

# Device Control

Preventing the unauthorized transfer of sensitive data to portable media is a critical component of a complete enterprise endpoint data protection strategy. GuardianEdge Device Control provides this protection, monitoring and restricting device usage and file transfer activity. When implemented with GuardianEdge Removable Storage Encryption, the combination provides complete protection for enterprise data on PCs from the risks of portable devices and media.

While portable storage devices and media drive productivity in the workplace they also pose a risk to critical enterprise data. Organizations need solutions that protect this mobile data—by ensuring only the authorized connection of devices and only the authorized transfer of information—while preserving productivity. Achieving this balance requires a comprehensive solution that pushes the data protection perimeter down to the endpoint through effective policy-based controls and comprehensive activity monitoring.

GuardianEdge Device Control addresses this need by providing safeguards such as monitoring device usage and file transfer activity, controlling access to ports, devices and wireless networks, and restricting users' ability to copy protected classes of information. It delivers this protection coupled with the flexibility and best-in-class enterprise manageability that organizations need.

As a key component of the GuardianEdge Data Protection Platform, GuardianEdge Device Control maximizes use of existing infrastructure and training investments while minimizing management, implementation and deployment costs with the industry's only native Microsoft Active Directory® integration, support for Novell eDirectory, and a single common management console that integrates with other GuardianEdge endpoint data protection products.

## Key features

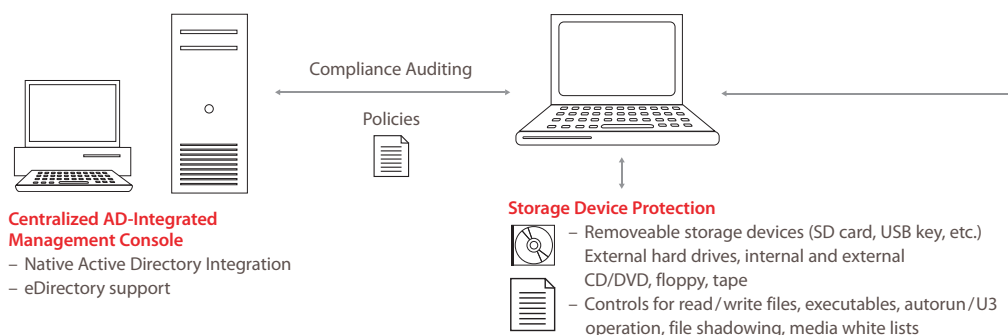
With GuardianEdge Device Control:

- Restrict the devices that connect to your PCs
- Know if unauthorized files are being copied off of your PCs, and prevent it

Combined with GuardianEdge Removable Storage Encryption:

- Safely and securely share data via portable storage devices
- Protect authorized data transferred to portable media when employees take work home
- Securely distributed sensitive documents attached to emails

### Ensure authorized transfer of sensitive information to portable devices



### Ports, Connections and Devices

Granular policy-based control, logging and alerts

- Wireless interfaces: Wifi, Bluetooth, IrDA
- External ports: USB, FireWire, PCMCIA, Secure Digital (SD), Parallel, Serial, Modem
- Internal ports: Log and alert on-IDE, SCSI, ATA, SATA, PCI and PCIX



– All Devices Connected to those Ports

# Feature Overview

GuardianEdge Device Control makes it easy to assess exposure to data leakage from portable devices with comprehensive auditing, alerting and reporting. Granular, policy based controls integrated with directory services then enable flexible, appropriate, restrictions that support legitimate business activity while protecting data.

GuardianEdge Device Control is offered in two tiers. The Platform Edition offers seamless integration with the GuardianEdge Data Protection Platform. This comprehensive solution enables data protection management in combination with GuardianEdge Hard Disk Encryption and Removable Storage Encryption for complete policy-based management using Microsoft Active Directory. Alternately, the Standard Edition allows independent control of policies using Novell eDirectory.

Data protection controls and reporting are simple to administer, highly granular, and easy to apply, allowing organization to tailor the usage of connected devices and networks to balance security and productivity. GuardianEdge Device Control also provides protection against malware, viruses, keyloggers and other potentially malicious intrusions that could compromise data and systems with controls for autorun, U3 devices and self-executing code.

## Features

### Standard and Platform Editions

- **Platform Edition**—Integrates with the GuardianEdge suite of data protection products using Active Directory-based policy services and management
- **Standard Edition**—Supports Novell eDirectory or the GuardianEdge provided Policy Server for synchronization, policy deployment, auditing, etc.

### Wireless Connections

- WiFi, Bluetooth, IrDA
- WiFi control includes MAC address, SSID and security level of the network
- Prevents bridging by blocking wireless connections (WiFi, Bluetooth, IrDA, and/or modem) while connected to the wired corporate LAN

### External Ports

- Allow, disable, or restrict read and write access
- USB, FireWire, PCMCIA, Secure Digital (SD), parallel, serial, modem

### Internal Ports

- Logging and Alert on change
- IDE, SCSI, ATA, SATA, PCI and PCIX

### Storage Control

- Restrict data transfer activity
- Removable storage devices, external hard drives, CD/DVD, floppy, tape

### Supported Devices

- All devices connected to ports, by type, serial number, manufacturer, etc.
- Whitelist approved devices

### File Control

- Control file types allowed to be read/written to devices
- Approximately 200 builtin file types and 14 file categories

### CD/DVD Media White Lists

- Allow use or viewing of only approved specific CDs and/or DVDs

### Anti-Hardware Keylogger

- Blocks USB and PS/2 hardware keyloggers

### U3 and Autorun Control

- Allows access to U3 drives only as regular USB drives
- Protects against autolaunch programs by blocking autorun

### Internal/External Database Support

- Supports either the internal, provided MySQL database, or an external SQL Server database

### Platform Edition—File Shadowing

- Log and/or mirror a copy of all files written to removable media to a central file share

### Platform Edition—Active Directory Integrated Administration and Management

- Tightly integrated with Active Directory, enabling GPObased policy deployment
- Role-based policy administration
- Detailed audit records to verify policy enforcement

### Platform Edition—GuardianEdge Removable Storage Integration

- Closely integrated for complete protection of data on removable storage devices using encryption

### OS Support

- Microsoft Windows™ XP SP2 and SP3, Windows 2000 Professional SP4, Windows XP Tablet PC Edition 2005, Windows Server 2003 SP1 and SP2, Windows Vista Business, Enterprise, and Ultimate Editions

Corporate Headquarters t. +1.800.440.0419  
475 Brannan St., Suite 400 t. +1.415.683.2200  
San Francisco, California f. +1.415.683.2349  
94107-5421

[www.GuardianEdge.com](http://www.GuardianEdge.com)

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