Kingston TECHNOLOGY

Explicación y exploración de la protección óptima de terminales en asociación con Matrix42

MATRIX42

#KingstonIsWithYou

Explicación y exploración de la protección óptima de terminales en asociación con Matrix42

Introducción

Hoy en día, la protección de los datos es un requisito básico para empresas, administraciones públicas y particulares.

Las vulneraciones de datos, el pirateo y el error humano son recordatorios constantes de las amenazas y riesgos que abundan a nivel global. Los costes —tanto económicos como en materia de reputación— asociados con una vulneración de datos pueden ser astronómicos. Los requisitos de estrategias avanzadas de ciberseguridad y DLP (prevención de pérdida de datos) en terminales se basan en métodos de almacenamiento y memorias fiables y eficientes.

El uso del cifrado, del almacenamiento rápido y de las memorias sólidas, combinados con las buenas prácticas, la normativa del sector y unas buenas políticas son todo un avance. Las pérdidas de portátiles y de unidades USB dejan a particulares y empresas vulnerables a la divulgación de información personal y privada. Kingston ofrece soluciones para la prevención de amenazas con las que podrá mitigar los riesgos y complementar su plan de seguridad existente o en vías de implementación.

Explicación y exploración de la protección óptima de terminales en asociación con Matrix42

Contenido

Este breve libro electrónico analiza las soluciones de terminales y presenta ejemplos de casos en que las unidades USB cifradas de Kingston, su programa de personalización y su software de protección de datos Matrix42 EgoSecure han contribuido a resolver seis problemas de sectores diferentes, proporcionándoles una solución a la medida de sus necesidades empresariales.

Exploraremos a fondo estos seis sectores y veremos cómo hacen frente a los retos en materia de protección de terminales.

Índice

Sección 1	Caso práctico – Administraciones públicas	4
Sección 2	Caso práctico – Sector sanitario	5
Sección 3	Caso práctico – Sector financiero	6
Sección 4	Caso práctico – Sector automotriz	7
Sección 5	Caso práctico – Sector de telecomunicaciones	8
Sección 6	Caso práctico – Sector industrial	9
Sección 7	Soluciones de Kingston y Matrix42	10
	Resumen	11
	Acerca de Kingston	12

Sección 1: Caso práctico
Administraciones públicas

Situación:

Dentro del sector público, el uso de dispositivos USB es muy habitual. Por ejemplo, los departamentos de orden público deben copiar las fotografías de infracciones de aparcamiento y administrativas desde cámaras digitales a los sistemas de las autoridades a través de cables USB. Las autoridades policiales reciben los datos de las investigaciones en dispositivos externos de almacenamiento de datos. Estos datos deben reescribirse y debe evitarse el acceso no autorizado a los mismos.

Problema:

Debido a la alta demanda de dispositivos USB, los empleados suelen solicitar habitualmente estas unidades. Por motivos de seguridad, es necesario impedir el uso de dispositivos de almacenamiento de datos privados y externos. Si un empleado necesita un dispositivo de almacenamiento USB nuevo, es necesario facilitárselo a la mayor brevedad a través del Servicio de asistencia al usuario para que su trabajo no se vea afectado. Es importante destacar que el uso de dispositivos USB adecuados no genera ningún problema de seguridad.

Solución:

La combinación de control de dispositivos con filtrado y cifrado de datos posibilita el siguiente escenario:

Bloqueo de dispositivos desconocidos en los terminales de los ordenadores. Los dispositivos de almacenamiento de datos, como las cámaras digitales, solamente están permitidos para determinadas funciones, como la lectura de archivos de imágenes. En general, las operaciones de escritura están cifradas y solo se permiten en dispositivos USB autorizados. Todos los accesos a los datos quedan registrados La administración de los dispositivos autorizados puede simplificarse personalizando los números de serie y los identificadores del hardware. Así, la función Administración de servicio de Matrix42 permite al usuario solicitar la unidad USB personalizada de Kingston Technology en el portal de autoservicio. Tras un proceso de aprobación, se autoriza automáticamente el uso del dispositivo USB a través de Protección de datos EgoSecure.

> “Nuestros empleados están encantados por el hecho de poder obtener los nuevos dispositivos USB rápida y fácilmente tras un breve procedimiento de aprobación. Estamos encantados con el programa de personalización de Kingston Technology y por la fácil administración de la combinación de gestión de servicio y protección de terminales de Matrix42.”
>
> **Director del Servicio de asistencia, Sector público**

Sección 2: Caso práctico
Sector sanitario

Situación:

Los dispositivos de almacenamiento externos suelen ser utilizados frecuentemente como medio para el intercambio de datos con empleados y otras instituciones.

Por ejemplo, los hospitales alemanes deben facilitar al Registro Oncológico información acerca de los casos de cáncer y su progresión. Para facilitar el procedimiento, estos datos suelen transferirse a través de dispositivos de almacenamiento móviles.

También los médicos suelen llevarse documentación, como datos de investigaciones, para sus conferencias utilizando dispositivos USB.

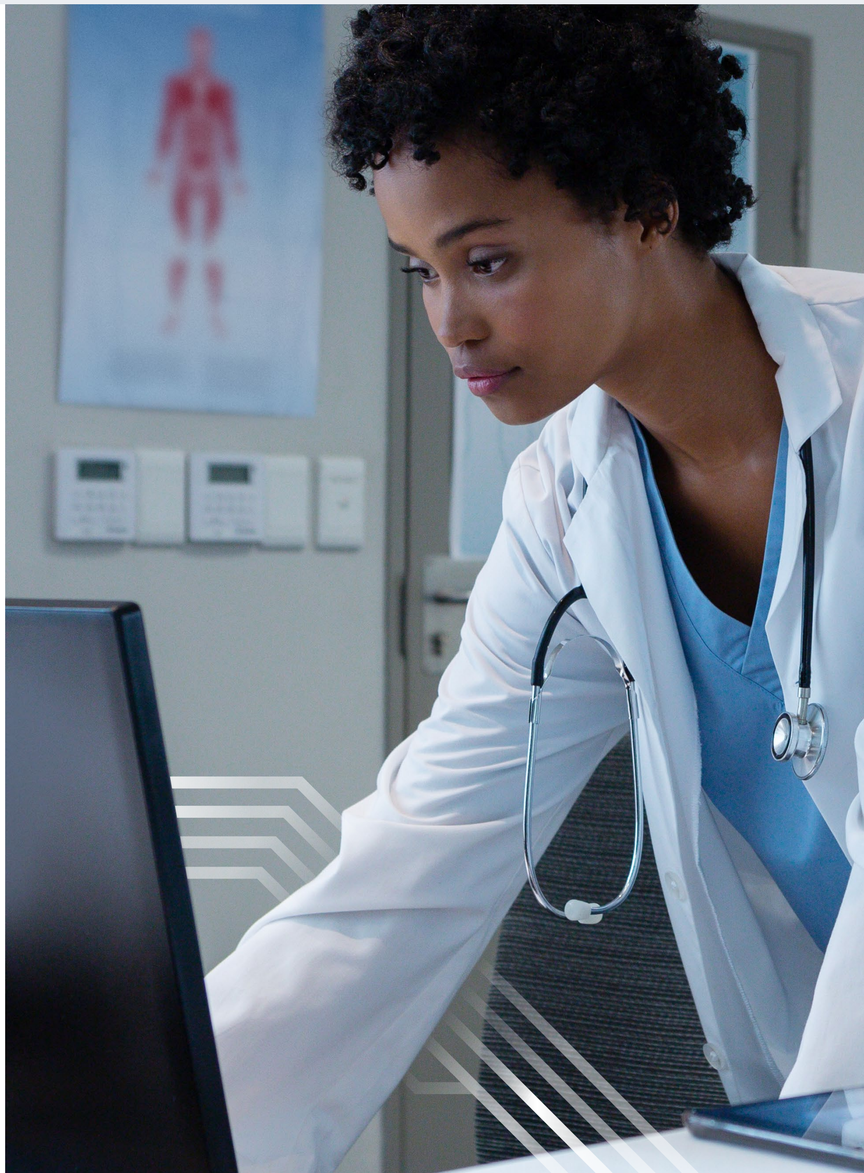
Problema:

Los datos de los pacientes son altamente sensibles y no pueden caer en las manos de personas no autorizadas. Por consiguiente, es necesario incrementar y reforzar la protección de datos. Si el portador de datos se pierde puede producirse un grave problema, no solo por el RGPD, sino también por el bienestar de los pacientes. Por este motivo es importante que el acceso a los datos de USB esté controlado, vigilado y cifrado.

Solución:

Protección de datos EgoSecure combina diversas medidas de protección, como el control de acceso y la auditoría, el filtrado y el cifrado de datos en una única solución. Los administradores de TI están habilitados para decidir a qué empleados se les permite el acceso y a qué dispositivos. Pueden establecerse excepciones, como por ejemplo por número de serie e identificador de hardware. Estos identificadores pueden definirse mediante el programa de personalización de Kingston Technology, de modo que en Protección de datos EgoSecure solo tiene que configurarse un solo valor para permitir usar únicamente los dispositivos aprobados por la organización. Esto minimiza enormemente las tareas administrativas e incrementa la protección de los datos (RGPD, CCPA, HIPAA, etc.), ya que el acceso está cifrado y controlado.

> “Ya habíamos utilizado unidades USB cifradas de Kingston. Ahora, con Protección de datos EgoSecure también es posible asegurar la trazabilidad de las transferencias de datos de pacientes, según lo estipula el RGPD de la UE.”
>
> **CISO, Hospital Universitario**



Sección 3: Caso práctico
Sector financiero

Situación:

Los bancos están sujetos a diversos requisitos de cumplimiento normativo. Uno de estos requisitos es el cumplimiento de las PCI-DSS (Normas de Seguridad de Datos de la Industria de Tarjetas de Pago). Los requisitos de PCI-DSS incluyen la necesidad del cifrado de datos, de análisis de vulnerabilidad y de filtrado de datos. El objetivo es minimizar, o impedir completamente, las amenazas y los riesgos de seguridad informáticos.

Problema:

En los terminales de conexión existen muchos riesgos en materia de seguridad informática. Los empleados tienen que trabajar con información de tarjetas de pago de consumidores y empresas, y procesar diariamente datos de instituciones financieras. Por consiguiente, están expuestos a la amenaza de que los datos de la nube, de los correos electrónicos y de la web resulten afectados por malware, o bien de que caigan accidentalmente en manos de terceros si no se protegen adecuadamente. Tales incidentes serían un riesgo con implicaciones financieras para el banco, no solo en lo referente al RGPD y a las PCI-DSS, sino también por vulnerar la Ley Sarbanes-Oxley. Además, los ciberdelincuentes intentan influir en los sistemas bancarios, o manipularlos, de diversas formas, y cada vez se muestran más creativos. Por ejemplo, recientemente se publicó la noticia de un ciberdelito con los cajeros automáticos: se les cortaba el suministro eléctrico y el sistema era iniciado con un dispositivo de arranque USB para robar el dinero.

Solución:

Los sistemas informáticos deben protegerse mediante medidas de seguridad multicapa. Esto puede conseguirse mediante control de aplicaciones y de dispositivos, detección de anomalías, análisis de comportamiento de usuarios y entidades (UEBA, por sus siglas en inglés), vigilancia y cifrado integral de disco con autenticación prearranque. Matrix42 puede implementar estas funciones en un ecosistema integral automatizado, de modo que solo se admitan las aplicaciones permitidas y dispositivos USB cifrados. Además, tras detectarse actividades sospechosas o maliciosas se implementan automáticamente medidas adicionales. En cuanto al uso de unidades USB, la combinación con unidades USB personalizadas de Kingston Technology contribuye a garantizar que los dispositivos sean incluidos en la lista de autorizados con mínimo esfuerzo, y que los datos sean cifrados de manera trazable. Esto refuerza enormemente el cumplimiento normativo sin esfuerzo adicional.

> “Con Protección de datos EgoSecure y la función de lista de dispositivos admitidos aprobamos solamente unidades USB cifradas de Kingston. Admitimos las unidades USB cifradas de Kingston con identificadores de hardware personalizados; así, se rechazan todos los demás dispositivos. Esto reduce drásticamente los esfuerzos de administración e incrementa enormemente la seguridad.”
>
> **Director de TI, compañía financiera**

Sección 4: Caso práctico
Sector automotriz

Situación:

En el sector automotriz se utilizan dispositivos USB en diversas áreas. Por ejemplo, los datos de investigación se guardan en dispositivos de almacenamiento externo, y se intercambian entre los ingenieros de la compañía. Para configurar las máquinas de producción, los archivos se transportan desde el entorno de TI al entorno de TO. Todos estos datos son muy sensibles y deben protegerse contra el espionaje industrial y el robo de datos, de lo contrario, los conocimientos técnicos acumulados y desarrollados podrían caer en manos erróneas.

Problema:

El sector automotriz está sujeto a requisitos de cumplimiento normativo como TISAX, protección de prototipos, ENX, ISO 27001, "conexiones con terceros" y el RGPD. En TISAX, los artículos 9.1, 9.5 y 10.1 regulan que el acceso a los datos debe ser controlado, vigilado, filtrado y cifrado. Estas medidas también son exigidas por otros cuerpos normativos, como el RGPD e ISO 27001, en todas las áreas de las empresas de automoción.

Solución:

Las unidades USB cifradas de Kingston Technology protegen los datos mediante cifrado basado en hardware. A estos dispositivos se les puede asignar un número de serie personalizado y un identificador de hardware, que Protección de datos EgoSecure utiliza para incluir automáticamente en la lista de dispositivos admitidos. Además, es posible vigilar y analizar los movimientos de datos si se producen actividades sospechosas.

> “Con Matrix42 y Kingston Technology podemos implementar los requisitos de TISAX, como los artículos de Control 9.5 (acceso a la información y aplicaciones) y Control 10.1 (criptografía) sin implementar cambios importantes en el comportamiento de los usuarios.”
>
> **Director de Tecnología, proveedor de componentes de automoción**

Sección 5: Caso práctico
Sector de telecomunicaciones

Situación:

Los proveedores de servicios de telecomunicaciones poseen abundante información acerca de sus clientes. Estos datos son altamente sensibles, en particular en lo que respecta al RGPD. Por consiguiente, es necesario adoptar suficientes medidas para evitar la pérdida y robo de datos.

Problema:

Los empleados de las empresas de telecomunicaciones trabajan diariamente con datos de los clientes. La mayoría de los datos se guardan dentro de aplicaciones empresariales. Sin embargo, existe el riesgo de que los contratos de los clientes, e incluso las exportaciones de bases de datos, se guarden en los terminales y en los dispositivos externos conectados a los mismos. Para el intercambio de datos, los usuarios suelen utilizar almacenamiento externo. Por consiguiente, es muy importante detectar y corregir, o proteger, las prácticas incorrectas de almacenamiento de datos.

Solución:

Para simplificar los procesos de suministro, es posible adquirir unidades USB cifradas de Kingston Technology que incorporen un ID personalizado del producto a través de una lista predefinida en Protección de datos EgoSecure, que se envía a través del Catálogo de servicio de Matrix42. El almacenamiento y exportación de datos que contengan información sensible podrá identificarse y subsanarse automáticamente mediante la inspección de contenidos profundos basada en exploraciones de "datos en uso" y "datos en reposo". Los movimientos de datos pueden registrarse de manera centralizada. Así, el empleado puede recibir nuevo hardware para almacenamiento de datos rápidamente después de haberlo solicitado. Esto garantiza el cumplimiento del RGPD.

> “Gracias al portal de autoservicio de Matrix42, nuestros usuarios pueden solicitar los soportes de almacenamiento que necesitan. Una vez que el pedido ha sido aprobado y entregado, el dispositivo es admitido por el control de dispositivos de EgoSecure. La combinación de Matrix42 con Kingston Technology incrementa la productividad y la seguridad de nuestra empresa.”
>
> **Director de Tecnología, proveedor de servicios de telecomunicaciones**

Sección 6: Caso práctico
Sector industrial

Situación:

El oro del futuro son los datos digitales. Entre los valiosos datos del sector industrial se incluyen los planes de producción, la información sobre clientes y proveedores, y los conocimientos de la empresa. Si estos datos se pierden, esto no solamente podría conllevar las graves sanciones previstas por el RGPD, sino también problemas exponenciales y reputacionales. Lamentablemente, todos los días se encuentran unidades USB en taxis, lavanderías, aeropuertos, estaciones ferroviarias y aparcamientos.

Problema:

Los dispositivos de almacenamiento suelen contener datos sensibles y, lamentablemente, no siempre están cifrados. También existe el riesgo de que técnicos de servicio utilicen los portadores de datos externos para instalar actualizaciones de máquinas de producción. Estos dispositivos externos conllevan el riesgo de introducir malware en la red.

Solución:

Las unidades USB cifradas de Kingston Technology protegen los datos mediante cifrado basado en hardware. Estos dispositivos pueden entregarse con un número de serie personalizado y un identificador de hardware, que Protección de datos EgoSecure utiliza para incluir automáticamente en la lista de dispositivos admitidos. Además, es posible vigilar y analizar los movimientos de datos si se producen actividades sospechosas.

> “El cifrado de nuestros datos de producción es muy importante para protegernos contra el robo de datos. Estos datos altamente sensibles solo pueden copiarse en unidades USB cifradas de Kingston mediante el cifrado de datos de Protección de datos EgoSecure. En todos los demás dispositivos USB, los datos de producción están bloqueados y el acceso a la escritura en unidades de almacenamiento externas está protegido mediante el cifrado y registro de EgoSecure.”
>
> **Responsable de seguridad informática, sector industrial**

Sección 7: Soluciones de Kingston Technology y Matrix42

El uso del cifrado, del almacenamiento rápido y de las memorias sólidas, combinados con las buenas prácticas, la normativa del sector y unas buenas políticas son todo un avance. Las pérdidas de portátiles y de unidades USB dejan a particulares y empresas vulnerables a la divulgación de información personal y privada. Kingston Technology ofrece soluciones para la prevención de amenazas con las que podrá mitigar los riesgos y complementar su plan de seguridad existente o en vías de implementación.

Unidades USB cifradas de Kingston Technology

Las unidades Flash USB con cifrado basado en hardware de Kingston Technology incorporan soluciones de protección de datos móviles dentro y fuera de los cortafuegos de una organización. Diseñadas para proteger datos que requieren la máxima protección, estas unidades contribuyen a satisfacer normas, directivas y reglamentos específicos. Los productos son compatibles con TAA, cuentan con homologación FIPS y se presentan en capacidades de hasta 128 GB, lo cual los convierte en ideales tanto para usuarios corporativos como para organismos de la administración pública.

Programa de personalización segura

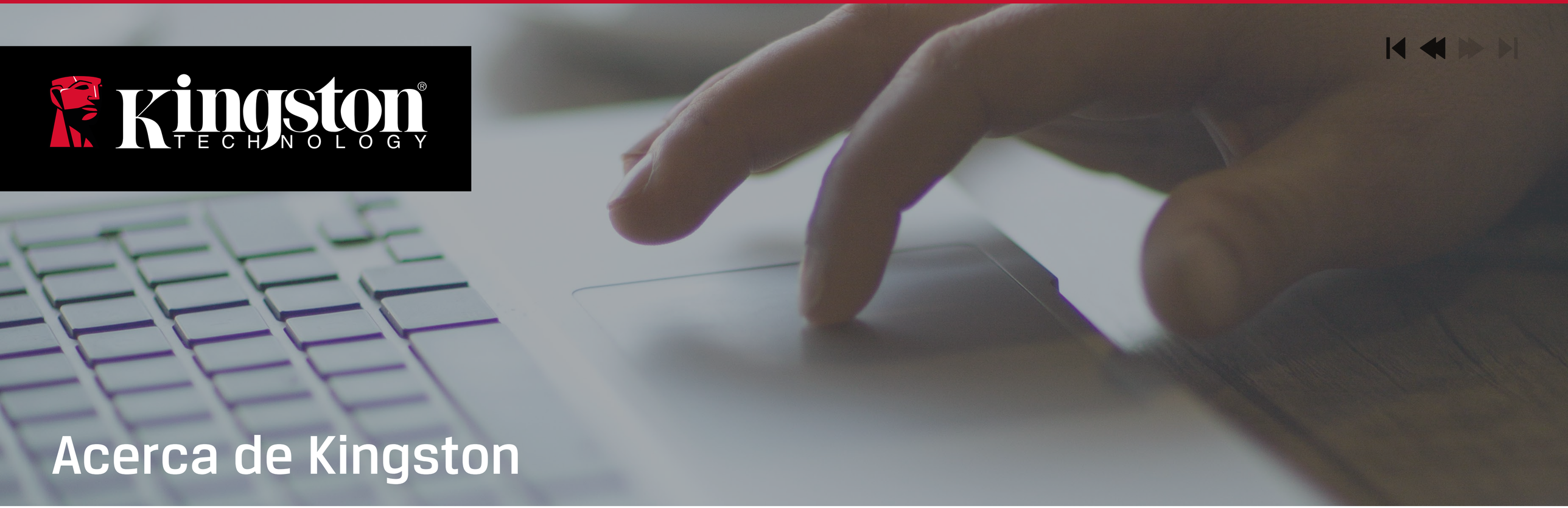
Es posible personalizar las unidades USB cifradas de Kingston Technology de diversas maneras en función de las necesidades de su organización. Añada las funciones de su preferencia para crear unidades únicas e imprescindibles. Kingston Technology le permite realizar de forma sencilla y cómoda pedidos de unidades USB cifradas personalizadas a través del distribuidor de su preferencia. La línea de productos USB cifrados de Kingston incluye las series DTVP30, DT4000G2 y IKD300S. Este programa ofrece las opciones más solicitadas por los clientes, incluyendo numeración en serie, doble contraseña y logotipos personalizados. Con un pedido mínimo de 50 unidades y un volumen de pedidos repetidos de 25, el programa satisface precisamente las necesidades de su organización.

Protección de datos EgoSecure de Matrix42

Protección de datos EgoSecure de Matrix42 ofrece a las empresas una solución integral de gestión de la seguridad para la prevención y protección de dispositivos, sistemas y datos. Esta solución automatiza todo el proceso, desde la prevención y detección hasta contramedidas en caso de daños, sin merma de la productividad.

Resumen

La protección de los datos y la seguridad pueden percibirse como una responsabilidad abrumadora. Los requisitos del trabajo digital han cambiado significativamente. Ahora los empleados pueden decidir cuándo, cómo y con qué dispositivos trabajar. La combinación adecuada de unidades USB con cifrado basado en hardware y administración de software de terminales ayuda a las organizaciones a controlar sus dispositivos. Por consiguiente, mitigan el riesgo de vulneraciones de datos y sustentan su estrategia de cumplimiento continuo del RGPD.



Acerca de Kingston

Con más de 30 años de experiencia, Kingston Technology posee los conocimientos necesarios para identificar y resolver los problemas de seguridad de terminales sin comprometer a su organización.

#KingstonIsWithYou