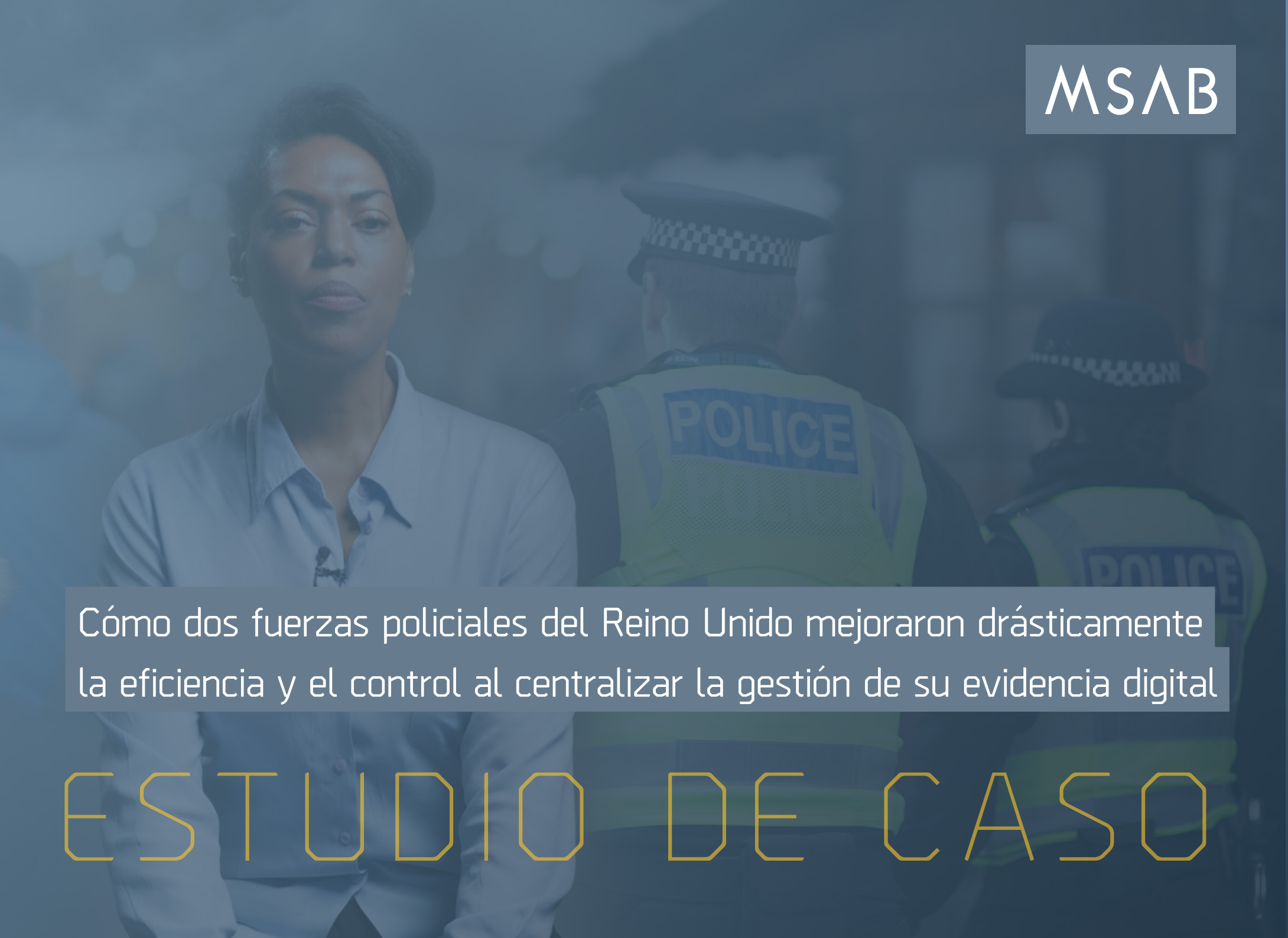

MSAB

Cómo dos fuerzas policiales del Reino Unido mejoraron drásticamente la eficiencia y el control al centralizar la gestión de su evidencia digital

ESTUDIO DE CASO

MSAB.com

Marzo 2022

El desafío

HACE UN PAR DE AÑOS, dos fuerzas policiales del Reino Unido combinaron sus equipos forenses digitales para ahorrar dinero y aumentar la eficacia. El equipo contaba con unos doscientos agentes capacitados repartidos por varios lugares remotos. Habían estado utilizando el software XRY para investigar cualquier cosa que tuviera un aspecto digital.

Pero la Unidad Forense Digital se enfrentaba a una serie de desafíos:

- Demoras con los dispositivos móviles deben ser extraídos y analizados
- Las computadoras utilizadas para almacenar los archivos de los casos de extracción forense móvil se quedaban constantemente sin espacio de almacenamiento. Como resultado, los agentes se mostraban a menudo reacios a descargar los teléfonos que se debían procesar
- Era difícil mantener el software XRY actualizado a la última versión porque las computadoras no estaban conectadas en red. Las actualizaciones de software se enviaban a las sedes en el campo en discos, pero lograr que el software se actualizara era un "ensayo y error".
- La coherencia y la calidad eran difíciles de mantener en todos los sitios
- Los usuarios solían cambiar los perfiles de descarga a pesar de las indicaciones del director de la unidad
- Los usuarios individuales cambiaban sus contraseñas, lo que dificultaba la recuperación de las credenciales de acceso
- Los archivos de casos extraídos se grababan en DVD y tenían que transportarse físicamente a donde se necesitaban los datos, lo que requería tiempos de transporte de hasta 3,5 horas y creaba "numerosos problemas y preocupaciones constantes".
- "No teníamos ni idea de quién accedía a las máquinas, por qué razón, con qué frecuencia, cuántos datos se descargaban, dónde estaban los datos y quién tenía acceso a ellos", resumió el analista forense digital y director de la unidad.

"Cuando vi quiosco MSAB y me enteré de las capacidades de la red, me enamoré de él", dijo el analista forense digital y director de la unidad. "Pero tardé literalmente años en que se aprobara".

En el Reino Unido, todos los laboratorios forenses digitales de la policía están obligados a seguir el sistema de gestión de calidad ISO 17025 para garantizar la coherencia y la calidad de su trabajo.

Cambiar el statu quo: El punto de inflexión

"Solicité que la ISO 17025 se implantara en la primera línea de la medicina forense móvil. Por lo tanto, si queremos tener las mismas capacidades para las áreas en las que tenemos personal de primera línea, con el fin de producir resultados válidos de manera consistente, necesitaremos una infraestructura en red en el futuro de todos modos. Por qué no implementarlo ahora. Nos ayudará a cumplir la norma ISO 17025".

"Sostenía que al implementar un entorno de red, podíamos tener un agente en cada cuerpo de policía que descargara los datos en lugar de estar sentados esperando a recibir los datos. Los desplazamientos y la actualización de las unidades requerían dos días. Ese tiempo podría utilizarse mucho mejor en ayudar con la investigación".

"Tenemos más de 30 estaciones de policía con personal que intenta realizar su trabajo diario, por lo que no es raro que cuando se descargue la información del teléfono del sospechoso, la persona que está esperando para analizar los datos se encuentre en otro lugar".

Otro factor que favoreció un cambio en el statu quo fue la adopción de las políticas del Reglamento General de Protección de Datos (RGPD) que protegen los derechos de privacidad y establecen elevadas multas monetarias para las infracciones.

"Mi argumento fue que si perdemos un disco con los datos personales de una persona, tendremos una multa de un millón de libras".

Puesta en marcha: Fase de implementación

"Fue muy rápido poner todo en marcha una vez que logramos todas las aprobaciones. Tardamos 8 semanas desde el día en que llegaron las plataformas de Kiosk hasta que entraron en funcionamiento". "No tuvimos ningún problema. Literalmente comenzamos a trabajar".

"MSAB nos ayudó y ofreció un apoyo excelente. Llamamos al equipo por teléfono varias veces. Necesitamos la presencia de miembros del equipo en el sitio varias veces para ayudar con la instalación y las pruebas. Eso ocurrió en el sitio antes de que estuviéramos listos para el lanzamiento. MSAB es el mejor en cuanto a apoyo. Desde entonces, todo ha funcionado bien".

Valor para el cliente

Desde que los dos cuerpos de policía instalaron el software XEC Director y conectaron todas sus plataformas de Kiosk, los archivos de extracción se envían ahora a un servidor central, por lo que los archivos ya no se graban en DVD y cada usuario de Kiosk tiene su propia carpeta. Ya no tenemos el problema de quedarnos sin espacio de almacenamiento.

"La solución de MSAB tuvo un impacto positivo en nuestras fuerzas combinadas;

- Los datos son accesibles a través de ambas fuerzas casi instantáneamente, de modo que si tenemos un homicidio en un condado y el equipo de investigación está en otro, no hay que esperar a que lleguen los DVD y copiarlos del disco. Ahora tenemos acceso a los datos casi en tiempo real.
- Realizar la gestión de todas las actualizaciones del software XRY mediante el uso del XEC Director. Esto significa que ya no hay que perder tiempo conduciendo y además nos ahorramos mucho dinero. Hasta ahora, las plataformas de Kiosk han sido excepcionalmente estables y su función de autodetección ha sido extraordinaria.
- Los usuarios no manipulan el XRY después de ingresarlos en las plataformas de Kiosk. Además, como el flujo de trabajo los ayuda paso a paso, ya no temen al uso del software. Les encanta lo rápido que es. No tienen que preocuparse de que el sistema se bloquee o se quede sin espacio.
- Los usuarios se sienten capacitados por el control que obtienen. Las actualizaciones de software se pueden enviar fácilmente. Si hay problemas, los administradores pueden ayudar a los usuarios sin necesidad de estar en el sitio. Como administrador, puedo ver la cantidad de datos que estamos produciendo. La función de informe me parece estupenda. Y como resultado de poder informar de forma clara y concisa a la alta dirección, vamos a intentar obtener más plataformas de Kiosk.

– En resumen. Ahora tengo un entorno configurado y controlado centralmente con todos los datos guardados en una solución de almacenamiento central. Nuestros usuarios pueden utilizar las últimas versiones de XRY y del software de datos forenses móviles XAMN. Y una ventaja adicional importante es que nuestros altos directivos han visto los beneficios".

"Pasar al Kiosk y sistemas de redes de MSAB ha sido la mejor decisión que hemos tomado. Hoy en día, por ejemplo, estamos más capacitados para apoyar a las víctimas de alto riesgo de la violencia doméstica.

Antes, el uso del laboratorio retrasaba el proceso al menos un mes. El uso de Kiosk nos permite ahora confrontar al delincuente con la evidencia extraída en la entrevista, y se podría presentar una acusación en las primeras 8 horas".

– Analista forense digital y director de unidad