tresorit

How can encryption protect – and deceive you?

Peter Budai

Chief Technology Officer

17/04/2024

itsa 365

HOME OF IT SECURITY

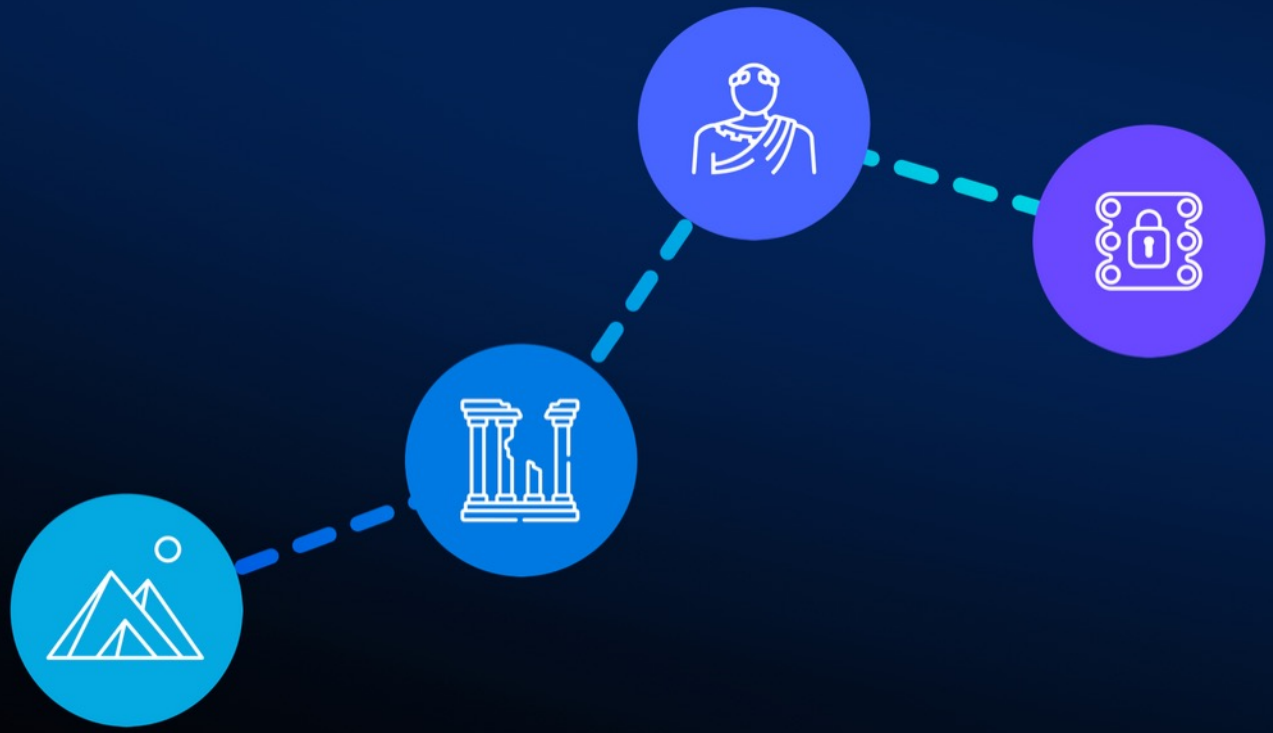
Agenda

- Encryption in the past and present
- Common myths around encryption
- Case study
- Conclusions

Encryption in the past and present

Encryption’s importance in the digital age

tresorit



A brief history of encryption

- The earliest written evidence of encryption can be traced to ancient Egypt
- The first recorded instance of encryption being used for military purposes dates to around 500 BC
- The era of World Wars - encryption changed dramatically as machine and electromechanical encryption and decryption were born
- RSA story – the introduction of public-private key pair for encryption and modern authentication methods
- World Wide Web – the desire to protect business communications and digitally stored materials

Not all encryption is created equal

In transit encryption

Data encryption in motion, between servers. E.g. HTTPS, TLS

At rest encryption

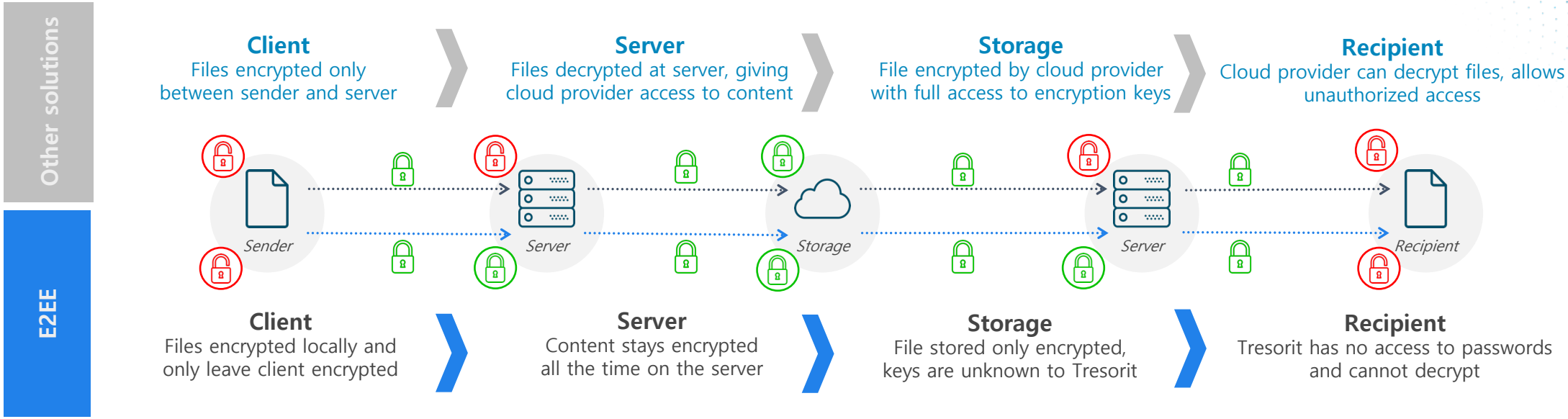
Data encrypted on the server. Encryption keys are stored on the server.

End-to-end encryption

Encryption done on the client side, keys never leave the client side in an unencrypted format.

tresorit

What is end-to-end encryption?



End-to-end encryption is a method of secure communication that ensures all information is encrypted before it leaves the sender's device and remains encrypted until it reaches the recipient

tresorit

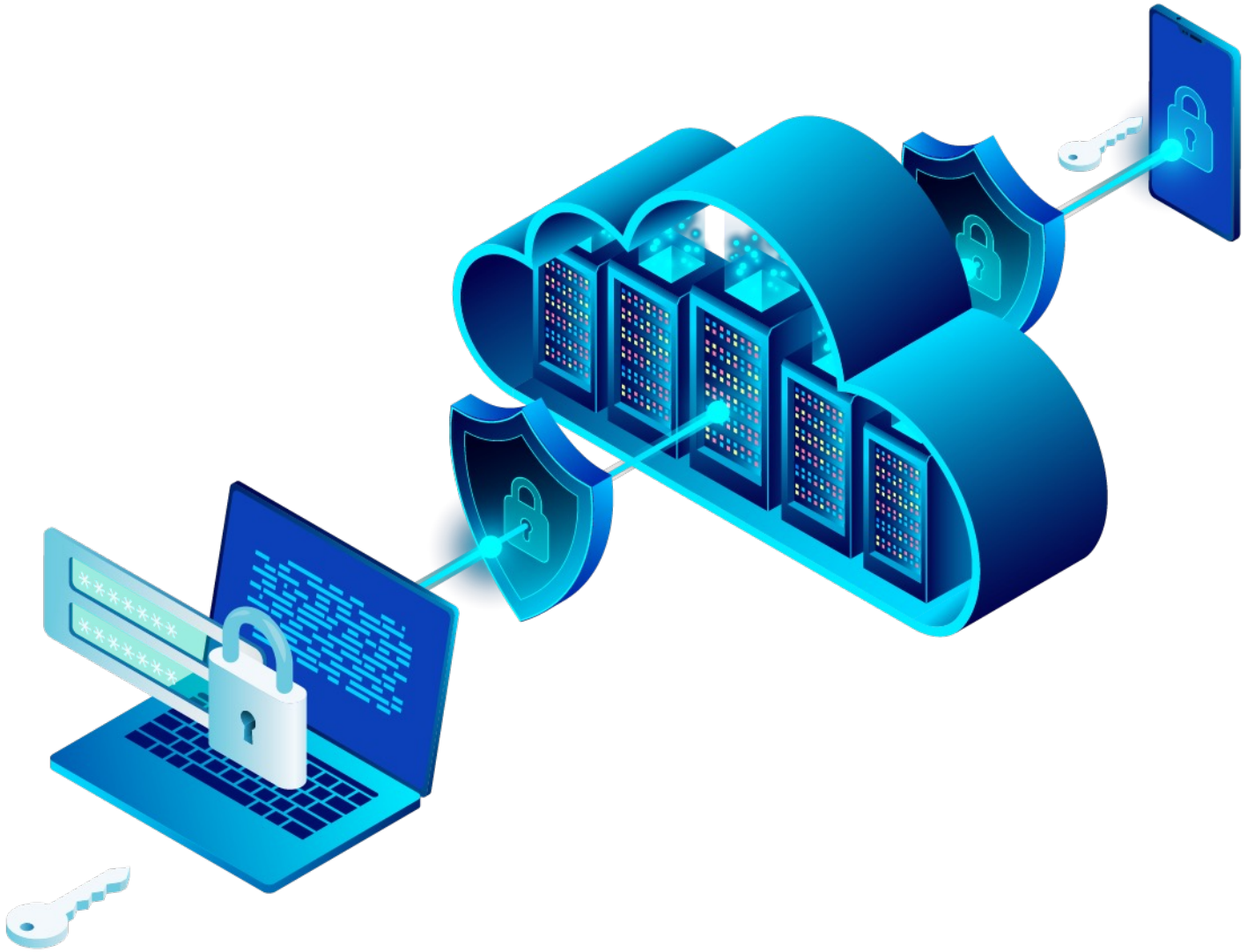
Common myths around encryption

Three examples

tresorit

Myth 1 – Encryption is unbreakable

- Some people believe that encryption is completely secure and impossible to break
- In reality, encryption is designed to withstand until the information it protects becomes obsolete
- Encryption can also be compromised by weaknesses in key management or implementation, or by attacks that exploit software or hardware vulnerabilities
- It is important to regularly update encryption methods and use strong passwords



tresorit

Myth 2 – Encryption in the cloud isn't secure

- When implemented properly, encryption in the cloud can be highly secure
- Cloud providers use industry-standard encryption algorithms and key management practices to protect data
- Cloud providers have more resources to invest in security and can offer more advanced security features.
- The main security risks are related to user error or misconfiguration

tresorit

Myth 3 – Encryption should only be used by businesses who have compliance requirements

- Many organizations assume that encryption is only necessary for companies that have specific compliance requirements
- Sensitive data can include anything from financial information to personal information (social security numbers or health records)
- Data breaches can be costly in terms of both financial losses and reputation damage
- Encryption can help companies comply with privacy regulations

tresorit

When end-to-end encryption is implemented with the least effort

Case Study

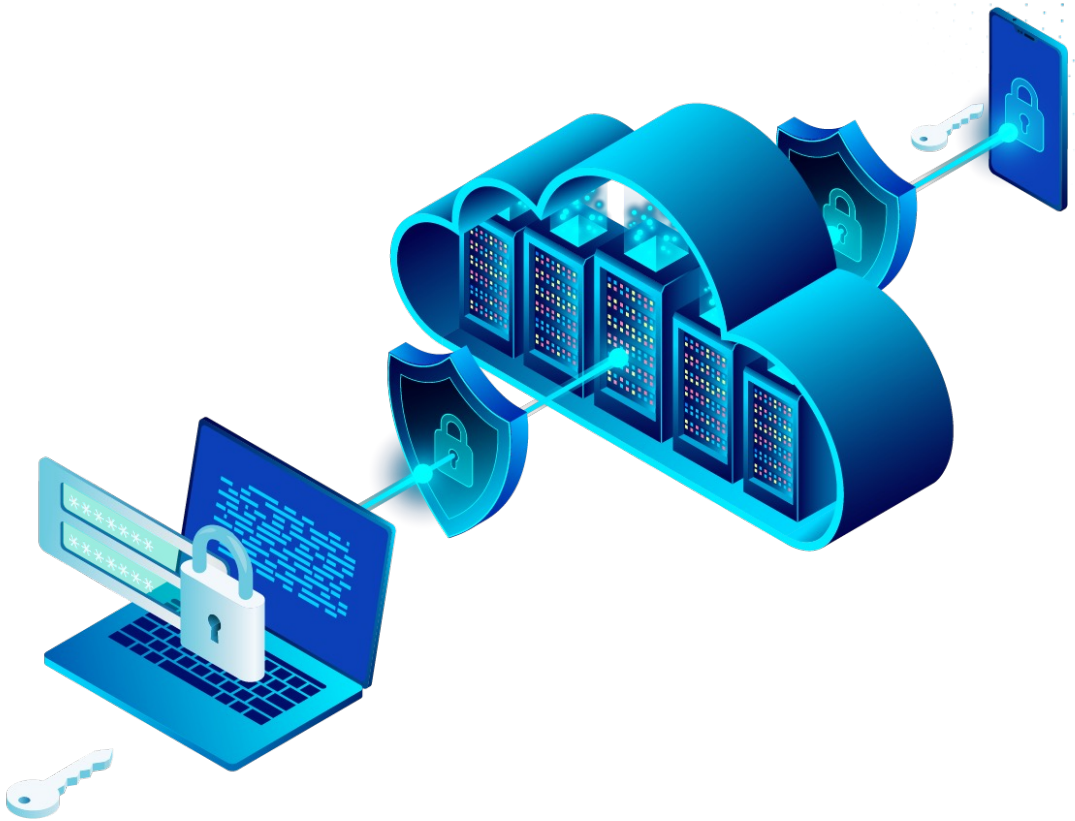
tresorit

~~Hypothetical~~ Password Manager Breach

The breach: compromised user email addresses, password reminders, authentication hashes, encrypted content, weak stretched passwords

The impact: no encrypted user vault data compromised, but still significant risk to users' account security

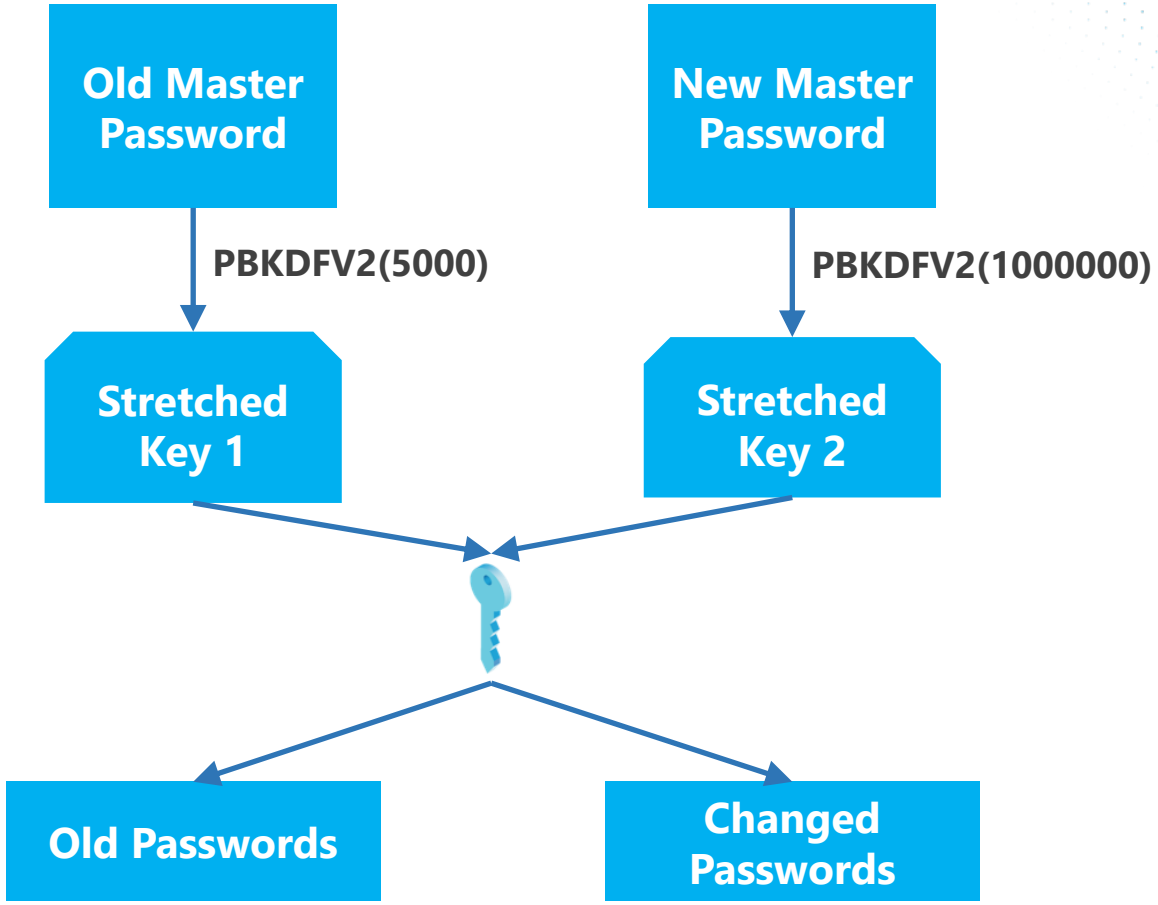
The response: all users to change their master passwords, strengthen password stretching and then change all passwords in vault



tresorit

Why changing passwords is not enough?

- At least one person will have a weak password, that is prone to brute force
- Even though the master passwords are changed, same keys will protect the new passwords
- Shared passwords within the organization can leak, even newly created ones
  - Removed employees
  - Broken accounts
  - Broken accounts of removed employees



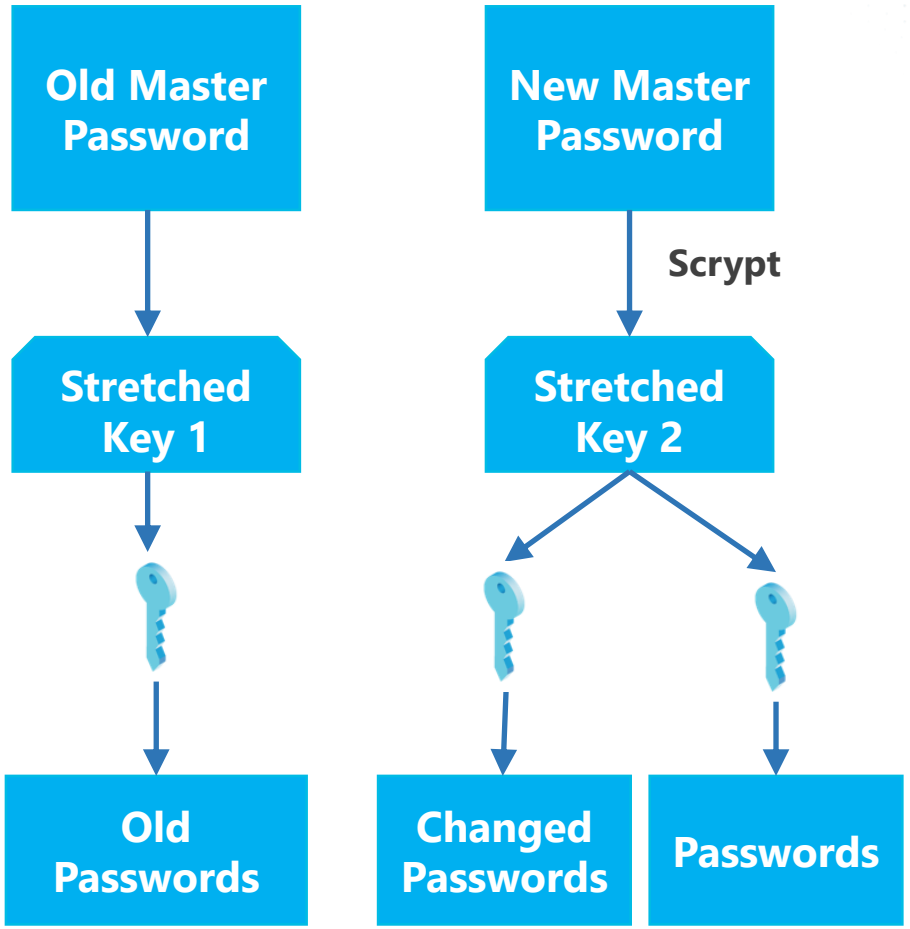
Encryption Engineering Remediations

Limit the number of breakable passwords

- Use Scrypt instead of PBKDFV2 as it needs a lot of memory and CPU power
- Always update parameters so that it takes 1/10th of a second to load on the user's machine
- This can make the difference of all <9 char passwords being broken or <12 char passwords being broken

Key Rotations

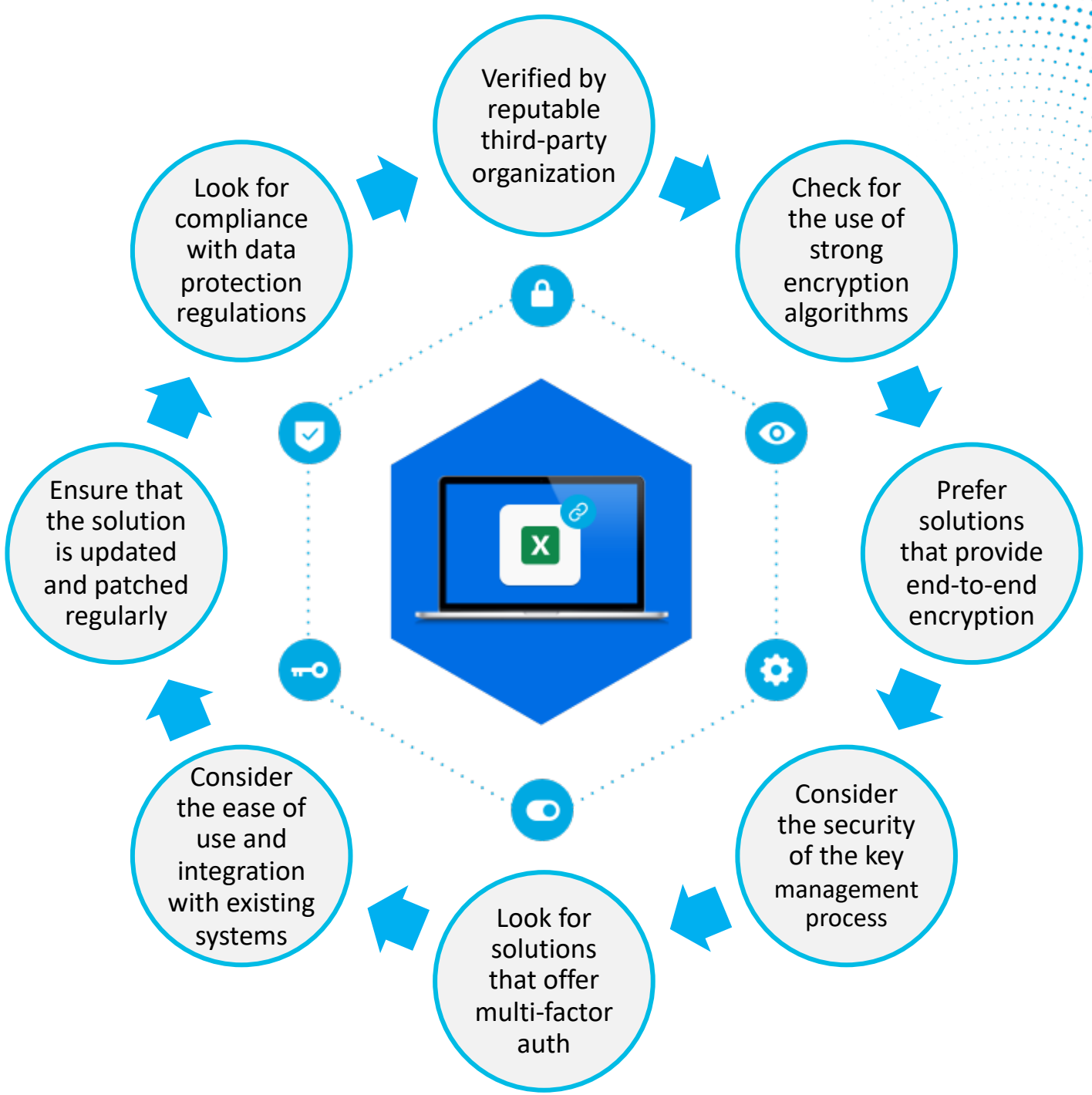
- Rotate a key if its parent key is rotated or changed
- Rotate the master key and all public private key pairs if the Password is changed
- Rotate a shared key if someone is removed from the group



Conclusion

What to take away from today

What to look for when evaluating encrypted solutions?



tresorit

Thank you

Peter Budai, CTO at Tresorit

itsa 365

HOME OF IT SECURITY

sales@tresorit.com

Tresorit @Tresorit