

Control Removable Media

Data Leakage

Removable storage devices have now invaded business in multiple ways: USB keys, external hard drives, iPods, PDAs, telephones, cameras, and more. USB or FireWire connectivity can transfer massive amounts of information to these media within seconds. These transfers are silent and leave behind no trace for IT managers to see.

Malicious Codes

External storage devices are used today as a vehicle for data exchange - authorized or not - between workstations, both within a company or externally. These devices can contain malicious codes that may then infect any workstation they connect to. Despite the robustness of installed security infrastructures, only one security solution integrated at the workstation level can effectively combat this threat.

Hijacking of Infrastructures

Removable storage devices can lead to the hijacking of communication infrastructures. By using the company's broadband connection, malicious individuals can download massive amounts of music and pirated films and then transfer them outside of the organization using CDs, DVDs or removable hard drives.

Control Wireless Connections

Wireless Connections Modes

The increasing new ways to communicate on LAN (Wi-Fi) and PAN (Bluetooth) networks contribute to the rapid development of nomadism by allowing users to easily connect to the network from outside the company: at home, in a hotel or airport, or at a client or partner site. These varied methods of usage present many security issues: connecting to public and nonsecure hotspots, simultaneously connecting to the company LAN and to a neighboring wireless network, using the ad-hoc mode for Wi-Fi connections, connecting to rogue Bluetooth devices, and more.

Access Points Control

It is difficult to guarantee that the Wi-Fi access points established in the company are the only ones that staff members can access. Uncontrolled access points present a confidentiality problem for a PC connected as well as a problem for overall security: a PC connected to the LAN over the Ethernet network and to a Wi-Fi access point at the same time may expose the internal network to an external attack. Maintaining control over access points from the workstation is one of the key elements of a secure wireless network.

Confidentiality of Data Transfers

Today, there are several methods for encryption and authentication on Wi-Fi networks. If some of them are well secured (WPA, WPA2), others may be only slightly so or not at all (WEP, Open). By allowing employee connections to external Wi-Fi hotspots, your company incurs the risk of PCs connecting to access points that do not ensure secure data transfers.

StormShield Device Control System is a powerful and intelligent module that controls the use of removable data storage devices. With its advanced technology, StormShield DCS finely and dynamically distinguishes the type of media authorized to run on each workstation. By managing and controlling wireless connections, StormShield Device Control System secures each and every mobile PC in your organization. Whether connected or disconnected from the company, your information is always protected from any fraudulent use.

“Control of portable storage devices needs to be understood strategically as a form of communication channel similar in impact to Internet services.”

Source : Gartner - Portable Storage Device Control Products, Worldwide, 2006

Features

- Fine-grained access rights to removable storage devices
 - control of devices by type, model, and serial number
 - control of CD/DVD burning
 - control of read and write access at the file type level
- Encryption of data stored on removable devices
 - automatically enforced and transparent for the user
 - encryption can be applied to the whole device or just to newly-written files
 - centralized management of encryption keys and centralized recovery
- Control over classes of USB devices (storage, scanners, mouse, etc.)
 - storage devices can be blocked while letting the user access the USB port
- Flexible monitoring of operations on removable devices
 - audit of plugged and unplugged devices
 - monitoring of operations on files, including the volume of copied data
 - monitoring of operations blocked by StormShield
 - configurable logging levels
- Control of Wi-Fi connectivity
 - control of the ad-hoc mode
 - enforcement authentication and encryption modes (Open, WEP, WPA, WPA2...)
 - white listing of authorized access points using either SSID or MAC addresses
- Control of Bluetooth connectivity
- Dynamic wireless and device access policies (with the complementary module DPE)

Proactive, Complete and Unequaled Protection

The SkyRecon StormShield Security Suite is the first proactive, multi-layer, real-time defense system for network endpoints. StormShield addresses every aspect of endpoint protection, from intrusion prevention to

application and device control, to content encryption, all through a single agent. With StormShield, endpoint policies are enforced on each workstation, protecting them from hackers, malware or even users with admin rights, whether it is used inside or outside the corporate network. Moreover, these policies can be dynamically switched and changed depending on the connectivity context, the current user or the health assessment of the machine.

StormShield Security suite

- Behavioral Host-Intrusion Prevention System
- Stateful Firewall
- Anti-virus and Anti-spyware
- Application Control
- Dynamic Policy Enforcement
- Network Access Control
- Removable Device Control
- Wireless Security
- File, Folder and Full-disk Encryption
- Removable Device Encryption
- Endpoint Event Monitoring

“StormShield from SkyRecon is a powerful, unique solution which addresses all the key issues of endpoint security.”

Marc Jalabert,
Director of Business & Marketing Operations -
Microsoft France