

Symantec™ Endpoint Encryption Device Control

Ensure authorized transfer of information to portable devices

Overview

Preventing the unauthorized transfer of sensitive data to portable media is a critical component of a complete enterprise endpoint data protection strategy.

Symantec™ Endpoint Encryption Device Control provides this protection, monitoring and restricting device usage and file transfer activity. When implemented with Symantec™ Endpoint Encryption Removable Storage Edition, the combination provides complete protection for data on PCs from the risks associated with portable devices and media.

While portable storage devices and media drive productivity in the workplace, they also pose a risk to critical enterprise data. Organizations need solutions that protect this data—by ensuring only the authorized connection of trusted devices and the authorized transfer of information—while preserving productivity. Achieving this balance requires a comprehensive solution that pushes the data protection perimeter down to the endpoint through effective policy-based controls and comprehensive activity monitoring.

Endpoint Encryption Device Control addresses this need by providing safeguards such as monitoring device usage and file transfer activity, controlling access to ports, devices and wireless networks, and restricting users' ability to copy protected classes of information. It delivers this protection coupled with the flexibility and best-in-class enterprise manageability that organizations need.

Endpoint Encryption Device Control maximizes use of existing infrastructure and training investments while minimizing management, implementation and deployment costs with the native Microsoft® Active Directory integration and support for Novell eDirectory™.

Key features

With Endpoint Encryption Device Control, administrators can:

- Ensure only approved devices are used on managed endpoints
- Mitigate unauthorized transfer of data
- Control the behavior of rogue devices
- Protect against device-borne malware
- Control wireless local area network (LAN) and remote network connections
- Detect if files are being copied off of your PCs, and prevent it

Feature overview

Endpoint Encryption Device Control makes it easy to assess exposure to data leakage from portable devices with comprehensive auditing, alerting, and reporting. Granular, policy based controls integrated with directory services then enable flexible, appropriate, restrictions that support legitimate business activity while protecting data.

Endpoint Encryption Device Control enables data protection management in combination with other Symantec Endpoint Encryption and PGP® encryption products for complete policy-based management.

Data protection controls and reporting are simple to administer, highly granular, and easy to apply, allowing organization to tailor the usage of connected devices and networks to balance security and productivity. Endpoint Encryption Device Control also provides protection against malware, viruses, keyloggers and other potentially malicious intrusions that could compromise data and systems with controls for autorun, U3 smart drives and self-executing code.

Data Sheet: Encryption

Symantec™ Endpoint Encryption Device Control

Features

Wireless connections

- Wi-Fi control includes MAC address, service set identifier (SSID) and security level of the network
- Prevents bridging by blocking wireless connections (Wi-Fi, Bluetooth, infrared, and/or modem) while connected to the wired corporate LAN

External ports

- Allow, disable, or restrict read and write access
- USB, FireWire, *Personal Computer Memory Card International Association* (PCMCIA), Secure Digital (SD), parallel, serial, and modem

Internal ports

- Logging and alert on change
- Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI), Advanced Technology Attachment (ATA), Serial Advanced Technology Attachment (SATA)

Storage control

- Restrict data transfer activity
- Control usage of USB flash drives, external hard drives, CD/DVD drives, floppy drives, and tape drives

Supported devices

- Control human interface devices, printers, personal digital assistants (PDAs), smartphones (including the Apple iPhone®), network adapters, smart cards, and content security devices
- Whitelist approved devices using the zero-footprint Device Control Auditor

File control

- Control file types allowed to be read/written to devices
- Approximately 200 built-in file types and 14 file categories

CD/DVD media white lists

- Allow use of only approved specific CDs and/or DVDs

Anti-hardware keylogger

- Blocks USB and PS/2 hardware keyloggers

U3 and autorun control

- Allows access to U3 smart drives only as regular USB drives
- Protects against automatically executed programs by blocking autorun

External database support

- Integrated with Microsoft® SQL Server 2005, 2008, and 2008 R2 (all editions supported, including Express Edition)

File shadowing

- Log and/or mirror a copy of all files written to removable media to a central file share

Directory services integrated administration and management

- Tightly integrated with Active Directory, enabling group policy object (GPO) based policy deployment
- Delegated, role-based administration with domain partitioning
- Detailed audit records to verify policy enforcement

Platform support

- Management server: Windows® Server 2003 (x86), Windows Server 2003 R2 (x86), Windows Server 2008 (x86 and x64), and Windows Server 2008 R2 (x86 and x64)
- Device control agent: Windows 7 (x86 and x64), Windows Server 2008 R2 (x86 and x64), Windows Server 2008 (x86 and x64), Windows Vista (x86), Windows Server 2003 R2 (x86), Windows Server 2003 (x86), Windows XP (x86)
- Device control auditor: Windows 7 (x86), Windows Server 2008 R2 (x86), Windows Server 2008 (x86), Windows Vista (x86), Windows Server 2003 R2 (x86), Windows Server 2003 (x86), Windows XP (x86)

Data Sheet: Encryption
Symantec™ Endpoint Encryption Device Control

More Information

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com