

Information leakage prevention at the endpoint

Industry statistics consistently show that the most significant threat to the organization comes from within. With more than 70% of corporate data residing on endpoints, pure gateway security solutions and written security policies alone cannot mitigate the risks of information leakage. Growing numbers of removable storage devices, physical and wireless interfaces, and users with access to sensitive data have made information leakage via endpoints—both accidental and malicious—a real enterprise threat. It is simply too easy to connect a USB stick, digital camera or iPod to an endpoint at an organization and walk away with sensitive material. It is just as easy to use Wi-Fi, Bluetooth or a 3G modem to bridge classified internal networks to open external networks.

These are exactly the security risks that SafeGuard PortProtector is designed to manage. It controls every endpoint and every device over every interface and guarantees easy-to-use and flexible information leakage prevention. SafeGuard PortProtector monitors real-time traffic and applies customized, granular security policies for all types of interfaces and external storage devices:

- Physical interfaces: USB, FireWire, PCMCIA, Parallel, Serial, etc.
- Wireless interfaces: Wi-Fi, Bluetooth, Infrared (IrDA)
- External storage devices: removable media, CDs/DVDs, floppy drives, etc.

SafeGuard PortProtector detects and allows restrictions of device type, model or even specific serial number. SafeGuard PortProtector enables administrators to block all storage devices completely, permit read-only mode or encrypt all data on devices. In addition, administrators can monitor, block and/or log files that are written to or read from these devices.

In addition to SafeGuard PortProtector, the comprehensive SafeGuard PortAuditor helps administrators visualize who is connecting to corporate endpoints. With SafeGuard PortAuditor, administrators can distinguish between secure productivity enhancers, such as authentication tokens, and potential security threats, such as mass-storage MP3 players. Using this report data, IT management can enforce granular security policies that exactly meet the business needs.

Comprehensive information leakage prevention, easy administration and ease of use make SafeGuard PortProtector the solution of choice.

Key benefits

Enhanced security

- » Prevents data leakage and theft, enterprise penetration and introduction of malware
- » Comprehensive reporting of security threats with SafeGuard PortAuditor
- » Detects and restricts data transfer by device type, device model and unique serial number
- » Inspects files for their type and controls the transfer of unauthorized file types to and from external storage devices
- » Enables file shadowing and stores copied files securely in a central repository
- » Protects enterprise data in motion by encrypting data on external storage devices and tracking offline use
- » Blocks both USB and PS/2 hardware keyloggers

Easy to manage

- » Separate policies can be defined for any domain, group, computer or user
- » Easier administration enabled by integration with Microsoft Active Directory and Novell eDirectory
- » Role-based administration
- » Encrypted logs and alerts can be viewed in the management console for easy reporting and auditing, or integrated with third-party software for comprehensive analysis

Easy to use

- » Runs transparently in the background
- » No change in users' working habits and no end-user training is necessary

Key Features/Functionality

Security

- Granular control: detects and restricts data transfers by device type, device model, unique serial number, file type and actual content
- Data protection: protects corporate data in motion by encrypting data on external storage devices and tracking offline use
- File shadowing: administrator determines who and which files should be shadowed and if any action (logging, alerting) should be triggered
- Secure agent: silent deployment, redundant multi-tiered anti-tampering prevents security policy circumvention

Auditing on endpoint security status

- Comprehensive visibility of who is connecting what to corporate endpoints
- Visibility over all USB, PCMCIA, FireWire and Wi-Fi ports
- Granular record of all current and past device connections
- Simple and powerful reporting

System administration

- Policy flexibility: separate policies can be defined for any domain, group, computer or user; policies are easily associated with Microsoft Active Directory or Novell eDirectory organizational objects
- Hierarchical administration permission settings through role-based management
- Intuitive management: seamlessly integrates into Microsoft Active Directory, Novell eDirectory or other network management software
- Easy auditing and visibility: encrypted logs and alerts can be viewed in the Management Console or integrated with third-party software for comprehensive analysis or immediate notifications
- Advanced policy enforcement via independent, kernel-level, real-time analysis of low-level port traffic
- Automatic load balancing between all SafeGuard Servers – synchronized management servers acting as one

Easy to use

- No need for changes to users' familiar working habits
- High level of acceptance by users: no additional training required

Security Features

- Port control
- Device control
- Storage control
- Removable media encryption
- File type control
- Content inspection
- File name logging
- Tracking of offline usage of encrypted devices
- Granular Wi-Fi control
- CD/DVD media whitelists
- Block hybrid network bridging
- Internal port control
- Granular Wi-Fi control
- U3 and autorun control
- Blocking of USB and PS/2 hardware keyloggers
- Cisco NAC integration

System requirements

Hardware

- » PC with Intel Pentium or similar processor
- » Minimum 25MB free hard disk space

Operating systems

- » Microsoft Windows 2000
- » Microsoft Windows XP Professional (all service packs)
- » Microsoft Windows XP Tablet PC Edition
- » Microsoft Windows 2003 (all service packs)
- » Microsoft Windows Vista

Language Versions

- » English, German*, Japanese*
- » Messages shown to end users may be customized by the administrator in any language

Port Control Overview

Physical interfaces

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Parallel
- » Serial
- » Modem
- » Internal ports

Wireless interfaces

- » Wi-Fi
- » Bluetooth
- » Infrared (IrDA)

Storage devices

- » Removable storage devices
- » External hard drives
- » CD/DVD drives
- » Floppy drives
- » Tape drives

**planned*