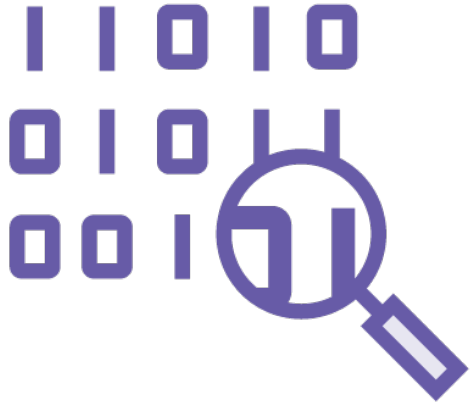
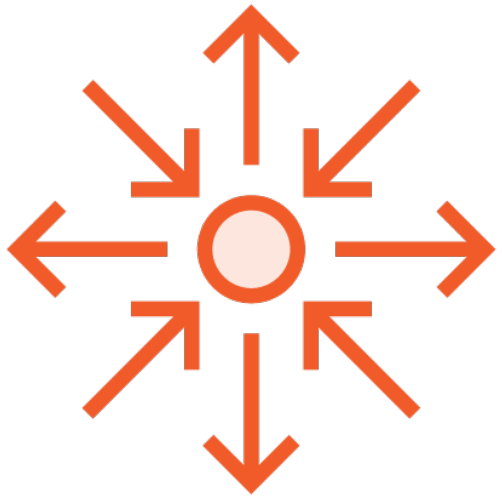
Protecting Data at Rest

Justin Boyer
PRINCIPAL CONSULTANT

@justinboyer4 www.justinboyerwriter.com

Threats to Data at Rest





Confidentiality

Only show the right data to the right people

Integrity

The data hasn't been changed

Availability

Is the data there when you need it?

What Is Symmetric Encryption?

One key

Same key used to encrypt and decrypt

Makes data unreadable

If you don't have the key, you can't read the data

Node.js Tools for Symmetric Encryption

Crypto.createCipheriv

Function provided to create symmetric ciphers.

Update and Final

Update to add data.
Final to encrypt data.

Keys Need Protection, Too

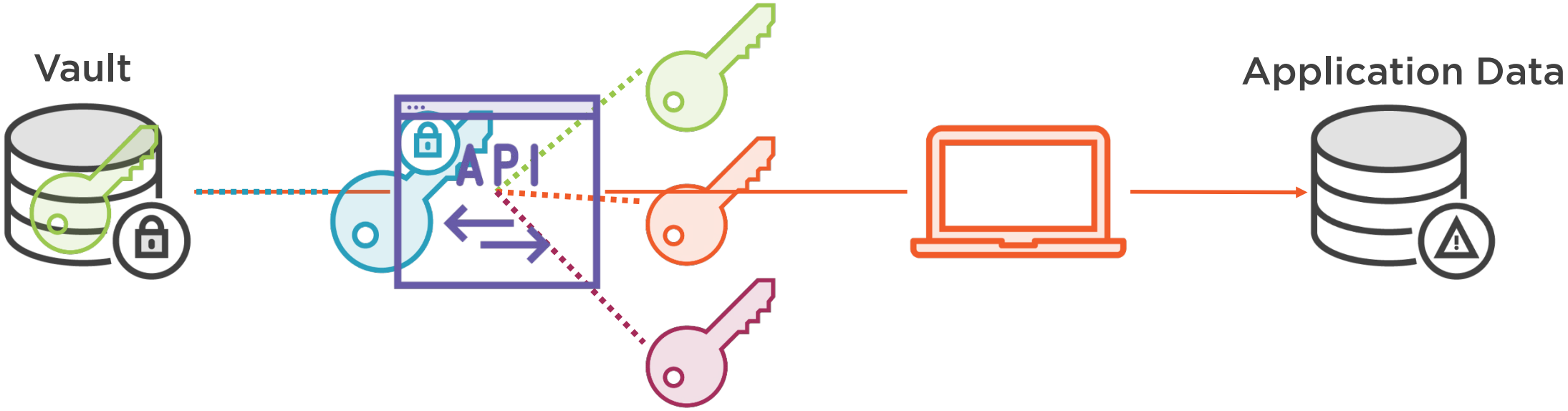
If an attacker finds the key, it's all over

Robust key management system (KMS)

Key management best practices

- Key store to protect keys
- Encryption keys encrypted by master key
- User requests key when data is needed
- Key store decrypts keys and sends to the user
- Keys can be rotated regularly for extra security

Introducing Vault



Summary

Sensitive data must be protected

Symmetric encryption is used to protect sensitive information

Node uses Crypto's createCipheriv function to create a cipher

Encryption keys are also sensitive and must be protected

Vault used as secure key store

- Master key
- Stores keys to other applications
- API for retrieval