

IT SECURITY & DATA LEAK PREVENTION

Support Automation service

Manage all data loss prevention policies and remediate from a single console



A surprising amount of enterprise data leaks, whether from malicious origins or not, happens because of authorized users. Forty-nine percent of companies reported they experienced an internal security breach in the past year, according to Deloitte's 2006 Global Security Survey. Of those, 31 percent experienced a breach from a virus/worm incident, 28 percent through insider fraud and 18 percent by means of data leakage (19 percent experienced the breach through other means). It's also somewhat significant that fully 96 percent of respondents reported that they are "concerned about employee misconduct involving their information systems."

The HandsFree Networks IT security & Data Leak Prevention is part of the HandsFree Networks support automation solution designed to set and manage all data loss prevention policies and remediate from a single console to prevent confidential data loss due to employee usage of data at the endpoint.

A powerful and fully automated method for data protection

The HandsFree Networks IT Security and Data Leak Prevention automation service prevent loss of confidential data by securing desktops from targeted attacks and protect your mobile workforce with nonstop security that travels with the laptops. When this power software detects a sequence of events corresponding to an attempted intrusion, or to an action not allowed (e.g. accepting incoming traffic on selected ports), it automatically runs one of the intrusion protection DARTs neutralizing both known, and zero-day attacks.

Advantages

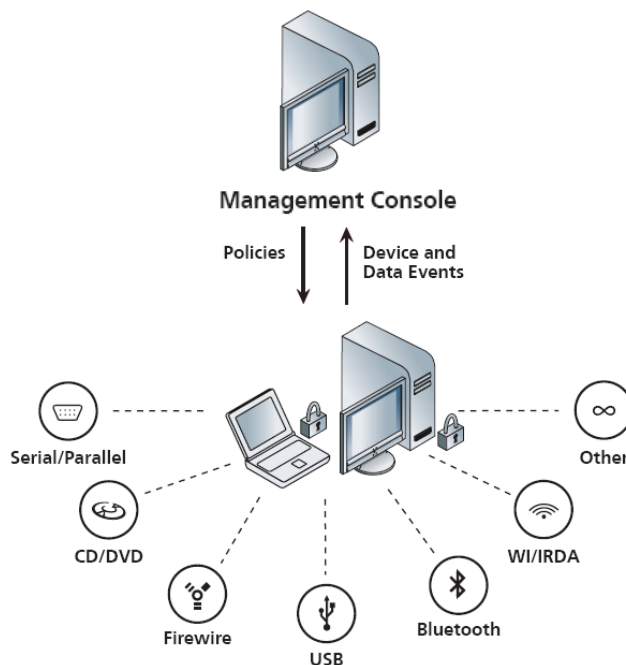
- From a single, centralized console, implement and enforce security policies that prevent confidential data from leaving the company's control and being lost or stolen.
- Support compliance with detailed user- and device-level logging; gather details such as device, time stamp, and data evidence for prompt and proper audits.

REGULATE THE USE OF REMOVABLE MEDIA ON YOUR NETWORK

HandsFree Networks helps you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control. Regulate how users copy data to USB drives, iPods, recordable CDs and DVDs, Bluetooth and infrared devices, COM and LPT ports, and more; block any copy attempts that violate your policies.

Advantages

- A Specify which devices can and can't be used by any Windows device parameter, including product ID, vendor ID, serial number and device name.



HandsFree Networks IT Security & Data leak prevention helps to manage and enforce data security policies for users even while off the corporate network.

- Specific file extension based download/upload filtering of confidential data on any storage device; ensure that employees continue to safely use allowed devices as part of their daily work activities

ENSURE ADHERENCE TO POLICY-BASED CONTROL

Handsfree Networks enables IT organization to Manage and enforce data security polices for users when on/off the corporate network. Protect against new or unknown zero-day threats by block users from downloading or even browsing to URLs known to contain malware or restrict any website from employee access.

Advantages

- Protects from adding key loggers, DLL injections (process hijacking), calling out over the network, or changing computer privileges an all other commonplace tactics.
- Block URLs and create a desired 'block list' and 'safe list' of all URLs for employee safe access.
- Blocks malicious intrusions on standard/non-standard ports.

REAL-TIME INFORMATION FILTERING AND CONTROL

HandsFree Networks leverages procedure based filtering unlike the filtering performed by virus scanning software, this procedures will filter out files regardless of whether they are known to carry a virus payload, or not.

Advantages

- Automated filtering of browser based file downloads via HTTP/HTTPS on a system-by-system basis.
- Automated filtering of e-mail attachments from POP mail or Web based e-mail messages.
- Filter and control sensitive information then index, query and analysis all content, and monitor file share access
- Enables IT staff to enforce rules and restrict the downloading and installation of unauthorized software.

ENABLES STRONG ACCESS CONTROL FOR ENDPOINTS

Protecting your data assets is tougher than ever. A wide range and enormous quantity of USB thumb drives and other media can connect to your endpoints daily. If keeping confidential data secure is keeping you up at night, rest easier with Port control. It provides strong access control, so that only authorized individuals can connect only approved devices to endpoints.

Advantages

- Prevent unauthorized access and use of removable devices- even when endpoints are not connected to the corporate network; identify and control all port.
- IP port and address control can be configured on a per adapter basis making it a powerful intrusion protection tool for mobile systems; ensures device-level network packet filtering.
- Logs any attempt by local/external source to open a TCP connection that is rejected by the local system because there is no process listening on that port; prevents port probing.
- View comprehensive reports about information- who sent it, where did it go, and how it was sent.

PROTECT YOUR BUSINESS FROM THE RISKS OF DATA LEAK

HandsFree Networks IT Security and Data Leak Prevention automation service prevents malicious applications from changing registry settings and tracks suspicious registry activities; reduces the burden of security management by enabling IT administrator to protect and cleanup Adware's and Spywares.

Advantages

- HandsFree Networks client software updates without direct access to the systems on an end-user network, minimizing the likelihood of unauthorized access to the system.
- Automatically monitor and prevent any attempt to change the contents of a system's registry, directories, or files making it a useful tool to alert you about attempts to replace or modify sensitive files and folders and, if desired, prevent them.

Technical Requirements

- No server infrastructure or VPN connections required
- Internet connection (56K or faster)
- Any version of Microsoft or non-Microsoft browsers
- Supported operating systems: Windows 98, ME, NT, 2000, XP, and Vista

Powered by HandsFree Networks Unique Framework

HandsFree Network IT Security and Data Leak Prevention is just one of HandsFree Networks support automation services which are powered by unique Next Generation Device Healthcare framework and its client-based engine architecture. Data communication between client and server happens in real-time via secure SSL transactions. Access to the DART configuration is controlled via MD5 hashing; Hashing is a one-way nonreversible function while encryption is a two-way reversible. This means that passwords are never stored anywhere, providing maximum security for access control.

For more information on the HandsFree Network IT Security & Data Leak Prevention, visit us at www.handSFreenetworks.com



HandsFree Networks Inc
1021 Main Campus Drive, Suite 300
Raleigh, NC 27606 (US)

HandsFree Networks Pvt. Ltd.,
4th Floor, Concorde Block, UB City,
Vittal Mallya Road, Bangalore-560001 (INDIA)

www.handSFreenetworks.com