Encryption Tools

1. **AxCrypt**

Function: AxCrypt comes with a master key for administrative control, a password manager, automatic cloud encryption syncing, and secure file sharing in addition to using the superior AES-256 algorithm to protect your data.

Use Case: In addition to potential future features like letting others verify digital signatures, it can be utilized to let others securely share files with you without requiring password sharing.

Open Source/ Paid: Open Source

Pros	Cons
● Good for Secure Encryption of files ● Easy to use ● Works in the Cloud on all devices	● Password Manager does not work well

2. **NordLocker**

Function: Anyone can secure their files from hackers, snoopers, and advertisers by using this encryption tool

Use Case: Your files are encrypted before they leave your device. Data is only then uploaded, safely stored in the cloud, and synchronized across all of your devices. On a shared device, you can even have private access to your files.

Open Source/ Paid: Closed Source

Pros	Cons
● Extremely secure encryption standards ● Transparent privacy policy ● Easy to set up and install ● No restrictions for file size or type. ● Securely share files between devices and users. ● Intuitive interface	● No option for two-factor authentication. ● No secure deletion for original files. ● No support for Android, iOS, or Linux. ● No browser access. ● Doesn't accept PayPal in select countries.

3. Trend Micro Endpoint Encryption

Function: It encrypts data on a wide range of devices, such as PCs and Macs, laptops and desktops, USB drives, and other removable media.

Use Case: To stop illegal access to and use of personal data, this solution combines enterprise-wide full disk, file/folder, and removable media encryption.

Open Source/ Paid: Open Source

Pros	Cons
● Configuration Flexibility ● Customer Support ● Deployment Ease ● Ease of use	● Slow Performance

4. CryptoForge

Function: With the help of the program CryptoForge Files, files on any kind of drive, regardless of size, can be encrypted

Use Case: It allows you to protect files while in transit or for secure storage on your device, the cloud, remote computers, or external drives, for instance.

Open Source/ Paid: Paid

Pros	Cons
● Ease of use ● Encryption ● Storage Capacity	● Limited Customer Service

5. VeraCrypt

Function: The software can create a virtual encrypted disk that works just like a regular disk but within a file. It can also encrypt a partition or (in Windows) the entire storage device with pre-boot authentication.

Use Case: You can encrypt a whole partition or storage device with VeraCrypt, or you can create a virtual encrypted disk inside a file. It is intended to encrypt data on-the-fly, which means that without user input, it will automatically encrypt and decrypt data as it is loaded and saved.

Open Source/ Paid: Open Source

Pros	Cons
● Supports file encryption, partition/device encryption, and disk encryption ● Can be used to create encrypted volumes within files or partitions and encrypt entire drives	● No sharing options ● No support for cloud storage drag-and-drop functionality

6. BitLocker

Function: With BitLocker, users can encrypt all of the data on the drive that Windows is installed on, shielding it from loss or unwanted access.

Use Case: It helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled.

Open Source/ Paid: Paid

Pros	Cons
● Easy to set up and use ● Utilizes Windows Credentials ● Integrated with Active Directory ● Can encrypt system and data drives	● Limited to Windows OS ● Requires specific Windows editions ● Not compatible with Mac or Linux ● May require TPM for full functionality

7. Advanced Encryption Package

Function: It supports all program functions, including secure file deletion, PKI encryption and decryption, password-protected encryption and decryption, and PKI key generation.

Use Case: It enables you to choose from 17 encryption algorithms, including AES 256-bit, Blowfish, and GOST. It features an advanced password generator for creating strong passwords. Additionally, you can add a riddle to recover your password if forgotten.

Open Source/ Paid: Paid

Pros	Cons
● Offers 17 encryption algorithms ● Supports PKI ● Secure deletion ● Password generator ● Encrypts text to/from the	● Awkward, dated user interface ● Password generator doesn't work well ● Some features described in Help

clipboard - Command-line operation	system are absent

8. IBM Security Guardium

Function: It offers a straightforward, reliable method for stopping data leaks from files and databases, assisting in maintaining the accuracy of the data in the data center, and automating compliance controls.

Use Case: It is used for audit compliance, critical database activity monitoring, and anomaly detection - be it from unexpected processes, malfunctioning applications, scanners, or real malicious activity.

Open Source/ Paid: Open Source

Pros	Cons
- Vulnerability scans - Auditing - Compliance - Enhanced security information	- Cleanup the menu bar- way too many items. - Integration-Related Issues