Samsung Knox, la seguridad de la movilidad a tu alcance

Samsung Knox ya no es un producto, es una plataforma. Lo que llegó al mercado en 2013 para que la incorporación de Android al mundo empresarial se hiciera con ciertas garantías de seguridad, ha evolucionado hasta ofrecer las mejores capacidades de seguridad, gestión de políticas y cumplimiento basadas en hardware de su clase más allá de las características estándar comunes en el mercado actual de dispositivos móviles.

SAMSUNG Knox

Samsung Knox, la seguridad de la movilidad a tu alcance

El dominio decreciente de los Blackberry y la presencia ascendente del iPhone de Apple como dispositivos estándar corporativos fue una de las razones que impulsó a Samsung a reforzar la seguridad del sistema operativo Android de manera específica para la empresa y los mercados B2B. Se sumaba lo que entonces se bautizaría como BYOD (Bring Your Own Device), que estaba llevando a que la plataforma de Google irrumpiera con fuerza en la empresa mientras los departamentos de TI luchaban para mantenerse al día.

Nace así la primera versión de Knox como parte de Samsung For Enterprise (SAFE), con el concepto de usar un enclave seguro, o un entorno de procesamiento separado dentro de la arquitectura de proceso ARM, llamada TrustZone, para incorporar capacidades de seguridad y autenticación de hardware y software en la plataforma Android. El lanzamiento inicial de Knox también introdujo el concepto de contenedorización para teléfonos Android desde la perspectiva OEM de un dispositivo nativo, lo que permite segmentar el trabajo y las aplicaciones personales y los datos en los dispositivos. En su lanzamiento Knox también trajo la verificación de arranque confiable y segura y la certificación remota, o la capacidad de verificar independientemente que un dispositivo esté en un “estado confiable” y que no haya sido alterado.

Desde aquellos primeros tiempos Samsung Knox se ha convertido en una plataforma que permite hacer muchas cosas, desde la personalización del dispositivo, a su gestión y añadiendo seguridad avanzada; una plataforma que permite dar respuesta a la necesaria estrategia de movilidad empresarial que debe adoptarse en un proceso de digitalización, o transformación digital; una plataforma basada en hardware que llega de fábrica en todos los dispositivos Samsung, tanto smartphones como tabletas.

Samsung Knox, la seguridad de la movilidad a tu alcance

“LA GESTIÓN DEL FIRMWARE EN DISPOSITIVOS MÓVILES ES ALGO EXCLUSIVO DE KNOX” (CÉSAR GARRO, SAMSUNG KNOX)

CLICAR PARA VER EL VÍDEO

Las empresas con decenas, cientos o miles de dispositivos móviles para empleados necesitan poder administrarlos de manera fácil, segura y eficiente

La movilidad empresarial se ha convertido en el gran habilitador del trabajo, que ha dejado de estar asociado a un lugar o ubicación física, ni siquiera a un horario. Cada vez más, el trabajo se ha convertido en una actividad que se puede realizar desde cualquier lugar, dispositivo y momento. De hecho, según datos de IDC, el porcentaje de trabajadores móviles respecto a la población activa en Europa Occidental será del 61% a finales de 2019 y alcanzará el 66% en 2023.

Vivimos en un mundo centrado en el móvil y las empresas se enfrentan a la compleja tarea de gestionar, aprovisionar y proteger los dispositivos móviles en las empresas, y Samsung Knox es la plataforma que proporciona el ecosistema de productos y servicios para asegurar y facilitar esa gestión de la movilidad. La plataforma Knox defiende contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware. Y lo hace a través de una suite de productos que, por un lado permiten el despliegue de los terminales, por otro la gestión de los mismos y además añadir seguridad a los dispositivos, la información que almacenan, e incluso las comunicaciones que establecen.

Seguridad por encima de todo

Asegurar y facilitar la gestión de los dispositivos móviles es una de las acciones que se pueden

Samsung Knox, la seguridad de la movilidad a tu alcance

llevar a cabo con Samsung Knox, que defiende contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware.

Ese entorno confiable permite separar el código crítico de seguridad del resto del sistema operativo, garantizando que sólo los procesos confiables que estén aislados y protegidos de ataques y exploits puedan realizar operaciones confidenciales, como el cifrado y descifrado de datos. Los entornos de confianza realizan verificaciones de integridad antes de ejecutar cualquier software, lo que les permite detectar intentos maliciosos de modificar el entorno de confianza y el software que se ejecuta en el dispositivo.

Y decíamos que es un entorno confiable que está respaldado por hardware porque es el hardware el que aísla el entorno del resto del sistema en ejecución, lo que garantiza que las vulnerabilidades en el sistema operativo principal no afecten directamente a la seguridad de dicho entorno confiable.

Por otra parte, Knox proporciona varias formas de aislamiento de aplicaciones para crear un espacio contenedor de aplicaciones protegidas en dispositivos Samsung sin olvidarnos de su capacidad para proteger los datos personales y profesionales mediante la autenticación de usuarios, de manera tan sencilla como introduciendo un PIN, o tan compleja como a través de autenticación biométrica; el cifra-

Samsung Knox, una historia de éxito

A lo largo de su historia, Samsung ha establecido asociaciones clave con más de 15 proveedores de soluciones de gestión de movilidad empresarial y dispositivos móviles para permitir la activación y el control de las funciones integradas de Knox.

Tener una estrategia de soporte lo más amplia posible con los diferentes EMM (Enterprise Mobile Management) ha sido una de las calves para que Samsung adoptara y activara los dispositivos habilitados para Knox. El éxito de esta estrategia se refleja en un fuerte crecimiento en las activaciones de Knox en los últimos años. Según los datos de la compañía más de 40 millones de trabajadores móviles empresariales usaron Knox en 2018, un número que se ha más que duplicado año tras año desde 2013. Samsung pronostica que este mismo crecimiento para el uso de Knox continuará hasta 2020.

Samsung Knox, la seguridad de la movilidad a tu alcance

Terminales Samsung para el mercado profesional

Entre su amplia oferta de productos, Samsung cuenta con ediciones pensadas especialmente para empresas y entornos profesionales que requieren de unas especificaciones específicas en términos de seguridad, personalización según las necesidades de cada negocio, y soporte técnico de calidad. Algunos de estos modelos son:

- **Samsung Galaxy Note 10,** una potencia nunca antes vista

- **Samsung Galaxy Tab Active Pro,** una Tablet robusta para llevar su negocio a todas partes)

- **Samsung Galaxy Xcover 4S,** ideado para trabajar al aire libre

- **Samsung Galaxy Tab S6,** Portátil y con el rendimiento de un PC

- **Samsung Galaxy S10,** un teléfono de nueva generación para la nueva generación

do de los datos del dispositivo, que garantiza que los datos se descifren sólo en el dispositivo donde están almacenados, y sólo por el propietario del dispositivo; el cifrado de los datos de red mediante la más amplia selección de características avanzadas de VPN; y la capacidad de localizar, bloquear y borrar el dispositivo de forma remota en casa de que sea robado o salga de un perímetro geográfico especificado.

Con respecto a la opción de VPNs, destacar VPN Chaining, que permite el uso de dos túneles VPN para cifrar doblemente el tráfico, mejorar el anonimato y evitar que un solo error de seguridad en una capa VPN comprometa el cifrado de la red.

Gestión del dispositivo

Las empresas con decenas, cientos o miles de dispositivos móviles para empleados necesitan poder

Samsung Knox, la seguridad de la movilidad a tu alcance

administrarlos de manera fácil, segura y eficiente. Los administradores de TI pueden controlar los dispositivos Samsung Knox de manera integral, administrando las funciones del dispositivo con facilidad.

En cuanto al despliegue, se cuenta con Knox Mobile Enrollment, un servicio gratuito para terminales empresariales que hace que, una vez encendido, el terminal se ponga en contacto con la herramienta de gestión que tenga el cliente, y se quedará bloqueado hasta que el usuario introduzca sus credenciales corporativas

Es decir que con Knox Mobile Enrollment las empresas pueden automatizar la inscripción de dispositivos, ya sea individualmente o en masa. Después de que un administrador de TI registra un dispositivo con este servicio, el usuario del dispositivo simplemente lo enciende y lo conecta a una red Wi-Fi o 3G / 4G para inscribirlo en un sistema EMM. No hay inscripción manual de dispositivos individuales, y no hay necesidad de gestión y verificación de IMEI, todas tareas onerosas que requieren mucho tiempo y son propensas a errores.

Una vez dado este paso, se puede aplicar una personalización de los dispositivos, permitiendo o restringiendo casi todos los aspectos de la configuración del dispositivo y la experiencia de usuario, incluidas las animaciones de arranque que incorporan logotipos empresariales personalizados, configuraciones de pantalla, fondos de pantalla, configuraciones de red, quitar aplicaciones del sistema que no se requieran en el terminal, o poner aplicaciones que sí se quiere poner.

Un aspecto muy interesante son las 1.200 API con las que cuenta Samsung para la gestión granular y flexible del dispositivo, que se incluyen dentro de lo que se conoce como Samsung Knox SDK, y que permite a los administradores de TI empresariales implementar políticas de TI para administrar y proteger todos los aspectos de los dispositivos Knox

Uno de los avances importantes que ha hecho Samsung dentro de la parte de gestión es la posibilidad de gestionar el firmware de los dispositivos. ¿Qué pasa cuando el terminal ya se ha desplegado y lo tienen los usuarios? Que se pierde parte del control, sobre todo a la hora de gestionar el firmware de ese dispositivo, algo que puede ser funda-

> Samsung Knox defiende los dispositivos móviles contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno confiable respaldado por hardware

Samsung Knox, la seguridad de la movilidad a tu alcance

Knox E-FOTA (Enterprise Firmware Over The Air) permite que sean las empresas quienes puedan decidir cuándo quieren actualizar los smartphones o tabletas y cómo se va a hacer exactamente

Enlaces de interés...

- Samsung Knox
- Samsung Knox Security Solution
- Samsung Knox Manage
- 'Knox es la solución integrada de seguridad endpoint de Samsung'

mental en caso de querer solucionar una vulnerabilidad.

En el mundo de los dispositivos móviles, la única manera de actualizar el firmaware era contar con el usuario, que al fin y al cabo tenía que hacer una acción indispensable: aceptar de forma proactiva la actualización. Y en Samsung pensaron que eso no tenía sentido desde el punto de vista de la seguridad, que es la prioridad de Knox; no tiene sentido teniendo en cuenta que esto es algo que se lleva haciendo mucho tiempo en el mundo del PC, y no tiene sentido teniendo en cuenta que hoy en día los terminales móviles son un vector de ataque importantísimo en el que cada vez tenemos más información, y en los que cada vez delegamos más acciones.

Samsung lo ha resuelto con Knox E-FOTA, un acrónimo de Enterprise Firmware Over The Air, que permite que sean las empresas quienes puedan decidir cuándo quieren actualizar los smartphones o tabletas y cómo se va a hacer exactamente: que se descargue por ejemplo el día 1 en toda la flota de terminales, y que además se descargue siempre que tenga conectividad WiFi, y que una vez que esté descargada se instale entre las 2 y las 3 de la mañana. Y cuando se cumplen esas condiciones, la instalación se hará de forma automatizada y de forma transparente para el usuario. En definitiva, lo que se ha diseñado es una forma en que las empresas pueden controlar desde un punto de vista de seguridad y de gestión cómo quieren que se comporten sus terminales.

Compartir en RRSS