

INFORMATION SECURITY[®]

INFOSECURITYMAG.COM

Products

ENDPOINT SECURITY

Sanctuary Device Control 3.0.1

SecureWave, www.securewave.com

Price: Starts at \$45 per managed PC

It's your company's equipment and your company's intellectual property. If you don't want employees treating either as if it were their own, you need an effective way to enforce corporate policy. SecureWave's Sanctuary Device Control allows security managers to exercise granular control over user interactions with hardware devices, such as removable media, local hard drives, printers, network adapters and scanners.

Device Control's rich feature set allows you to create general or specific rules that control device usage. For example, you can dictate, "No users may access USB storage devices," and be as specific as "Richard Jones may only listen to music CDs on the weekend, when he is not connected to the corporate network."

The Sanctuary client is installed on each managed system and interacts with a Sanctuary Application Server, which can manage up to 5,000 clients. Sanctuary includes MSDE, although larger enterprises may choose SQL Server.

Device Control also allows administrators to control the export of data to removable media without enforcing a complete ban. Shadow-copying creates an image of all data copied to removable media for review; while this won't stop theft, it's certainly a deterrent and aids the investigation of data leaks. Managers can also place a byte limit on what users may export to removable devices, preventing large-scale data theft by flagging high-volume transfer attempts.

One of the most impressive new features is the Media Authorizer, which allows administrators to take control of removable media and grant specific permissions on a user-level basis. Device Control facilitates this by maintaining a cryptographic

infrastructure and encrypting all controlled media. It retrieves the encryption key and decrypts files to handle requests from authorized users. Administrators can set rules by general media classification (such as music CDs) or for specific pieces of media (such as a CD contain-



Sanctuary Device Control is a powerful tool to manage user interactions with hardware devices on managed systems.

Hotpick

ing proprietary software).

Installation is fairly straightforward. HTML documentation and wizard-based installers guide you through each stage of the process.

In this release, Device Control abandons its proprietary grouping of devices in favor of the standard Windows PnP organization, making it much easier to locate devices in the hierarchy. Another new feature is the establishment of online and offline profiles that enable you to allow different functionalities depending on whether a user is connected to your intranet or offline. For example, you can authorize wireless use when a user is traveling, but still prohibit it in the office to minimize the risk posed by rogue access points.

Device Control allows granular auditing of user and administrator activity. The Log Explorer tool monitors unsuccessful device access attempts, views application errors and controls access to shadow files. The Audit Logs Viewer allows a security manager or auditor to monitor the activity of subordinate administrators.

This latest version of Sanctuary Device Control adds functionality to an already strong product. While nothing can guarantee that data won't walk out the door, this makes it tough and gives you a strong tool for investigating violations. »

—MIKE CHAPPLE



SecureWave
Sanctuary[™]
Safeguarding Tomorrow

Test Notes

- ↑ Granular device control
- ↑ Valuable forensics tool
- ↑ Strong auditing/reporting