Trellix

ENCRYPTION

THERE ARE TWO BASIC TYPES OF ENDPOINT ENCRYPTION:

1. Whole drive encryption renders a laptop, server, or other device unusable except for holders of the correct PIN. It protects the operating system and data on laptops and desktops by encrypting the entire drive except for the master boot record. This is left unencrypted so the machine can boot and locate the encryption driver to unlock the system. When a computer with an encrypted drive is lost, it's unlikely that anyone will be able to access the data on it. Whole drive encryption is automatic, so any content stored on the drive is automatically encrypted.

2. File, folder, and removable media (FFRM) encryption locks only designated files or folders. It encrypts selected content on local drives, network shares, or removable media devices. The encryption software deploys agents that encrypt files based on an organization's policies. File-based encryption supports both structured and unstructured data, so it can be applied to a database as well as documents and images.

TRELLIX DRIVE ENCRYPTION

features deliver encryption that protects data from unauthorized access, loss, and exposure using preboot authentication and a powerful encryption engine.

The Drive Encryption suite provides multiple layers of defense against data loss with integrated modules that address specific areas of risk.

DRIVE ENCRYPTION ALLOWS YOU TO:

- Enforce access control with pre-boot authentication
- Use certified encryption algorithms (FIPS, Common Criteria)
- Support mixed device environments, including solid-state drives
- Support Trusted Computing Group (TCG) Opal v1.0 self-encrypting drives

Drive Encryption provides protection for individual computers and roaming laptops with Basic Input Output System (BIOS) and Unified Extensible Firmware Interface (UEFI).

Policies determine how Drive Encryption software functions on the user's computer. The disk encryption process is transparent to the user and has little impact on the computer's performance.

The Drive Encryption features provide full disk encryption for Microsoft Windows laptops and desktop PCs and prevent the loss of sensitive data, especially from lost or stolen equipment.

- **Centralized management —** Drive Encryption integrates fully into Trellix ePO, leveraging the Trellix ePO infrastructure for automated security reporting, monitoring, deployment, and policy administration.
- **Transparent encryption —** Drive Encryption enables transparent encryption without hindering users or system performance.
- **Access control —** Drive Encryption enforces access control with Pre-Boot Authentication.
- **Recovery —** The recovery feature allows the user to perform emergency recovery when the system fails to reboot or its Pre-Boot File System (PBFS) is corrupt.
- **Support for self-encrypting drives —** Drive Encryption and Trellix ePO enable centralized management of self-encrypting drives that conform to the Opal standard from Trusted Computing Group (TCG), including locking and unlocking, reporting, recovery, policy enforcement, and user management.
- **Trusted Platform Module (TPM) —** Drive Encryption supports TPM 2.0 on Windows 8 and later UEFI systems to provide platform authentication without the need for Pre-Boot Authentication (PBA).

TRELLIX FILE AND REMOVABLE MEDIA PROTECTION (FRP)

Trellix FRP delivers policy-enforced, automatic, and transparent encryption of files and folders stored or shared on PCs, file servers, cloud storage services, emails, and removable media such as USB drives, CD/DVDs, and ISO files. Trellix FRP makes sure that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved. You can create and enforce central policies based on users and user groups for specific files and folders, without user interaction.

Trellix FRP allows you to:

Access encrypted data anywhere, without any additional software installation or local administrator rights on the device host

Encrypt or block writes to removable media at VDI workstations

Keep files and folders secure wherever they are saved, including local hard disks, file servers, removable media, and cloud storage such as Box, Dropbox, Google Drive, and Microsoft OneDrive

Typical Trellix FRP use cases include:

- Encrypting files such as spreadsheets and sensitive documents
- Allowing access to a specific folder on a shared network
- Encrypting files synchronized to cloud storage services
- Encrypting removable media or blocking the copying of non-encrypted files
- Sending self-extracting files in email attachments to partners or clients

KEY FEATURES

File and Removable Media Protection features provide encryption for data on network files and folders, removable media, USB portable storage devices, and cloud storage.

- **Centralized management —** Provides support for deploying and managing Trellix FRP using Trellix ePO software.
- **User Personal Key —** A unique encryption key is created for each user. You can reference "user personal key" generally in policies.
- **Delegated administration through Role Based Key Management —** Enables the logical separation of management between multiple administrators. This capability is critical for separation across business functions and subsidiaries.
- **Key management and policy assignment auditing —** Key management and policy assignment actions performed by Trellix ePO administrators are recorded in the Audit Log. This feature is critical to ensure compliance and prevent abuse by privileged administrators.
- **Protection of data on removable media —** Enables encryption of removable media and access to encrypted content, even on systems where Trellix FRP is not installed.
- **Protection of data (including auditing and reporting) for cloud storage services —** Enables encryption of sync folders on PCs for Dropbox, Box, Google Drive, and OneDrive. It also provides secure access to encrypted files on mobile devices using the Trellix Endpoint Assistant application.
- **Network encryption —** Enables secured sharing and collaboration on network shares.
- **User-initiated encryption of files and email attachments —** Allows users to create and attach password encrypted executable files that can be decrypted on systems where Trellix FRP is not installed.
- **USB removable media and CD/DVD/ISO event auditing and reporting —** Captures all user actions related to USB removable media and CD/DVD/ISO events. The auditing capability provides an effective feedback loop for administrators making policy decisions.
- **Use of Trellix Common Cryptographic Module (MCCM) —** Trellix FRP uses the MCCM user and kernel FIPS 140-2 cryptographic modules. You can install Trellix FRP in FIPS mode.