Trend Micro™

ENDPOINT ENCRYPTION

Data protection with encryption for desktops, laptops, and removable media

The proliferation of data and devices in today's enterprises has increased the complexity of protecting confidential data, meeting compliance mandates, and preventing costly data breaches. These challenges are further amplified as more and more employees bring their own computing devices to work in the name of productivity. Ensuring that sensitive data is secured in the case of device loss has never been more difficult.

Trend Micro™ Endpoint Encryption encrypts data on a wide range of devices, such as PCs and Macs, laptops and desktops, USB drives, and other removable media. Available as a separate agent, this solution combines enterprise-wide full disk, file/folder, and removable media encryption to prevent unauthorized access and use of private information. A single, well-integrated management console allows you to manage your users holistically—using the same console for endpoint protection and other Trend Micro security products. Deploying the Endpoint Encryption agent helps ensure that your data will continue to be protected as your mobile computing devices and organizational needs change.

SOFTWARE AND HARDWARE

Protection Points

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

Threat Protection

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

ADVANTAGES

Maximize Platform Coverage for Data and Device Encryption

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

- Encrypt private data with fully integrated full disk, file folder, USB, and removable media encryption
- Support and leverage flexible hardware and software-based encryption across mixed environments
- Support self-encrypting TCG OPAL and OPAL 2 SED drives from Seagate, SanDisk®, and Intel®
- Simplify deployment and management with support for unified extensible firmware interface (UEFI), multiple physical drives, and pre-boot screen customization
- Enable automatic and transparent encryption without performance degradation

Lower Total Cost of Ownership (TCO) with Centralized Policy Administration and Transparent Key Management

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

- Manage the encryption policy alongside all endpoint security policies with integration to a common management console, Trend Micro™ Control Manager™
- Gain visibility and control over encryption, monitoring, and protection of data
- Automate policy enforcement with remediation of security events, without the burden of encryption key management
- Tight integration with Trend Micro™ Integrated Data Loss Prevention (iDLP) delivers content-based encryption for data at rest and in motion

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, Macs, laptops, desktops, USBs, and removable media
- Collect device-specific information, such as device attributes, directory listing, unique device IDs based on device name, MAC address, and central processing unit (CPU) identifier
- Improve protection for remote devices with tools to remotely lock, reset, or "kill" lost or stolen devices—even before a device boots using network-aware pre-boot authentication

KEY FEATURES

Advanced Reporting and Auditing

- Unify visibility and policy deployment with other Trend Micro products through integration with Control Manager
- Automate enforcement of regulatory compliance with policy-based encryption
- Receive detailed auditing and reporting by individual, organizational unit, and device
- Assist compliance initiatives with an audit trail for all administrative actions
- Demonstrate compliance on demand with real-time auditing

Administrative Tools and Active Directory Integration

- Provide remote one-time passwords across all endpoint client applications
- Manage users and groups from multiple active directory domains in a single console, simplifying the existing IT infrastructure for deployment and management
- Gain access to the recovery console in Microsoft® Windows® pre-boot

Pre-Boot Authentication

- Gain flexible authentication, including active directory integration, fixed password, and multi-factor authentication for government and defense customers
- Ensure that lost or stolen devices can be remotely wiped or locked before they can boot using network-aware (WiFi and ethernet)
- Enable policy updates prior to authentication
- Trigger the lockout feature in response to incorrect authentication attempts
- Configure actions on failed password attempt threshold
- Support multiple user and administrator accounts per device

Support for a Consumerized Environment

- Provide management and visibility for Microsoft® BitLocker®, this is especially useful for employee-owned devices where corporate data needs to be protected
- Provide visibility and management of Apple® FileVault® to enforce policies on Macs, and protect them in the case of loss or theft

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 the Federal Information Processing Standard (FIPS) Publication 140-2 certification
- Maintains compliance and protects your data without disrupting users with remote management

Endpoint Encryption is a critical component of our **Smart Protection Suites**. Our suites deliver even more data protection capabilities like data loss prevention (DLP) and device control, as well as our XGen™ security-optimized threat protection capabilities like file reputation, machine learning, behavioral analysis, exploit protection, application control, and intrusion prevention. Having additional Trend Micro solutions extends your protection from advanced attacks with endpoint investigation and detection. All of this modern threat security technology is made simple for your organization with central visibility, management, and reporting.

	NATIVE OPERATING SYSTEM (OS) ENCRYPTION MANAGEMENT		TREND MICRO ENDPOINT ENCRYPTION	
	Microsoft BitLocker Support*	Apple FileVault Encryption Support*	Trend Micro Full Disk Encryption	Trend Micro File Encryption
Centralized policy and key management	●	●	●	●
FIPS 140-2 certification	●	●	●	●
Advanced encryption standard (AES) 256-bit encryption	AES128/AES256**	AES128/AES256**	AES 128 AND 256	AES 256
File and folder encryption				●
Removable media (USB/CD/DVD) encryption				●
Self-encrypting drive management			●	
Full disk encryption	●	●	●	
Network-aware pre-boot authentication			●	

* Management for Bitlocker and FileVault is included with Trend Micro Endpoint Encryption (requires separate agent).
** Dependent on the OS version and machine model.

MINIMUM REQUIREMENTS
Policy Server
• Microsoft® Windows® Server 2008, 2008 R2, 2012, 2012 R2, 2016 (64-bit only) • Physical or virtual server with 2.2 GHz Xeon Quad Core or above; 1 available vCPU • 8 GB RAM • 120 GB hard disk space
Full Disk and File Encryption
• Microsoft® Windows® 7, 8, 8.1, 10 • Windows Embedded POSReady 7 • Intel® Core™ 2 Duo 2.0 GHz processor and above • 1 GB RAM • 30 GB hard disk, 20 percent free space
BitLocker
• Windows 7, 8, 8.1, 10 • Windows Embedded POSReady 7 • Intel Core 2 Duo 2.0 GHz processor and above • 1 GB RAM • TPM 1.2 or higher • 30 GB hard disk with 20 percent free space
FileVault
• macOS® 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14 • Intel Core 2 Duo 2.0 GHz processor and above • 2 GB RAM • 8 GB hard disk, 400 MB free space

TREND MICRO™

Securing Your Connected World

www.trendmicro.com