

Trend Micro™

ENDPOINT ENCRYPTION for Healthcare

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

Protect personal health information, take advantage of the safe harbor provision of the HITECH Act Enforcement Rule, and prevent costly data breaches—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. The 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, as well as a complete audit trail to demonstrate compliance.

A single management console allows you to manage both hardware and software encryption for entire hard drives, specific files, folders, removable media, and storage devices. Trend Micro Endpoint Encryption also offers a simple process for data recovery from failed drives, user self-service capabilities, ready-to-go compliance reports, and easy enterprise-wide deployment.

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

KEY ADVANTAGES

Comprehensive Data & Device Encryption

- Encrypts private data with fully integrated full disk, file folder, USB, and removable media encryption
- Offers flexible hardware and software-based encryption for mixed environments
- Provides full disk encryption: master boot record, OS, system files, swap/hibernation files
- Supports self-encrypting drives from Seagate and OPAL/OPAL 2 secure drive standard
- Enables automatic and transparent encryption without performance degradation

Centralized Policy Administration & Self-Contained Key Management

- Provides visibility and control over encryption, monitoring and protection of data
- Supports unified data repository with single management server and console
- Automates policy enforcement with remediation of security events

Device Management

- Manages policies and protects data on PCs, laptops, tablets, USBs, CDs, and DVDs
- Collects device-specific information such as device attributes, directory listing, and unique device IDs based on device name, MAC address, and CPU identifier
- Tools to remotely lock, reset, or “kill” devices

Advanced Reporting & Auditing

- Facilitates compliance with data protection mandates
- Provides detailed auditing and reporting by individual, organizational unit, and device
- Real-time auditing, with logging of all administrative actions and continuous time stamping, demonstrates compliance at any time

Pre-Boot Multi-Factor Authentication

- Offers flexible authentication, including fixed password, CAC, PIV, Pin, and ColorCode®
- Enables policy update before authentication
- Triggers lockout feature in response to incorrect authentication attempts
- Offers configurable action on failed password attempt threshold
- Supports multiple user and administrator accounts per device

A COMPREHENSIVE SOLUTION TO MEET YOUR ENCRYPTION NEEDS

Trend Micro Endpoint Encryption

offers full-functionality endpoint encryption and includes:

- **Centralized Management:** Central management server for policy administration, authentication, reporting
- **Software based full disk encryption:** Full disk encryption for PCs, laptops, notebooks, and tablets
- **Support for Self-Encrypting Drives (SED):** Central management and remote tools for self-encrypting drives, including OPAL and OPAL 2 compliant drives
- **File and removable device encryption with device control:** File and folder encryption and port and device control

Trend Micro Full Disk Encryption encrypts PCs and laptops and includes:

- **Centralized Management:** Central management server for policy administration, authentication, reporting
- **Software based full disk encryption:** Full disk encryption for PCs, laptops, notebooks, and tablets
- **Support for Self-Encrypting Drives (SED):** Central management and remote tools for self-encrypting drives, including OPAL and OPAL 2 compliant drives

Trend Micro Endpoint Encryption for Removable Media encrypts data on CDs, DVDs, USB drives, and includes:

- **Centralized Management:** Central management server for policy administration, authentication, reporting and remote tools
- **File and removable device encryption with device control:** File folder encryption and port and device control

Key Benefits

- **Privacy and Compliance:** automates and demonstrates regulatory compliance enforcement with policy-based encryption
- **Low TCO:** ensures easy deployment, configuration, and management for enterprise-wide deployment
- **Broad Platform Coverage:** helps secure data on laptops, desktops, removable media, and mobile devices
- **Validated Protection:** delivers robust security through certifications including FIPS 140-2 Level 2
- **Remote Device Management:** in the event a device is lost or a password is forgotten, remote management tools let you maintain compliance and protect your data without disrupting users with features such as remote kill, password reset, etc.

These new solutions extend our data protection and encryption portfolio.
 With Trend Micro you can now protect data no matter where it resides—from endpoints to the cloud.

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		●	

SYSTEM REQUIREMENTS
Client Devices <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Microsoft® Windows Server® 2003 • Microsoft Windows Server 2008 • Microsoft® SQL Server® 2008 • Microsoft SQL Server 2005 • 32 and 64-bit Standard or Enterprise
Management Server Hardware Requirements <ul style="list-style-type: none"> • Pentium III class or above • 256 MB memory • 4 GB (IDE and SATA) drives • Video card with XVESAs compliance
Endpoint Client Requirements <ul style="list-style-type: none"> • Intel™ Core™ 2 or compatible processor • Full Disk Encryption <ul style="list-style-type: none"> - 1 GB memory - 30 GB Disk Space • File Encryption <ul style="list-style-type: none"> - 512 MB memory - 2 GB Disk Space



Securing Your Journey to the Cloud

©2012 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro Control Manager, and Trend Micro Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS02_TMEE_forHealthcare_121221US]