TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro™

Endpoint Encryption

Robust data protection and device control for desktops, laptops, and removable media

Protect confidential data, meet compliance mandates, 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. 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

KEY ADVANTAGES

Comprehensive Data & Device Encryption

- Encrypts private data with fully integrated, full disk, file folder, USB, 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 emerging TCG Opal SED standard
- Enables automatic and transparent encryption without performance degradation

Centralized Policy Administration & 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 helps protect data on PCs, laptops, tablets, USBs, CDs, 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
- Assists compliance initiatives with audit trail for all administrative actions
- Real-time auditing can demonstrate compliance at any time

Pre-Boot Network-Aware 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

Administrative Tools & Active Directory Integration

- Provides remote one-time password
- Leverages Active Directory and existing IT infrastructure for deployment and management
- User self-serve capabilities take the burden off IT staff, allowing users to change and reset passwords and accounts

KEY BENEFITS

- **Privacy and Compliance:** Automates regulatory compliance enforcement with policy-based encryption
- **Low TCO:** Makes it easy to deploy, configure, and manage encryption as an integrated solution
- **Broad Platform Coverage:** Helps secure data on laptops, desktops, removable media, and mobile devices
- **Validated Protection:** Helps ensure robust security through certifications including FIPS 140-2 Level 2 and Common Criteria EAL4+
- **Manage Remote Devices:** 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.

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, and reporting
- **Software-based full disk encryption:** Full disk encryption for PCs, laptops, notebooks, tablets, and smartphones
- **Support for Self-Encrypting Drives (SED):** Central management and remote tools for self-encrypting drives, including OPAL compliant drives
- **File and removable device encryption with device control:** File 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, and reporting
- **Software-based full disk encryption:** Full disk encryption for PCs, laptops, notebooks, tablets, and smartphones
- **Support for Self-Encrypting Drives (SED):** Central management and remote tools for self-encrypting drives, including OPAL compliant drives

Trend Micro™ Endpoint Encryption for Removable Media encrypts data on CDs, DVDs, and USB drives. It 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

Trend Micro Secure USB is a fully encrypted USB hardware flash drive with embedded antivirus protection. It is centrally managed through the same encryption management console.

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

	Trend Micro			
Key Features	Endpoint Encryption	Full Disk Encryption	Endpoint Encryption for Removable Media	Secure USB Drive
Centralized policy and key management	✓	✓	✓	✓
FIPS 140-2 encryption certification	Level 2	Level 2	Level 2	Level 3
AES 256-bit encryption	✓	✓	✓	✓
File and folder encryption	✓		✓	
Removable media (CD/DVD/USB) encryption	✓		✓	
Granular port and device control	✓		✓	
Self-encrypting drive management	✓	✓		
Full disk encryption	✓	✓		
Network-aware pre-boot authentication	✓	✓		
Tamper-proof, hardened, encrypted USB flash drive with integrated antivirus protection–4GB				✓

SYSTEM REQUIREMENTS

Client Devices:

- Microsoft® Windows® 7
- Microsoft Windows Vista™
- Microsoft Windows XP
- Microsoft Windows Mobile 6
- 32 and 64-bit
- Microsoft .NET Framework 2.0 SP1 or higher installed

Management Server Console:

- 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:

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