Kingston TECHNOLOGY

Óptima seguridad de punto final explicada y estudiada en colaboración con Matrix42

MATRIX42

#KingstonIsWithYou

Óptima seguridad de punto final explicada y estudiada en colaboración con Matrix42

Introducción

La protección de datos es un requisito básico para las empresas, los gobiernos e individuos en el mundo de hoy.

La filtración de la información, la piratería y el componente humano son recordatorios continuos de amenazas y riesgos en todo el mundo. Tanto los costos monetarios como de reputación asociados con una filtración de datos pueden ser astronómicos. Los requisitos de las estrategias avanzadas en seguridad informática y de punto final DLP (Protección de pérdida de datos), dependen de almacenamiento y memoria confiables y eficientes.

El uso del encriptado, el almacenamiento rápido y la memoria combinados con las mejores prácticas, estándares y políticas es un gran avance. Las computadoras portátiles y los dispositivos USB perdidos dejan a las personas y empresas vulnerables a la exposición de información personal y privada. Kingston ofrece soluciones de prevención de amenazas para ayudar a mitigar los riesgos mientras complementa un plan de seguridad existente o en desarrollo.

Óptima seguridad de punto final explicada y estudiada en colaboración con Matrix42

Contenido

Este breve eBook analizará soluciones de punto final, y cómo los dispositivos USB encriptados de Kingston, su programa de personalización y el software de protección de datos Matrix42 EgoSecure han ayudado a resolver seis desafíos de diferentes sectores de la industria y les han brindado una solución que se adapta a sus necesidades comerciales.

Profundizaremos en estos seis sectores y veremos cómo abordaron los desafíos de seguridad de punto final.

Tabla de contenidos

Sección 1: Caso de uso de la industria
Sector público

Situación:

Dentro del sector público, el uso de dispositivos USB es muy común. Por ejemplo, las oficinas de orden público deben copiar las fotografías tomadas de los infractores de estacionamiento y las infracciones administrativas desde las cámaras digitales a los sistemas de las autoridades mediante un cable USB. Las autoridades policiales reciben datos de la investigación en dispositivos externos de almacenamiento de datos. Estos datos deben reescribirse y se debe evitar el acceso no autorizado.

Desafío:

Debido a la gran necesidad de dispositivos USB, los empleados solicitan unidades USB con regularidad. El uso de dispositivos de almacenamiento de datos privados y no autorizados debe bloquearse por razones de seguridad. Si un empleado necesita un nuevo dispositivo de almacenamiento USB, debe estar disponible lo más rápido posible a través del punto de atención al usuario para que los empleados no interrumpan su trabajo. Es importante tener en cuenta que los problemas de seguridad no surgen por usar dispositivos USB adecuados.

Solución:

Al combinar el control de dispositivos, el filtrado de datos y el encriptado, se puede recrear el siguiente escenario:

Los dispositivos desconocidos generalmente se bloquean en los puntos finales de las computadoras. Los dispositivos de almacenamiento de datos como cámaras digitales, solo están permitidos para determinadas funciones, como leer los archivos de imágenes. Las operaciones de escritura generalmente están encriptadas y solo se permiten en dispositivos USB autorizados. Se registran todos los accesos a los datos. La administración de dispositivos autorizados se puede simplificar personalizando los números de serie y las identificaciones (ID) de Hardware. De este modo, la administración de servicios de Matrix42 permite al usuario solicitar el dispositivo USB personalizado de Kingston Technology en el portal de autoservicio. Después de un proceso de aprobación, el dispositivo USB permite automáticamente su uso en el protector datos EgoSecure.

> “Nuestros empleados están entusiasmados con el hecho de que los nuevos dispositivos USB se suministran fácil y rápidamente después del breve proceso de aprobación. Estamos muy contentos con el programa de personalización de Kingston Technology, y la fácil aplicación de la combinación de gestión de servicios y seguridad de punto final de Matrix42.”
>
> **Jefe del punto de atención, Sector Público**

Sección 2: Caso de uso de la industria
Cuidado de la salud

Situación:

Los dispositivos de almacenamiento externos continúan utilizándose con frecuencia como medio para intercambiar datos con empleados y otras instituciones.

Por ejemplo, los hospitales en Alemania deben proporcionar al Registro de Cáncer información sobre los casos de cáncer actuales y su progresión. Para mayor comodidad, estos datos se transfieren a menudo a través de dispositivos móviles de almacenamiento de datos.

A los médicos también les gusta llevar documentos, como datos de investigación, a sus respectivas conferencias a través de dispositivos USB.

Desafío:

Los datos de los pacientes son muy sensibles y no deben caer en manos de personas no autorizadas. Por lo tanto, es necesario aumentar y fortalecer la protección de datos. Si se pierde un portador de datos, esto puede convertirse en un problema importante, no solo por la GDPR, sino también por el bienestar de los pacientes. Por esta razón, es importante que el acceso a los datos en el almacenamiento USB esté controlado, monitoreado y encriptado.

Solución:

La protección de los datos EgoSecure combina varias medidas de protección tales como control de acceso, auditoría de datos, filtrado y encriptado en una sola solución. Los administradores de IT pueden decidir qué empleados tienen acceso a qué dispositivos. Se pueden hacer excepciones, por ejemplo, por número de serie e ID de hardware. Estos identificadores se pueden definir gracias al programa de personalización de Kingston Technology, de modo que solo se debe configurar un valor en el control de protección de datos de EgoSecure para permitir que solo se utilicen dispositivos aprobados por la empresa. Esto minimiza enormemente el esfuerzo de administración y aumenta la seguridad de los datos (GDPR, CCPA, HIPAA, etc.), ya que el acceso está encriptado y monitoreado.

> “Ya estábamos utilizando dispositivos USB encriptados de Kingston. Ahora, con la protección de datos EgoSecure, también podemos asegurarnos de que la trazabilidad de las transferencias de datos de los pacientes se realice de acuerdo con la GDPR de la UE.”
>
> **CISO (Oficial de protección de datos), Hospital Universitario**

Sección 3: Caso de uso de la industria Finanzas

Situación:

Los bancos están sujetos a varios requisitos de cumplimiento. Uno de estos requisitos es el cumplimiento del PCI-DSS (Payment Card Industry Data Security Standard) "Estándar de seguridad de datos de la industria de tarjetas de pago". Los requisitos del PCI-DSS incluyen la necesidad del encriptado de datos, análisis de vulnerabilidades y filtrado de datos. El objetivo es minimizar o prevenir por completo las amenazas y los riesgos a la seguridad de IT.

Desafío:

Existen muchos riesgos que existen en el punto final cuando se habla de seguridad de IT. Los empleados tienen que trabajar con información de tarjetas de pago de consumidores y empresas y procesar a diario datos confidenciales de instituciones financieras y, por lo tanto, están expuestos a la amenaza de que los datos de la nube, el correo electrónico, los USBs y la web puedan verse comprometidos por malware, o que los datos puedan caer accidentalmente en manos de terceros si no están protegidos correctamente. Tal incidente sería un riesgo con implicaciones financieras para un banco, no solo en términos de la GDPR, el PCI-DSS sino también de la ley Sarbanes-oxley. Además, los ciber delincuentes intentan influir o manipular los sistemas bancarios de diversas formas y se están volviendo más creativos en el proceso. Más recientemente, por ejemplo, hubo un delito cibernético en relación con los cajeros automáticos donde se interrumpió el suministro de energía, y el sistema se inició con un dispositivo USB de arranque para robar el dinero.

Solución:

Los sistemas de IT deben estar asegurados mediante medidas de protección de múltiples capas. Esto se puede lograr mediante el control de aplicaciones, control de dispositivos, detección de anomalías, UEBA (User and Entity Behaviour Analytics) "Analíticas de comportamiento de entidades y usuarios", monitoreo y encriptado completo del disco con autenticación previa al arranque. Matrix42 puede implementar esto en un ecosistema integral y automatizado, de modo que solo se admitan las aplicaciones permitidas y los dispositivos USB encriptados. Además, se detectan actividades sospechosas o maliciosas y se inician automáticamente otras medidas. Con respecto al uso de dispositivos USB, la combinación de dispositivos USB personalizados de Kingston Technology ayuda a garantizar que los dispositivos se incluyan en la lista blanca con un mínimo de esfuerzo y que los datos se encripten de forma rastreable. Esto aumenta el cumplimiento enormemente y sin esfuerzo adicional.

> “Con la protección de datos EgoSecure y la función de listas blancas, solo permitimos que se aprueben los dispositivos USB encriptados de Kingston. Incluimos en la lista blanca los dispositivos USB encriptados de Kingston con ID de hardware personalizado, no permitimos otros dispositivos. Esto reduce enormemente el esfuerzo de administración, ¡y aumenta la seguridad!”

Gerente de IT, Compañía financiera

Sección 4: Caso de uso de la industria Automotor

Situación:

En la industria del automóvil, el uso de dispositivos USB está presente en varios sectores. Por ejemplo, los datos relativos a las investigación se almacenan en dispositivos de almacenamiento externos y se intercambian entre los respectivos ingenieros de la empresa. Para configurar las máquinas de producción, los archivos se transportan desde el entorno de IT 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 pueden caer en las manos equivocadas.

Desafío:

La industria automotriz está sujeta a requisitos de cumplimiento como TISAX, protección de prototipos, ENX, ISO27001, "conexión de terceros" y la GDPR. En TISAX, los artículos Control 9.1, 9.5 y 10.1 regulan que los accesos a los datos deben ser controlados, monitoreados, filtrados y encriptados. Estas medidas también deben observarse en los otros requisitos de cumplimiento como la GDPR e ISO27001 en todas las áreas de las empresas del sector automotriz.

Solución:

Los dispositivos USB encriptados de Kingston Technology protegen los datos con encriptado basado en hardware. Estos dispositivos pueden obtener un número de serie personalizado y una identificación de hardware (ID), que se pueden usar en el protector de datos EgoSecure para ser incluidos automáticamente en la lista blanca para uso específico de datos. Además, los movimientos de datos se pueden monitorear y analizar en caso de que hayan actividades sospechosas.

> “Con Matrix42 y Kingston Technology, hemos podido implementar requisitos TISAX como Control 9.5 (acceso a la información y aplicaciones) y Control 10.1 (criptografía) sin cambios importantes en el comportamiento del usuario.”
>
> **CTO (Jefe de tecnología), Proveedor automotriz**

Sección 5: Caso de uso de la industria Telecomunicaciones

Situación:

Los proveedores de telecomunicaciones tienen mucha información sobre los clientes. Esta información es muy sensible, particularmente con respecto a la GDPR. Por lo tanto, se deben tomar las medidas necesarias para evitar la pérdida y el robo de datos.

Desafío:

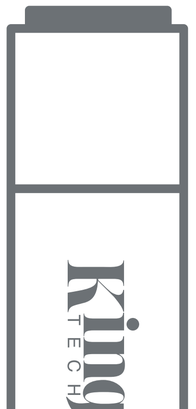
Los empleados de las empresas de telecomunicaciones trabajan con los datos de los clientes todos los días. La mayoría de los datos se almacenan en aplicaciones comerciales. Sin embargo, existe el riesgo de que los contratos de los clientes o incluso las exportaciones de bases de datos se almacenen en el punto final y en los dispositivos externos conectados a ellos. Para el intercambio de datos, los usuarios suelen utilizar almacenamiento externo. Por lo tanto, es muy importante que las prácticas incorrectas de almacenamiento de datos se detecten y corrijan o se eviten.

Solución:

Para simplificar el proceso de adquisición, los dispositivos USB encriptados de Kingston Technology con una identificación de producto personalizada se pueden comprar rápidamente a través de una lista blanca predefinida en el protector de datos EgoSecure y entregarse a través del catálogo de servicios Matrix42. El almacenamiento y la exportación de datos, que pueden contener información confidencial, se pueden identificar y corregir automáticamente mediante una inspección profunda del contenido basada en escaneos de "datos en uso" y "datos en reposo". Los movimientos de datos se registran de forma centralizada. Así, el empleado puede recibir nuevo hardware para el almacenamiento de datos rápidamente después de que haya sido solicitado y aprobado. Esto puede garantizar que cumplirá con la GDPR.

> “Gracias al portal de autoservicio de Matrix42, nuestros usuarios pueden solicitar los medios de almacenamiento que necesiten. Una vez que el pedido se aprueba y se entrega, el dispositivo está autorizado por el control de dispositivos de EgoSecure. La combinación de Matrix42 y Kingston Technology aumenta la productividad y la seguridad en nuestra empresa.”

CTO (Jefe de tecnología),
Proveedor de telecomunicaciones



Sección 6: Caso de uso de la industria
Industria manufacturera

Situación:

El oro del futuro son los datos digitales. Estos valiosos datos de las industrias manufactureras incluyen planes de producción, datos sobre clientes y proveedores y conocimientos de la empresa. Si estos datos se pierden, no solo puede dar lugar a sanciones muy severas considerando la GDPR, sino también a problemas exponenciales y de reputación. Desafortunadamente, USBs son encontrados en taxis, lavanderías, aeropuertos, estaciones de tren o estacionamientos, todos los días.

Desafío:

Los dispositivos de almacenamiento a menudo contienen datos muy confidenciales y, lamentablemente, estos datos no suelen estar encriptados. También existe el riesgo de que los técnicos de servicio utilicen soportes de datos externos para instalar actualizaciones en las máquinas de producción. Estos dispositivos externos tienen el riesgo de introducir malware en la red.

Solución:

Los dispositivos USB encriptados de Kingston Technology protegen los datos con encriptado basado en hardware. Estos dispositivos se pueden entregar un número de serie personalizado y una identificación de hardware (ID), que se pueden usar en el protector de datos EgoSecure para ser incluidos automáticamente en la lista blanca para uso específico de datos. Además, los movimientos de datos se pueden monitorear y analizar en caso de que hayan actividades sospechosas.

> “El encriptado de nuestros datos de producción es muy importante para protegernos contra el robo de datos. Estos datos altamente confidenciales solo se admiten en dispositivos USB encriptados aprobados por Kingston a través del filtrado de archivos del protector de datos EgoSecure. En todos los demás dispositivos USB, los datos de producción están bloqueados y el acceso a escritura de los almacenamientos de datos externos está protegido por el encriptado y el registro de EgoSecure.”
>
> **Oficial de seguridad IT, Industria manufacturera**

Sección 7: Soluciones de Kingston Technology y Matrix42

El uso del encriptado, el almacenamiento rápido y la memoria combinados con las mejores prácticas, estándares y políticas es un gran avance. Las computadoras portátiles y los dispositivos USB perdidos dejan a las personas y empresas vulnerables a la exposición de información personal y privada. Kingston Technology ofrece soluciones de prevención de amenazas para ayudar a mitigar los riesgos mientras complementa un plan de seguridad existente o en desarrollo.

Dispositivos USB encriptados de Kingston Technology

Los dispositivos USB encriptados de Kingston Technology basados en hardware, ofrecen soluciones para la protección de la información para datos móviles dentro y fuera del firewall de una organización. Diseñados para proteger datos que requieren una seguridad hermética, estos dispositivos lo ayudan a cumplir con los estándares, directivas y regulaciones específicas de la industria. Los productos cumplen con TAA, tienen certificación FIPS y están disponibles en capacidades de hasta 128GB, lo que los hace ideales tanto para usuarios corporativos como para agencias gubernamentales.

Programa seguro de personalización

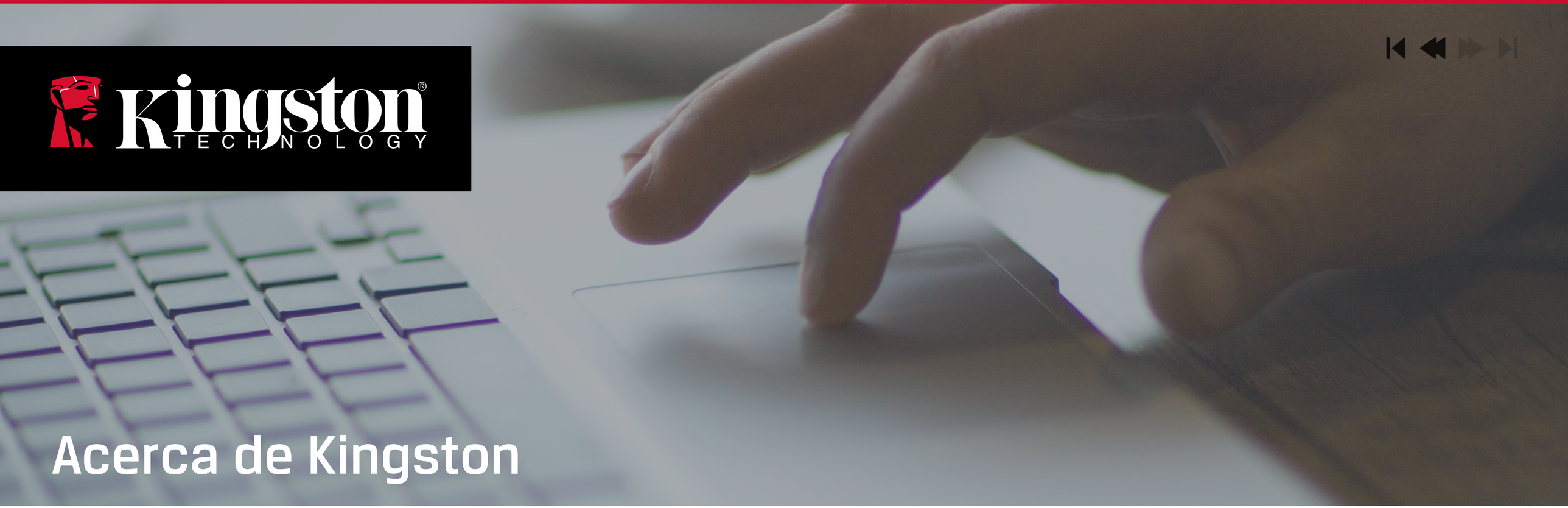
Usted puede personalizar los dispositivos de memoria USB encriptados de Kingston Technology de diversas maneras, con el fin de satisfacer las necesidades de su organización. Agregue características seleccionadas para crear dispositivos únicos e indispensables. Kingston Technology ofrece un proceso fácil y conveniente de para realizar pedidos de su dispositivo USB encriptado personalizado a través de su distribuidor preferido. La línea de productos USB encriptados de Kingston Technology incluyen las series DTVP30, DT4000G2 y IKD300S. Este programa ofrece las opciones más pedidas por los clientes, incluyendo numeración en serie, contraseña doble y logos personalizados. Con un pedido mínimo de 50 unidades y una cantidad de re-orden de 25 unidades, el programa ofrece exactamente lo que su organización necesita.

Protección de datos Matrix42 EgoSecure

La protección de datos Matrix42 EgoSecure proporciona a las empresas una gestión de seguridad de 360° para la prevención y protección de dispositivos, sistemas y datos. La solución automatiza todo el proceso desde la prevención y detección hasta las medidas de respuesta en caso de daño, sin pérdida de productividad.

Manufactura

La protección de datos y la seguridad cibernética pueden parecer una responsabilidad abrumadora. Los requisitos para el trabajo digital han cambiado significativamente y ahora los empleados tienen la capacidad de decidir por sí mismos cuándo, dónde y con qué dispositivos trabajar.
La combinación correcta de dispositivos USB encriptados basados en hardware y la gestión del software de punto final puede ayudar a las organizaciones a obtener el control de los dispositivos de su organización. Por lo tanto, mitigar el riesgo de las filtraciones de datos y respaldar su estrategia de cumplimiento de la GDPR en curso.



Acerca de Kingston

Con más de 30 años de experiencia, Kingston Technology tiene el conocimiento para identificar y resolver sus desafíos de seguridad de punto final sin comprometer a su organización.

#KingstonIsWithYou