

Forum:[Hack Forums](#)

Thread: [On-Demand Recovery and Decryption for Encrypted Drives](#)

Anthrax GTX - July 24, 2026, 1:54 am

Full-disk encryption is widely used to protect sensitive information stored on HDDs and SSDs. Two commonly used solutions are Microsoft BitLocker and McAfee Drive Encryption, which is now associated with the Trellix brand following the transition of McAfee Enterprise to Trellix.

These solutions encrypt most or all of a drive's contents. During startup, the system requests an authorized password, recovery key, smart card, or hardware-backed credential before allowing access to the operating system and stored data.

Full-disk encryption is especially common in business environments where organizations need to protect confidential information if a computer is lost, stolen, damaged, or accessed without authorization.

The Service Concept

The proposed service would provide secure, on-demand data recovery for supported BitLocker and Trellix/McAfee Drive Encryption configurations.

The platform could be implemented as a web application using ASP.NET Core, FastAPI, Spring Boot, or another suitable backend framework. An authorized user would upload an encrypted disk image or partition image together with the required recovery credentials.

The service would then:

Detect whether the uploaded data uses a supported BitLocker or Trellix/McAfee encryption format.

[list=2]

[*]Validate the recovery password, recovery key, or authorized enterprise credentials.

[/list]

[list=3]

[*]Decrypt the data inside an isolated processing environment.

[/list]

Make the successfully recovered files available for secure download.

Permanently remove uploaded and processed data according to a defined retention policy.

The service could charge customers based on the amount of data processed, such as a fixed price per gigabyte. Separate plans could be offered to individuals, IT support providers, data-recovery specialists, and enterprise customers.

Security and Privacy Requirements

Because customers may upload highly sensitive business or personal information, security must be a core part of the platform.

The service should include:

Encrypted data transfer.

Strong account authentication and multi-factor authentication.

- Isolated processing environments for each recovery job.
- Encryption of temporary files and storage.
- Clearly defined data-retention periods.
- Automatic deletion after processing.
- Detailed security and access logs.
- Independent security testing.
- Transparent privacy and data-processing policies.

Where technically possible, a local recovery agent could perform decryption directly on the customer's computer. This approach would reduce the need to upload complete disk images and could prevent passwords, recovery keys, and decrypted files from being exposed to the service provider.

Technical Limitations

Not every BitLocker or Trellix-encrypted drive can be recovered remotely.

Some computers protect their encryption keys using a Trusted Platform Module, or TPM. The TPM is designed to keep cryptographic information connected to a specific computer and its trusted system state. In some configurations, the required key cannot be exported or accessed by a remote service.

Recovery may still be possible when the authorized owner has access to one of the following:

- A BitLocker recovery key.
- A valid password or PIN.
- A Trellix/McAfee enterprise recovery key.
- An escrowed key managed by the organization.
- Another supported authentication method.

However, the platform should never promise that every encrypted disk can be decrypted.

Recovery may also fail because of:

- Missing or incorrect recovery credentials.
- TPM-bound encryption keys.
- Damaged drives.
- Corrupted encryption metadata.
- Unsupported BitLocker or Trellix configurations.
- Incomplete disk images.
- Hardware failure.

Legal and Ethical Safeguards

The platform should only process drives and data that users are legally authorized to access.

Before starting a recovery job, users should be required to confirm that they own the device or have documented authorization from the device or data owner.

The service should not attempt to break encryption, bypass authentication, extract protected TPM secrets, or access data without valid credentials.

- A clear disclaimer should explain that:
 - Successful recovery is not guaranteed.
 - Valid recovery credentials are normally required.

TPM-protected configurations may not be recoverable remotely.

Some Trellix/McAfee enterprise configurations may require assistance from the organization's system administrator.

Processing time depends on the amount of data, encryption configuration, upload speed, and condition of the storage device.

Customers must have legal authorization to access all submitted data.

The service is intended only for legitimate recovery, migration, and enterprise IT use.

A Practical Product Direction

Rather than advertising the platform as a universal disk-decryption service, it should be presented as a secure BitLocker and Trellix encrypted-drive recovery and migration platform.

Potential use cases include:

- Recovering files from an old BitLocker-encrypted computer.

- Recovering authorized business data from a Trellix-protected device.

- Migrating encrypted information to a replacement computer.

- Helping IT teams use stored enterprise recovery keys.

- Recovering data after an operating-system or boot failure.

- Supporting authorized employee offboarding.

- Extracting files from encrypted backups or disk images.

With strong privacy protections, clear technical limitations, and strict authorization requirements, this service could provide a practical solution for individuals and organizations that need legitimate access to data protected by BitLocker or Trellix/McAfee Drive Encryption.

MadScientist - July 24, 2026, 2:51 am

Thanks for the post ChatGPT