

Device Control

Many peripheral devices possess dozens of gigabytes of portable storage space; large enough to store all the data found in a typical PC. A malicious user can swipe volumes of sensitive data with a few drag-and-drops. In a coffee shop or airline lounge, a laptop left unattended for even a few moments could be breached – without the user ever knowing it and without any audit trail for administrators to track.

StormShield's device control features give you control over all of your end users' peripherals, including removable USB devices, USB drives, iPods, CD/DVD burners, network cards, serial/parallel ports, and Firewire devices. Policies can be set to prevent copy/paste functions. The plug-and-play functionality of USB devices and the autorun features used for CDs and DVDs represent a serious gap in your security profile.

Device-related operations can be audited to help track activity related to each peripheral. For example, administrators can track which files or how many gigabytes of information have been loaded onto a particular peripheral, to assess whether inappropriate file transfers may be taking place.

StormShield gives you the ability to create policies for all I/O operations. You can outright block the devices, block them in certain settings, or block only certain features, such as CD burning, while allowing CDs to play.

You can also exert more fine-grained control, protecting I/O devices with passwords or allowing only devices that have been authenticated via model or serial number. Furthermore, since lost USB drives pose a serious threat, you can enforce the encryption of any data copied to those drives, helping to ensure compliance with HIPAA, SOX, GLBA, and other regulatory standards.

With I/O device control you can:

- Protect against IP theft, fraud and data loss
- Ensure that data remains on PC and cannot be removed without permission
- Create policies to block or restrict various I/O operations
- Password protect all peripheral operations
- Guarantee that removed data is encrypted – even if the device or media is lost or stolen, the data is still protected
- Protect against malware introduced via removable media
- Ensure compliance with HIPAA, SOX, GLBA, and other regulations