

El principal agente de bienes raíces irlandés, Hamilton Osborne King, evita que sus datos comerciales confidenciales caigan en manos equivocadas

La compañía

Hamilton Osborne King es el principal agente de bienes raíces irlandés con un volumen de ventas de 35 millones de Euros en 2005. Con sede en Dublín, Hamilton Osborne King también tiene oficinas en Cork y Belfast, una oficina asociada en Limerick y un total de 240 empleados. La compañía opera tanto en el sector comercial como en el residencial y se enorgullece de su alto nivel de servicio al cliente.

El reto

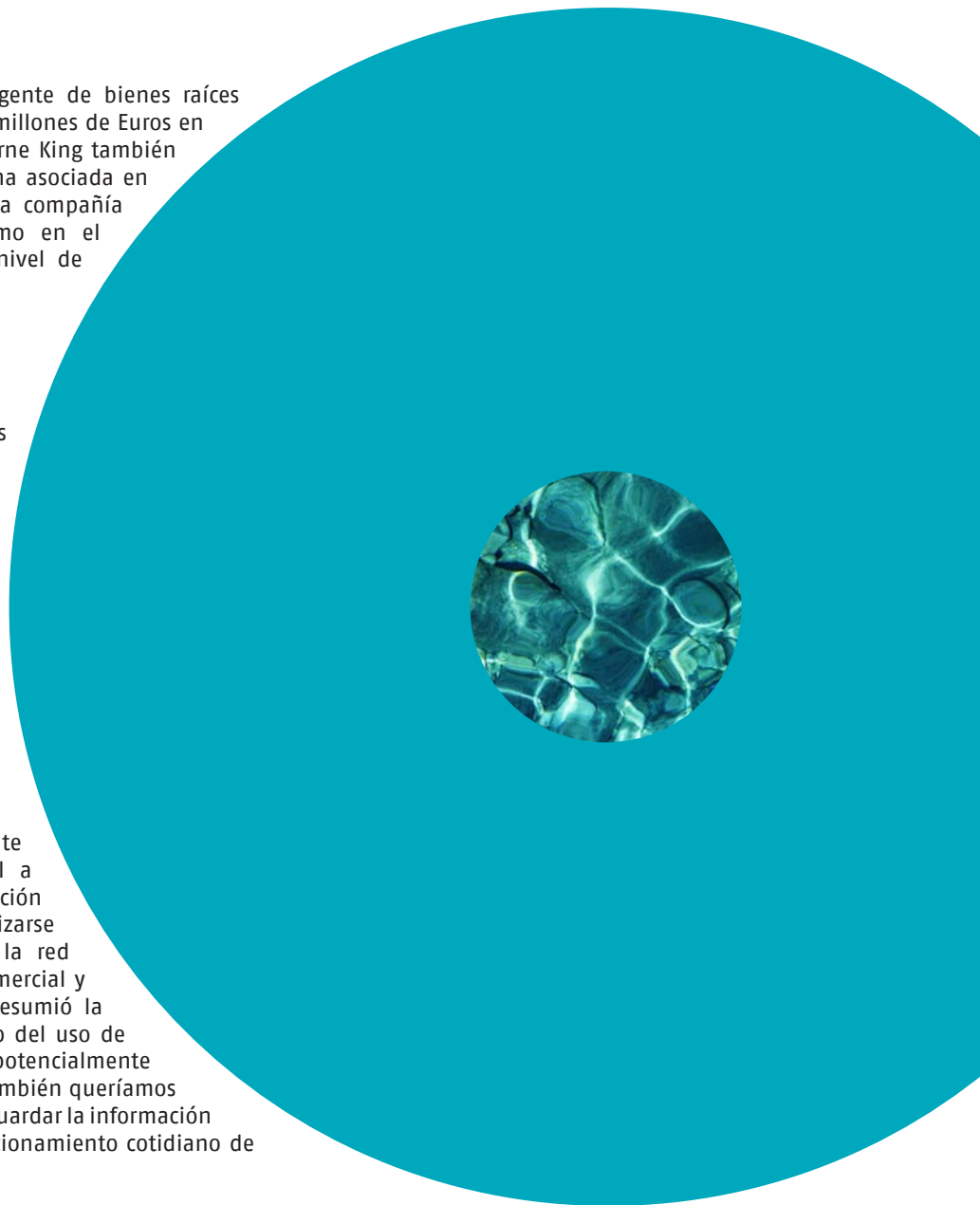
Siendo el líder del mercado en propiedades comerciales en Irlanda, Hamilton Osborne King maneja una cantidad significativa de datos comercialmente confidenciales. Sus sistemas informáticos almacenan información privada sobre los precios de las propiedades así como los datos de los clientes y contactos. La infraestructura informática de Hamilton Osborne King proporcionaba un nivel estándar de seguridad, pero la gerencia sentía la necesidad de mejorarla como consecuencia de la creciente preocupación de potenciales brechas de seguridad.

La sociedad estaba particularmente preocupada sobre la amenaza potencial a la seguridad que representa la proliferación de las memorias USB, que pueden utilizarse para descargar datos confidenciales de la red de la empresa. Kevin Gregory, gerente comercial y tecnológico de Hamilton Osborne King, resumió la situación así: "Sentíamos que el aumento del uso de dispositivos USB dejaba nuestro negocio potencialmente vulnerable y deseamos remediarlo, pero también queríamos lograr un equilibrio razonable entre salvaguardar la información comercialmente delicada y facilitar el funcionamiento cotidiano de la agencia".

La compañía también sentía que una solución de seguridad más robusta aseguraría que se cumpliesen todos los requisitos del Acta de Protección de Datos.

Seleccionando una solución

Hamilton Osborne King condujo una cuidadosa evaluación de las varias opciones disponibles para controlar el acceso a las redes de la compañía vía dispositivos periféricos tales como memorias USB. La empresa deseaba una solución flexible que permitiese que ciertos miembros del personal típicamente los gerentes hiciesen uso de los dispositivos USB para llevar presentaciones a los clientes y documentos a las distintas sucursales de Hamilton Osborne King. Al mismo tiempo, deseaban asegurar que los usuarios no autorizados no podrían aprovecharse de una PC sin control y descargar documentos confidenciales. Después de evaluar las distintas soluciones que ofrecían compañías que incluían SecureWave y Hewlett-Packard, Hamilton Osborne King seleccionó Sanctuary Device Control de SecureWave debido a su flexibilidad inherente y su interfaz de fácil uso.



El señor Gregory dijo del proceso de selección: "Elegimos Sanctuary Device Control de SecureWave porque nos dio la flexibilidad de permitir que el personal seleccionado tuviese acceso a ficheros y aplicaciones específicas de la red a través de sus memorias USB. Era la única solución que nos ofreció la precisión de control que necesitábamos. Otros productos sólo ofrecían tener todo o nada – se podía conceder el acceso a todos los usuarios o a ninguno. También nos gustó la interfaz de usuario intuitiva de Sanctuary Device Control, que hace que el programa sea fácil de instalar, modificar y mantener".

También comentó: "Añada a todo esto la ayuda y soporte recibida de parte de VigiTrust, revendedor de SecureWave, y la decisión era obvia".

La instalación

Hamilton Osborne King comenzó a instalar Sanctuary Device Control a principios de enero de 2006, después de una revisión del acuerdo interno de política de seguridad de la compañía. Sanctuary Device Control de instaló en un servidor Windows no dedicado, localizado en una habitación bajo llave, y el programa cliente requerido se instaló en los ordenadores de 130 usuarios de las jefaturas comerciales de Hamilton Osborne King en un período de cuatro semanas.

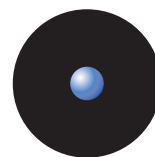
Kevin Gregory comentó: "La primera fase de la instalación de Sanctuary Device Control marchó sobre ruedas. No ha habido problemas técnicos con la instalación y los gerentes en nuestras jefaturas – que requeríamos conquistar para que el proyecto tuviese éxito – respaldaron la solución indicando que les permitía la flexibilidad requerida sin comprometer la seguridad de la compañía".

Hamilton Osborne King planea instalar Sanctuary Device Control en las ramas comerciales de Cork y Belfast en marzo de 2006, desplegando la solución en su sede principal después de esto. Al final del proceso, Sanctuary Device Control quedará instalado en los 240 puestos de los empleados.

Las ventajas

Según Kevin Gregory, "los gerentes de nuestra compañía utilizan regularmente las memorias USB en su trabajo cotidiano, lo que significa que necesitamos adoptarlos como parte integral de nuestra estrategia informática. Sin embargo, al mismo tiempo, deseábamos bloquear nuestras PC para asegurarnos de que no fuesen un blanco fácil de las brechas potenciales de seguridad. Debido a que Sanctuary trabaja definiendo una lista de dispositivos a los que se les permite el acceso a la red y rechaza a todos los demás, hemos podido asegurar que nuestros gerentes tengan acceso a los datos que necesitan de una forma controlada y manejable, mientras que se bloquea todo intento de acceso no autorizado".

El señor Gregory resume: "Instalando Sanctuary Device Control estamos tranquilos sabiendo que nuestros datos comercialmente confidenciales están seguros, lo que significa que el riesgo de que se inculpe a nuestros gerentes de cualquier fuga de información es mínimo. La decisión de invertir en Sanctuary Device Control fue fácil – simplemente comparamos el coste de comprarlo e instalarlo contra el riesgo financiero y de imagen que nuestro negocio sufriría al ser víctima de una brecha de seguridad."



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com