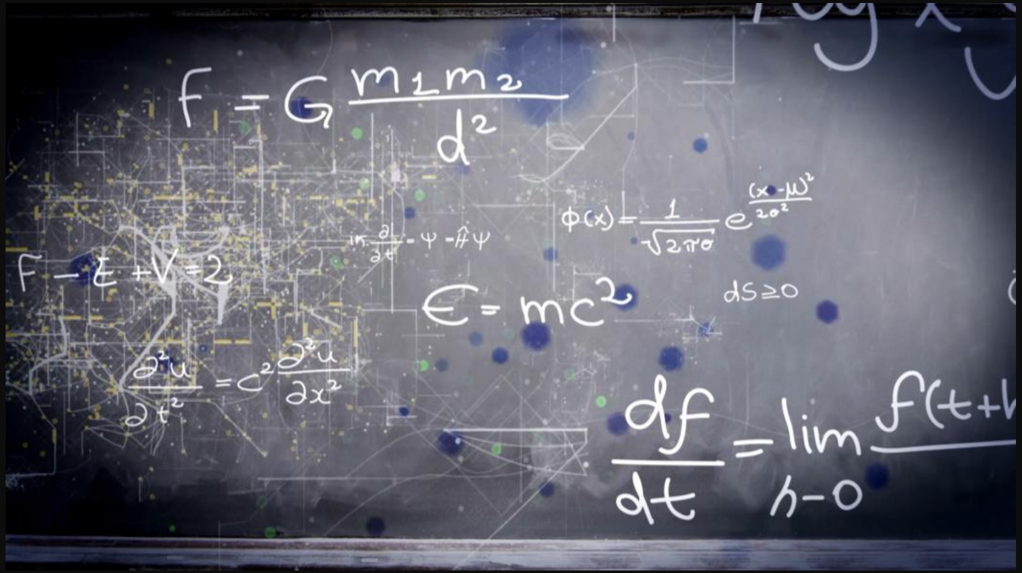
Use FileVault disk encryption for macOS with Intune



Beata Zalewa, 11th meeting of AppleCommunity.pl, 17.09.2024

About me

Security Architect

Consultant

Microsoft Certified Trainer

AI & Cybersecurity Practitioner

Developer

Freelancer

Azure

Azure @ ❤

aws

Google Cloud

1 Husband

1 Daughter

2 cats

2 dogs

Detective stories

Photography

zalnet BEATA ZALEWA

https://www.linkedin.com/in/beatazalewa/

beata@zalnet.pl

https://zalnet.pl/

Agenda

- Introduction
- Understanding FileVault
- Setting Up FileVault on macOS
- Integrating FileVault with Intune
- Challenges and Considerations
- Q&A Session

Let’s go !

„I broke people, not passwords”

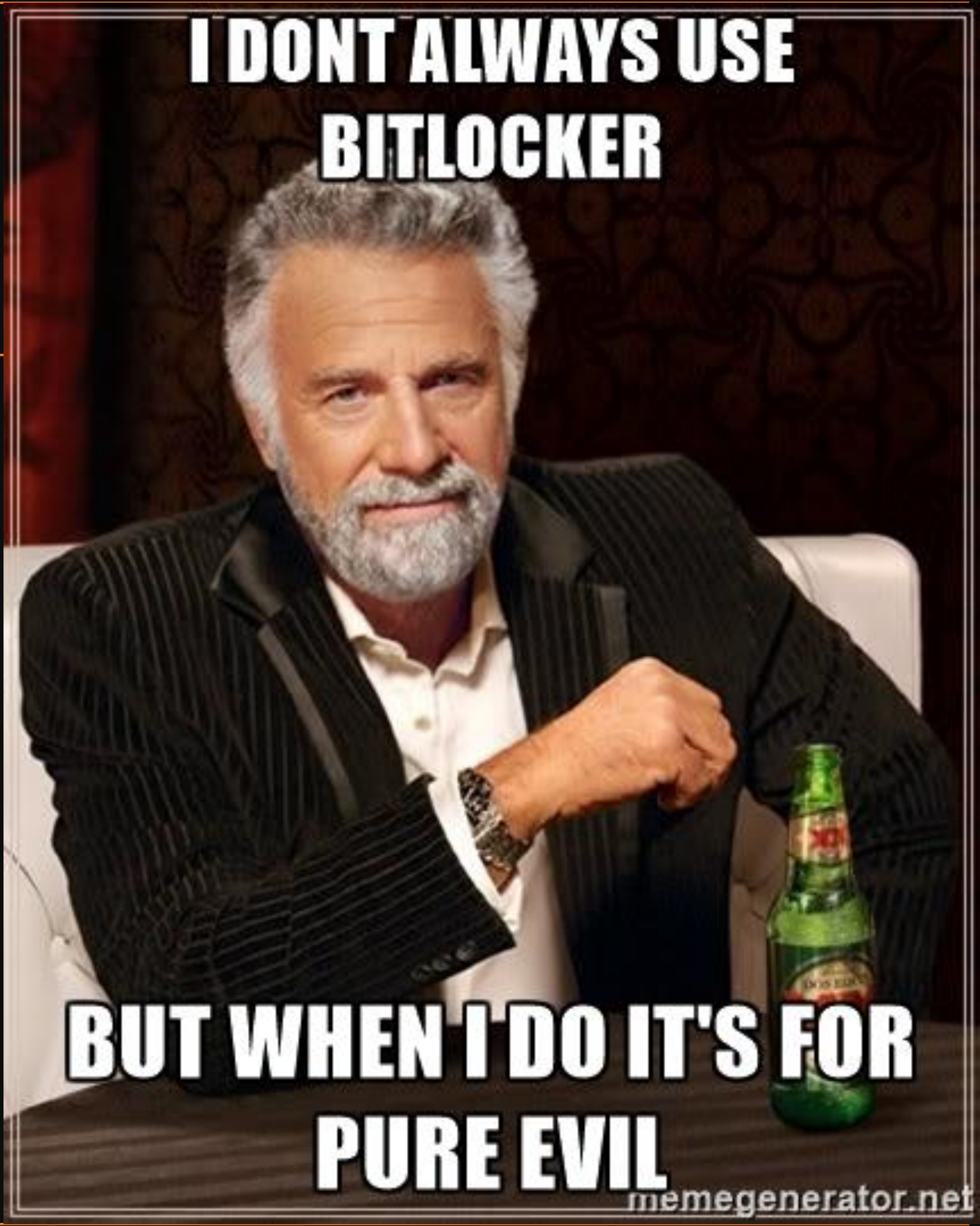
Kevin Mitnick

Introduction to FileVault

- FileVault is a built-in disk encryption program in macOS that protects all data stored on the startup disk.
- It uses the AES-XTS encryption algorithm with a 256-bit key, ensuring that sensitive information remains secure from unauthorized access.
- FileVault encrypts data in real-time, allowing users to work without interruptions while their data is being encrypted.

Importance of Disk Encryption

In today's digital landscape, protecting sensitive information is crucial, especially for organizations that handle confidential data.



Importance of Disk Encryption

- Disk encryption not only safeguards against data breaches but also ensures compliance with various regulatory requirements.
- FileVault provides a robust solution for securing Mac devices within an enterprise environment.

IT Guy: „i just need to delete C:\Windows\System32\drivers\CrowdStrike\C-00000291*.sys using safe mode
BitLocker: Enter the recovery key for this drive
IT Guy:

Data Security

FILEVAULT ENCRYPTS ALL DATA ON THE STARTUP DISK, INCLUDING THE OPERATING SYSTEM AND USER FILES.

ENCRYPTED DATA IS UNREADABLE WITHOUT THE CORRECT LOGIN CREDENTIALS OR RECOVERY KEY.

FILEVAULT PREVENTS UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION IN CASE OF THEFT OR LOSS.

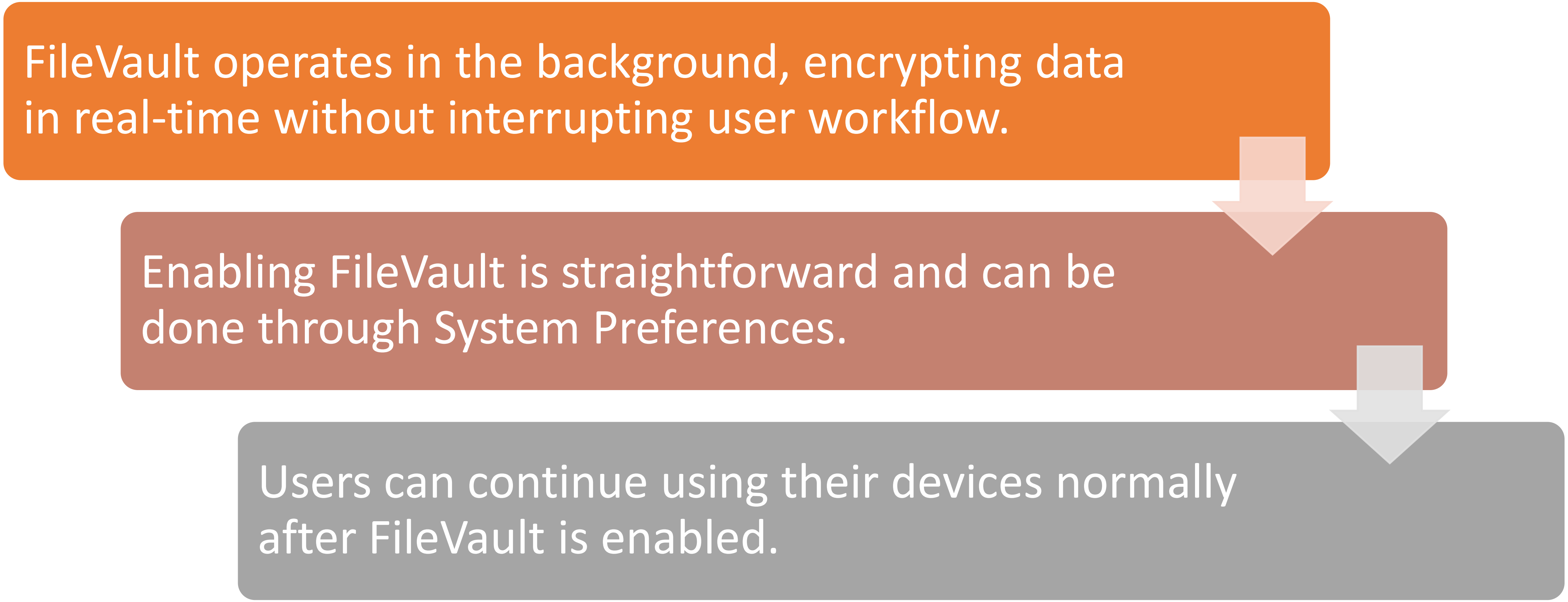
Compliance

FileVault helps organizations meet data protection regulations such as GDPR, HIPAA, and PCI-DSS.

Disk encryption is a key requirement for protecting sensitive data like customer information.

Using FileVault demonstrates a commitment to data security and privacy.

Ease of Use



FileVault operates in the background, encrypting data in real-time without interrupting user workflow.

Enabling FileVault is straightforward and can be done through System Preferences.

Users can continue using their devices normally after FileVault is enabled.

Performance Impact

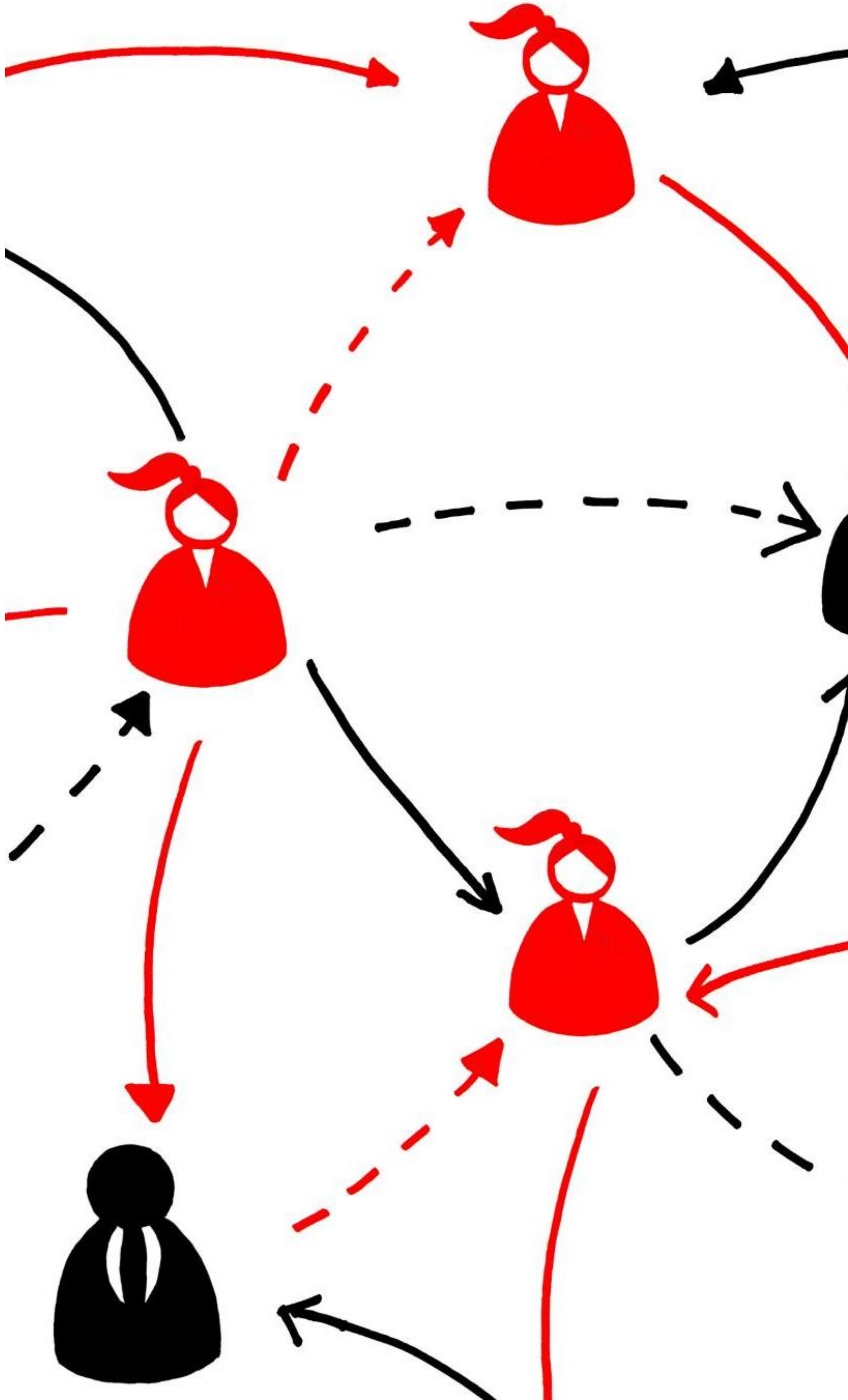
FileVault has minimal impact on system performance, especially on Macs with AES-NI support.

The I/O performance penalty is around 3% on average, according to studies.

FileVault's efficiency ensures that data security does not come at the cost of productivity.

Centralized Management

- FileVault can be managed centrally using MDM solutions like Intune or Jamf
- IT administrators can deploy FileVault settings, monitor compliance, and manage recovery keys
- Centralized management simplifies the deployment and maintenance of disk encryption



Recovery Key Management

- FileVault generates a recovery key that can be used to unlock encrypted disks if needed
- Recovery keys can be stored securely with Apple or an institutional keychain
- Proper management of recovery keys is crucial for data recovery in case of lost passwords

Compatibility

- FileVault is compatible with all Macs running macOS 10.7 (Lion) or later.
- It works seamlessly with the Apple File System (APFS) introduced in macOS High Sierra.
- FileVault integrates with hardware security features like the Apple T2 Security Chip.

Protecting Against Threats

- FileVault safeguards against physical attacks, such as removing the disk and connecting it to another device.
- It prevents malware from being planted on unused disk space, reducing the attack surface.
- FileVault is the last line of defense for protecting data if all other security measures fail.

Shared Device Support

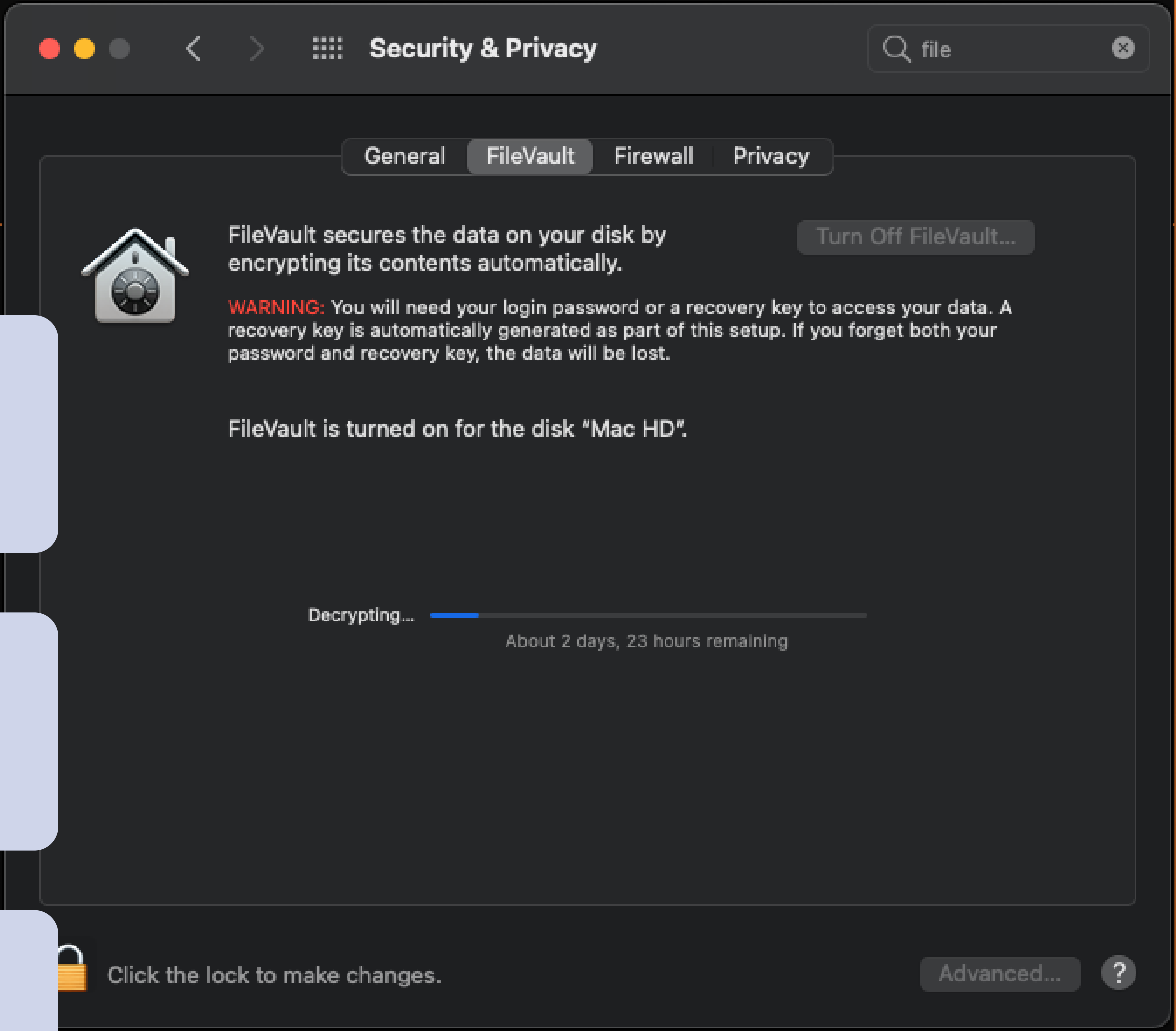
- FileVault supports multiple users on a single device, each with their own encryption keys.
- Users can log in and access their encrypted data after a FileVault-enabled user unlocks the disk.
- This feature is useful for devices shared among a group of trusted users.

Remote Wipe Capability

FileVault enables remote wiping of encrypted disks using the Find My Mac feature.

If a device is lost or stolen, IT administrators can remotely erase the disk to prevent data theft.

Remote wipe ensures that sensitive information remains secure even if a device falls into the wrong hands.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned on for the disk "Mac HD".

Decrypting...

About 2 days, 23 hours remaining

Click the lock to make changes.

Protecting Offline Data

FileVault encrypts data at rest, ensuring that it remains secure even when the device is powered off.

This safeguards against attacks targeting offline data, such as cold boot attacks or physical access to the disk.

FileVault provides comprehensive protection for data stored on Mac devices.

Protecting Data in Transit

- FileVault works in conjunction with other security features like FileProtection in macOS.
- FileProtection encrypts data in transit, ensuring that it remains secure while being transferred between applications or over the network.
- The combination of FileVault and FileProtection provides end-to-end data security.

Protecting Data in Use

- FileVault encrypts data in use, preventing unauthorized access to sensitive information while it is being processed by applications.
- This safeguards against attacks targeting running processes, such as memory dumps or code injection.
- FileVault's encryption of data in use ensures that sensitive information remains secure throughout its entire lifecycle.

Summary

- FileVault is a powerful and essential tool for protecting data on Mac devices.
- It provides comprehensive security, ease of use, and centralized management capabilities.
- Enabling FileVault is a crucial step in ensuring the privacy and integrity of sensitive information on macOS systems.

I am actively seeking new opportunities and exciting challenges.
If you would like to get in touch, please feel free to reach out through the following channels:

zalnet
BEATA ZALEWA

Email: beata@zalnet.pl

LinkedIn: https://www.linkedin.com/in/beatazalewa/

Blog: https://zalnet.pl/blog/

X: https://x.com/beatazalewa

GitHub: https://github.com/beatazalewa/Conferences/

Bibliography

https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control

https://learn.microsoft.com/en-us/mem/intune/protect/encrypt-devices-filevault

https://github.com/jamf/FileVault2_Scripts/blob/master/reissueKey.sh

https://github.com/microsoft/shell-intune-samples/blob/master/macOS/Config/FileVault/