Trend Micro™

# ENDPOINT ENCRYPTION

Robust encryption and device control for desktops, laptops, and removable media

With the proliferation of data and devices in today's enterprises, it has become increasingly complex to protect confidential data, meet compliance mandates, and prevent costly data breaches. But an even bigger challenge is to implement comprehensive data protection at the endpoint without hindering employee productivity.

**Trend Micro™ Endpoint Encryption** encrypts data on a wide range of devices—laptops, desktops, tablets, CDs, DVDs, USB drives and any other removable media. This solution offers enterprise-wide full disk, file/folder, and removable media encryption, combined with granular port and device control to prevent unauthorized access and use of private information. A single management console allows you to manage both hardware and software encryption—enterprise-wide—for entire hard drives, specific files, folders, removable media, and storage devices. With the flexibility to seamlessly transition between multiple forms of encryption, Trend Micro Endpoint Encryption helps ensure that your data will continue to be protected as your mobile computing devices and organizational needs change.

## SOFTWARE & HARDWARE

### Protection Points

- Laptops, desktops
- Removable media: CD/DVD/USB
- Files and file volumes (folders)

### Threat Protection

- Privacy
- Data protection
- Regulatory compliance
- Securing Intellectual property

## ADVANTAGES

### Maximize Platform Coverage for Data & Device Encryption

Get comprehensive data protection on laptops, desktops, removable media, and mobile devices

- Encrypt private data with fully integrated full disk, file folder, USB, and removable media encryption
- Leverage flexible hardware and software-based encryption across mixed environments
- Implement full disk encryption with master boot record, OS, system files, swap/hibernation files
- Support self-encrypting drives from Seagate and emerging TCG OPAL and OPAL 2 SED standard
- Enable automatic and transparent encryption without performance degradation

### Lower TCO with Centralized Policy Administration & Key Management

Save more with an integrated solution that makes it easy to deploy, configure, and manage encryption

- Gain visibility and control over encryption, monitoring and protection of data
- Simplify operations with a unified data repository with single management server and console
- Automate policy enforcement with remediation of security events

### Simplify Remote Device Management

- Maintain compliance and protect your data without disrupting users in the event of a lost device or forgotten password
- Manage policies and protect data on PCs, laptops, tablets, USBs, CDs, DVDs
- Collect device-specific information such as device attributes, directory listing, and unique device IDs based on device name, MAC address, and CPU identifier
- Improve protection for remote devices with tools to remotely lock, reset, or "kill" lost or stolen devices

## KEY FEATURES

### Advanced Reporting & Auditing

- Automate enforcement of regulatory compliance with policy-based encryption
- Receive detailed auditing and reporting by individual, organizational unit, and device
- Assist compliance initiatives with audit trail for all administrative actions
- Demonstrate compliance on demand with real-time auditing

### Pre-Boot Multi-Factor Authentication

- Gain flexible authentication, including fixed password, CAC, PIV, Pin, and ColorCode®
- Enable policy update before authentication
- Trigger lockout feature in response to incorrect authentication attempts
- Configure actions on failed password attempt threshold
- Support multiple user and administrator accounts per device

### Administrative Tools & Active Directory Integration

- Provide remote one-time passwords across all endpoint client applications
- Leverage Active Directory and existing IT infrastructure for deployment and management
- Take the burden off IT staff by allowing users to change and reset passwords and accounts.
- Gain access to recovery console in Windows and preboot

## Key Benefits

- Helps ensure privacy and compliance enforcement with policy-based encryption
- Lowers TCO with simplified deployment, configuration, and management
- Provides comprehensive data security for laptops, desktops, removable media, and mobile devices
- Helps ensure robust security through certifications including FIPS 140-2 Level 2
- Maintains compliance and protect your data without disrupting users with remote management

## TREND MICRO ENDPOINT ENCRYPTION

| KEY FEATURES | Endpoint Encryption | Full Disk Encryption | File Encryption |
|---|---|---|---|
| Centralized policy and key management | ● | ● | ● |
| FIPS 140-2 encryption certification | Level 2 | Level 2 | Level 2 |
| AES 256-bit encryption | ● | ● | ● |
| File and folder encryption | ● | | ● |
| Removable media (CD/DVD/USB) encryption | ● | | ● |
| Granular port and device control | ● | | ● |
| Self-encrypting drive management | ● | ● | |
| Full desk encryption | ● | ● | |
| Network-aware pre-boot authentication | ● | ● | |
| Automatic Synchronization and Sharing | | ● | |

## Expand Data Security—for Complete End User Protection

Trend Micro Endpoint Encryption is an essential part of an enterprise data protection strategy. If you already have a Trend Micro threat protection suite, consider adding Trend Micro™ Enterprise Data Protection, which includes:

- Trend Micro™ Endpoint Encryption
- Trend Micro™ Email Encryption Gateway
- Trend Micro™ Mobile Security
- Trend Micro™ Integrated Data Loss Prevention

By combining threat and data protection in a flexible, centrally-managed suite, it lowers the cost and effort to deploy and manage while closing critical security gaps—for complete end user protection. Enterprise Data Protection is also included in our most comprehensive enterprise security suite: Trend Micro™ Enterprise Security and Data Protection.

## SYSTEM REQUIREMENTS

### Client Devices

- Microsoft® Windows® 8 (32/64-bit)
- Microsoft® Windows® 7 (32/64-bit)
- Microsoft Windows Vista™ (32/64-bit)
- Microsoft Windows XP (32bit)
- Microsoft® .NET Framework 2.0 SP1 or higher installed

### Management Server Console

- Microsoft® Windows Server® 2003
- Microsoft Windows Server 2013
- Microsoft® SQL Server® 2008
- Microsoft SQL Server 2005
- 32 and 64-bit Standard or Enterprise

### Management Server Hardware Requirements

- Pentium III class or above
- 256 MB memory
- 4 GB (IDE and SATA) drives
- Video card with XVESA compliance

### Endpoint Client Requirements

- Intel™ Core™ 2 or compatible processor
- Full Disk Encryption
  - 1 GB memory - 30 GB Disk Space
- File Encryption
  - 512 MB memory - 2 GB Disk Space