Protecting your stored data

Encryption best practices

kaspersky

Your guide to encryption best practices

Data Protection….Act!

Proactive data protection is a global business imperative. Kaspersky can help you implement best practices around the encryption and protection of all corporate and sensitive data.

The business case for encryption

According to the Identity Theft Resource Center, major breaches in the first half of 2021 have already reached more than two thirds the annual totals for 2019 or 2020[1]. The top 3 causes of these breaches have been:

1. phishing/smishing/BEC
2. system/human error
3. physical theft/loss

Top security concerns
According to Kaspersky survey data for 2020, the topmost concern for practically every type and size of organization is data loss/exposure, particulary

- data loss exposure due to targeted attacks
- electronic leakage of data from internal systems
- physical loss of devices or media containing data

Kaspersky research found that the average cost of a data loss incident in 2020 was **$1.09m** for an Enterprise and **$101k** for a Small-to-Medium Business.But targeted and combined cyber-blackmail operations are rapidly becoming one of the most devastating cyberattack scenarios. And as these invariably involve not only encrypting ransomware but also sensitive, hand-picked data theft and exposure threats, the payouts here can be much higher[2].

It's not just about the direct cost of a breach, the loss of loyal customers or damage to your business reputation (and 72 per cent of organizations surveyed have been obliged to publicly acknowledge an incident). In most major markets, data security and privacy are now mandated by law, with many jurisdictions obliging organizations to encrypt sensitive data.

With the EU GDPR and similar non-industry-specific legislation now setting new standards in the secure handling of any personally identifiable and/or third party data, the use of crypto-algorithms to protect data both at rest and in motion has become a de-facto standard. Failure to follow these recommendations may well result in regulatory action, with heavy fines adding to already considerable financial losses.

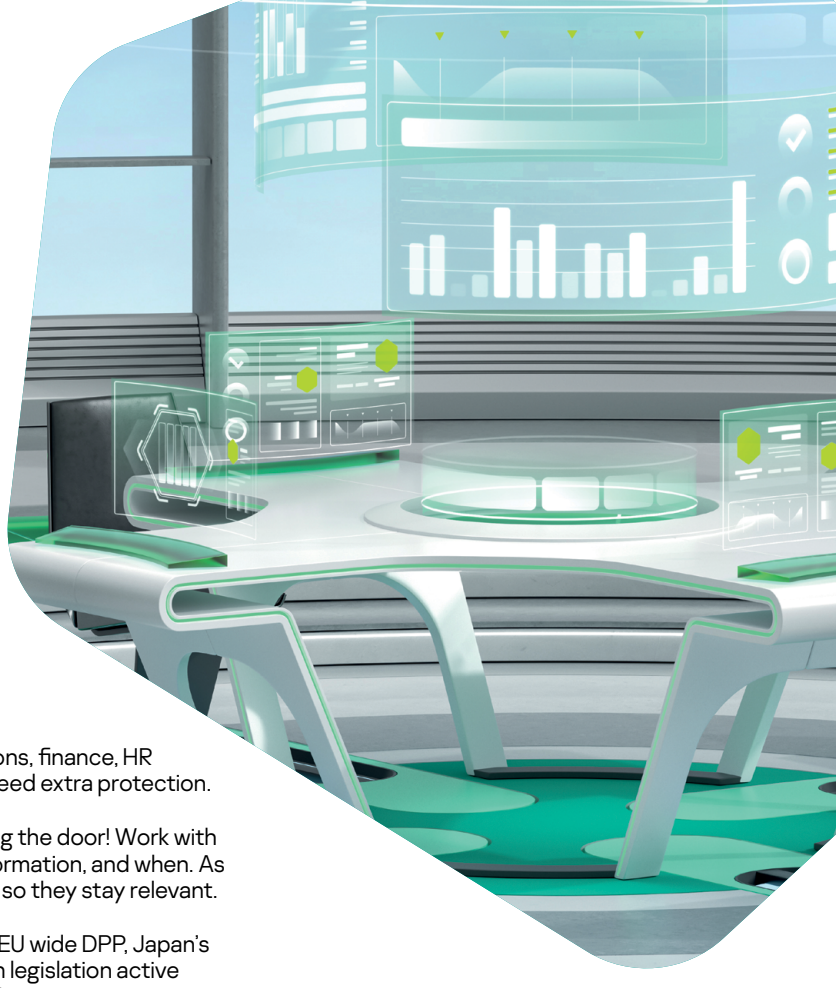
Whether you're faced with data theft via your IT network, a stolen laptop or a lost data storage device, **encryption means your sensitive data is impenetrable and useless to criminals or unauthorized viewers.**

So how best to go about it?

[1] Identity Theft Resource Center: 2021 1st Half Data Breach Analysis

[2] Kaspersky 2020 IT Security Risks Report

Best practice approaches to encryption



1. Policy first, technology second

As with so many security strategies, encryption best practice begins with establishing strong policies: Are you going to encrypt entire disk drives? Removable storage devices? Or just certain types of data, files and folders? Maybe you want specific documents to be unreadable by some users, but not by others? Or maybe a little bit of both?

For most businesses, making information accessible to the right people at the right time is a priority. Good policies, coupled with the right technologies, will get you there without compromising on security.

Some good places to start include:

- **Involving all relevant stakeholders** – IT management, operations, finance, HR etc. They can help you to identify the kinds of information that need extra protection.
- **Access control** – If everyone has a key, there's no point in locking the door! Work with stakeholders to identify who needs access to which kinds of information, and when. As an added precaution, aim to audit your access controls regularly so they stay relevant.
- **Know your compliance needs** – GDPR, PCI-DSS, HIPAA, SOX, EU wide DPP, Japan's PIPA, the UK's Data Protection Act - or any other data protection legislation active in your geography, or applicable when you deal with data from other nation states' citizens. If you're not yourself fully conversant with the growing number of data protection regulations out there, you may well have internal resources, such as your Legal Department or even a Data Protection Officer, to turn to here. It's important to identify the regulations, laws, guidelines and other external factors that govern the way data must be secured or exchanged in your organization. Set policies to work with these – for example the automatic encryption of customer credit card data or employee social security numbers.
- **All in or all out** – Put your policy in writing, have senior management endorse it and communicate it to your end-users – including any third parties who handle your sensitive data. If they don't like it, fair enough – but they don't get to access your data.
- **Back it up** – best practice always involves backing up your data before installing any new software. Encryption is no different – make sure you back up all your end-users' data before proceeding with your encryption program.
- **Keep it simple** – minimize the end-user burden and intrusiveness by implementing a technology that supports single-sign on.

2. Full disk encryption or file level encryption?

The simple answer in terms of best practice is - both.

Encryption solutions typically come in two key types – Full Disk Encryption (FDE) and File Level Encryption (FLE). Each has its own benefits.

Benefits of full disk encryption (FDE):

FDE is one of the most effective ways any organization can protect its data from theft or loss and is pretty well essential. Regardless of what happens to the device, FDE allows you to ensure that all sensitive data is completely unreadable and useless to criminals or prying eyes.

FDE protects 'data at rest' at a level as close to the hardware as possible – i.e. every single sector of the drive is encrypted. The means all the data on your hard drive is encrypted, including file content, metadata, file system information and directory structure. Only authenticated users can access data on the encrypted drive. In addition to hard drives, FDE technology can be applied to removable media, such as USB drives or hard drives in a USB enclosure.

- Look for Pre-Boot Authentication (PBA) – this requires users to present and authenticate their credentials before the operating system even boots, adding an extra layer of security. Nothing can be read directly from the hard drive's surface by thieves, nor can the OS be started.

- Look for an encryption solution that features compatibility checks with all network hardware **before** implementation, saving headaches later. Solutions that offer support for UEFI-based platforms, including the latest laptops and workstations carrying Windows 10 or even Windows 11, will ensure you're future-proofed.

- Similarly, support for Intel AES NI – a new improvement to the Advanced Encryption Standard (AES) that accelerates encryption for Intel's Xeon and Core processor families (as well as some AMD) – and for modern GPT disk standards, both contribute to a well-rounded encryption strategy.

- Enable secure data sharing within the business by using FDE encryption on removable drives.

FDE's greatest advantage is that it simply encrypts the whole file system of the data storage, automatically solving the issue of device loss/theft.. On the downside, it can't protect data in transit, including information shared between devices. It's also useless against unsolicited data access (e.g. via the network or via a C&C connection already established by running malware) attempted when the device is up and running. If you're following best practices, and have chosen a solution that also offers File Level Encryption, this won't be a problem for you.

Benefits of file level encryption (FLE):

Operating at file system level, FLE not only enables 'data at rest' protection, but also secures 'data in use'. Using FLE, specific files and folders on any given device can be encrypted. This makes selected information unreadable to unauthorized viewers, regardless of where it's stored or copied to. FLE allows administrators to automatically encrypt files based on attributes such as location (e.g. all files in My Documents folder), file type (e.g. all text files, all Excel spreadsheets etc) or the name of the application that writes the file. For example, a best-in-class solution might support the encryption of data written by Microsoft Word, independently of the folder or disk.

- FLE offers great flexibility to businesses seeking to apply granular information access policies - only data defined as sensitive (according to administrator-set policies) is encrypted, supporting mixed data usage scenarios.

- FLE also facilitates easy and secure systems maintenance – encrypted file data can remain secure while software or systems files are open, to facilitate updates or other maintenance. If, for example, if you're a CFO wanting to keep confidential business information out of the sight of systems administrators, FLE will support this.

- FLE supports effective application privilege control, allowing administrators to set clear encryption rules for specific applications and usage scenarios. Through application privilege control, administrators can decide when to provide data only in its encrypted form, or even completely block access to encrypted data for specified applications. They can, for example:

  - Simplify secure backups by ensuring encrypted data remains encrypted during transfer, storage and restoration, regardless of the policy settings at the endpoint to which the data is restored.

  - Prevent the exchange of encrypted files over IM or emailing to external recipients , without restricting legitimate message exchange.

Best of both

By adopting a combined FDE/FLE approach to encryption, businesses can enjoy the best of both worlds – you might, for example, choose file encryption only for desktop PCs, while enforcing full disk encryption on all laptops.

Symmetric vs. asymmetric encryption

The choice between symmetric (as AES) and asymmetric (as RSA) data encryption is usually defined by use case.

AES is speedy, and not too heavy on system resources – so great for encrypting large volumes of data and frequent or even 'on-the-fly' cryptographic operations. It requires all parties permitted to access the data to securely share the same secret key, though, which can be an issue.

RSA asymmetric (or public-key) algorithms are more resource-heavy and slower than symmetric ones , so really only workfor smaller volumes of data. they do, though, provide convenient options for secure key sharing to ensure protected information exchange between remote parties, so are suitable for highly secure case-by-case packaged data transfer, when encryption and decryption times are less critical.

Casual data transfer during everyday web usage – as well as network communications across a VPN connection – involves both asymmetric AND symmetric cryptography (for key exchange and session data encryption, respectively). But when there are serious data security concerns, the files transferred can be encrypted regardless of connection security status. This avoids the risk of in-system compromise (i.e. if the data lands at an already-compromised system) – as well as configuration errors or failed-to-timely-update systems configurations allowing a Man-in-the-Middle type attack to compromise the session.

3. Enforce removable media encryption

USB flash drives can now hold 100GB+ of data, while portable drives smaller than your hand can hold terabytes of data – that's a lot of potentially business-critical information being found in jackets at the dry cleaners, left behind in the security tray at the airport or simply falling out of your pocket.

You can't control user carelessness or accidents, but you can control the consequences.

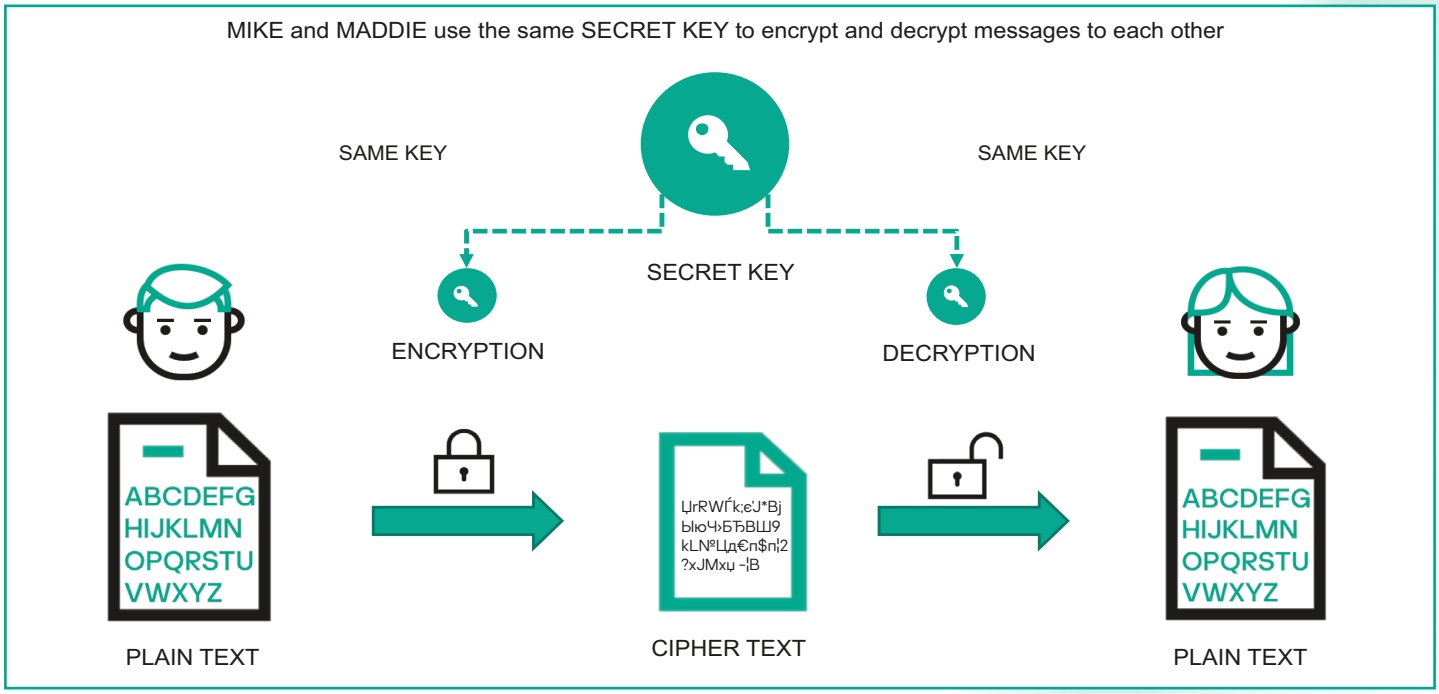
Effective encryption strategies include device encryption as standard. Ensure that every time sensitive data is transferred from an endpoint to a removable device, it's encrypted. You can do this by applying FDE or FLE policies to all devices, ensuring that even if they're lost or stolen, your sensitive data is secure.

The most effective encryption solutions integrate with extended device control capabilities, supporting the granular application of policies all the way down to specific device serial numbers.

When working with sensitive information both inside and outside the perimeter, so-called 'portable mode' should be adopted by users. An example might be a user making a presentation at a conference, who has to use a flash drive to transfer corporate data to a public computer without encryption software installed. You need to ensure that your data remains secure, even while its travelling from the laptop to the presentation system. Portable Mode offered by best-in-class solutions will allow you to do this, ensuring the transparent use and transfer of data on encrypted removable media – even on computers without encryption software installed.

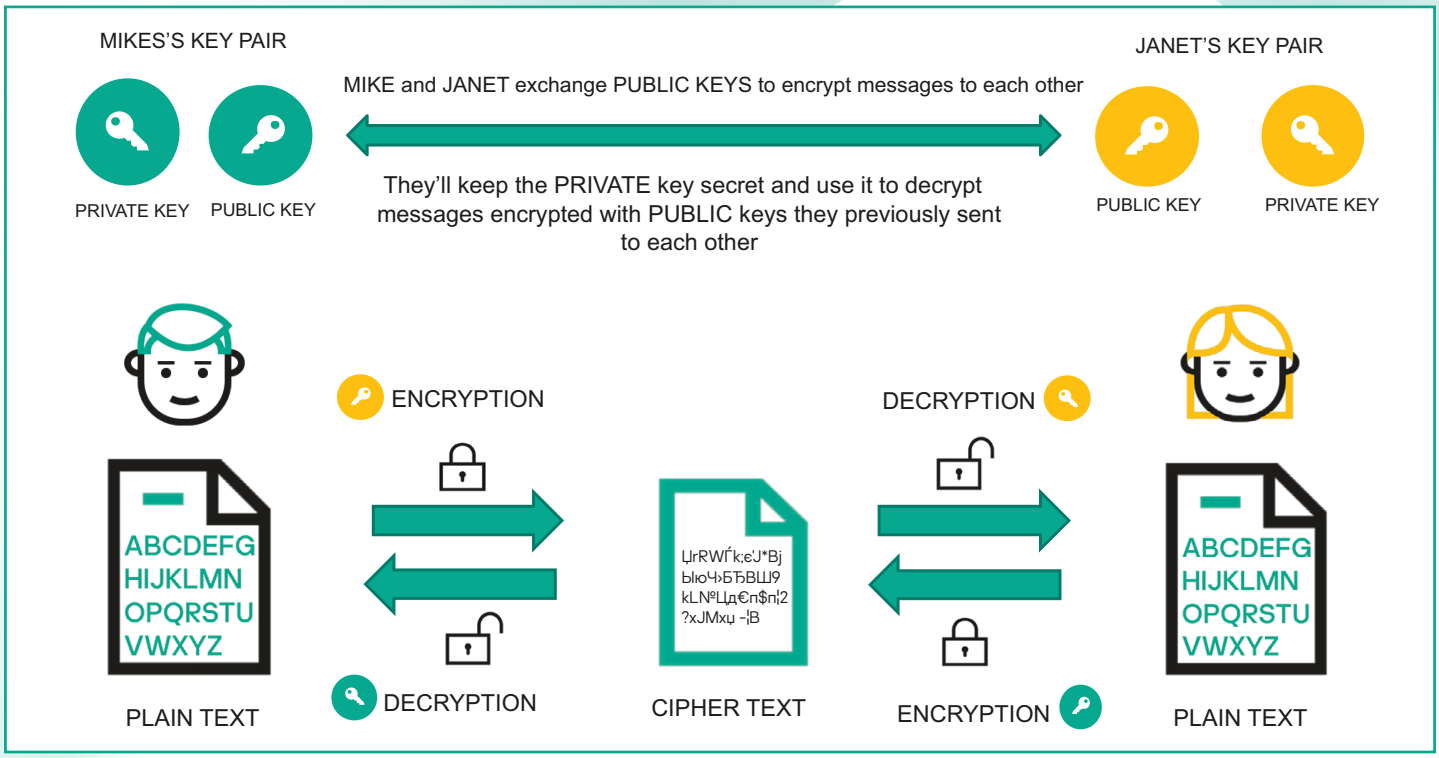
Use industry proven secure cryptography

Your encryption strategy can stand or fall depending on the technology that underlies it. Easily cracked encryption algorithms are worthless. The two most widespread – and, the same time, powerful encryption algorithms are the symmetric Advanced Encryption Standard (AES) with 256 bit key length (likely to be used for file-level encryption) and the asymmetric RSA algorithm, which should have a key length equal or longer than 2048 bit[3], Support for Intel® AES-NI technology, UEFI and GPT platforms will future-proof your strategy.



AES symmetric encryption: how it works

[3] The trend for switching to RSA 4096 has already gained momentum, so if you're not constrained by legacy, low powered hardware and are ok with longer encryption times, it's worth considering using 4096 bit keys right from the off



RSA asymmetric encryption: how it works

Don't underestimate the importance of keys – your encryption algorithm is only as good as the key needed to unlock it. Easily hacked keys make your entire encryption program worthless. Similarly, effective key management is a vital component of effective encryption – there's no point in having the world's best lock on the door if you put the key under the mat.

Keep encryption keys in a centralized storage location/escrow – this also makes it a lot easier for you to decrypt data in emergency situations.

Forgot your password? Not a problem!

Users forget their passwords almost as often as they lose their USB keys or smartphones.

Sometimes even the best hardware or operating system can fail, leaving users without access to vital information.

A quality encryption solution should provide administrators with tools for straightforward data recovery in the following cases:

- When the end user requires it (e.g. forgotten password)
- When the administrator needs it for maintenance, or when faced with a technical issue, such as an OS that won't load or a hard drive has physical damage that must be repaired.

When a user forgets their password, alternative authentication can be achieved by requiring them to give the correct response to a series of alternative questions.

Choose multi-layered security

End users and lost devices aren't the only causes of data loss. Data thieves are developing increasingly sophisticated malware, capable of accessing systems and quietly stealing data, and often going undetected for years. While encryption can help render any stolen data useless, it's much more effective when viewed as a complementary layer of a broader, integrated security strategy that includes high quality anti-malware, device and application controls working together to reduce the opportunities criminals have to access systems and steal sensitive data.

No encryption best practice strategy is complete without integrated layers of anti-malware and system hardening-based protection, capable of detecting and mitigating malicious code while scanning for, detecting and managing the kinds of vulnerabilities that expose organizations to data loss. All of this can and should be done with minimal end-user interference or even awareness.

Manage centrally

Encryption has acquired a reputation for being too complex to implement and manage. That's largely because more traditional, dated solutions tend to be provided separately from anti- malware and other IT security technologies, generating unnecessary complexity. Managing diverse solutions – endpoint controls, anti-malware and encryption – even from a single vendor is not only expensive, it's time-consuming at all phases of the implementation cycle. Purchasing, staff education, provisioning, policy management, maintenance and upgrade all need to be treated as separate projects for each component.

Today's operating systems such as Windows or MacOS now include built-in encryption tools that make the implementation of corporate-level encryption and usage easier. But, as with any additional, separately managed security measure, this offers a separate workflow which doesn't integrate with other cybersecurity solutions – unless this issue is specifically addressed.

A fully integrated, multi-layered security solution not only saves time and money, but makes the software adoption process as easy and painless as possible.

Easy-to-manage solutions leave less room for error, so are more effective as well as saving time and stress. Choose one that enables single console, single policy management from day one, reducing overheads and eliminating compatibility issues between separately managed components, as well as the hassle of dodging between management tools.

Implementing Role Based Access Management (RBAC) is also good practice in larger organizations and those with a well-developed IT Dept, where administrators each have their own of responsibillty.

It's good practice to apply endpoint encryption settings under the same policy as anti-malware protection, device control and all other endpoint security settings. This enables the best practice approach of integrated, coherent policies – for example, IT can not just allow only approved removable media to connect to a laptop, but can also enforce encryption policies to the device. A closely integrated technology platform has the added benefit of improving overall system performance.

Finally...

Offering all the features and capabilities discussed above and more, our Kaspersky Endpoint Security for Business and Kaspersky Endpoint Security Cloud solutions can help enable organizations of all sizes to adopt and adhere to encryption best practice. Complete integration with Kaspersky's best-in-class anti-malware, system hardening and management technologies delivers true multi-layered security. This enables the application of encryption settings under the same policy as anti-malware, device control and other endpoint security elements.

These products support the management of both Microsoft's Windows BitLocker and Apple's MacOS FileVault encryption technologies, allowing tight integration of encryption into the unified corporate cybersecurity workflow. If you prefer a more organic solution, you can opt for our own encryption toolset, available in Kaspersky Endpoint Security for Business[4], This offers the benefits of more comprehensive – and thus more effective - security policies as well as reduced security management hassle.

The availability of both on-premise and cloud-hosted SaaS versions of Kaspersky Security Center[5] adds to the convenience of unified management 'from everywhere' – critical when the whole approach to doing business is moving so rapidly towards a 'remote working' and 'cloud first' paradigm.

Most tested, most awarded multi-layered protection, full visibility, unified management – everything you need to implement best practice encryption, brought together in one integrated security solution.

Contact us for more about how to implement encryption best practices using Kaspersky solutions

[4] Encryption-related tools are available in Kaspersky Endpoint Security Advanced. They also can be found in Kaspersky EDR Optimum and our comprehensive Kaspersky Total Security for Business solutions.

[5] Kaspersky Endpoint Security Cloud is managed via its own cloud console, specifically designed with ease of use in mind.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

kaspersky BRING ON THE FUTURE