Controlguard: Port and Device Control for the enterprise

Controlguard is an enterprise-level **port and device control** solution. Prevent data leaks through centralized control of I/O devices and removable media.

ATROG's Controlguard gives you complete control over how I/O devices and removable media are used throughout your organization. Controlguard monitors and enforces device control and data transfer policies on all computers on the network to provide active protection against security breaches and data loss. Device control policies can be defined to block a wide range of media and devices, restrict Print Screen options, limit access to specific files or file content, and limit file transfer permissions. A centralized management console provides real-time updates about device access and data movement, highlighting any potential security issues. Powerful reporting tools provide detailed reports for regulatory compliance and auditing.

Benefits

Active device control policy enforcement on every computer

Controlguard detects and blocks any attempt by users to access unauthorized I/O devices, or to copy unauthorized or unencrypted files. The agent installed on every desktop, server and laptop in the network implements the device control policy that has been set for the computer and for the user who is logged in. All access to I/O devices is actively monitored and controlled even when the computer is being used offline, or is connected to the network via VPN.

Control access to sensitive files and data

Controlguard enables administrators to block or enable user access to sensitive files or file content, and to set a limit on the file size that particular users are allowed to transfer. Controlguard integrates with Cryptzone's Secured eUSB to provide maximum USB security eg. preventing unencrypted files from being copied to removable media.

Flexibility to meet users' needs

A user may need temporary permission to access an otherwise unauthorized device. One-time access can be granted to users, even when they are working offline, by using built-in one-time-password technology. A request for temporary permission is initiated by the user at the workstation and authenticated using a one-time password generated from the management console by the administrator.

Full reporting for compliance and auditing

All authorized and unauthorized attempts to access I/O devices are logged and stored centrally providing a full audit trail if required. Reports can be customized to allow administrators to easily monitor and analyze the network security status and user activity. Different options are available for formatting reports to allow easy integration with business management systems.

Blocks all access unless authorized

Each computer on the network defaults to blocking all access to i/o devices and removable media until a user logs in. When a user logs into the network, the agent installed on the computer enforces the device and port control policies for that computer and for that user. Administrators can check the combined permissions in force on a particular computer to ensure device control policies will prevent any data breach.

Precise control over approved media and devices

Controlguard dynamically monitors and locks removable media (eg. USB flash drives, floppy disks, CD-ROM, DVD), i/o devices (Bluetooth, Wireless, Smartphones, Palm, Windows Mobile, card readers, imaging devices, modems, cameras, printers, etc.), and ports including 1394/Firewire, PCMCIA, infrared, serial (COM) and parallel (LPT). Administrators can configure both whitelists and blacklists of specific devices, for example by device type, device model, or serial number.

Device control policies support business needs

Controlguard can help managers to research current usage of I/O devices across the organization as a baseline for developing device control policies that support business requirements. Administrators can view all the permissions that are to be applied for a particular user working at a particular computer, thereby ensuring that security policies have been defined correctly. End user prompts can be used to inform and educate users about device control policies and to reduce calls to the helpdesk.

Top Features

Control over a wide range of devices

eDevice can control user access to a wide range I/O devices and removable media such as modems, USB drives, SD cards, MP3 and media players, floppy disks, CD's and DVD's. Options exist for configuring WiFi networks access rules, Print Screen action and VMWare devices.

Granular control of device usage

Administrators can define which I/O devices and removable media can be used on specific computers or groups of computers on the network, and which devices and media each user or group of users is permitted to use. Different permissions can be defined depending on whether the user is working in the office, from home over a VPN link, or working offline. Specific media can be approved for use, eg. particular USB devices or CD-ROMs. A user can be authorized to read data from a particular approved CD-ROM even if access to all other CD's is blocked.

Centralized management and control

The central management console provides the management and administrative tools for setting device control policies, user administration, monitoring of all devices on the network, and reporting. Detailed security events and alerts are displayed in real time, making it easy to identify if a security breach has been committed. Administrators can see at a glance which endpoint has an agent on it, its status, and can even shut the computer down from the central console if an issue is suspected.

Fast deployment across all computers

Deploying device control on all computers in the network is quick and easy. Controlguard synchronizes with Active Directory to simplify user and computer administration. The built-in intelligent client notification mechanism ensures that agents are installed automatically when new computers are added to the network.

Define device control policies for online and offline working

Controlguard enables administrators to create different port and device control policies to be enforced when users are working online, offline or via a VPN connection. By scanning the user IP address and matching

it to the predefined IP ranges, eDevice detects the connection state of the computer and applies the relevant device control policies.

Active monitoring and control at all times

Agents installed on the endpoint computers remain active even when the computer is not connected to the network and cannot be bypassed or removed by the endpoint user.

Hot-plug support

I/O devices can have various plug-in modes; for example a modem can be built into the PC, plugged in via a USB port or connected via GPRS. The eDevice Hot Plug feature ensures that a policy blocking access to a particular I/O device is enforced regardless of the way the device is plugged in.

Scalable and flexible for business continuity

Controlguard can be easily scaled up to support additional business requirements by clustering servers. Automatic load balancing across multiple servers ensures optimum performance and high availability should one of the servers become unavailable. Alternatively specific servers can be assigned to specialized tasks to maximize workflow.

Technical Specifications

Controlguard Agent
Client Hardware: •Pentium 4 1.5 GHz processor
•150MB of available hard disk space
•32-bit and 64-bit
Supported Operating Systems: •Windows® 7 (Ultimate, Business, Enterprise)
•Windows® Vista SP 1 (Ultimate, Business, Enterprise)
•Windows® XP Pro SP 3
•Microsoft Windows® 2008 Server
•Microsoft Windows® 2003 Server Standard Edition
General Requirements: •Microsoft MSI® Version 2 or higher

Controlguard Server

- Client Hardware Minimum Requirements:
    - Pentium 4 2.8 GHz
    - 1GB of RAM
    - 2GB available hard disk space
    - 32-bit and 64-bit

Supported Operating Systems: •Microsoft Windows® 2008 Server
•Microsoft Windows® 2003 Server Standard Edition
•Microsoft Internet Information Server® with ASP.NET 2.0
Supported Databases: •Microsoft SQL® 2008
•Microsoft SQL Express® 2008
•Microsoft SQL® 2005
•Microsoft SQL Express® 2005
•Microsoft SQL® 2000
•Microsoft MSDE® 2000 (supplied on the installation kit)
General Requirements: •Microsoft Internet Explorer® 5.5 or higher