

Device Control Auditor

In today's regulatory and security environment, data breaches can result in substantial costs for organizations—not only in legal liability, customer service and remediation costs but also in damage to image and brand equity. This makes it crucial to know your vulnerability to data loss and data leakage via removable media. Device Control Auditor enables immediate assessments of these risks by quickly and easily determining what is connecting to your PC laptops and desktops.

GuardianEdge Device Control Auditor gives organizations immediate, actionable information about the devices and WiFi networks to which PCs are connecting. This visibility enables IT staff to identify both imminent and potential threats to private, sensitive and legally protected data.

Eliminating the need for client software on PC endpoints makes it fast and easy to implement GuardianEdge Device Control Auditor software. This agent-less architecture also means audits are very light in terms of resource consumption and have no adverse affects on network or client PC performance.

Intuitive and easy to use, the GuardianEdge solution runs audits in just minutes, giving organizations an immediate, highly detailed view into activities at their endpoints. Administrators can also choose to exclude specific devices that represent no threat, such as keyboards and mice. Simple-to-generate report summaries provide detailed data that can be easily exported to XML spreadsheets for further analysis. The solution also streamlines the selection of target systems through full integration with Microsoft® Active Directory™. IT staff can apply targeting against complete domains, OUs, groups, individual systems or against a name or IP address range.

Key features

- Fast, comprehensive reporting of all external media device and WiFi network connections
- Agentless operation
- Precise, current and historical device, network and port connection information
- Integration with GuardianEdge Device Control makes it easy to create white/black lists

Audit Summary Report	Total	Connected
Total Computers	233	
Accessed Computers	92	
Successfully Audited	92	
Protected by GuardianEdge	8	
USB Devices	864	93
PCI/PCMCIA Devices	401	0
FireWire Devices	0	0
Internal Storage Devices	0	0
WiFi Networks	55	
Storage Devices	608	15
Communications Adapters	0	0

Quickly and Easily Identify Critical Risks



Quickly and easily create audits and receive immediate results – no client software deployment required



Reports are easily viewable with actionable information highlighted, or may be exported to spreadsheet compatible format for further analysis



Easily limit or expand the scope of an audit to target specific devices and quickly assess specific, critical exposures

Technical Information

With its lightweight, agentless architecture, GuardianEdge Device Control Auditor delivers the visibility required to identify and effectively manage vulnerability to data loss and data leakage from removable storage media on PCs.

Supported Ports

- USB, FireWire, PCMCIA, PCI, internal storage, WiFi

Supported Devices

- Human interface devices
- Printing devices
- PDAs – Windows Mobile/PocketPC/BlackBerry
- Mobile phones
- Network adapters
- Imaging devices
- Audio/Video devices
- Smart cards
- Content security devices
- Other

Storage Device Support

- Removable media
- Floppy and CD/DVD drives
- Tape devices
- Hard disks
- iPods and MP3 players

WiFi Networks

- Network (infrastructure)
- Peer to Peer (ad hoc)

Client Connection Protocols and Privileges

- Active Directory domain controller membership
- Local administrative privileges on the endpoint
- Setup API (does not support Vista)
 - Remote Registry service running
 - File and print sharing enabled
 - Port 445 or 139 open in PC firewall
- WMI
 - WMI service running
 - WMI communications port open (135+WMI protocol selected port)

Additional Features

- Easily export lists for Device Control white list creation
- Command line operation

Computer Audit Selections

- Organizational units (Active Directory) – all or specific
- Computer name
- IP range

Client OS Support (audited computers)

- Microsoft Windows™ XP SP1 / SP2, Windows 2000, Windows Server 2003, Windows Vista

Device Control Auditor Host OS Support

- Microsoft Windows™ XP SP1 / SP2, Windows 2000, Windows Server 2003

Corporate Headquarters
475 Brannan St., Suite 400
San Francisco, California
94107-5421

t. +1.800.440.0419

t. +1.415.683.2200

f. +1.415.683.2349

www.GuardianEdge.com

GuardianEdge is a trademark of GuardianEdge Technologies Inc.
All other products and services mentioned are the trademarks of their respective companies.