



ControlGuard Endpoint Access Manager



Enterprise data is vulnerable to theft and misuse

Information theft and proprietary data leakage are making headlines frequently. Major organizations have been forced to inform the public regarding compromised private customer records.

Most occurrences of data leakage and theft are attributed to insiders. While enterprise networks are typically protected by a variety of security applications, PCs and laptops (endpoints) are often left exposed to threats from within. Anyone with access to endpoints can easily download proprietary information or infect them with viruses, Trojan horses or other malware, using common portable devices and removable media such as CDs, memory sticks and iPods. These unmanaged portable devices and removable media pose a serious security threat. ControlGuard provides a solution to address this threat: Endpoint Access Manager.

Endpoint Access Manager prevents information leakage and unauthorized access to ANY device or interface.



ControlGuard Endpoint Access Manager effectively protects your data by



- ➔ **Controlling** and monitoring how information is downloaded from endpoints.
- ➔ **Shielding** your network from malware copied to endpoints from removable media and portable devices.
- ➔ **Securing** your network from exposure to the outside world through wireless modems, WiFi, Bluetooth and other interfaces.

Protecting Your Enterprise Data

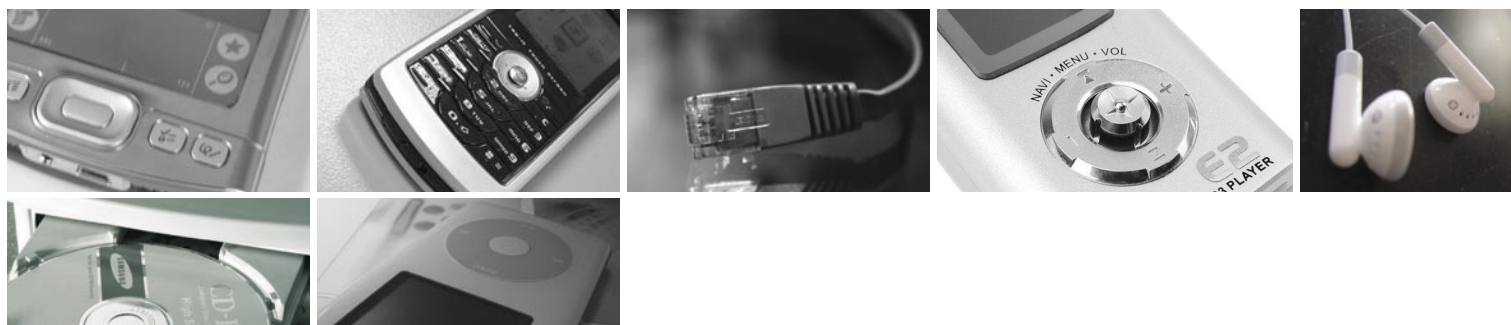
Endpoint Access Manager is an enterprise-grade solution for controlling, monitoring and logging how information is downloaded and uploaded to the endpoints. By implementing policy-based control of endpoint access to portable devices and removable media, ControlGuard's solution effectively prevents unauthorized use of enterprise data.

Endpoint Access Manager is deployed and managed centrally. Security administrators define policies that are automatically distributed to the endpoints. These policies are enforced and all relevant events are communicated back to the Management Server. Close integration with enterprise directories and enterprise management systems enables easy deployment and extensive monitoring and reporting.



I/O devices

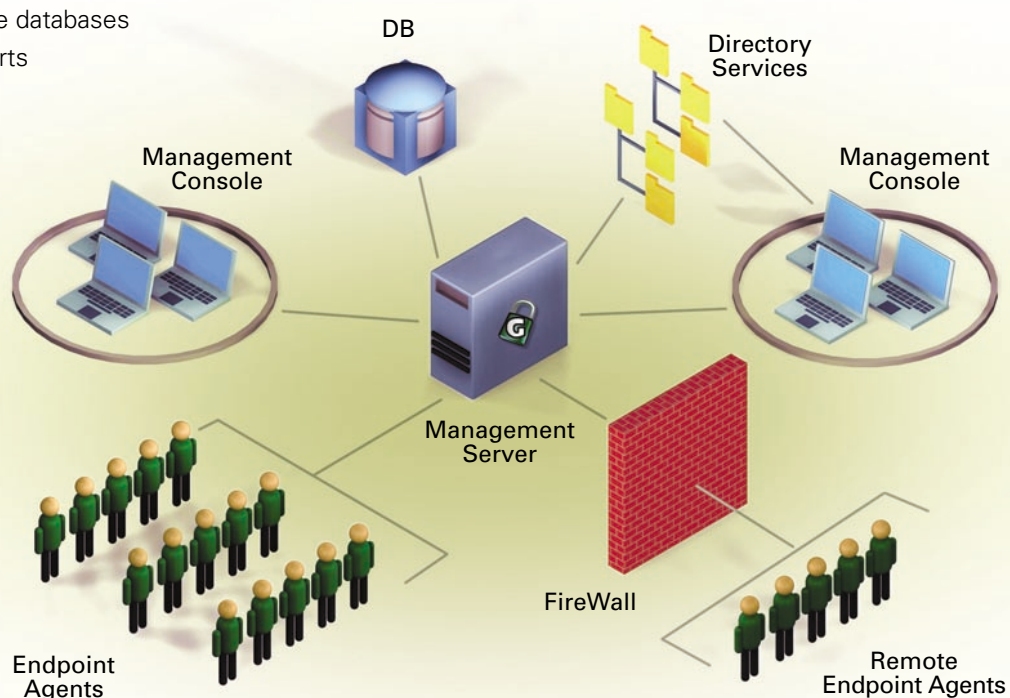
- Internal Modems
- External Modems
- PDA's
- Network Printers
- Local Printers
- MP3 Players
- Tape Devices
- Biotech Devices
- CD/DVDs, Burners
- Memory Sticks
- LAN Adapters
- Camcorders
- Digital Cameras
- Scanners
- iPods
- Optical Devices
- Smart Phones
- Floppy Disks
- Mass Storage
- SD Cards
- Zip/Jazz Drives



Endpoint Access Manager Implementation

Endpoint Access Manager includes a Management Server, a Management Console and Endpoint Agents. The Management Server is deployed at a central location within the enterprise network. The Endpoint Agents are deployed seamlessly to the endpoints using standard enterprise distribution tools. The Management Server intelligently communicates security policies to the Agents. The Agents enforce the policies, monitor endpoint activities and communicate back to the Management Server relevant data. The Management Console offers robust tools to display and report endpoint activities, including:

- Real-time notifications
- Audit logs stored in corporate databases
- Customized web-based reports



The Management Console displays endpoint configurations and reveals connected devices and media interfaces. Any I/O activity at the endpoint is immediately logged and displayed by the Management Console and is subjected to the appropriate policy enforced by the Endpoint Agent. The policy can be limited to monitoring only, or to permitting a specific action on a specific set of devices by specific users.

The Endpoint Agents are intelligent and independent modules that remain active even when the endpoint is not connected to the network. They are protected from attacks by processes, services or other drivers, and cannot be bypassed by endpoint users, even if they have administrative rights on the endpoint.

Endpoint Access Manager tightly integrates with directory services, enterprise management systems, application infrastructure and distribution systems enabling easy deployment and minimal administration overhead.

Key Features

Intelligent and Granular Policies

Endpoint Access Manager allows you to authorize specific devices, media and interfaces for specific PCs and users leveraging directory services. The policies are communicated to the endpoints in real-time and immediately enforced by the Endpoint Agents. Administrators can grant temporary permissions to on-line and mobile users.

Intelligent Distribution

Endpoint Agents are distributed and installed seamlessly and efficiently across your network. The Agents can also be distributed by common enterprise software distribution tools like Microsoft System Management Server.

Hot-Plug Support

Endpoint Agents monitor Plug-and-Play device drivers that are installed at the endpoint. Based on the policy of that endpoint, the Agent will report the newly installed device to the Management Server and enforce the appropriate access permissions to it.

Mobile Users Support

Mobile user endpoints are monitored and protected. The Endpoint Agent continues to enforce the policy even when the endpoint is not connected to the network. It may apply different access permissions to interfaces (like WiFi) when the endpoint is off the network. Security administrators can temporarily grant mobile users access to a required removable device.

Real-Time Notifications and Auditing

All I/O activities of the managed endpoints are notified in real-time to the Management Server and logged in a database. The events are displayed on the Management Console and communicated to security administrators in a variety of formats such as popup messages and email. The events are also made available to enterprise management systems in SNMP traps.

Advanced Security Agent

The Endpoint Agent is protected from attacks by processes, drivers, services and malicious code on your endpoint. It cannot be bypassed even by users who have administrative privileges to their endpoints.

LiveUpdate Mechanism

The LiveUpdate function controls the software version of the Endpoint Agents. It automatically deploys updates when necessary, minimizing the administrative overhead.

Directory Integration

Endpoint Access Manager is well integrated with enterprise directory infrastructure such as Microsoft Active Directory and Novell eDirectory. This enables administrators to leverage the existing organizational logical layout of objects and groups. It also allows dynamic discovery of new objects added to the network, and optionally installing an agent on any new endpoint.

Enterprise Management Systems Integration

Endpoint Access Manager is well integrated with enterprise management systems such as CA Unicenter, CA eTrust and HP OpenView. This enables administrators to leverage existing management infrastructure and consolidate endpoint security events in unified logs and existing management consoles.

Comprehensive Reporter

Endpoint Access Manager records all endpoint I/O events in an SQL database. A flexible and intuitive reporting module allows administrators to submit customized queries and generate comprehensive reports on endpoint and end user activities.

About ControlGuard

ControlGuard is a leading provider of enterprise-grade endpoint security solutions. Global companies around the world are turning to ControlGuard to protect their endpoints from internal breaches of security. The ControlGuard team has extensive experience in information security and enterprise management, complemented by partnerships with key solution providers in this space. For more information on ControlGuard's solutions, please visit www.controlguard.com.

ControlGuard Ltd. - Headquarters:

1 Abba Eban Blvd.
Herzlia 46725 Israel
Tel +972-9-9578781
sales@controlguard.com

ControlGuard Inc. - US

1200 Route 22 East, Suite 2000
Bridgewater, NJ 08807
Tel +1-908-203-4685
sales@controlguard.com

www.controlguard.com