Kingston TECHNOLOGY

Optimal Endpoint Security Explained and Explored in Partnership with Matrix42

MATRIX42

#KingstonIsWithYou

Optimal Endpoint Security Explained and Explored in Partnership with Matrix42

Introduction

Data protection is a baseline requirement for businesses, governments, and individuals in today's world.

Data breaches, hacking and the human element are continuous reminders of threats and risks worldwide. Both the monetary and reputational costs associated with a data breach can be astronomical. Requirements of advanced cybersecurity and endpoint DLP (data loss protection) strategies all rely on dependable and efficient storage and memory.

The use of encryption, fast storage and memory combined with best practices, standards, and policies is a big step. Lost laptops and USB drives leave individuals and companies alike vulnerable to exposing personal and private information. Kingston offers threat prevention solutions to help mitigate risks while complementing an existing or developing security plan.

Optimal Endpoint Security Explained and Explored in Partnership with Matrix42

Content

This short eBook will look at endpoint solutions, and where Kingston's encrypted USB drives, its customisation program and Matrix42 EgoSecure Data Protection software have helped solve six different industry sectors challenges and provide them with a solution that matched their business needs.

We deep dive into these six sectors and see how they dealt with their endpoint security challenges.

Table of content

Section 1	Industry Use Case - Public Sector	4
Section 2	Industry Use Case - HealthCare	5
Section 3	Industry Use Case – Finance	6
Section 4	Industry Use Case – Automotive	7
Section 5	Industry Use Case – Telecommunication	8
Section 6	Industry Use Case – Manufacturing	9
Section 7	Kingston and Matrix42 Solutions	10
	Summary	11
	About Kingston	12

Section 1: Industry Use Case
Public Sector

Situation:

Within the public sector, the use of USB devices is very common. For example, public order offices must copy the pictures taken by parking offenders and administrative offences from digital cameras to the authorities' systems via USB cable. Police authorities receive investigation data on external data storage devices. This data needs to be rewritten and unauthorised access must be prevented.

Challenge:

Due to the high demand for USB devices, employees ask for USB drives regularly. The use of private and unauthorised data storage devices must be blocked for security reasons. If an employee needs a new USB storage device, it should be made available as quickly as possible via the User Help Desk so that the employees are not disturbed in their work. It is important to note that no security problems arise from the use of the appropriate USB devices.

Solution:

By combining device control, data filtering and encryption, the following scenario can be made possible:

Unknown devices are generally blocked on computers endpoints. Data storage devices such as digital cameras are only allowed for certain functions such as reading image files. Write operations are generally encrypted and only allowed on authorised USB devices. All data accesses are logged. The management of authorised devices can be simplified by customising serial numbers and hardware IDs. Thus, Matrix42 Service Management allows the user to request the personalised Kingston Technology USB Drive in the Self-Service Portal. After an approval process, the USB device is automatically allowed for use in EgoSecure Data Protection.

> "Our employees are excited about the fact that new USB devices are provided easily and quickly after the short approval process. We are very happy with Kingston Technology's customisation program and easy administration of Matrix42's combination of service management and endpoint security."
>
> **Head of Helpdesk, Public Sector**

Section 2: Industry Use Case
Health Care

Situation:

External storage devices continue to be frequently used as a means of exchanging data with employees and other institutions.

For example, hospitals in Germany must provide the Cancer Registry with information about current cancer cases and their progression. For ease, this data is often transferred via mobile data storage devices.

Doctors also like to take documents, like research data, to their respective lectures via USB drives.

Challenge:

Patient data is highly sensitive and must not fall into the hands of unauthorised persons. Therefore, data protection needs to be increased and strengthened. If a data carrier is lost, this can become a major problem, not only because of GDPR, but the well-being of patients. For this reason, it is important that access to USB data storage is controlled, monitored and encrypted.

Solution:

EgoSecure Data Protection combines various protection measures such as access control, data auditing, filtering and encryption in one solution. IT administrators are enabled to decide which employees are granted access to which devices. Exceptions can be made, for example, by serial number and hardware ID. These identifiers can be defined thanks to Kingston Technology's customisation program, so that only one value needs to be configured in the EgoSecure Data Protection management to allow only company approved devices to be used. This minimises the administration effort enormously and increases data security (GDPR, CCPA, HIPAA, etc), as access is encrypted and monitored.

> "We had already used Kingston encrypted USB drives. Now, with EgoSecure Data Protection, we can also ensure that the traceability of data transfers of patient data is realised in accordance with the EU-GDPR."
>
> **CISO, University Hospital**

Section 3: Industry Use Case Finance

Situation:

Banks are subject to various compliance requirements. One of these requirements is PCI-DSS (Payment Card Industry Data Security Standard) compliance. The PCI-DSS requirements include the need for data encryption, vulnerability analysis and data filtering. The goal is to minimise or completely prevent threats and IT security risks.

Challenge:

There are many risks in terms of IT security that exist at the endpoint. Employees have to work with payment card information from consumers and businesses and process sensitive data from financial institutions on a daily basis, and they are therefore exposed to the threat that data from the cloud, email, USB and web could be compromised by malware, or that data could accidentally fall into the hands of third parties if it is not adequately protected. Such an incident would be a risk with financial implications for a bank, in terms of GDPR, PCI-DSS but also the Sarbanes-oxley act. Furthermore, cyber criminals try to influence or manipulate banking systems in various ways and are becoming more creative in the process. More recently, for example, there was a cybercrime in relation to ATMs where the power supply was interrupted, and the system was started with a bootable USB device in order to steal the money.

Solution:

IT systems must be secured by multi-layered protective measures. This can be achieved through application control, device control, anomaly detection, UEBA (User and Entity Behaviour Analytics), monitoring and full-disk encryption with PreBoot Authentication. Matrix42 can implement this in an automated and integral ecosystem, so that only permitted applications and encrypted USB devices are allowed. Furthermore, suspicious or malicious activity is detected, and further measures are automatically initiated. Regarding the use of USB drives, the combination of customised USB drives from Kingston Technology helps to ensure that devices are included in the whitelisting with a minimum of effort and that data is encrypted in a traceable manner. This increases compliance enormously and with no additional effort.

> “With EgoSecure Data Protection and the whitelisting functionality, we only allow Kingston encrypted USB drives to be approved. We whitelist Kingston encrypted USB drives with personalised hardware ID - other devices are not allowed. This reduces the administration effort enormously - but increases security!”
>
> **IT Manager, Financial Company**

Section 4: Industry Use Case Automotive

Situation:

In the automotive industry, the use of USB devices is present in various areas. For example, research data is stored on external storage devices and exchanged between the respective engineers of the company. To configure production machines, files are transported from the IT environment to OT environment. All this data is highly sensitive and must be protected against industrial espionage and data theft, otherwise the built-up know-how can fall into the wrong hands.

Challenge:

The automotive industry is subject to compliance requirements such as TISAX, prototype protection, ENX, ISO27001, "third-party connection" and GDPR. In TISAX, the Control 9.1, 9.5 and 10.1 articles regulate that data accesses must be controlled, monitored, filtered and encrypted. These measures must also be observed in the other compliance requirements such as GDPR and ISO27001 in all areas of automotive companies.

Solution:

Kingston Technology encrypted USB drives secure data with hardware-based encryption. These devices can get a personalised serial number and hardware-ID, which can be used in EgoSecure Data Protection to be whitelisted for specific usage of data, automatically. Furthermore, data movements can be monitored and analysed if there are any suspicious activities.

> "With Matrix42 and Kingston Technology, we have been able to implement TISAX requirements such as Control 9.5 (access to information and applications) and Control 10.1 (cryptography) without major changes in user behaviour."
>
> **CTO, automotive supplier**

Section 5: Industry Use Case Telecommunication

Situation:

Telecommunication providers have a lot of information about customers. This information is highly sensitive, particularly with respect to GDPR. Therefore, sufficient measures need to be taken to prevent data loss and data theft.

Challenge:

Employees of telecommunications companies work with customer data every day. Most of the data is stored within business applications. However, there is a risk that customer contracts or even database exports are stored on endpoint and external devices connected to them. For data exchange the users often use external storage. It is therefore very important that incorrect data storage practises are detected and corrected or protected.

Solution:

To simplify the procurement process, Kingston Technology encrypted USB drives with a personalised Product ID can be quickly purchased via a predefined whitelist in EgoSecure Data Protection and delivered via the Matrix42 Service Catalog. Data storage and export, which may contain sensitive information, can be automatically identified and remediated by deep-content-inspection based on "data in use" and "data at rest" scans. Data movements are logged centrally. Thus, the employee can receive new hardware for data storage quickly after it has been requested and approved. This can guarantee that it will be GDPR compliant.

> “Thanks to Matrix42's self-service portal, our users can request the storage media they need. Once the order is approved and delivered, the device is allowed by EgoSecure's device control. The combination of Matrix42 and Kingston Technology increases productivity and security in our company.”
>
> **CTO, Telecommunications Provider**

Section 6: Industry Use Case
Manufacturing Industry

Situation:

The gold of the future is digital data. This valuable data in manufacturing industries includes production plans, data about customers and suppliers, and company know-how. If this data is lost, it may not only lead to very severe penalties in view of the GDPR, but also to exponential & reputational problems. Unfortunately, USBs are found in taxis, laundries, at airports, train stations or parking lots, every day.

Challenge:

Storage devices often contain highly-sensitive data and unfortunately, this data is often not encrypted. There is also the risk that service technicians use external data carriers to install updates for production machines. These external devices carry the risk of introducing malware into the network.

Solution:

Kingston Technology encrypted USB drives secure data with hardware-based encryption. These devices can be delivered with personalised serial number and hardware-ID, which can be used in EgoSecure Data Protection to be whitelisted for specific usage of data, automatically. Furthermore, data movements can be monitored and analysed if there are any suspicious activities.

> “The encryption of our production data is very important for us to protect ourselves against data theft. This highly-sensitive data is only allowed on approved Kingston encrypted USB drives via file filtering by EgoSecure Data Protection. On all other USB devices, production data is blocked and write access to external data storages is secured by EgoSecure's on-the-fly encryption and logging.”

IT Security Officer, Manufacturing Industry

Section 7: Kingston Technology and Matrix42 solutions

The use of encryption, fast storage and memory combined with best practices, standards, and policies is a big step. Lost laptops and USB drives leave individuals and companies alike vulnerable to exposing personal and private information. Kingston Technology offers threat-prevention solutions to help mitigate risks while complementing an existing or developing security plan.

Kingston Technology Encrypted USB Drives

Kingston Technology's hardware-based encrypted USB drives feature data-protection solutions for mobile data in and outside of an organisation's firewall. Designed to protect data that requires airtight security, these drives help you meet specific industry standards, directives and regulations. Products are TAA compliant, FIPS certified and are available in capacities up to 128GB, making them ideal for both corporate users and government agencies alike.

Secure Customisation Programme

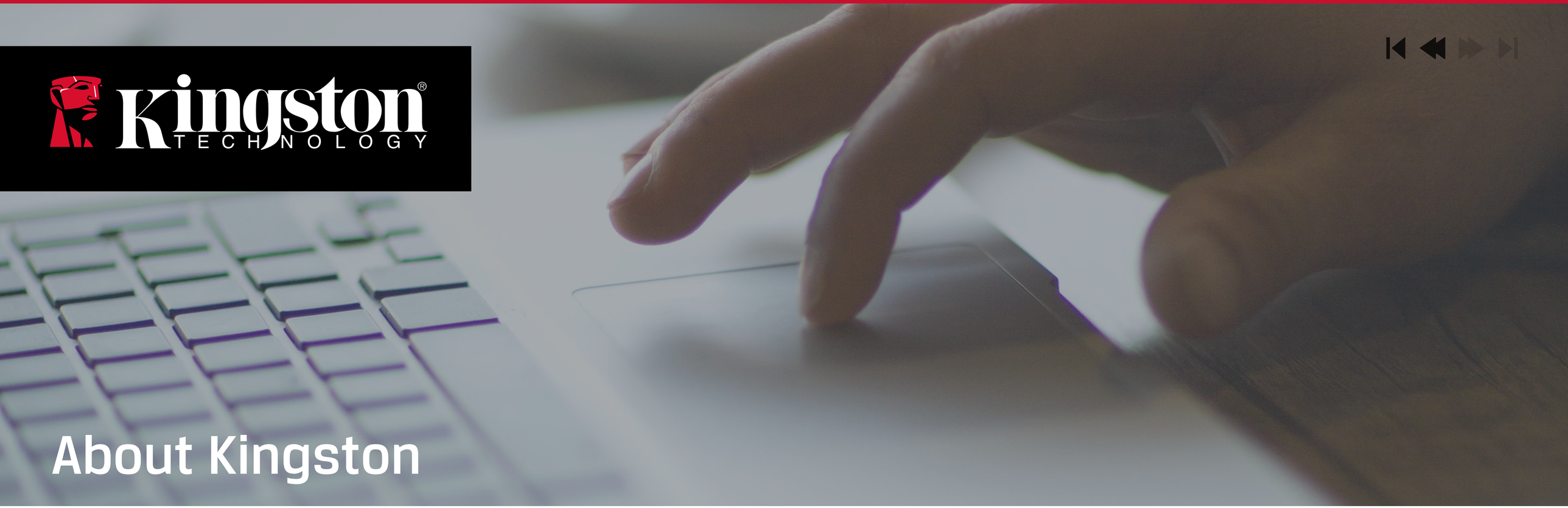
You can customise Kingston Technology's encrypted USB drives in a variety of ways to meet your organisation's needs. Add selected features to create unique, indispensable drives. Kingston Technology offers easy and convenient ordering for your customised encrypted USB drive through your preferred reseller. Kingston Technology's line of encrypted USB products includes the DTVP30, DT4000G2 and IKD300S series. This programme offers the options most frequently requested by customers, including serial numbering, dual password and custom logos. With a minimum order of 50 pieces and re-order quantity of 25 pieces, the program delivers precisely what your organisation needs.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection provides companies with 360° security management for the prevention and protection of devices, systems and data. The solution automates the entire process from prevention and detection to counter measures in the event of damage, without loss of productivity.

Summary

Data protection and cyber security can feel like a daunting responsibility. The requirements for digital work have changed significantly with employees having the ability decide for themselves when, where and with which devices they work with. The right combination of hardware-based encrypted USB drives and endpoint software management can help organisations to gain control of their organisation's devices. Therefore, mitigating risk of data breaches and supporting their ongoing GDPR compliance strategy.



About Kingston

With over 30 years of experience, Kingston Technology has the knowledge to identify and resolve your endpoint security challenges without compromising your organisation.

#KingstonIsWithYou