Trellix

DATA SHEET

Trellix Device Control

Prevent unauthorized use of removable storage devices

Overview

Key benefits

- **Unrivaled data protection.** Specify hardware and content-based filtering, monitoring, and blocking of confidential data on any removable storage device.
- **Comprehensive device management.** Enable safe use of removable media devices with no need to "block all" and hinder work productivity.
- **Trellix ePolicy Orchestrator (ePO) centralized management platform.** Centrally deploy and manage security policies to prevent confidential data loss via removable media.
- **Complete visibility.** Prove internal and regulatory compliance measures to auditors, board members, and other stakeholders.

USB drives, MP4 players, external hard drives, and other removable media, however useful, pose a real threat to your organization. Their small size and enormous storage capacity make it easy for confidential customer data and intellectual property to walk right out the front door and fall into the wrong hands—whether through loss or theft. How do you know who is storing what on which type of device? And even if the person or persons have permission to use the data, how can you be sure they're keeping it secure?

Trellix Device Control helps keep critical information from leaving your company through removable media like USB drives, iPods, Bluetooth devices, and recordable devices. It gives you the tools to monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go and even when they're not connected to the corporate network.

System requirements for Trellix ePO Server Management Console

Operating system

- Microsoft Windows Server 2012 or later

Hardware requirements

- CPU: 64-bit Intel compatible, 4 cores (minimum)
- RAM: 8 GB (minimum)
- Disk space: 20 GB (minimum)

System requirements for Trellix Device Control Endpoint

Operating systems

- Microsoft Windows XP Professional SP1 or higher
- Microsoft Windows 2000 SP4 or higher
- Mac OS X Lion, OS X Mountain Lion, and OS X Mavericks

Hardware requirements

- Disk space: 200 MB minimum
- RAM: 512 MB, 1 GB (recommended)
- Network connection: TCP/IP for remote access

Device Control management

Comprehensive device management helps control and block confidential data copied to removable storage devices. Parameters, such as product ID, vendor ID, serial number, device class, and device name, can be specified and categorized. And different policies like block or encrypt can be enforced based on the content loaded onto devices.

Managed policies include, but aren't limited to:

- Support for plug-and-play and removable storage devices; removable storage device definitions are supported on both Microsoft and Mac OS X
- Blocking removable storage devices or making them read-only
- Content-aware protection for removable storage devices
- Integration with Trellix File & Removable Media protection and digital rights management solutions to encrypt sensitive data being copied to removable storage
- File access protection for files that reside on removable storage devices
- The Citrix device rule that blocks access to thin-client device mapping—local drives, removable storage, printers, CDs/DVDs, clipboards, and more
- Non-system hard disks rule that blocks and monitors read-only files and provides notifications of user actions on fixed disk drives

Centralized management through Trellix ePO

Integration with the Trellix ePO platform offers real-time event monitoring and centralized policy and incident management. It allows for easy collection of critical-usage data, such as sender, recipient, time stamp, and data evidence. With a click of a button, Trellix ePO offers detailed reports to prove to auditors, senior management, and other stakeholders that internal and regulatory compliance measures are in place.

Some of the advantages include:

- Deploy and update Trellix Device Control agents via Trellix ePO
- Manage Device Control policies and incidents via Trellix ePO
- Integrate with Trellix ePO for event monitoring, centralized reporting, and auditing capabilities
- Set role-based access control (also known as separation of duties) by Trellix ePO for incident review
- Notify violators and/or managers automatically
- Access help desk interface

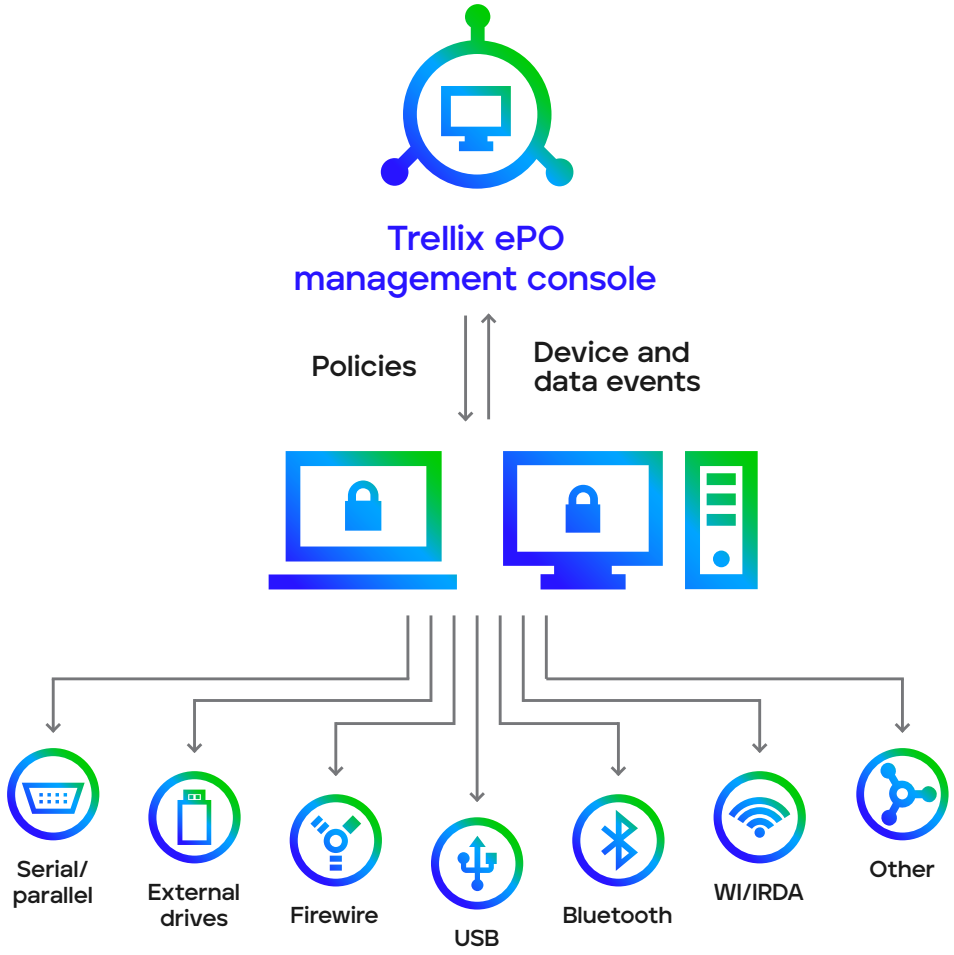

Figure 1. Trellix Device Control specifies which devices can be used and what data can be copied

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

Copyright © 2022 Musarubra US LLC 072022-01