BitLocker

Quick Look

BitLocker is a full disk encryption feature integrated into Windows operating systems, designed to protect user data by encrypting entire drives.

It secures information on a device by preventing unauthorized access, especially in cases of device theft or loss.

BitLocker utilizes Trusted Platform Module (TPM) hardware to enhance security by verifying system integrity during startup. It supports encryption for system drives as well as fixed and removable drives, ensuring versatile protection.

BitLocker is user-friendly with seamless integration in Windows, providing transparent encryption without compromising system performance. It is recommended for civil society organizations seeking robust data security on Windows devices.

Features

BitLocker offers robust features to provide comprehensive full disk encryption for Windows users:

- **Encrypts entire system, fixed, and removable drives to protect data at rest**
- **Integrates with Trusted Platform Module (TPM) hardware for enhanced security**
- **Provides seamless, transparent encryption with minimal impact on system performance**
- **Supports multifactor authentication options like PINs and USB keys**

How to Use

How to use BitLocker on Windows:

- **Access BitLocker through the Control Panel or Windows Settings under "Device encryption" or "BitLocker Drive Encryption"**
- **Select the drive to encrypt and choose encryption options (e.g., full or used disk space only)**
- **Configure authentication methods such as TPM, PIN, or USB key**
- **Save or print the recovery key securely for emergency access**
- **Start the encryption process and monitor progress through the BitLocker interface until completion**