are compatible with devices that are owned by the company. In other cases, employee-owned devices are part of the parallel system known as instant IT: hardware or software within a company that is not compatible with the central IT department of the organization. Whether the hardware and software of the employees are compatible or not, they are security risks for the organization if they connect to the corporate network or access corporate data. To minimize risk and adapt to consumer technologies, companies are implementing BYOD (Bring Your Own Device) policies.

BYOD policies allow employees of the company to work on the device they choose: access corporate email on their iPhone or using an Android to view company text documents. The companies' goal is to increase productivity and reduce costs. But if BYOD is not fully understood and regulated, it can threaten IT security and put a company's sensitive business systems at risk.

In this work, we seek to deepen the integration of security required by the systems that accept BYOD policies, analyzing current risks, establishing criteria and designing measures that guarantee the integral security of the system.

After analyzing the different measures in depth, a kind of MDM system will be proposed to apply in devices of a company with BYOD policies, and it will be analyzed on a practical level.

Índice

Índice de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El mundo de la tecnología siempre se caracteriza por estas en continuo cambio, evolución, desarrollo e innovación. Día a día se ha evolucionado del ordenador convencional, a los portátiles, y luego a los dispositivos móviles, como *smartphones*, *tabletas*, *smartwatchs*, etc. que a ofrecen mayores beneficios, versatilidad y capacidades a los consumidores y usuarios finales, como pueden ser:

- Movilidad: son dispositivos fáciles de transportar y de utilizar.
- Tamaño: son dispositivos pequeños, se pueden guardar fácilmente.
- Capacidad de conexión y sincronización con ordenadores.
- Capacidad de almacenamiento y memoria limitada.
- Capacidad de conexión a redes (Telefónicas, Wifi, otras) de forma permanente o intermitente

Dadas estas características, se diferencian claramente los dispositivos móviles, de los ordenadores portátiles. Estos dispositivos móviles en su constante evolución, masificación de uso y penetración en el mercado de consumo, se han convertido en pequeños ordenadores de bolsillo, cuya versatilidad permite que cada usuario los personalice y adapte a sus necesidades personales y laborales.

Por lo tanto, dada esta tendencia a la reducción del tamaño y versatilidad de los dispositivos, cada vez es más fácil tener el máximo de información en cualquier parte, y llevarla con nosotros incluso a la empresa, y eso provoca que la seguridad de las empresas se vea afectada por la "intrusión" de estos dispositivos en entornos de trabajo.

El término BYOD es relativamente joven. Apareció por primera vez en un artículo de 2005 presentado en UBICOMP [1], la conferencia anual sobre computación. Des de entonces, la adopción de este término ha seguido aumentando y la familiaridad es cada vez mayor.

Esta expansión ha sido posible en parte por dispositivos móviles más inteligentes, más capaces y más flexibles. La revolución de BlackBerry BYOD fue posiblemente el comienzo de todo. Los dispositivos BlackBerry permitieron el acceso a correo electrónico, internet y aplicaciones sobre la marcha, y allanaron el camino para dispositivos inteligentes similares. Desde entonces, el mercado se ha unido a usuarios como Android, Apple, Microsoft y otros, y ahora está en el punto de saturación. Parece que se introducen nuevos dispositivos inteligentes cada semana, y cada uno se anuncia como más capaz o más exclusivo que el siguiente.

Adoptar BYOD como forma de trabajo, no es una tarea fácil, teniendo en cuenta cómo pueden ser las industrias y cuán lentas pueden ser para adoptar nuevas tecnologías. Sin embargo, como muestran las estadísticas, las empresas se han apresurado a adoptar BYOD [2]. Y es sorprendente, cuando pensamos que el primer BlackBerry se lanzó en 1999. Desde los primeros días de la revolución BYOD de BlackBerry, la industria ha avanzado a gran velocidad sin mirar atrás.

1.2 Objetivos del Trabajo

A. Saber cómo integrar un sistema con políticas BYOD en las empresas
B. Tener claros los riesgos actuales que existen en una empresa con políticas BYOD
C. Conocimiento claro de las medidas que garantizan la seguridad del sistema BYOD
D. Buscar un MDM, probarlo y compararlo con otro, para establecerlo en una empresa

1.3 Enfoque y método seguido

La metodología que se ha aplicado es la siguiente:

1. Profundizar en la integración del BYOD en las empresas
2. Analizar los riesgos actuales en el BYOD en las empresas
3. Diseñar medidas que garanticen la seguridad del sistema
4. Probar y configurar diferentes aplicaciones MDM con el objetivo de encontrar una que podamos establecer en una empresa.
5. Elaboración de conclusiones y consideraciones finales

1.4 Planificación del Trabajo

La planificación del trabajo se ha seguido a base de objetivos y tareas a cumplir en el periodo de tiempo determinado para realizar este trabajo:

Objetivo A: Saber cómo integrar un sistema con políticas BYOD en las empresas:

- Tarea 1: Búsqueda de información y definición sobre el estado del BYOD
- Tarea 2: Búsqueda de información de cómo se integra el BYOD en una empresa
- Tarea 3: Establecer ventajas de los sistemas que aplican políticas BYOD

Objetivo B: Tener claros los riesgos actuales que existen en una empresa con BYOD

- Tarea 4: Establecer los riesgos que sufren las empresas sin BYOD
- Tarea 5: Establecer los riesgos que sufren las empresas que aplican BYOD

Objetivo C: Conocimiento de las medidas que garantizan la seguridad del sistema BYOD

- Tarea 6: Establecer las diferentes medidas de seguridad que garantiza BYOD

Objetivo D: Elección de un MDM para establecerlo en una empresa

- Tarea 7: Buscar diferentes sistemas MDM para los dispositivos establecidos.
- Tarea 8: Implementación del MDM y pruebas en los dispositivos
- Tarea 9: Elección y definición del sistema MDM recomendado

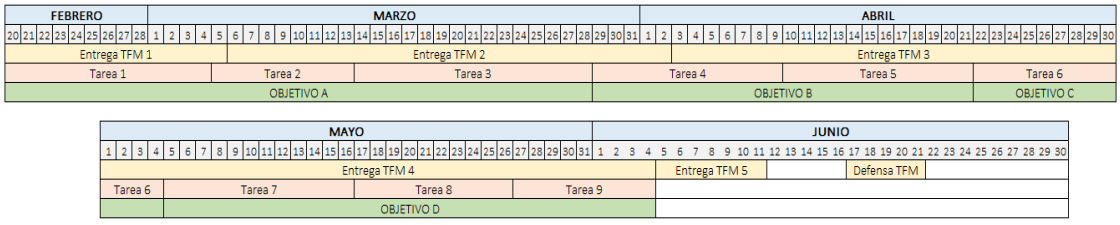

Figura 1: Planificación

1.5 Breve descripción de los otros capítulos de la memoria

1. Estado del BYOD: Se describe el estado actual del BYOD, así como desde cuando existe
2. Ventajas y riesgos de un sistema BYOD: se establecen las ventajas e inconvenientes de un sistema BYOD y cómo puede afectar a las empresas y sus usuarios
3. Integrar BYOD en una empresa: Se analizarán las consideraciones previas a implementar un sistema BYOD en una empresa, de forma que nos ayudara a establecer las primeras pautas antes de instalar BYOD.
4. Establecer una solución BYOD para una empresa: En este apartado definimos una empresa ejemplo con unas necesidades de aplicaciones BYOD en su entorno. Después, proponemos una aplicación a priori MDM que pensamos podría ayudar a la implementación de un sistema BYOD para esta empresa.

2. Integración segura del BYOD

2.1 Estado del BYOD

El concepto de "Bring Your Own Device" ha existido desde 2004, por lo que no es exactamente una nueva tendencia. Sin embargo, la importancia de BYOD ha aumentado exponencialmente en los últimos años, lo que se ha hecho más convincente por el aumento en el uso de especialistas independientes y la saturación del mercado de dispositivos móviles, como tabletas y smartphones.
Si bien los beneficios en costes de alentar a los empleados y visitantes a que suministren el equipo que necesitan para el trabajo son claros, los riesgos de seguridad de permitir el acceso a recursos corporativos desde dispositivos privados desalientan a muchas empresas a adoptar la política.
A pesar del ahorro de costes de BYOD, las empresas de las economías desarrolladas tienen una tasa de BYOD más baja que las de los países en desarrollo. Las empresas norteamericanas y europeas tienden a ser más adversas al riesgo que las empresas en Brasil, India y Medio Oriente porque son más propensas a ser blanco de ataques cibernéticos. Así, en países como Rusia, Brasil y los Emiratos Árabes Unidos, el 75 por ciento de los trabajadores utilizaban sus propios dispositivos personales en el trabajo para 2013, mientras que, en las naciones más desarrolladas, esa tasa era de solo el 44 por ciento.

2.2 Ventajas y riesgos de un sistema BYOD

2.2.1 Ventajas de BYOD

Aunque hay muchos riesgos involucrados en BYOD, las compañías están comenzando a implementar esta política, por lo que debe haber beneficios que podría obtener siguiendo la tendencia [3].
Las principales ventajas de un sistema BYOD son:

1. **Reduce los costes de tecnología para las compañías**: los programas BYOD transfieren los costes al usuario individual, ahorrando a las empresas dinero en la compra de dispositivos por adelantado con tarifas mensuales de servicios de voz y datos. Incluso subsidiar a los empleados los planes de móviles y datos cuesta mucho menos que comprar dispositivos pagados en su totalidad con una iniciativa móvil de toda la empresa.
2. **Mejora del rendimiento del usuario:** la fuerza laboral de hoy en día es experta en tecnología. Con BYOD, los técnicos usan dispositivos que ya comprenden, lo que requiere menos capacitación. Los trabajadores de campo sabrán cómo aprovechar al máximo las funciones del dispositivo, lo que aumenta la productividad de los trabajadores y maximiza los ingresos del negocio.
3. **Mantiene a los empleados satisfechos:** mantener a los técnicos de campo fuertes es extremadamente importante, pero también difícil. Cuando los técnicos usan los dispositivos que ya conocen, trabajan mejor para su empresa y también son más productivos. Los estudios han demostrado que los empleados disfrutan del uso de sus

dispositivos personales en los dispositivos de emisión masiva de los departamentos de IT, a pesar de ser responsables de sus propios costes y cobertura.

4. Aprovecha los dispositivos más nuevos y las características de vanguardia: los usuarios generalmente se actualizan al hardware más reciente y obtienen acceso a dispositivos más rápidos, más elegantes y más capaces. Los dispositivos más nuevos con características como Siri y 4G LTE se ocupan de las tareas de trabajo de campo, y la actualización de la velocidad, almacenamiento, foto, video, documentación de facturación y más. De hecho, en los informes de Field Service News los gerentes de campo usan dispositivos portátiles para el seguimiento y la programación de vehículos, mitigan los accidentes de vehículos y reducen los costes de mantenimiento.
5. Proporciona fácil acceso a la información: El tiempo de entrega rápido significa clientes felices y más ingresos. Los técnicos de servicio necesitan información disponible en cualquier momento y lugar para hacer bien su trabajo. Los dispositivos antiguos recuperan información lentamente, lo que lleva a un tiempo de respuesta más lento. La implementación de plataformas de contenido flexibles y actualizadas brinda a los empleados acceso a datos a pedido, lo que aumenta la productividad

2.2.2 Los riesgos de BYOD

Existen dos categorías de riesgos cuando hablamos de una política BYOD [6]:

- Empleados que traen sus propios dispositivos personales a la oficina.
- Empleados fuera de la oficina que desean conectarse a la red desde su ubicación remota

De estos dos modelos de acceso, el escenario de acceso remoto presenta un mayor riesgo para la empresa porque existe un problema de seguridad física además de las complicaciones de la integridad de los datos.

Los empleados de ventas son particularmente competentes en el uso de smartphones para hacer cálculos rápidos, anotar recordatorios y almacenar detalles de contacto. Probablemente ya estén usando su propio dispositivo para los negocios de la compañía si no les ha proporcionado uno de la compañía. Sin embargo, estos dispositivos a menudo se quedan atrás, son vulnerables de robo o pérdida.

Un ordenador portátil, smartphone o tableta perdidos o robados puede interrumpir seriamente un negocio solo por la pérdida de la información almacenada en él. Si ese dispositivo también tiene acceso a la red de la empresa, el ladrón puede venderlo rápidamente a un pirata informático y luego su red y los datos de la empresa se verán comprometidos. Este es particularmente el caso cuando las personas no se molestan en bloquear sus dispositivos con un código de acceso.

Los riesgos físicos de BYOD pueden ser el factor principal que lo aliente a no permitir que los empleados utilicen sus propios dispositivos para las actividades de la empresa. Sin embargo, como ya se ha señalado, es probable que ya estén utilizando sus propios dispositivos para almacenar la información de su trabajo y, como están fuera de la oficina, no hay mucho que se pueda hacer para detener este hábito.

Por otro lado, también existe el riesgo de no implementar la política BYOD más adecuada, lo que podría aumentar aún más la exposición de la empresa a todos los riesgos mencionados anteriormente.

2.2.3 Soluciones a los riesgos de seguridad física BYOD.

Si no puede evitar que los empleados remotos usen sus propios dispositivos, la única opción es adoptar la práctica y controlar el acceso a la información.
Conseguir que la información de contacto de ventas sea respaldada desde el dispositivo móvil y al sistema CRM de la empresa es una prioridad. Un teléfono perdido no solo pierde los detalles de las oportunidades de ventas, sino que un vendedor que es contratado por su competencia lleva todos los datos almacenados con él. Desea proporcionar aplicaciones en línea que alienten a los empleados remotos a almacenar toda la información potencialmente rentable en sus servidores y no en sus propios dispositivos. Entonces, si ellos caminan, pierden el acceso a toda la inteligencia que les pagaste para que se reúnan.
Los sistemas de administración de dispositivos móviles (MDM) pueden rastrear la ubicación de todos los dispositivos utilizados por la empresa, sin importar quién los posee, por lo que también se ubican los dispositivos BYOD. Necesita un sistema que le permita bloquear dispositivos móviles de forma remota o borrar todos los datos en caso de que los usuarios designados los pierdan de vista.
La limpieza remota es una solución común para los dispositivos propiedad de la empresa, pero puede resultar controvertida para los propietarios de BYOD. Si una encuesta de empleados demuestra que no estarían dispuestos a permitir que se borren todos los datos de sus teléfonos, existen otras estrategias que puede emplear para garantizar que el sistema de su empresa no se vea comprometido.

2.2.4 Alternativas a BYOD

A causa de los riesgos que tiene BYOD, analizamos también existen diferentes alternativas [7] a los sistemas BYOD:

A. CYOD: Choose Your Own Device

La opción CYOD (Choose Your Own Device) consiste en que los trabajadores pueden elegir dispositivo de un listado previamente aprobado por la empresa. De esta forma, la empresa tiene un control total sobre el gasto y obtiene la posibilidad de elegir cómo los trabajadores van a financiar su movilidad (sin coste, como una parte del sueldo, ofreciendo un pago renovable u otros).
En este escenario el trabajador puede hacer un uso personal o profesional del dispositivo, pero siempre ajustándose a las exigencias de seguridad de la compañía y al control de la misma, ya sea vía hardware o software.
El CYOD presenta un equilibrio entre las necesidades de la empresa y la libertad del empleado, pero de debe tener en cuenta que no siempre las opciones ofrecidas son del gusto de los trabajadores (dispositivos antiguos o poco atractivos, lejos de las opciones del mercado de consumo). Por otro lado, las estadísticas dicen que estos modelos sufren de más peticiones de reemplazos y reparaciones, aumentando el gasto para la compañía.

Ventajas de CYOD

- Coste de adquisición razonable (comparado con COPE)
- Mayor control sobre el usuario final (comparado con BYOD)
- Soporte simplificado gracias al control sobre el parque de dispositivos desplegado

B. COPE: Corporate Owned, Personally Enabled

El modelo COPE ha sido el último en llegar, pero está ganando mucha popularidad especialmente en las grandes compañías. Presenta un escenario donde el control por parte de la empresa es total y el dispositivo está diseñado para el uso profesional, si bien algunas entidades dotan de cierto grado de libertad para que también se pueda utilizar en otros ámbitos de forma segura.
Esta opción resulta especialmente interesante para las empresas con trabajadores que necesitan el acceso remoto como práctica habitual de su flujo de trabajo y es imprescindibles que vayan acompañadas de una política de seguridad adecuada y actualizada, así como un sistema de control y monitorización constante.

Ventajas de COPE

- Ofrece las ventajas del equilibrio entre el uso profesional y el uso personal seguro
- Alto grado control sobre el dispositivo
- Mayores garantías de seguridad
- Más capacidad de respuesta y menor tiempo de reacción ante un problema técnico o de seguridad

C. COBO: Company Owned, Business Only

El siguiente paso por el control y la seguridad sería el modelo COBO, donde el dispositivo es propiedad de la empresa y solo está permitido el uso corporativo. Un ejemplo clásico de este modelo eran las BlackBerry de hace unos años, que se hicieron muy populares en ciertos entornos por su seguridad y la posibilidad de ser controladas en remoto.
En el mundo actual aplicar este modelo puede ser muy complicado y es necesario recurrir a implementaciones personalizadas que, sobre una base iOS, Android o Windows, desplieguen una plataforma controlada y monitorizada donde se puedan restringir la navegación, las llamadas, la instalación o el uso de aplicaciones, etc. En realidad, y, exceptuando ámbitos muy concretos donde la seguridad es una prioridad por encima de cualquier otra variable (incluyendo la productividad), estamos ante un modelo demasiado restrictivo y con el que es complicado beneficiarse de las ventajas de la movilidad en la empresa.

Ventajas de COBO

- Restringe el uso de dispositivos al ámbito profesional
- Máximo control sobre el dispositivo
- Máximas garantías de seguridad
- Menor coste de despliegue y mantenimiento

2.2.5 ¿Qué debemos escoger?

En los próximos años, las empresas seguirán invirtiendo en movilidad (para que sus empleados puedan trabajar de forma remota), pero antes de distribuir nuevos dispositivos a todos los miembros del equipo hay que tener en cuenta qué forma de movilidad se adapta mejor a las necesidades de la organización, ya sea BYOD, COPE o CYOD [7].
Entonces, ¿cuál es el programa correcto para elegir? La respuesta es que no hay una respuesta perfecta. Muchas empresas pueden necesitar una combinación de los tres para administrar de manera más eficiente sus entornos móviles. El coste, las necesidades de seguridad y las funcionalidades del trabajo pueden variar drásticamente en función del rol del usuario final dentro de una empresa, y la movilidad no es un entorno único para todos. Mantener la flexibilidad para satisfacer las necesidades de los empleados, proporcionar el soporte para un entorno de movilidad robusto, y tener una idea del uso y la facturación a menudo es difícil de lograr para las empresas sin la experiencia de un proveedor de MMS.
La aplicación de un método que continúe esforzándose por un uso óptimo, la utilización basada en la función de trabajo y el coste general es el objetivo. A través del seguimiento intencional y la visibilidad, las propias empresas pueden crear un programa eficaz que permita una verdadera gestión de estilo de vida móvil para el entorno de movilidad, incluso a medida que evoluciona y crece.

2.3 Integrar BYOD en una empresa

2.3.1 Consideraciones previas antes de implementar BYOD

Como hemos dicho, cada vez más y más empresas están cambiando a una política de traer su propio dispositivo (BYOD) para ordenadores de empleados. En la teoría, la empresa ahorra dinero y los empleados pueden trabajar en dispositivos con los que ya están familiarizados.
En la práctica, BYOD es a menudo difícil de administrar desde un punto de vista de IT y generalmente conlleva costes inesperados [8].
Una de las mayores desventajas de las políticas BYOD cuando se trata de ordenadores y ordenadores portátiles es la dificultad para administrarlo desde un punto de vista de IT. En la mayoría de las configuraciones de BYOD, los empleados usan sus ordenadores portátiles existentes, que generalmente son ordenadores portátiles para uso doméstico, lo que significa que tienen una versión doméstica del sistema operativo si están en una máquina con Windows.
Tenemos dos opciones aquí, las cuales nos costarán: pagar por una actualización a una versión comercial de Windows (Windows Pro o Enterprise) o enfrentarnos a serios problemas con la administración de dispositivos y los costes ocultos.
Las versiones domésticas de Windows no se pueden unir correctamente a las herramientas utilizadas para administrar equipos desde un punto de vista de IT (Windows Active Directory o Azure Active Directory Domains). Esta falta de administración centralizada significa que su equipo de IT tendrá que hacer mucho más manualmente (por ejemplo, no pueden lanzar nuevas versiones de software a todos al mismo tiempo, tendrán que hacerlo individualmente). En el mejor de los casos, esto será molesto. En el peor de los casos, va a ser una pérdida de tiempo y coste.

La administración de las máquinas BYOD desde un punto de vista de seguridad se vuelve mucho más difícil cuando el ordenador no se puede unir a una plataforma de administración de dispositivos como Azure Active Directory. Cosas como la gestión de dispositivos móviles que borran de forma remota los datos de la empresa de un dispositivo no son posibles.
Si se pierde un ordenador o lo roban, o si un empleado se va, no hay mucho que se pueda hacer si tiene datos de la empresa en el ordenador.
También debemos considerar que las máquinas BYOD también pueden tener problemas de compatibilidad con aplicaciones de línea de negocio u otros sistemas críticos. Las aplicaciones de línea de negocios generalmente tienen requisitos técnicos específicos, como sistemas operativos diseñados para uso comercial, no personal. Los usuarios con máquinas más antiguas, incluso si ejecutan algo como Windows Pro, también pueden tener problemas de compatibilidad.
Todas estas complejidades con la administración de dispositivos BYOD, junto con la falta de estandarización, se suman a los principales costes ocultos que la mayoría de las empresas no consideran. Los costes ocultos pueden incluir todo, desde actualizaciones de licencias hasta costes adicionales de administración de IT, hasta lidiar con una fuga de datos de un ordenador portátil robada no segura. Dado que no hay una configuración BYOD estándar, estos costes pueden ser impredecibles y difíciles de administrar.
Esto no significa que BYOD no sea la opción correcta para la empresa. Si la mayoría de todos sus sistemas están en la nube, estos factores pueden no ser un gran obstáculo para nosotros. Pero es necesario que se tengan en cuenta antes de implementar BYOD y siempre que estemos hablando de presupuestos de IT.
Después de estas consideraciones previas, para la implementación entonces deberíamos seguir los siguientes pasos:

A. Decidir si BYOD es adecuado para nuestra empresa

Consideraremos las ventajas y desventajas [9] de traer primero nuestra propia política de dispositivo. En esto hemos concluido ya antes que, con una política bien diseñada, BYOD ahorra dinero a la empresa y brinda a los empleados una mayor flexibilidad.

B. Crearemos nuestra política en papel antes de ponerla en sistemas

Comprar un sistema de administración BYOD antes de tener una política es un desperdicio masivo de dinero. Es posible que compremos el sistema equivocado, por lo que primero crearemos una política. La política debe detallar lo siguiente: objetivos para BYOD (por ejemplo, experiencia del empleado, productividad), uso aceptable, prácticas de monitoreo y gobernanza.

C. Decidir el alcance de los dispositivos aceptables

Crearemos una lista de los dispositivos que aceptaremos que los empleados utilicen para el trabajo. Por ejemplo, podemos listar smartphones Android o modelos específicos de iPhone. Lo ideal es tener una aplicación multiplataforma.
Para crear nuestra lista, tendremos en cuenta algunos factores. Primero, ¿qué dispositivos poseen ya los empleados? En segundo lugar, ¿qué dispositivos podemos monitorear efectivamente con nuestros sistemas de administración BYOD?

D. Datos de empresa y personales separados

Para evitar un riesgo significativo de una violación de datos, necesitamos un enfoque BYOD multifacético.

- Tecnología: Proporcionaremos aplicaciones especializadas, idealmente con autenticación de dos factores, que contengan todos los datos de la compañía. Buscaremos aplicaciones que se puedan eliminar de forma remota en caso de que se pierda el dispositivo.
- Capacitación: ofreceremos capacitación a los empleados anualmente como parte del programa de ciberseguridad de su empresa. Dejaremos claro que existen riesgos de pérdida de información y que los empleados tienen un papel en la gestión de esa exposición.
- Consideraciones sobre responsabilidad: tomaremos nota de las preocupaciones sobre responsabilidad que se aplican en la empresa. Nuestra compañía aseguradora puede requerir ciertos procedimientos y registros para mantener una póliza de seguro de ciberseguridad válida. Por ejemplo, es posible que debamos mostrar que los datos de la empresa permanecen cifrados en los dispositivos BYOD.

E. Plan de protección de datos personales de los empleados

BYOD significa que los empleados están usando sus dispositivos personales en el trabajo. Eso significa que debemos estar muy atentos a la protección de nuestra privacidad al evaluar nuestras aplicaciones y las políticas de BYOD para la protección de la privacidad. Específicamente, el software y los procesos de administración de nuestros dispositivos nunca deben copiar, almacenar o interactuar con los datos y aplicaciones personales de un empleado. No limitaremos nuestra revisión a las aplicaciones, tampoco. La mayoría de los smartphones recopilan automáticamente datos de ubicación, pero no hay razón para recopilar dichos datos de los usuarios.

F. Configurar un proceso de monitoreo de uso de datos

Este paso de implementación es el más importante para las situaciones BYOD que utilizan muchos datos. Por ejemplo, si tenemos empleados que viajan frecuentemente con BYOD, pueden exceder su plan de datos personales. Para abordar esta situación, primero, alentaremos a los empleados a usar las conexiones Wifi tanto como sea posible. Segundo, diseñaremos un proceso de reembolso para que los empleados puedan hacer reclamos por cargos de datos más altos de lo habitual.

G. Simplificar el proceso de registro

Si queremos que los empleados se registren en BYOD en grandes cantidades, lo haremos más sencillo. Eso significa que no hay formularios en papel, y minimizaremos el número de

aprobaciones y tecnología. Idealmente, el proceso de inscripción o inscripción incluirá los siguientes elementos críticos:

- Solicitud de BYOD: pediremos a los empleados que envíen sus solicitudes a través de un sistema de tickets de IT, por ejemplo, de modo que todas las solicitudes puedan ser rastreadas.
- Configuración: haremos que la configuración sea lo más sencilla posible, como descargar algunas aplicaciones especializadas.
- Ganancias rápidas: ofreceremos a los empleados una ganancia rápida con BYOD en su primer día de uso, como poder revisar el correo electrónico corporativo en sus teléfonos.

E. Implementar monitoreo continuo de cumplimiento

Desde el punto de vista de la administración, BYOD no es autogestionado. Necesitaremos un proceso para revisar BYOD mensualmente desde una perspectiva de uso de datos, cumplimiento de políticas y seguridad. Cuando notemos problemas, nos pondremos en contacto con los usuarios para recordarles sus obligaciones para que puedan mejorar.

2.4 Establecer una solución BYOD para una empresa

2.4.1 ¿Qué es una solución MDM?

Para poder controlar, monitorizar y administrar de forma fácil y segura todo el parque de terminales en una empresa, existe un amplio conjunto de soluciones comúnmente llamadas MDM (Mobile Device Management), que permiten la administración de forma remota y centralizada.
Las funcionalidades más básicas que podemos encontrar en las soluciones de los diferentes fabricantes son:

- Control de aplicaciones: Permite a los administradores desplegar las instalaciones de forma centralizada, permitiendo y controlando aquellas que son necesarias y restringiendo de cualquier futura instalación, blindando así la posibilidad de manipulación por parte del usuario.
- Gestión de perfiles por dispositivo: Posibilidad de pre configurar perfiles de correo, calendario, contactos, accesos VPN por terminal y/o usuario de forma centralizada, pudiendo revocar fácilmente los privilegios en casos de pérdida, robo o bajas.
- Protección de los datos: Capacidad de forzar a utilizar el cifrado de disco y tarjeta en aquellos terminales que lo permitan.
- Borrado seguro remoto de los datos: En caso de pérdida o robo de los terminales, se podrá gestionar la eliminación del contenido de forma remota y segura.
- Monitorización: Capacidad de registrar las acciones producidas por el terminal, intentos de violación de la seguridad o de los mecanismos de protección, así como disponer de la geolocalización del terminal.
- Reportes de datos: Estadística de las variables de monitorización, para conocer la evolución del estado del dispositivo.

- Acceso a los dispositivos: Capacidad de añadir mecanismos de autenticación antes de poder acceder a la información de los terminales.

El funcionamiento de las soluciones MDM se compone de dos elementos: cliente y servidor. Los servidores suelen estar compuestos del aplicativo de gestión del MDM, la base de datos, el panel de administración web y los servicios utilizados por los clientes como podría ser los servidores de directorio activo, de certificados, de correo, etc.

Mientras que en el lado del cliente, se suele instalar un software de gestión para poder administrar el terminal remotamente y poder hacer tareas como actualizar el software, hacer monitorización o como añadir políticas de bastionado del terminal.

Para que se pueda establecer la comunicación con los servidores, es indispensable que los clientes tengan una conexión de datos a través de telefonía móvil o de una conexión Wifi. Otra característica de la aplicación cliente es que no necesita privilegios de administrador para ejecutarse, por lo que sus funcionalidades pueden verse limitadas.

2.4.2 ¿Cómo seleccionamos una aplicación MDM?

En el proceso de selección de una solución MDM se deben tener en cuenta ciertas consideraciones:

- Soporte de múltiples dispositivos como podrían ser teléfonos y tabletas con múltiples sistemas operativos. Normalmente cualquier terminal con Android, iOS o Windows Phone están soportados por los MDM.
- Buena integración con los servicios internos corporativos que la empresa ya utiliza.
- Garantizar la seguridad de la información interna de los dispositivos y de la transmisión de esta.

La mayoría de empresas que despliegan este tipo de soluciones proporcionan un dispositivo a cada empleado, pero en nuestro caso los empleados también podrán usar su propio dispositivo. En este caso se les instalará la aplicación cliente del MDM que permitiría a los terminales tener acceso a los servicios internos de la empresa y dotarlos de seguridad adicional en las comunicaciones, en el acceso físico y en la utilización de cifrado en los datos internos.

2.4.3 Estructura de la empresa Revital S.A: punto de partida

La empresa Revital S.A es una empresa de cosmética que fabrica cremas para un público principalmente femenino. Esta establecida en Barcelona y cuenta con un total de 125 empleados de los cuales:

- 5 usuarios son cargos directivos

- 7 son usuarios de administración y contabilidad
- 15 son usuarios de comunicación y redes sociales
- 10 son usuarios de diseño grafico
- 10 son usuarios de marketing
- 2 son usuarios del departamento legal
- 20 son usuarios de logística y almacén
- 15 son usuarios de desarrollo y laboratorio
- 20 son comerciales nacionales
- 15 son formadoras
- 5 son usuarios del departamento informático
- 1 usuario es del departamento de recursos humanos

Esta empresa cuenta con los siguientes elementos:

- 1 servidor físico con los archivos de la compañía
- 5 máquinas virtuales
- 1 ERP que externaliza a otra empresa que lo desarrolla
- Cada usuario cuenta con un ordenador, ya sea portátil o de mesa.
- 1 servidor Cloud con los archivos gráficos de la compañía
- 1 servidor web que gestiona una empresa externa.

Se debe tener en cuenta que cada usuario tiene un ordenador (no siempre de la empresa), ya sea portátil o de mesa, y que se trabaja con 25 ordenadores con sistema operativo MacOS y 100 ordenadores con sistema operativo Windows 10.
10 comerciales, 10 formadoras, todos los directivos, todos los informáticos y 10 usuarios de comunicación y redes sociales cuentan con móvil empresarial, todos en sistema operativo Android excepto los 5 directivos que son iOS, lo cual nos deja con un total de 35 dispositivos Android y 5 dispositivos iOS.
Existen 3 ordenadores portátiles que pertenecen al director comercial, a una traductora del departamento de comunicación y a un diseñador gráfico que no pertenecen a la empresa y que cada día deben acceder a recursos internos. De esos 3 ordenadores, uno de ellos cuenta con sistema operativo MacOS.
Además, recientemente los directivos han regalado a cada jefe de departamento un iPad como regalos de navidad y otro para ellos mismos que usan tanto dentro como fuera de la empresa y albergan datos de empresa y personales, en total 16 iPads.
Los comerciales nacionales y las formadoras no se encuentran todos en la oficina central, sino que están repartidos por diferentes puntos de España y acceden al servidor de archivos por VPN. No todos los que no se encuentran en la empresa cuentan con ordenador de empresa, o con dispositivo móvil de empresa. Pero al menos una vez al mes, pasan por la empresa y se reúnen con sus respectivos equipos presencialmente.

2.4.4 Propuesta para Revital S.A

Primeramente, se propondrá una política BYOD seguida de una aplicación MDM para los dispositivos móviles que accedan a datos empresariales. El software de administración de dispositivos móviles (MDM) permite a TI configurar, asegurar, monitorear y borrar los teléfonos inteligentes y tabletas. MDM es también un elemento de un conjunto más amplio de funciones,

a menudo llamadas gestión de movilidad empresarial, que puede hacer cumplir la política BYOD y otros requisitos.

2.4.5 Criterios de implementación de BYOD en Revital S.A

2.4.5.1 ¿BYOD es adecuado para Revital S.A.?

Si establecemos los riesgos actuales sin BYOD en la empresa tenemos:

- Uso de portátiles propios que acceden a recursos internos.
- Uso de portátiles de empresa que se encuentran fuera de ella casi siempre y con datos y acceso de recursos internos y privados.
- Uso del móvil personal en la empresa.
- Una política débil de restricción de acceso cuando el usuario deja la empresa

Por lo tanto, si aplicábamos una correcta política BYOD en Revital S.A podríamos resolver todos estos riesgos para la seguridad que ahora nos preocupan y brindaríamos a los empleados la opción de usar sus dispositivos sin peligro.

2.4.5.2 Creación de nuestra política

En un primer borrador de la política BYOD, estableceremos los objetivos y el uso aceptable de aplicaciones. Los objetivos son:

- Acceso seguro a nuestros archivos, aplicaciones y datos de empresa
- Protección de nuestros dispositivos de empresa y de los usuarios
- Una correcta política de restricción de acceso de un usuario sin que afecte a un dispositivo propio del usuario
- Que el usuario mejore su experiencia y productividad al darle la opción de traer sus propios dispositivos de forma segura.

2.4.6 Uso aceptable de aplicaciones

Implementar un programa BYOD no quiere decir que los empleados vayan a poder utilizar cualquier dispositivo. Para que el programa se implemente con éxito deberemos definir con que dispositivos estarán soportados en los diferentes perfiles de la empresa. Por ejemplo, se podrá acceder a un escritorio virtual completo en un teléfono Android, pero probablemente no sea práctico debido al reducido tamaño de la pantalla. Pero ese mismo escritorio en un iPad puede ser factible para algunos usuarios. Será necesario definir claramente las necesidades de los usuarios y seleccionar aquellos dispositivos que encajen con ellas. El área de TI también debe desarrollar, implementar y hacer cumplir una política BYOD que gobierne el acceso de los usuarios a la infraestructura y datos corporativos desde sus dispositivos. ¿Qué sucederá cuando un empleado no cumpla una política? ¿Y cuando deje la compañía? ¿Cómo se actuará en el caso de robo o pérdida del dispositivo? ¿El BYOD puede afectar al cumplimiento de alguna normativa o legislación? Hay que asegurarse de que las políticas cubren todos los escenarios y áreas que se verán impactadas por el BYOD.
La política no afectara sólo a los usuarios, también a los directivos que tendrán que fomentar su cumplimiento, al área de TI que tendrá que establecer sistemas para implementarla, y al área de

soporte de TI que deberá conocer los niveles de soporte que tendrá que proporcionar. Sera igual de importante la comunicación y formación en estas políticas a todos los implicados, por lo que el área de Recursos Humanos también debe estar involucrada. Para evitar responsabilidades legales, es necesario notificar a los empleados por escrito la política que detalle como tratará la organización los datos y comunicaciones corporativas y personales.

2.4.7 Alcance de los dispositivos aceptables

Definimos aquí una lista de los dispositivos que aceptaremos que los empleados utilicen para el trabajo. De cara a nuestra aplicación MDM, establecemos una lista de dispositivos permitidos teniendo en cuenta los dispositivos que ya poseen los empleados y los que podremos monitorear con una aplicación MDM multiplataforma.
Estos dispositivos permitidos son:

- Móviles con Android hasta Android 9
- Móviles con iOS hasta iOS 8
- Ordenadores con Windows 10
- Ordenadores con MacOS

2.4.8 Datos de empresa y personales separados

Para evitar un riesgo significativo de una violación de datos, necesitamos un enfoque BYOD multifacético.

- Tecnología: Se usará la doble autenticación en aplicaciones de correo electrónico de Microsoft Office 365, a parte de una aplicación MDM que controle el acceso a nuestros archivos y recursos internos, que contengan todos los datos de la compañía.
- Capacitación: ofreceremos capacitación a los empleados anualmente como parte del programa de ciberseguridad de su empresa. Dejaremos claro que existen riesgos de pérdida de información y que los empleados tienen un papel en la gestión de esa exposición.
- Consideraciones sobre responsabilidad: tomaremos nota de las preocupaciones sobre responsabilidad que se aplican en la empresa.

2.4.9 Plan de protección de datos personales de los empleados

Nuestro software MDM deberá cumplir con los siguientes requerimientos:

- Control de acceso: Los terminales implementan diversos controles para limitar el acceso al propio dispositivo o a sus recursos. Entre ellos: el PIN de acceso a la tarjeta SIM, la contraseña de acceso a la partición cifrada o el mecanismo de seguridad utilizado para desbloquear la pantalla.
- Políticas de seguridad: Fuerzan a los terminales a cumplir un mínimo de los requisitos de seguridad establecidos a nivel corporativo. Las directivas pueden ser, entre otras, denegar el acceso a instalar nuevas aplicaciones, restringir el acceso a determinadas funcionalidades (como la cámara, el thetering, bluetooth, etc.) o incrementar la complejidad de las credenciales utilizadas por el usuario.

- Análisis de los permisos: Es conveniente estudiar si las aplicaciones permitidas en los dispositivos pueden requerir funcionalidades no necesarias para la correcta operatividad. Estas funcionalidades son requeridas en el proceso de instalación y en la ejecución de las aplicaciones. Además, se deben considerar también los permisos que las aplicaciones asignan a los recursos de disco del terminal.
- Protecciones técnicas: Son todas aquellas medidas generales que pretenden incrementar el nivel de seguridad y que se deberían analizar:
- Seguridad del sistema: El acceso a procesos en ejecución, el acceso a ficheros o directorios, la ejecución de aplicaciones no firmadas, la configuración del firewall, etc.
- Seguridad de los datos: El cifrado de los datos almacenados, el borrado remoto en el caso de pérdida o robo, o el borrado automático de los datos en caso de que se sobrepase el número máximo de intentos erróneos de acceso.
- Aplicaciones de seguridad externas o complementarias: Por ejemplo, los antivirus, así como todas las aplicaciones que aporten una capa extra de seguridad.
- Análisis de las contraseñas: Los terminales pueden ser entregados a los empleados con una contraseña (de bloqueo o de cifrado) que pueda resultar poco robusta o, incluso, pueda ser la contraseña por defecto del terminal. Es por ello que se debe validar la existencia de políticas de bastionado que garanticen unos mínimos niveles de seguridad. Por ejemplo, a nivel de contraseñas, podría ser el uso de credenciales con caracteres alfanuméricos y signos de puntuación, una longitud mínima de diez caracteres, etc.
- Análisis de datos: Se debe contemplar el análisis sobre los sistemas de ficheros con el objetivo de encontrar fugas de información que puedan haber generado las aplicaciones. Por ejemplo, ficheros temporales o ficheros con credenciales (cifradas o no), información sensible en ficheros de log, contenidos de bases de datos o ficheros XML, etc.
- Análisis de la navegación por Internet: Si los dispositivos utilizan redes Wifi, las comunicaciones pueden ser interceptadas. Todas las comunicaciones deberían realizarse cifradas y los dominios permitidos deberían gestionarse a través de ACL en la pasarela proxy.
- Análisis de la aplicación cliente: Se debe analizar el funcionamiento interno de la aplicación para verificar que las especificaciones de seguridad descritas en el producto realmente se cumplen. Sobre todo, es importante verificar la seguridad del proceso de registro del terminal (enrollment) en el MDM.
- Actualizaciones de aplicaciones y del sistema: Debe existir un mecanismo que, de forma transparente, aplique parches de seguridad en el sistema, así como las actualizaciones de las aplicaciones.

2.4.10 Configurar un proceso de monitoreo de uso de datos

Como contamos con bastantes empleados que viajaran frecuentemente con BYOD, pueden exceder su plan de datos personales. Para abordar esta situación, primero, alentaremos a los empleados a usar las conexiones Wifi tanto como sea posible. Segundo, los empleados podrán solicitar un reembolso para que puedan hacer reclamos por cargos de datos más altos de lo habitual.

2.4.10.1 Simplificar el proceso de registro

Si queremos que los empleados se registren en BYOD, lo haremos de la siguiente forma:

- **Solicitud de BYOD:** pediremos a los empleados que envíen sus solicitudes a través de un sistema de tickets de IT, de modo que todas las solicitudes puedan ser rastreadas.
- **Configuración:** lo mejor será que el usuario solo tenga que descargar una o dos aplicaciones e iniciar sesión en ellas, de forma que no sea muy complicado el proceso de registro y configuración.

2.4.10.2 Implementación de monitoreo continuo de cumplimiento

Monitorizaremos mensualmente el uso de datos, cumplimiento de políticas y seguridad. Cuando notemos problemas, nos pondremos en contacto con los usuarios para recordarles sus obligaciones para que puedan mejorar.

2.4.11 Selección de una aplicación BYOD: Sophos Unified Endpoint Management.

Sophos Mobile es una solución de seguridad y de gestión unificada de endpoints (UEM) que ayuda a las empresas a invertir menos tiempo y esfuerzo en la gestión y la protección de endpoints tradicionales y móviles. Sophos Mobile es la única solución UEM que se integra de forma nativa con una plataforma líder de seguridad next-gen para endpoints y admite la gestión de dispositivos Windows 10, macOS, iOS y Android.

2.4.11.1 ¿Porque una solución UEM en vez de MDM?

Después de estudiar las soluciones MDM, sabemos que un MDM trata de administrar los dispositivos de forma remota, permitiendo a los usuarios realizar ciertas tareas prescritas en sus teléfonos y tabletas. MDM incluye funciones como aprovisionamiento de dispositivos, inscripción, seguridad de dispositivos y seguimiento de ubicación. También ayuda a borrar los datos en caso de que el dispositivo sea robado o perdido. Una herramienta básica de MDM tiene la capacidad de hacer cumplir las políticas de seguridad, rastrear el inventario y realizar el monitoreo y los informes en tiempo real.

Desde el punto de vista de la seguridad, esta es una forma perfectamente razonable de administrar un dispositivo propiedad de la empresa. Pero algunos empleados no se sentirán muy cómodos llevando dos dispositivos separados para uso comercial y personal. Por lo tanto, a las empresas nos interesa considerar la demanda de BYOD de los empleados. Un solo dispositivo que les da a los empleados la flexibilidad y la facilidad para pasar del uso personal al uso en el trabajo, en cualquier lugar y en cualquier momento.

Entonces hemos visto que el rápido crecimiento de los teléfonos inteligentes, el mercado de aplicaciones móviles y la necesidad de seguridad de datos condujeron entonces a la creación de la solución de administración de aplicaciones móviles (MAM), que limitó la administración y el control de aplicaciones comerciales específicas. Mobile Application Management es como MDM, excepto que solo se aplica a aplicaciones específicas en un dispositivo en lugar de todo el dispositivo. MAM ayuda a crear una tienda de aplicaciones empresariales y a impulsar o actualizar las aplicaciones necesarias en dispositivos empresariales de forma remota. Pero a veces MAM también tiene su propio conjunto de desafíos. Dado que cada aplicación empresarial requiere una codificación única para funcionar con cada producto MAM individual, la disponibilidad de las aplicaciones para una plataforma independiente específica puede ser limitada.

No obstante, MAM fue un acuerdo perfecto entre empleados y empleadores sin comprometer la seguridad de los datos e interferir en la privacidad de los empleados. Pero en la práctica, la experiencia no es tan buena, ya que no se puede extender fácilmente para que sea compatible con la mayoría de las aplicaciones nativas de la tienda de aplicaciones. Después de eso, hubo varias etapas de desarrollo pequeñas donde la experiencia se redefinió con la evolución de aplicaciones como MIM (Mobile Information Management) y MCM (Mobile Content Management). Se centran en la seguridad de un repositorio de documentos en particular donde los empleados y empleadores acceden y comparten documentos o archivos sin afectar a todo el dispositivo u otras aplicaciones.

Y finalmente, llegamos a la etapa de EMM. EMM no es más que la combinación de soluciones MDM y MAM equipadas con un contenedor seguro que mantiene seguros los datos comerciales. Una solución de EMM además de MDM ofrece administración de aplicaciones móviles, administración de contenido móvil, ajuste de aplicaciones y “contenedorización”. EMM es un paquete completo de servicios que ofrece seguridad de datos completa en BYOD y Dispositivos Dedicados (anteriormente llamados COSU o Corporativo de Uso Único) para empresas.

Mientras que las soluciones MAM y MDM han pasado por actualizaciones continuas para satisfacer las crecientes necesidades de seguridad de datos en las empresas, BYOD como concepto entró en escena, lo que permitió a los usuarios finales incorporar sus propios dispositivos móviles e inscribirlos en los recursos corporativos de TI. BYOD se habilita a través del concepto de "contenedorización", lo que permite a los administradores de TI separar los datos personales y de la empresa en el mismo ordenador portátil. Ayuda a los administradores de TI a crear contenedores cifrados, habilitados para políticas y distintos en los dispositivos personales de los empleados para usar las aplicaciones del navegador y entregar correo electrónico y datos específicos.
En pocas palabras, la principal diferencia entre MDM y EMM es que MDM administra todas las funciones del dispositivo, mientras que EMM administra todo el dispositivo. EMM proporciona cumplimiento de políticas, personalización de aplicaciones, seguridad de datos y documentos, e incorpora en los servicios de directorio de red.

El paso de MDM a EMM ha sido bastante rápido a medida que más organizaciones se están dando cuenta de la necesidad de proteger sus redes y garantizar el cumplimiento de los datos. Y con las nuevas tecnologías progresivas que ingresan al mercado global, el mundo está avanzando hacia un nuevo conjunto de soluciones de EMM como Unified Endpoint Management (UEM), que permite a las empresas administrar todos los puntos finales como ordenadores portátiles, móviles, tabletas, PC, impresoras y dispositivos portátiles utilizando una sola solución extensa de EMM.

Es por esto que proponemos para Revital S.A. la aplicación Sophos Unified Endpoint Management.

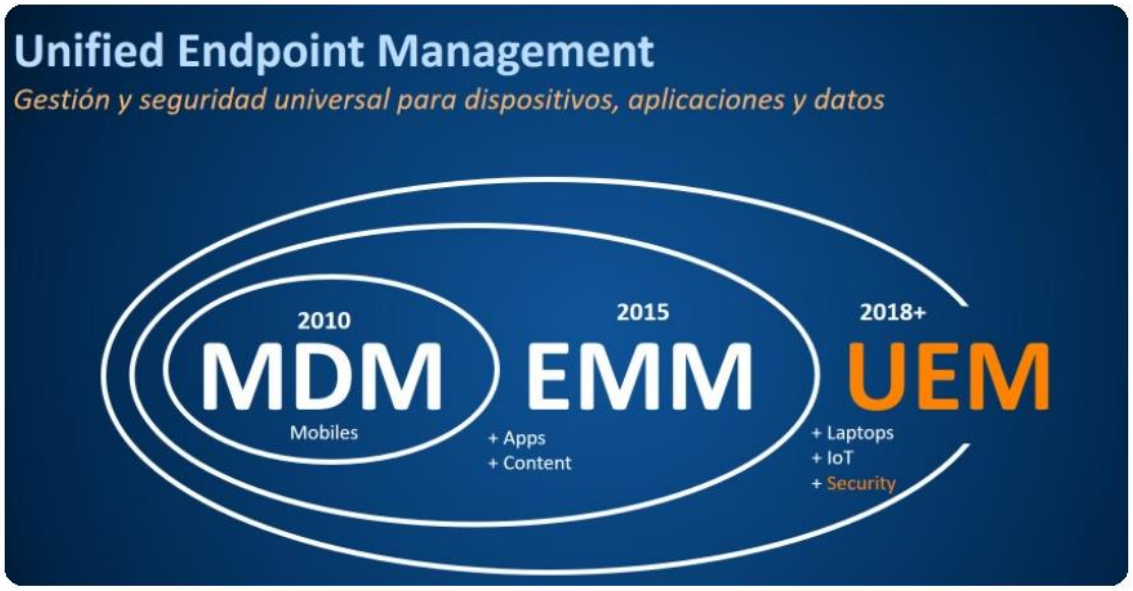

Figura 1: Evolución de MDM a UEM

En la Figura 1 podemos ver la representación de lo explicado, como el MDM a partir de 2015 pasa a ser Enterprise Mobile Management, ya que vienen de la gestión de móviles y añaden el control de apps, de contenido, etc. Después, a partir de 2018, se dan cuenta de que la diferencia de un Smartphone y un portátil es tan pequeña que a veces no se diferencia. Por eso sale el concepto

UEM (Unified Endpoint Management), Por lo tanto, aquí añaden la parte de laptops, IOT y seguridad, para poder controlarlo todo.

Figura 2: Dispositivos Sophos Mobile

De esta forma gestionamos todos estos dispositivos con configuración de políticas, como prohibir el uso de la cámara, prohibir acceso a apps, gestión de inventarios, etc. Y otras funcionalidades que vamos a ver a continuación.

2.4.11.2 Características destacadas de Sophos UEM

1. **Gestión unificada de endpoints segura**

Gestiona y protege los endpoints móviles, Windows 10 o macOS personales o corporativos de un sistema para lograr una estrategia de gestión más sencilla que garantice unas políticas de seguridad de empresa uniformes y un acceso seguro a los recursos de la empresa. Para hacer posible una productividad máxima, las organizaciones como Revital S.A. que han adoptado el uso de dispositivos personales en el trabajo (BYOD) pueden aplicar políticas coherentes, independientemente del tipo o propiedad de dispositivo. Sophos Mobile protege los datos empresariales, los usuarios, los endpoints y los dispositivos móviles.

2. **Administración moderna con Sophos Security**

Establece una primera línea de defensa en el nivel de los dispositivos móviles con la tecnología antivirus para móviles (que puede ser opcional) y la protección web de prestigio de la aplicación Sophos Mobile Security. Impone las políticas de la empresa con comprobaciones de cumplimiento que limitarán automáticamente el acceso a los recursos empresariales o iniciarán acciones correctivas en caso de infracciones.

3. **Mantiene la seguridad de los datos empresariales y la privacidad de los datos personales**

La protección de los datos empresariales en dispositivos móviles tanto corporativos como personales es fundamental. Para garantizar la seguridad de los datos corporativos y la privacidad de la información personal, en la licencia completa el contenedor de Sophos seguro y cifrado mediante AES-256, incluye un contenedor para correo electrónico y documentos que se puede desplegar con o sin administrar el propio dispositivo en sí. La administración exclusiva de contenedores ofrece a los administradores control sobre el contenido corporativo sin incidir en la privacidad de los usuarios, algo ideal en escenarios BYOD como el nuestro. De esta manera, con el concepto "contenedores" podemos separar lo personal de lo corporativo, por lo que, si el usuario compromete de alguna forma el dispositivo, no tiene que afectar al contenido de éste.
Las siguientes apps fáciles de usar para iOS y Android permiten a los usuarios acceder al contenido del contenedor que nos ofrece la administración de dispositivos: Sophos Secure Email para el correo electrónico, los contactos y el calendario, y Sophos Secure Workspace para documentos y la navegación web corporativa. El contenedor de Sophos ahorra tiempo con una configuración sencilla del correo electrónico y del acceso a los datos y protege a los usuarios frente a enlaces maliciosos con tecnología antiphishing. Podrimos incluso restringir el acceso al contenedor en función de la hora, la red Wifi o la ubicación geográfica.
Otra funcionalidad de la gestión de contenido que podríamos aplicar, por ejemplo, es si quisiéramos enviarles a los comerciales de la empresa Revital S.A. la lista de precios del año 2020, se lo podría enviar a todos los móviles del grupo "comerciales". Eso se puede hacer público, para que ellos lo puedan enviar, y lo mismo podríamos hacer para todos los grupos que tengamos. Con la gestión de contenido podemos hacer esto y podemos usar a parte los contenedores de Android Enterprise, integración de AE.

4. Instalación y configuración remotas

Podemos dedicar menos tiempo a gestionar y proteger los endpoints móviles y tradicionales para aumentar la productividad, y tener la tranquilidad de que se han reducido los riesgos asociados. Podemos configurar los endpoints Windows 10, MacOS, iOS o Android corporativos o BYOD de forma remota con una potente selección de políticas (como gestionar el uso de aplicaciones específicas con una lista negra de las aplicaciones que no queremos usar, o una lista blanca de las que si queremos que se puedan usar), perfiles y opciones de configuración. Reduciremos así el número de llamadas al servicio de asistencia gracias a nuestro flexible portal de autoservicio que permite a los usuarios solucionar sus propios problemas, sin que intervenga el departamento informático en absoluto. A través de ese portal podremos ver en qué estado se encuentra el dispositivo, si queremos que sea localizado, etc.

Figura 3: Características y aplicaciones de Sophos Mobile

2.4.11.3 Ventajas de Sophos UEM

1. **Productividad – Los usuarios pueden trabajar con el dispositivo que prefieran**

Mejora de la productividad al permitir que los empleados utilicen de forma segura dispositivos móviles para trabajar. Una extensa serie de opciones de seguridad y administración garantiza que los datos de la empresa están seguros, por ejemplo, mediante la configuración del acceso a la información y al correo electrónico corporativos tanto en dispositivos móviles personales como corporativos.

2. **Seguridad – Para usuarios, datos y dispositivos**

Sophos Mobile es el único producto de gestión unificada de endpoints que se integra de forma nativa con una plataforma líder de seguridad next-gen para endpoints, y que protege a los usuarios de endpoints tradicionales y móviles. Mantiene en contenedores el correo electrónico y los documentos empresariales de los dispositivos móviles para asegurarse de que el acceso a los datos corporativos está controlado y protegido, incluso para los usuarios con dispositivos personales que pueden tener acceso a la información de la empresa sin que se incida en su privacidad. Su tecnología de defensa contra amenazas móviles protege a los usuarios de apps y sitios web maliciosos.

3. **Simplicidad – Fácil de configurar, administrar y mantener**

Sophos Mobile nos permite ponernos en marcha en cuestión de minutos como solución alojada en Sophos Central o bien puede instalarse de forma local, según las necesidades de la empresa. El flujo de trabajo de administración intuitivo y el portal de autoservicio flexible permiten que los administradores inviertan menos tiempo en las tareas diarias de protección y administración de endpoints tradicionales y móviles, con un coste total de propiedad menor.
Sophos Mobile también se puede utilizar para gestionar y configurar las apps de Microsoft Office 365 en dispositivos móviles. Los administradores se ahorrarán tiempo al usar una sola consola, lo que hace que la creación y distribución de políticas sea sencilla desde la interfaz de administración de Sophos Mobile.

4. Valor – Protege los dispositivos móviles de forma asequible

Sophos Mobile se comercializa en forma de licencias por usuario y constituye una solución muy rentable, puesto que permite a las empresas administrar y proteger los dispositivos de toda la organización sin gastar de más en funciones infrautilizadas

2.4.11.4 Sophos UEM: Panel de configuración

En este apartado esquematizaremos como es el portal de administración de Sophos Mobile UEM y cómo puede el usuario iniciar sesión y descargar la aplicación en el dispositivo escogido para que podamos administrarlo.

El portal de autoservicio BYOD:

- Permite a los usuarios gestionar sus propios móviles
- Geolocaliza, bloquea, resetea…
- Posibilidad mensaje de preinstalación y post instalación

Aunque no nos gusta mucho confiar en el usuario, a veces es necesario. Ellos mismo acceden al portal de autoservicio de Sophos, y preconfiguramos las cosas que queremos que se instalen en el dispositivo que el elija, de forma que automatizamos el proceso para que el usuario lo haga solo sin intervención del departamento de IT.
Tiene que haber un mensaje de preinstalación, porque como puede ser un dispositivo personal del usuario, existen políticas de geolocalización, por lo tanto, hay que avisarlo de esto, de que instalaremos apps en su dispositivo, etc. Este mensaje debe ser redactado por el departamento legal correspondiente. Si lo aceptan, se instalará el UEM, en caso contrario, no podremos.
También se tienen un SSO con Azure, si estamos federados y podemos hacer uso del single sign-on y el usuario solo tiene que logarse en el portal con su usuario de dominio y descargarlo todo.
Se recomienda factor de doble autenticación para más seguridad:

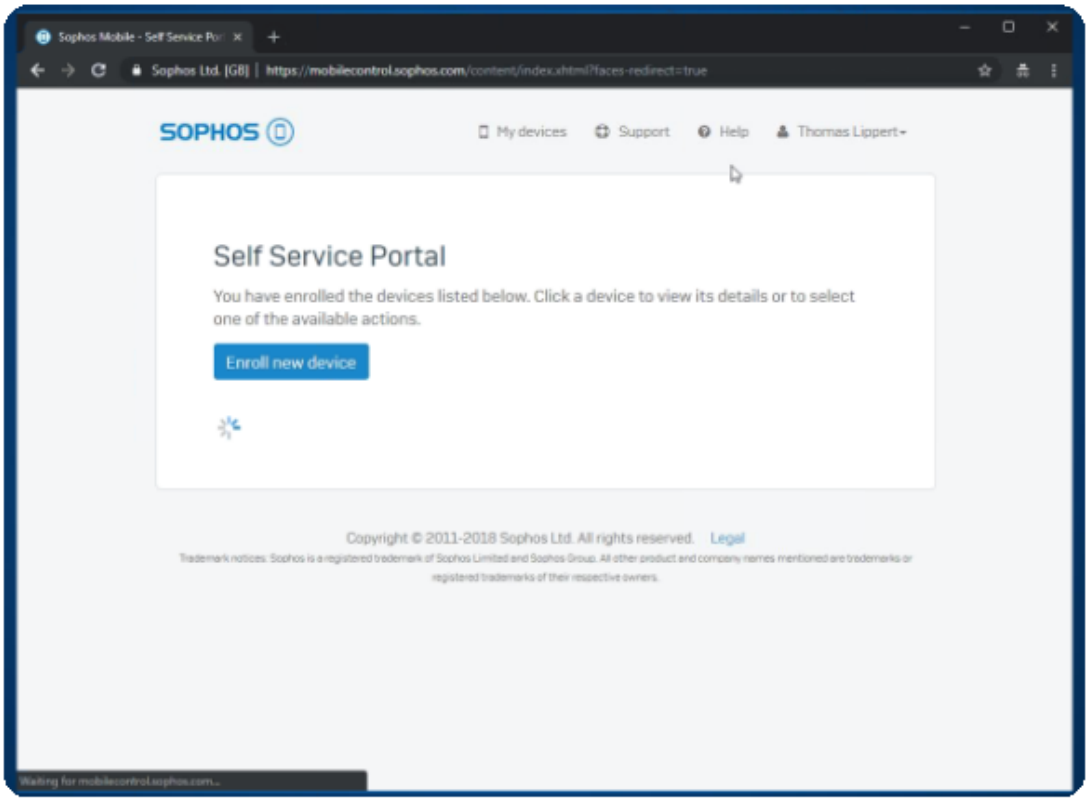

Figura 4: Self Service Portal Federated Authentication

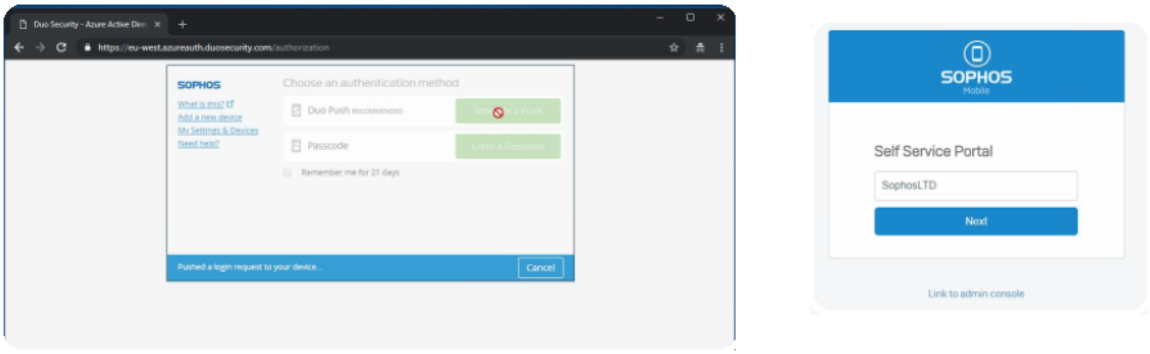

Figura 5: Self Service Portal Federated Authentication

Algunas de las funcionalidades que podremos hacer desde aquí serán:

- Control remoto gracias a la integración con TeamViewer
- Escanear aplicaciones al instalarlas
- Escanear aplicaciones ya instaladas tanto en dispositivos como en sistemas de almacenamiento
- Escanear aplicaciones a petición o intervalos establecidos
- Mostrar aplicaciones no deseadas
- Utilizas información sobre amenazas en tiempo real a través de la nube
- Control Web, web filtering y sms filtering.

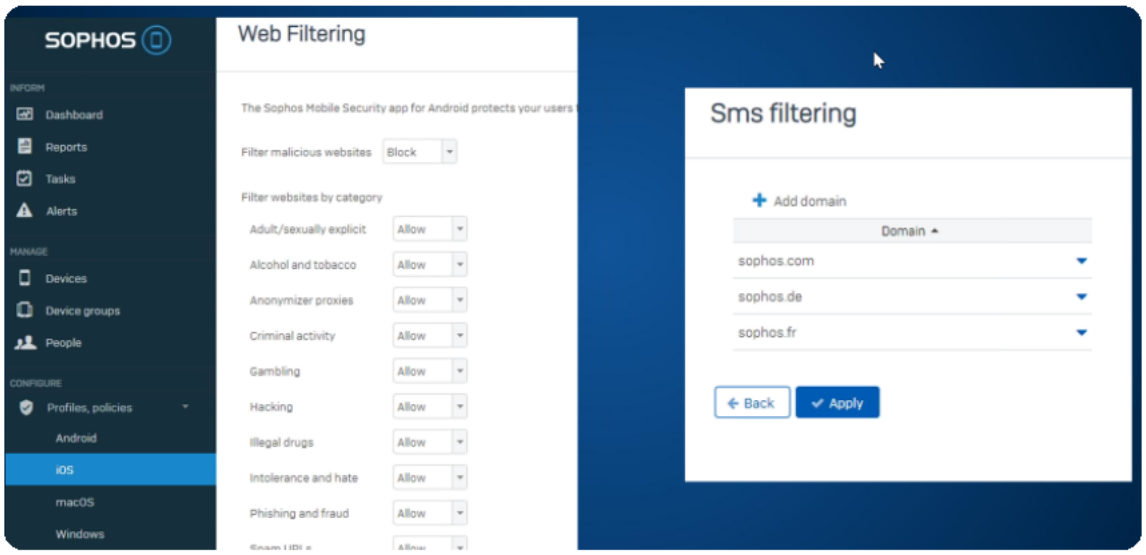

Figura 6: Filtrado Web para iOS y Android

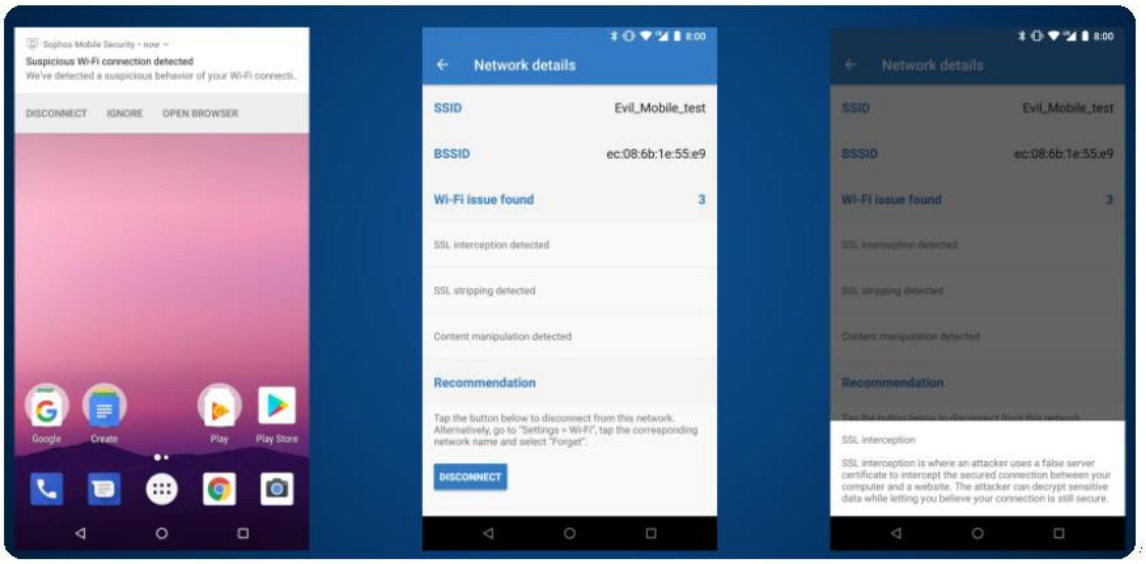

Figura 7: Detección MitM

Integra también la posibilidad de detectar “Man in The Middle” (MitM). Un usuario podría conectarse a una red wifi publica y ser víctima de un ataque MitM, por lo que, con esta funcionalidad, veríamos una conexión sospechosa y nos avisaría de los datos de esta conexión sospechosa, tanto en iOS como en Android.

Después de registrar los dispositivos que necesitemos el panel de administración de Sophos Mobile se muestra de esta forma:

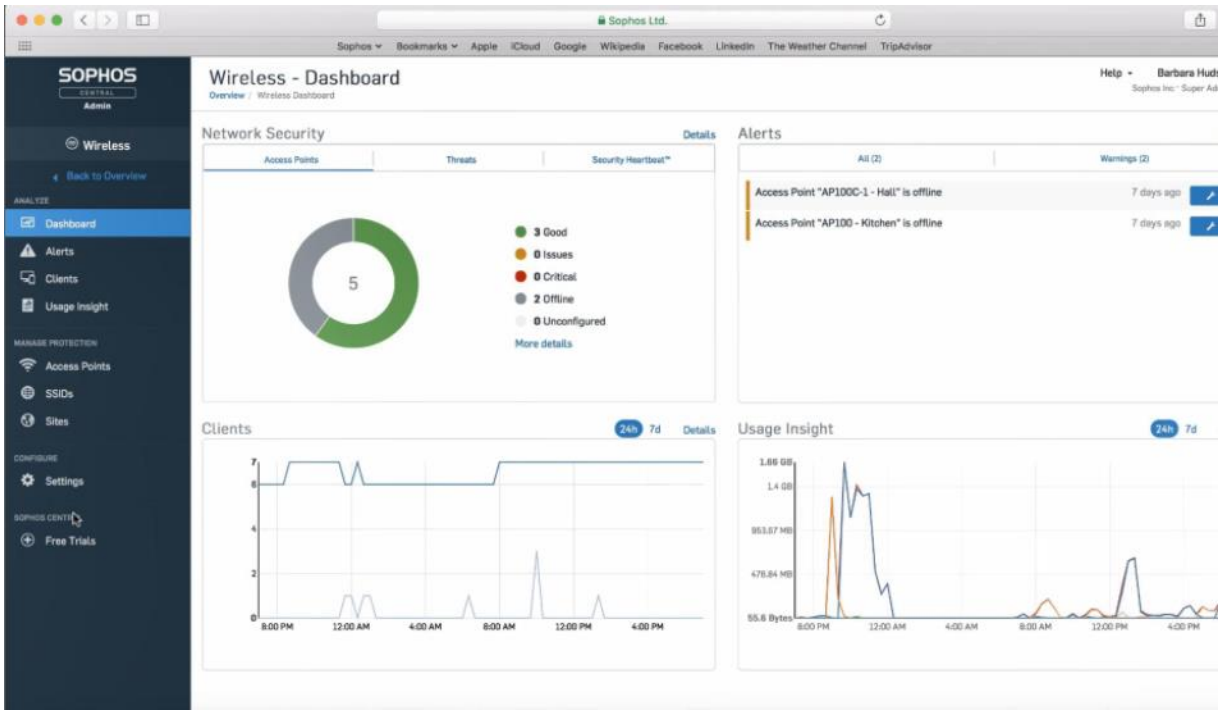

Figura 8: Sophos Control Panel

Si quisiéramos aplicar políticas o reglas a un dispositivo, nos mostraría el panel siguiente al seleccionarlo:

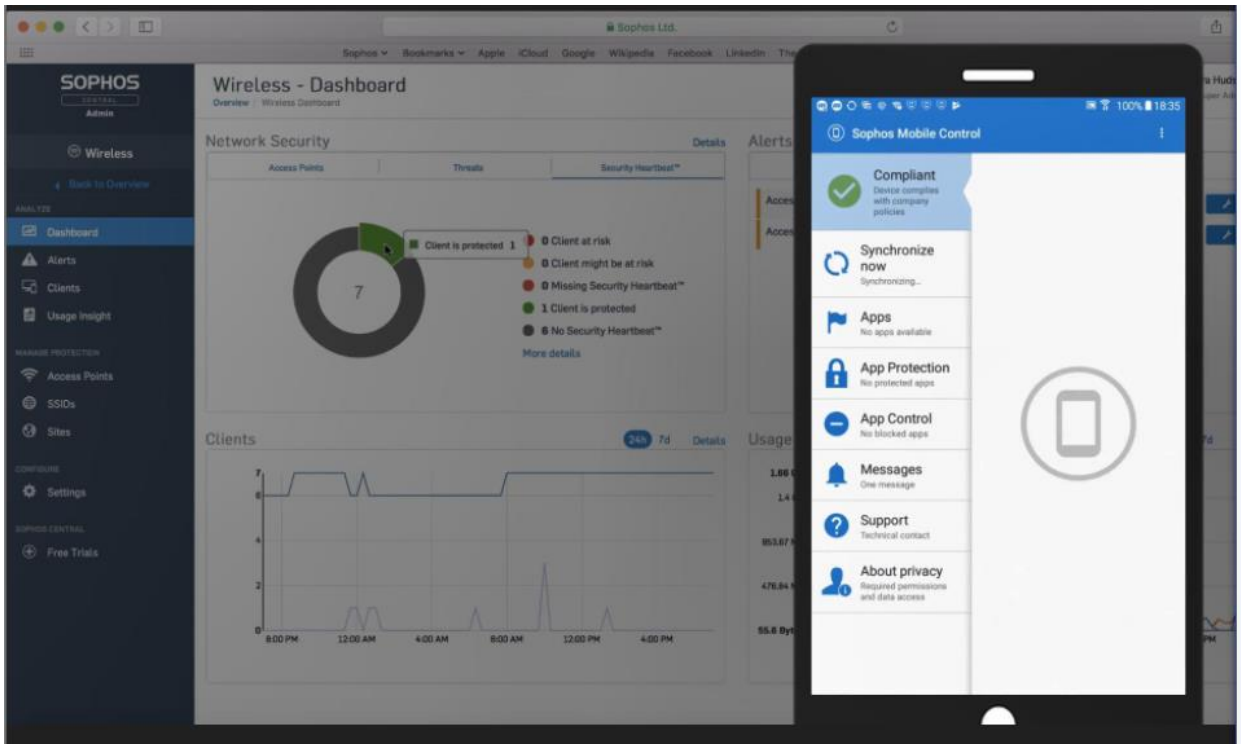

Figura 9: Sophos Mobile Control Device Panel

Desde aquí, podemos aplicar las reglas que necesitemos en directo y comprobar en remoto como las aplica.

2.4.11.5 Método de despliegue y licenciamiento

1. MÉTODO DE DESPLIEGUE

A. Administrar Sophos Mobile totalmente alojado en Sophos Central:
   - Opción ideal si se quiere dedicar menos tiempo y esfuerzo a la administración de sus dispositivos tradicionales y móviles.
   - Solución completa de gestión unificada de endpoints (UEM) junto con la protección para endpoints, redes y servidores gestionada desde la misma interfaz de administración
   - Póngase en marcha en cuestión de minutos y ahorre recursos informáticos sin instalaciones de servidor
   - Disfrute de la misma consola, el mismo diseño y la misma simplicidad en todos sus productos de seguridad de Sophos

B. Instalación a nivel local
   - Si se quiere que todos los datos permanezcan en sus propios servidores, esta es la versión ideal.
   - Totalmente integrado en el entorno informático
   - Instalación local; todos los datos permanecen en sus servidores
   - Conexión con el directorio de usuarios existente

2. LICENCIAMIENTO

Como vemos, si tenemos la opción Sophos Mobile Advanced, tendremos integradas Sophos Standard y Sophos Mobile Security.
Sophos además nos da la opción de que, si tuviésemos otros MDM, podemos añadir Sophos Mobile Security. Con lo cual la capa de UEM nos la daría el MDM que tendríamos ahora y la capa de MTD (protección de los dispositivos móviles) nos la daría Sophos.

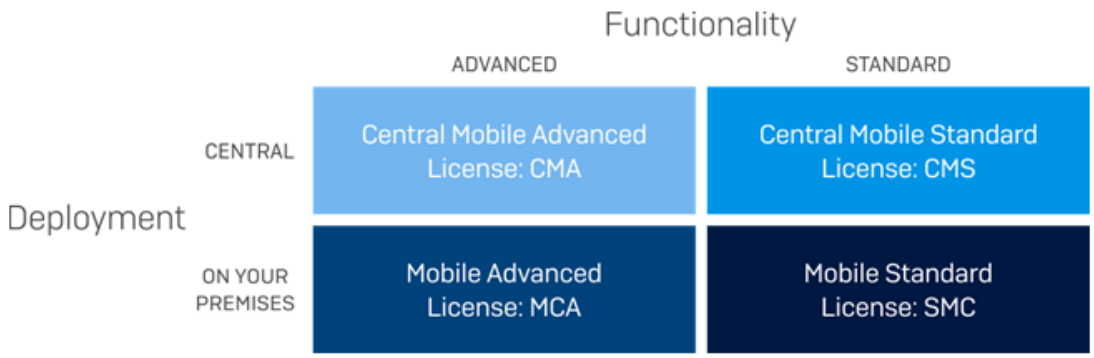

Figura 10: Licencias Sophos Mobile

Características

	SOPHOS MOBILE ADVANCED	SOPHOS MOBILE STANDARD	SOPHOS MOBILE SECURITY
Opción de administración en Sophos Central o local	✔	✔	Sophos Central solamente
Gestión de dispositivos	✔	✔	
Administración de aplicaciones	✔	✔	
Administración de contenidos	✔		
Contenedor de Sophos (Secure Workspace, Secure Email)	✔		
Sophos Mobile Security (para Android)	✔		✔
Kit de desarrollo del software (SDK) de Sophos Mobile	✔		

Figura 11: Características de las licencias de Sophos Mobile

3. Conclusiones finales

Es evidente que los empleados son más productivos y están más satisfechos cuando se les deja elegir sus propias herramientas de trabajo. En un escenario tan cambiante como el tecnológico, pocas son las empresas que pueden evitar que los usuarios utilicen sus dispositivos para aspectos relacionados con trabajo, algo que podría equiparase a un BYOD sin los elementos de control necesarios.

Por su parte, modelos como CYOD o COPE surgen como alternativas que combinan un mayor control (y, por ende, más seguridad) para la compañía con la libertad de elección del empleado. La realidad es que, independientemente de la postura de la empresa (incluso si esta no existe) ya hay trabajadores que utilizan sus dispositivos así que se hace necesario establecer una estrategia coherente e integral de movilidad empresarial.
La labor de los responsables de IT es evitar que las aplicaciones y los datos corporativos puedan estar expuestos a los posibles riesgos del uso personal. Por ello, cualquier estrategia de movilidad debería incluir la solución técnica necesaria para dotar de independencia los dispositivos en caso de problemas, como un robo, extravío, infección por virus o cualquier otra circunstancia.

Así como los modelos como BYOD varían de forma significativa en su aplicación final en función de las necesidades y el sector de cada empresa, implementarlas es una tarea que debe afrontarse de forma global e implicar no solo a los departamentos tecnológicos, sino al financiero, al legal y a los responsables de recursos humanos, y una conciencia global de la empresa. Solo así las empresas pueden beneficiarse de las ventajas inherentes a la movilidad empresarial.

Se ha seguido la planificación, excepto en que al principio se tenía en mente aplicar un sistema MDM, pero al final se ha aplicado un sistema UEM, por lo que ha sido un cambio significativo que mejora la seguridad de lo que teníamos en mente en la primera fase.

Después de implementar un sistema UEM en la empresa Revital S.A. los empleados pueden usar sus dispositivos de forma segura para ellos y para la compañía, con lo cual podemos corroborar que hemos conseguido el principal objetivo del trabajo: encontrar una aplicación que recomendar a una empresa que aplique políticas BYOD, a parte de las reglas de seguridad establecidas.

Respecto a lo aprendido durante el trabajo, podríamos concluir en que la seguridad en la empresa es cada día un factor de mayor importancia y mayor riesgo. Considero que, como administradora de IT de una empresa, aplicar políticas BYOD es esencial porque, al fin y al cabo, no podemos controlar nunca al 100% todo lo que ocurre en nuestra empresa ni todo lo que hace el usuario en su día a día. Además, si se trata de una empresa internacional con usuarios distribuidos en diferentes partes del mundo y sin un control de TI al menos semanal, perderíamos el control totalmente de sus dispositivos y de los datos de empresa. Si no tenemos políticas, reglas y aplicaciones que nos ayuden en esta tarea, podríamos ser víctimas de ataques o fuga de información, y al final el responsable de que eso suceda no es el usuario que lo ha provocado, sino el administrado de TI que no lo ha previsto. Es por esto que termino afirmando que

actualmente, cualquier empresa debería estar preparada para todos estos riesgos, empezando por aplicar una política BYOD.

4. Trabajo Futuro

El mercado BYOD está programado para alcanzar casi 367 mil millones de dólares para 2022, un aumento de solo 30 mil millones en 2014. Es evidente que continuará siendo adoptado por las empresas, obligadas por los beneficios, así como por los empleados interesados en disfrutar de una mayor flexibilidad. En resumen, BYOD está aquí para quedarse.

Sin embargo, parece más probable que las empresas encarguen los programas "traiga su propio dispositivo" para aumentar, en lugar de revisar, su forma tradicional de trabajar. Lo mejor de ambos mundos, en otras palabras, estará a la orden del día.

La relación entre los departamentos de TI y BYOD también está sujeta a cambios a medida que más empleados utilicen sus propios dispositivos en el trabajo. Los administradores de TI debemos estar atentos a los empleados y los dispositivos que traen al trabajo para asegurarnos de que la empresa esté protegida y de que el empleado no esté violando ningún problema de cumplimiento.

Aunque siempre habrá división de opinión con respecto al uso de BYOD. Si bien algunos empleados prefieren separar su trabajo y sus vidas privadas por completo, y son rechazados por la idea de usar un dispositivo personal en la oficina, otros abrazan con entusiasmo la eliminación de dichas barreras.

La evolución de BYOD necesariamente incluirá cambios en la política y el cumplimiento, y un mayor perfeccionamiento de las expectativas de la empresa y del empleado. Los protocolos de seguridad también pueden estandarizarse a medida que las compañías buscan fortalecer sus defensas de datos, y algunas compañías pueden expandirse creando aplicaciones internas y herramientas de administración de proyectos para usar en dispositivos portátiles.

5. Glosario

SMARTPHONES: es el término en ingles que se utiliza para denominar a un teléfono inteligente, es un equipo celular con funciones más avanzadas que las de un teléfono corriente.

SMARTWATCHES: Un smartwatch es un reloj inteligente. Smartwatch es el nombre comercial que se ha venido empleando para designar productos de alta tecnología, como teléfonos celulares (smartphone) o televisores (Smart TV), y que se distinguen, entre otras cosas, por tener la capacidad para funcionar en red y proporcionar acceso a internet.

BYOD: siglas en inglés de Bring Your Own Device. Es una tendencia en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

CYOD: siglas en inglés de Choose Your Own Device, o elije tu propio dispositivo. Consiste en permitir que los usuarios elijan su propio dispositivo de un listado de dispositivos que cumplan con unos requisitos mínimos, y ese dispositivo pase a pertenecer a los empleados, bien porque la empresa se lo regale o porque los usuarios lo compren y la empresa asuma el pago de las facturas de consumo.

COPE: siglas en inglés de Corporate Owned, Personally Enabled. Método diseñado para brindarles a las organizaciones más control sobre la movilidad empresarial. Los empleados reciben los dispositivos elegidos y pagados por la organización.

MDM: método integral que permite a una empresa unificar todos sus datos críticos en un solo repositorio.

UEM: es un enfoque para asegurar y controlar las computadoras de escritorio, laptops, teléfonos inteligentes y tabletas de una manera conectada y cohesiva desde una única consola.

EDR: detectar dentro de los móviles lo que está ocurriendo.

MTD: protección de los dispositivos móviles

PHISING: técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

MAN IN THE MIDDLE: es un tipo de ataque informático en el que el atacante tiene conexiones independientes con las víctimas y trasmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante

WEB FILTERING: software diseñado para restringir los sitios web que un usuario puede visitar en su equipo.

THETERING: proceso por el cual un dispositivo móvil con conexión a Internet actúa como pasarela para ofrecer acceso a la red a otros dispositivos, cualesquiera que estos sean, asumiendo dicho dispositivo móvil un papel similar al de un módem o enrutador inalámbrico. Esto se puede realizar mediante una conexión red inalámbrica, Bluetooth o mediante un cable, como el USB.

SINGLE SIGN- ON: es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación.

WINDOWS ACTIVE DIRECTORY: son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de ordenadores.

AZURE ACTIVE DIRECTORY: es un servicio de administración de acceso y de identidades basado en la nube de Microsoft que ayuda a los recursos de acceso y de inicio de sesión de los empleados en recursos externos, como Microsoft Office 365, Azure Portal y miles de otras aplicaciones SaaS.

ENDPOINT: Dispositivo informático remoto que se comunica con una red a la que está conectado.

ENROLLMENT: registro de un usuario en una plataforma

SEGURIDAD NEXT-GEN: Concepto promocionado por algunos proveedores de software de seguridad para el Endpoint como una forma para mejorar la eficacia en la protección de los endpoints ante un peligro, dado el importante papel que juegan los endpoints en los ataques de ciberseguridad, la forma en la que la movilidad y las apps Cloud han ampliado la superficie de ataque, y la multitud de amenazas que esquivan los antivirus basados en firmas.

6. Bibliografía

[1] "The Evolution of BYOD", December 10, 2013 By Beth Kindig: https://collabink.com/evolution-byod/

[2] "What is BYOD (Bring Your Own Device)?" Chad Brooks, Business News Daily Senior Writer, May 22, 2013: https://www.businessnewsdaily.com/4526-byod-bring-your-own-device.html

[3] "What Are the Benefits of BYOD?" by Josh Bouk, 19 April 2018: https://www.casstelecom.com/blog/what-are-the-benefits-of-byod

[4] "El fenómeno BYOD: qué es y qué ventajas y riesgos tiene para empleado y empresa", Blog Bankia, 09 de mayo de 2018: https://www.blogbankia.es/es/blog/el-fenomeno-byod-que-es-y-que-ventajas-y-riesgos-tiene-para-empleado-y-empresa.html

[5] "BYOD: Current State and Security Challenges", Abril 25, 2014, Meisam Eslahi, Maryam Var Naseri , H. Hashim , N.M. Tahir , Ezril Hisham Mat Saad https://www.researchgate.net/publication/261871646_BYODCurrent_State_and_Security_Challenges

[6] "The Pros and Cons of BYOD", Neil Aitken https://whatphone.com.au/guide/pros-and-cons-of-BYOD-bring-your-own-device

[7] "BYOD, CYOD, COPE o COBO", 12 junio, 2018, Tomás Cabacas https://www.muycomputerpro.com/2018/06/12/byod-cyod-cope-o-cobo-que-modelo-de-movilidad-empresarial-elegir

[8] "8 Steps for Successfully Implementing a BYOD Policy", Jan 24, 2019, Miranda Cheatham https://blog.devicemagic.com/8-steps-successful-byod-policy

[9] "What You Need to Consider Before Implementing BYOD", 09/18/2018, https://blog.goptg.com/what-you-need-to-consider-before-implementing-byod

[10] "Implementing the BYOD Model: 7 Do's and Don'ts to Remember", Sep 27, 2018, Staff Writer https://www.hrtechnologist.com/articles/safety/implementing-the-byod-model-7-dos-and-donts-to-remember/

[11] "The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future" , Lilach Bullock, https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#5959a0361f30

[12] "BYOD is becoming more popular than ever: Is your business ready?" https://www.itconsultants.com.au/byod-is-becoming-more-popular-than-ever-is-your-business-ready/

[13] "The Ultimate Guide to BYOD in 2019", January 2, 2019, Stephen Cooper https://www.comparitech.com/net-admin/ultimate-guide-to-byod/

[14] "Diez mejores prácticas para la gestión de BYOD", https://searchdatacenter.techtarget.com/es/cronica/Diez-mejores-practicas-para-la-gestion-de-BYOD

[15] "Estrategia móvil para las empresas (3): BYOD y aplicaciones privadas", Rubén Razquin https://www.ttandem.com/blog/empresas-byod-y-aplicaciones-privadas/

[16] "Elabore una política de seguridad para un entorno BYOD basado en la nube", 10 mayo, 2013, Judith Myerson, https://www.ibm.com/developerworks/ssa/cloud/library/cl-cloudbasedBYOD/index.html

[17] "Soluciones aplicadas a BYOD", 21 noviembre, 2015, https://blogs.deusto.es/master-informatica/soluciones-byod/

[18] "What You Need to Consider before Implementing BYOD", 09/18/2018, https://blog.goptg.com/what-you-need-to-consider-before-implementing-byod

[19] "Cómo crear una política de BYOD", Craig Mathias https://searchdatacenter.techtarget.com/es/consejo/Como-crear-una-politica-de-BYOD

[20] “Key Strategies to Capture and Measure the Value of Consumerization of IT”, Trend Micro http://www.trendmicro.com.cn/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

[21] “What is the Difference between MDM, EMM and UEM?” April 24, 2017, https://www.42gears.com/blog/difference-between-mdm-emm-uem/

7. Anexos

A. Funcionalidades completas de Sophos Mobile 9.0

SOPHOS

Security made simple.

Sophos Mobile 9.0

Feature Matrix

	Deployment		Device Platform				
	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Server							
Admin User Interface							
Easy-to-use web interface	✓	✓	✓	✓	✓	✓	✓
Flexible Dashboard with 33 different user-selectable widgets	✓	✓	✓	✓	✓	✓	✓
Flexible filter mechanism	✓	✓	✓	✓	✓	✓	✓
Role-based access	✓	✓	✓	✓	✓	✓	✓
Multi-tenancy	✓	✓	✓	✓	✓	✓	✓
Sophos Central Partner Dashboard for Managed Service Providers	✓		✓	✓	✓	✓	✓
Communication from superadmin to all tenants (administration and self service portal UI)		✓	✓	✓	✓	✓	✓
Sophos technical notifications	✓	✓	✓	✓	✓	✓	✓
Sending of text messages (via APNs, GCM, Baidu, WNS)	✓	✓	✓	✓	✓	✓	✓
Customizable administrator UI branding	✓	✓	✓	✓	✓	✓	✓
Self Service Portal							
Register new device	✓	✓	✓	✓	✓	✓	✓
Device wipe	✓	✓	✓	✓	✓	✓	✓
Device lock	✓	✓	✓	✓	✓		✓
Device locate	✓	✓	✓	✓	✓	✓	
Passcode reset for Device, App Protection (Android), Sophos Container (iOS, Android)	✓	✓	✓	✓	✓		
Trigger device check-in	✓	✓	✓	✓	✓	✓	✓
Decommission device (incl. corporate wipe on iOS, Samsung, LG, Sony, and Windows 10 Mobile)	✓	✓	✓	✓[5,6,7]	✓	✓	✓
Delete decommissioned device from inventory	✓	✓	✓	✓	✓	✓	✓
Monitor device status and compliance information	✓	✓	✓	✓	✓	✓	✓
Show acceptable use policy with new device registration	✓	✓	✓	✓	✓	✓	✓
Display post-enrollment message	✓	✓	✓	✓	✓	✓	✓
Control registration by OS type	✓	✓	✓	✓	✓	✓	✓
Configure maximum number of devices per user	✓	✓	✓	✓	✓	✓	✓
Company-specific configuration of commands available to users	✓	✓	✓	✓	✓	✓	✓
Customizable branding	✓	✓	✓	✓	✓	✓	✓
User Directory and Management							
Comprehensive password policies	✓	✓	✓	✓	✓	✓	✓
Password recovery by the user	✓	✓	✓	✓	✓	✓	
Internal user directory including batch upload capability	✓	✓	✓	✓	✓	✓	✓
Microsoft ActiveDirectory integration	✓	✓	✓	✓	✓	✓	✓
Novell eDirectory integration		✓	✓	✓	✓	✓	✓
Lotus Notes Directory integration		✓	✓	✓	✓	✓	✓
Red Hat Directory integration		✓	✓	✓	✓	✓	✓
Zimbra Directory integration		✓	✓	✓	✓	✓	✓
Device compliance enforcement rules							
Group assignment or ownership-based compliance rules	✓	✓	✓	✓	✓	✓	✓
Compliance violations analytics	✓	✓	✓	✓	✓	✓	✓
Device under management	✓	✓	✓	✓	✓	✓	✓
Jailbreak or rooting detection	✓	✓	✓	✓			
Encryption required	✓	✓		✓	✓	✓	✓
Passcode required	✓	✓	✓	✓	✓	✓	
Minimum OS version required	✓	✓	✓	✓	✓	✓	✓
Maximum OS version allowed	✓	✓	✓	✓	✓	✓	✓
Last synchronization of the device	✓	✓	✓	✓	✓	✓	✓
Last synchronization of the Sophos Mobile Control app	✓	✓	✓	✓	✓		
Blacklisted apps	✓	✓	✓	✓			✓
Whitelisted apps	✓	✓	✓	✓			✓
Mandatory apps	✓	✓	✓	✓		✓	✓
Block installation from unknown sources (sideloading)	✓	✓		✓			
Data roaming setting	✓	✓	✓	✓	✓		
USB debugging setting	✓	✓		✓			
Sophos Mobile client version	✓	✓	✓	✓	✓		
Malware detection (classical AV plus maschine learning)	✓	✓		✓[4]		✓[8]	
System Integrity Protection required	✓	✓					✓
Firewall required	✓	✓					✓
Suspicious apps detection	✓	✓		✓[4]			
Sideloaded apps detection	✓	✓	✓				

	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Unmanaged configuration profile detection	✓	✓	✓				
Device compliance enforcement rules (continued)							
Potentially unwanted apps detection	✓	✓		✓[4]			
Last malware scan	✓	✓		✓[4]		✓[8]	
Locate for Sophos Mobile Control app enabled	✓	✓	✓	✓	✓		
Compliance rule templates for HIPAA and PCI	✓	✓	✓	✓	✓	✓	✓
Administrator guidance to resolve compliance issues	✓	✓	✓	✓	✓	✓	✓
MitM attack detection	✓	✓	✓[4]	✓[4]			
Security							
Encrypted connection to web interface	✓	✓	✓	✓	✓	✓	✓
Encrypted communication with devices	✓	✓	✓	✓	✓	✓	✓
Control email access by compliance state (Exchange gateway, Office 365 access control)	✓	✓	✓	✓	✓	✓	✓
2FA device authentication at the Exchange gateway (password, certificate)	✓	✓	✓	✓	✓	✓	✓
Define allowed email clients at the Exchange gateway	✓	✓	✓	✓	✓	✓	✓
Control network access by compliance (Generic NAC interface, Sophos UTM or Wireless, Cisco ISE, Check Point)	✓	✓	✓	✓	✓	✓	✓
USSD code protection (e.g. *#2314#)	✓	✓		✓[4]			
Text message phishing detection	✓	✓	✓				
Protection from malicous websites (web filtering)	✓	✓	✓[2]	✓[4]			
Protect corporate apps with additional authentication (App Protection)	✓	✓		✓[4]			
Web productivity filtering by 14 categories + allow/deny lists by IP address, DNS name and IP range	✓	✓	✓[2]	✓[4]			
Manage and store passwords using KeePass format	✓	✓		✓[4]			
Inventory							
Device groups	✓	✓	✓	✓	✓	✓	✓
User-oriented device view	✓	✓	✓	✓	✓	✓	✓
Automatic transfer of unique device ID (IMEI, MEID, UDID) and further device data	✓	✓	✓	✓	✓	✓	✓
Automatic OS version detection	✓	✓	✓	✓	✓	✓	✓
Automatic device model resolution into a user-friendly name	✓	✓	✓	✓	✓	✓	✓
Use actual device name for device inventory	✓	✓	✓				
Marker for company-owned and privately-owned devices	✓	✓	✓	✓	✓	✓	✓
Customer defined device properties with template support	✓	✓	✓	✓	✓	✓	✓
Import/export of device information	✓	✓	✓	✓	✓	✓	✓
Savable extended filters for devices	✓	✓	✓	✓	✓	✓	✓
Provisioning / Device enrollment							
Device management (MDM) enrollment	✓	✓	✓	✓	✓	✓	✓
Container-only Management enrollment	✓	✓	✓	✓			
Device enrollment wizard for admins	✓	✓	✓	✓	✓	✓	✓
Device enrollment by emails	✓	✓	✓	✓	✓	✓	✓
Online registration from the device	✓	✓	✓	✓	✓	✓	✓
Bulk provisioning (by email)	✓	✓	✓	✓	✓	✓	✓
Apple Configurator deployment	✓	✓	✓				
Apple DEP enrollment (Device Enrollment Program)	✓	✓	✓				✓
Android Zero-touch device enrollment	✓	✓		✓			
Samsung Knox Mobile Enrollment	✓	✓		✓[5]			
Admin enrollment w/o installed app (no iTunes account required)	✓	✓	✓				✓
Definition of standard rollout packages for personal or corporate devices	✓	✓	✓	✓	✓	✓	✓
Automatic assignment of initial policies and groups based on user directory group membership	✓	✓	✓	✓	✓	✓	✓
Enrollment using provisioning package files (*.ppkg)	✓	✓			✓	✓	
Task management							
Scheduled task generation	✓	✓	✓	✓	✓	✓	✓
Tasks can be generated for single devices or groups	✓	✓	✓	✓	✓	✓	✓
Detailed status tracking for each task	✓	✓	✓	✓	✓	✓	✓
Intelligent strategies for task repetition	✓	✓	✓	✓	✓	✓	✓
Reporting							
Export inventory using applied filters	✓	✓	✓	✓	✓	✓	✓
Export all reports as XLS or CSV	✓	✓	✓	✓	✓	✓	✓
Compliance log of all administrator activities	✓	✓	✓	✓	✓	✓	✓
Detailed Alert log	✓	✓	✓	✓	✓	✓	✓
Malware reports (2 different reports)	✓	✓	✓	✓	✓	✓	✓
Compliance violation reports (2 different reports)	✓	✓	✓	✓	✓	✓	✓
Device reports (9 different reports)	✓	✓	✓	✓	✓	✓	✓
App reports (8 different reports)	✓	✓	✓	✓	✓	✓	✓
Certificate reports (2 different reports)	✓	✓	✓	✓	✓	✓	✓
Programming interface (API)							
Web service (REST) API for device information and provisioning from 3rd party systems		✓	✓	✓	✓	✓	✓
Devices							
Sophos Mobile Control app functionality							
Enterprise App Store	✓	✓	✓	✓	✓		
Show compliance violations (including help for the enduser to fix reported compliance issues)	✓	✓	✓	✓	✓		
Show server messages	✓	✓	✓	✓	✓		
Show technical contact	✓	✓	✓	✓	✓		

	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Trigger device synchronization	✓	✓	✓	✓	✓		
Co-branding of the Sophos Mobile Control app		✓	✓	✓	✓		
Show privacy information	✓	✓	✓	✓	✓		
Application management							
Installing apps (with or without user interaction, including managed apps on iOS)	✓	✓	✓	✓	✓	✓	✓
Uninstalling apps (with or without user interaction)	✓	✓	✓	✓		✓	
List of all installed apps	✓	✓	✓	✓		✓	✓
Support for Apple Volume Purchasing Program (VPP)	✓	✓	✓				✓
Allow/forbid installation of apps	✓	✓	✓	✓	✓	✓	
Block app deinstallation	✓	✓		✓5,6,7			
Remote configuration of company apps (managed settings)	✓	✓	✓2				
Block specific apps from running (app blocker)	✓	✓	✓2	✓	✓	✓	
Manage and configure Microsoft Office 365 apps	✓	✓	✓	✓			
Security							
Jailbreak (iOS)/Rooting (Android) detection	✓	✓	✓	✓			
Tamper detection	✓	✓	✓	✓	✓		
Anti-theft protection: Remote wipe	✓	✓	✓	✓	✓	✓	✓
Anti-theft protection: Remote lock	✓	✓	✓	✓	✓		✓
Anti-theft protection: Device locate	✓	✓	✓	✓	✓	✓	
Enforce password strength and complexity	✓	✓	✓	✓	✓	✓	✓
Inactivity time (time in minutes until password is required)	✓	✓	✓	✓	✓	✓	✓
Maximum number of attempts until the device will be reset	✓	✓	✓	✓	✓	✓	✓
Minimum password length	✓	✓	✓	✓	✓		✓
Password history	✓	✓	✓	✓	✓	✓	✓
Password expiration time	✓	✓		✓	✓	✓	✓
Minimum length of lower/upper case, non-letter or symbol characters in the passcode	✓	✓	✓	✓	✓		✓
Passcode reset (unlock)/administrator defines new passcode	✓	✓	✓	✓	✓		
Activation lock bypass	✓	✓	✓2				
Activation of storage encryption	✓	✓	✓3	✓	✓		
Access to the memory card can be prohibited	✓	✓		✓5,6,7	✓	✓	
Activation/deactivation of device data encryption	✓	✓		✓	✓		
Block installation from unknown sources (sideloading)	✓	✓		✓5,6,7			
Block Wi-Fi	✓	✓	✓2	✓1,5,6,7			
Block Bluetooth	✓	✓		✓1,5,6,7		✓	
Block data transfer via Bluetooth	✓	✓		✓5	✓	✓	
Block data transfer via NFC	✓	✓		✓5,6,7	✓		
Block USB connections	✓	✓		✓1,5,6,7	✓		
Block camera	✓	✓	✓	✓	✓	✓	✓
Protection of settings against modification/removal by the user	✓	✓	✓	✓1,5,6,7		✓	
Allow/forbid use of iTunes Store / Google Play / Windows Store	✓	✓	✓	✓5,6,7	✓		
Allow/forbid use of Browser	✓	✓	✓	✓	✓		
Allow/forbid explicit content	✓	✓	✓				
Allow/forbid camera on lock screen	✓	✓		✓			
Allow/forbid 3rd party app usage of email	✓	✓	✓				
Allow/forbid iCloud autosync	✓	✓	✓				
Allow/forbid manual Wi-Fi configuration	✓	✓	✓2	✓5			
Allow/forbid to send crash data to Apple / Google / Samsung / Microsoft (Telemetry)	✓	✓	✓	✓5	✓	✓	
Allow/forbid certificates from untrusted sources	✓	✓	✓		✓		
Allow/forbid WiFi auto-connect	✓	✓	✓			✓	
Allow/forbid shared photo stream	✓	✓	✓				✓
Allow/forbid Apple Wallet/Passbook on lock screen	✓	✓	✓				
Allow/forbid device act as hotspot	✓	✓	✓			✓	✓
Allow/forbid recent contacts to sync	✓	✓	✓				
Allow/forbid Siri (iOS) or Cortana (Microsoft)	✓	✓	✓		✓	✓	
Allow/forbid Siri to query content from the web	✓	✓	✓2				
Allow/forbid "Open with..." functionality to share data between managed and unmanaged apps	✓	✓	✓				
Allow/forbid fingerprint reader (Touch ID) to unlock device	✓	✓	✓	✓			✓
Allow/forbid account modification	✓	✓	✓2				
Allow/forbid modification of cellular data usage per app	✓	✓	✓2				
Allow/forbid Control Center on lock screen	✓	✓	✓				
Allow/forbid Notification Center on lock screen	✓	✓	✓		✓		
Allow/forbid Today view on lock screen	✓	✓	✓				
Allow/forbid over-the-air PKI updates	✓	✓	✓				
Allow/forbid find my friends modification	✓	✓	✓2				
Allow/forbid host pairing	✓	✓	✓2				
Allow/forbid iris scan authentication	✓	✓		✓5			
Prevent email forwarding	✓	✓	✓				
S/MIME enforcement	✓	✓	✓				
Support for SCEP certificate provisioning (incl. auto-renew)	✓	✓	✓	✓	✓	✓	✓
Security (continued)							
Allow/forbid AirDrop	✓	✓	✓2				
Allow/forbid single app mode (app lock or kiosk mode)	✓	✓	✓2	✓5,6,7			

	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Trigger device synchronization	✓	✓	✓	✓	✓		
Co-branding of the Sophos Mobile Control app		✓	✓	✓	✓		
Show privacy information	✓	✓	✓	✓	✓		
Application management							
Installing apps (with or without user interaction, including managed apps on iOS)	✓	✓	✓	✓	✓	✓	✓
Uninstalling apps (with or without user interaction)	✓	✓	✓	✓		✓	
List of all installed apps	✓	✓	✓	✓		✓	✓
Support for Apple Volume Purchasing Program (VPP)	✓	✓	✓				✓
Allow/forbid installation of apps	✓	✓	✓	✓	✓	✓	
Block app deinstallation	✓	✓		✓5,6,7			
Remote configuration of company apps (managed settings)	✓	✓	✓2				
Block specific apps from running (app blocker)	✓	✓	✓2	✓	✓	✓	
Manage and configure Microsoft Office 365 apps	✓	✓	✓	✓			
Security							
Jailbreak (iOS)/Rooting (Android) detection	✓	✓	✓	✓			
Tamper detection	✓	✓	✓	✓	✓		
Anti-theft protection: Remote wipe	✓	✓	✓	✓	✓	✓	✓
Anti-theft protection: Remote lock	✓	✓	✓	✓	✓		✓
Anti-theft protection: Device locate	✓	✓	✓	✓	✓	✓	
Enforce password strength and complexity	✓	✓	✓	✓	✓	✓	✓
Inactivity time (time in minutes until password is required)	✓	✓	✓	✓	✓	✓	✓
Maximum number of attempts until the device will be reset	✓	✓	✓	✓	✓	✓	✓
Minimum password length	✓	✓	✓	✓	✓		✓
Password history	✓	✓	✓	✓	✓	✓	✓
Password expiration time	✓	✓		✓	✓	✓	✓
Minimum length of lower/upper case, non-letter or symbol characters in the passcode	✓	✓	✓	✓	✓		✓
Passcode reset (unlock)/administrator defines new passcode	✓	✓	✓	✓	✓		
Activation lock bypass	✓	✓	✓2				
Activation of storage encryption	✓	✓	✓3	✓	✓		
Access to the memory card can be prohibited	✓	✓		✓5,6,7	✓	✓	
Activation/deactivation of device data encryption	✓	✓		✓	✓		
Block installation from unknown sources (sideloading)	✓	✓		✓5,6,7			
Block Wi-Fi	✓	✓	✓2	✓1,5,6,7			
Block Bluetooth	✓	✓		✓1,5,6,7		✓	
Block data transfer via Bluetooth	✓	✓		✓5	✓	✓	
Block data transfer via NFC	✓	✓		✓5,6,7	✓		
Block USB connections	✓	✓		✓1,5,6,7	✓		
Block camera	✓	✓	✓	✓	✓	✓	✓
Protection of settings against modification/removal by the user	✓	✓	✓	✓1,5,6,7		✓	
Allow/forbid use of iTunes Store / Google Play / Windows Store	✓	✓	✓	✓5,6,7	✓		
Allow/forbid use of Browser	✓	✓	✓	✓	✓		
Allow/forbid explicit content	✓	✓	✓				
Allow/forbid camera on lock screen	✓	✓		✓			
Allow/forbid 3rd party app usage of email	✓	✓	✓				
Allow/forbid iCloud autosync	✓	✓	✓				
Allow/forbid manual Wi-Fi configuration	✓	✓	✓2	✓5			
Allow/forbid to send crash data to Apple / Google / Samsung / Microsoft (Telemetry)	✓	✓	✓	✓5	✓	✓	
Allow/forbid certificates from untrusted sources	✓	✓	✓		✓		
Allow/forbid WiFi auto-connect	✓	✓	✓			✓	
Allow/forbid shared photo stream	✓	✓	✓				✓
Allow/forbid Apple Wallet/Passbook on lock screen	✓	✓	✓				
Allow/forbid device act as hotspot	✓	✓	✓			✓	✓
Allow/forbid recent contacts to sync	✓	✓	✓				
Allow/forbid Siri (iOS) or Cortana (Microsoft)	✓	✓	✓		✓	✓	
Allow/forbid Siri to query content from the web	✓	✓	✓2				
Allow/forbid "Open with..." functionality to share data between managed and unmanaged apps	✓	✓	✓				
Allow/forbid fingerprint reader (Touch ID) to unlock device	✓	✓	✓	✓			✓
Allow/forbid account modification	✓	✓	✓2				
Allow/forbid modification of cellular data usage per app	✓	✓	✓2				
Allow/forbid Control Center on lock screen	✓	✓	✓				
Allow/forbid Notification Center on lock screen	✓	✓	✓		✓		
Allow/forbid Today view on lock screen	✓	✓	✓				
Allow/forbid over-the-air PKI updates	✓	✓	✓				
Allow/forbid find my friends modification	✓	✓	✓2				
Allow/forbid host pairing	✓	✓	✓2				
Allow/forbid iris scan authentication	✓	✓		✓5			
Prevent email forwarding	✓	✓	✓				
S/MIME enforcement	✓	✓	✓				
Support for SCEP certificate provisioning (incl. auto-renew)	✓	✓	✓	✓	✓	✓	✓
Security (continued)							
Allow/forbid AirDrop	✓	✓	✓2				
Allow/forbid single app mode (app lock or kiosk mode)	✓	✓	✓2	✓5,6,7			

	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Allow/forbid iBooks store	✓	✓	✓				
Allow/forbid explicit sexual content in iBooks store	✓	✓	✓				
Allow/forbid iMessage	✓	✓	✓				
Allow/forbid user to reset the device	✓	✓		✓ 1,5,6,7	✓		
Allow/forbid device unenrollment from MDM management	✓	✓	✓ 2	✓ 5,6,7	✓	✓	
Allow/forbid user to create screenshots	✓	✓		✓ 1,5,6,7	✓		
Allow/forbid user to use copy/paste	✓	✓	✓	✓ 5,6,7	✓		
Filter access to web sites (blacklisting) or whitelist web sites with bookmarks	✓	✓	✓ 2				✓
Delay or block OS upgrade	✓	✓	✓	✓ 1,5,7			✓
Allow/forbid password auto-fill	✓	✓					✓
Allow/forbid password sharing	✓	✓					✓
Allow/forbid password proximity requests	✓	✓					✓
Configure Device Guard settings	✓	✓				✓	
Device configuration							
Microsoft Exchange settings for email	✓	✓	✓	✓ 5,6,7	✓	✓	✓
IMAP or POP settings for email	✓	✓	✓		✓		✓
LDAP, CardDAV and CalDAV settings	✓	✓	✓				✓
Configuration of access points	✓	✓	✓	✓			
Proxy settings	✓	✓	✓	✓			✓
Wi-Fi settings	✓	✓	✓	✓	✓	✓	✓
VPN settings	✓	✓	✓	✓ 1,5,6,7			✓
Install root certificates	✓	✓	✓	✓ 5	✓	✓	✓
Install client certificates	✓	✓	✓	✓	✓	✓	✓
Per app VPN	✓	✓	✓				
Single sign-on (SSO) for 3rd party apps (app protection) and company webpages	✓	✓	✓	✓			✓
Distribution of bookmarks (Web Clips)	✓	✓	✓				✓
Force iOS update on supervised devices (and display pending iOS updates)	✓	✓	✓ 2				
Configure the iOS lock screen and home screen	✓	✓	✓ 2				
Automatically receive Wi-Fi and VPN settings from Sophos UTM appliances	✓	✓	✓	✓			
Managed domains	✓	✓	✓				✓
Firewall configuration	✓	✓					✓
Kernal Extension policy	✓	✓					✓
Kiosk Mode	✓	✓	✓	✓ 1,5,6,7			✓
App permissions	✓	✓		✓ 1			
Enable iOS Lost Mode	✓	✓	✓				
Configure Google Accounts	✓	✓	✓				
Integrate with Duo Security		✓	✓	✓			
Android enterprise: Configure password policy (workspace)	✓	✓		✓ 1			
Android enterprise: Configure password policy (device)	✓	✓		✓ 1			
Android enterprise: Configure restrictions	✓	✓		✓ 1			
Android enterprise: Configure Wi-Fi	✓	✓		✓ 1			
Android enterprise: Configure app protection	✓	✓		✓ 1			
Android enterprise: Configure app control	✓	✓		✓ 1			
Android enterprise: Configure app permissions	✓	✓		✓ 1			
Android enterprise: Configure Exchange	✓	✓		✓ 1			
Android enterprise: Install root certificate	✓	✓		✓ 1			
Android enterprise: Install client certificate	✓	✓		✓ 1			
Android enterprise: Install client certificate via SCEP	✓	✓		✓ 1			
Samsung Knox: Container handling (create, lock, decommission)	✓	✓		✓ 5			
Samsung Knox: Configure restrictions	✓	✓		✓ 5			
Samsung Knox: Configure Exchange	✓	✓		✓ 5			
Samsung Knox: Manage container password	✓	✓		✓ 5			
Samsung Knox: Allow/block data and file sync between Knox Workspace and personal area	✓	✓		✓ 5			
Samsung Knox: Allow/block Iris scan authentication for Knox Workspace	✓	✓		✓ 5			
Configure devices to use AirPrint printers	✓	✓	✓				✓
Device information							
Internal memory utilization (free/used)	✓	✓	✓				✓
Battery charge level	✓	✓	✓	✓			
IMSI (unique identification number) of SIM card	✓	✓	✓	✓	✓		
Currently used cellular network	✓	✓	✓	✓			
Roaming mode	✓	✓	✓	✓	✓		
OS version	✓	✓	✓	✓	✓	✓	✓
List of installed profiles	✓	✓	✓	✓	✓	✓	✓
List of installed certificates	✓	✓	✓		✓	✓	✓
Malware detected on device	✓	✓		✓ 4		✓ 8	
Remote screen sharing (requires Teamviewer or AirPlay device)	✓	✓	✓	✓			
Secure Email (with Sophos Secure Email app)							
Exchange email	✓	✓	✓ 4	✓ 4			
Exchange contacts	✓	✓	✓ 4	✓ 4			
Exchange calendar	✓	✓	✓ 4	✓ 4			
Geo-fencing / Time-fencing / Wi-Fi fencing	✓	✓	✓ 4	✓ 4			
Control cut and copy	✓	✓	✓ 4	✓ 4			

	Managed with Sophos Central	Installed On Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Control screenshot	✓	✓		✓[4]			
Show event details	✓	✓	✓[4]	✓[4]			
Export contacts to device	✓	✓	✓[4]	✓[4]			
Define out of office message in the email app	✓	✓	✓[4]	✓[4]			
Unfied calendar view	✓	✓	✓[4]	✓[4]			
Anti-phishing protection for links in emails	✓	✓	✓[4]	✓[4]			
Corporate Browser (with Sophos Secure Workspace)							
Browsing restricted to predefined corporate domains	✓	✓	✓[4]	✓[4]			
Preconfigured corporate bookmarks	✓	✓	✓[4]	✓[4]			
Password manager	✓	✓	✓[4]	✓[4]			
Client or user certificates to authenticate against corporate websites	✓	✓	✓[4]	✓[4]			
Root certificates	✓	✓	✓[4]	✓[4]			
Restricted cut, copy, and paste	✓	✓	✓[4]	✓[4]			
Content Management (with Sophos Secure Workspace app)							
Publish documents from Sophos Mobile server	✓	✓	✓[4]	✓[4]			
Geo-fencing / Time-fencing / Wi-Fi fencing	✓	✓	✓[4]	✓[4]			
Content storage: Dropbox	✓	✓	✓[4]	✓[4]			
Content storage: Google Drive	✓	✓	✓[4]	✓[4]			
Content storage: Microsoft OneDrive personal and business	✓	✓	✓[4]	✓[4]			
Content storage: Box	✓	✓	✓[4]	✓[4]			
Content storage: Telekom MagentaCloud	✓	✓	✓[4]	✓[4]			
Content storage: Egnyte	✓	✓	✓[4]	✓[4]			
Content storage: OwnCloud	✓	✓	✓[4]	✓[4]			
Content storage: WebDAV (for example Windows Server, Strato Hi-Drive, etc.)	✓	✓	✓[4]	✓[4]			
User authentication	✓	✓	✓[4]	✓[4]			
FIPS 140-2 encryption with AES256	✓	✓	✓[4]	✓[4]			
DLP setting: Allow offline viewing	✓	✓	✓[4]	✓[4]			
DLP setting: Allow copy to clipboard	✓	✓	✓[4]	✓[4]			
DLP setting: Allow emailing in encrypted form	✓	✓	✓[4]	✓[4]			
DLP setting: Allow "open with" unencrypted, including emailing unencrypted	✓	✓	✓[4]	✓[4]			
Add files from mail or download to content app	✓	✓	✓[4]	✓[4]			
Select existing encryption key or create new user key		✓	✓[4]	✓[4]			
Integrated with SafeGuard Encryption for Cloud Storage		✓	✓[4]	✓[4]			
Shared keyring with Sophos SafeGuard		✓	✓[4]	✓[4]			
Lock container access on non-compliant devices	✓	✓	✓[4]	✓[4]			
Request call home based on time or by unlock count	✓	✓	✓[4]	✓[4]			
Edit or create Word, Excel, PowerPoint, and text format files	✓	✓	✓[4]	✓[4]			
Annotate PDF files	✓	✓	✓[4]	✓[4]			
Fill PDF forms	✓	✓	✓[4]	✓[4]			
View SafeGuard format password-protected HTML5 files	✓	✓	✓[4]	✓[4]			
Share documents as password-protected HTML5 files	✓	✓	✓[4]	✓[4]			
Anti-phishing protection for links in documents	✓	✓	✓[4]	✓[4]			
"View with Secure Workspace" access to encrypted documents from other apps	✓	✓	✓[4]	✓[4]			
Unlock app via fingerprint reader	✓	✓	✓[4]	✓[4]			
View, manage, and create Zip and 7z compressed archives	✓	✓	✓[4]	✓[4]			
Manage and store passwords secrely using KeePass format	✓	✓	✓[4]	✓[4]			
Mobile SDK (to be embedded in apps)							
App expiration date	✓	✓	✓[4]	✓[4]			
App embedded EULA	✓	✓	✓[4]	✓[4]			
App password (with SSO across all SDK-enabled apps)	✓	✓	✓[4]	✓[4]			
Geo-fencing of the app	✓	✓	✓[4]	✓[4]			
Time-fencing of the app	✓	✓	✓[4]	✓[4]			
Block app start on jailbroken or rooted devices	✓	✓	✓[4]	✓[4]			
Make Wi-Fi network mandatory for app usage	✓	✓	✓[4]	✓[4]			
Make available corporate Wi-Fi mandatory for app usage	✓	✓	✓[4]	✓[4]			
Telecom Cost Control							
Disable data while roaming	✓	✓	✓	✓[1,5]	✓		
Disable voice while roaming	✓	✓	✓	✓[5]			
Control sync while roaming	✓	✓		✓[5]			
Configure APN or Carrier settings	✓	✓	✓	✓			
Define data usage upper limit per device	✓	✓	✓	✓			
Compare data usage against limit	✓	✓	✓	✓			
Per app network usage rules	✓	✓	✓				

(1) Support for Android Enterprise (former "Andriod for work")
(2) Requires a supervised device
(3) By setting a pin or passcode
(4) Requires a Mobile Advanced or Central Mobile Advanced license
(5) Requires a device compatible with Samsung Knox Standard V2.1 or higher
(6) Required Sony extended MDM API enabled device
(7) Requires LG GATE enabled device
(8) With Windows Defender

B. Manuales para la correcta implementación de Sophos:

- Ayuda al administrador de Sophos Mobile: https://docs.sophos.com/esg/smc/9-0/admin/es-es/index.html

- Ayuda al usuario de Sophos Mobile: https://docs.sophos.com/esg/smc/9-0/ssp/es-es/index.html

- Manual de instalación de Sophos Mobile: https://docs.sophos.com/esg/smc/9-0/admin/es-es/PDF/smc_ig.pdf