



## ControlGuard Endpoint Access Manager

### Enterprise data is vulnerable to theft and misuse

Information theft and data leakage are making headlines frequently. Several organisations have been forced to inform the public about compromised customer records containing personal data and there are many other instances where data may have been lost and the organisation is still unaware. Most occurrences of data leakage and theft are caused by staff either accidentally losing a PC or other data storage device or a deliberate desire to steal data. 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, trojans or other malware, using common portable devices and removable media such as CDs, memory sticks, Smartphones and iPods. These unmanaged portable devices and removable media pose a significant security threat. ControlGuard provides a solution to address this threat with the Endpoint Access Manager.

Endpoint Access Manager prevents information leakage and unauthorised access to ANY device or interface and 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 a policy-based control of endpoint access for portable devices and removable media, ControlGuard's solution effectively prevents unauthorised 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.

### Managed Input and Output Devices

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

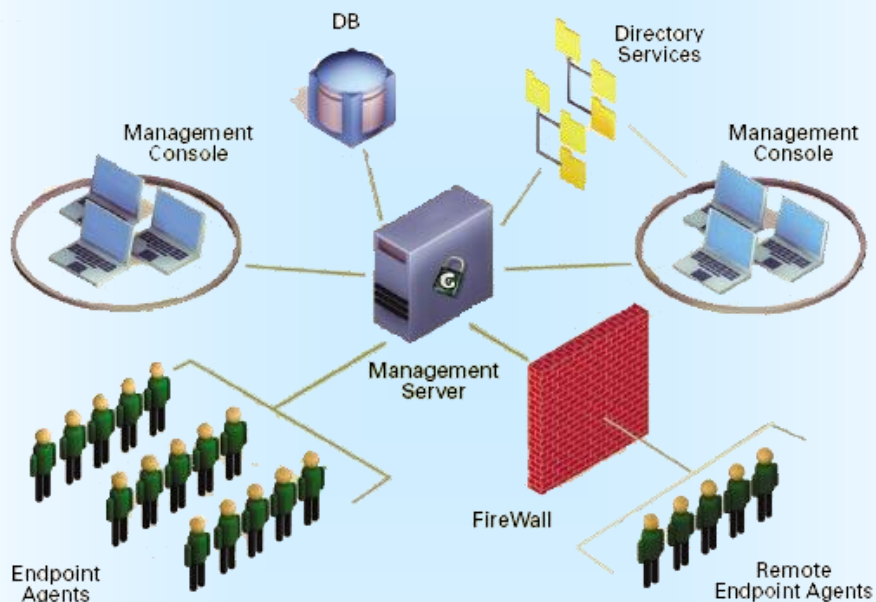




## Endpoint Access Manager Implementation

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
- Customised web-based reports



The Management Console displays endpoint configurations and reveals connected devices and media interfaces. Any upload or download 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.



## ControlGuard Key Features

### Intelligent and Granular Policies

Endpoint Access Manager allows you to authorise 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 realtime 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, minimising 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 organisational 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 customised queries and generate comprehensive reports on endpoint and end user activities.





## Endpoint Access Manager Case Study

*“ControlGuard’s innovative technology allows us to centrally manage security policies and authorise the use of removable media as needed”.*

### ABN AMRO Secures Trading Desktop Computers with Endpoint Security Software

#### The Challenge

ABN AMRO Global Futures provides clearing and execution services on a global basis. In 2005, the division built a new trading floor in Singapore. The company’s challenge was to mitigate the security risks associated with remotely managing a professional trading centre from its location in the United States. In order to do so, ABN AMRO would need to secure endpoints of all the trading computers in the new facility.

#### The Solution

ABN AMRO turned to endpoint security software from ControlGuard. Endpoint Access Manager, allows ABN AMRO to centrally control, monitor and record how data is uploaded and downloaded from removable media and portable devices to desktop and laptop computers. Unauthorised transactions are blocked, monitored and communicated in real time to the management consoles. The solution shields networks from malware copied to endpoints, and it secures networks from exposure to the outside world through wireless modems, WiFi, Bluetooth and other interfaces. ABN AMRO has deployed Endpoint Access Manager to protect the PCs and laptops in its new trading floor from any viruses, malware or data leakage caused by external software or memory device.

#### Results

*“Preventing unauthorised usage of removable media and portable devices is essential in order to manage a secure IT environment,” said Joseph Kelly, senior vice president and chief technology officer of ABN AMRO Global Futures. “ControlGuard’s innovative technology allows us to centrally manage security policies and authorise the use of removable media as needed.”*

With security measures in place, ABN AMRO is able to successfully manage the Singapore trading office from its Chicago, Illinois location. External devices, such as memory sticks or CDs that can be used to glean sensitive data from PCs or laptops are no longer a threat because users do not have the ability to use them to remove protected information from the corporate network. ABN AMRO is benefiting from the auditing features of the policies which help the company to comply with federal and global regulations like Sarbanes-Oxley that hold financial services accountable. For ABN AMRO, centrally controlled and enforceable policies create an excellent environment for secure trading.



**Between 1991 and 2007, ABN AMRO was one of the largest banks in Europe and had operations in about 63 countries around the world.**

**ABN AMRO has recently been acquired by a consortium of banks led by Royal Bank of Scotland Group.**

### e-Solutions & Services UK Ltd

Upper Linbrook Farm, Needwood,  
Burton-upon-Trent, Staffordshire  
DE13 9PF

Phone: 0870 855 0631

Email: [enquiries@e-solutions.uk.com](mailto:enquiries@e-solutions.uk.com)

Web: [www.e-solutions.uk.com](http://www.e-solutions.uk.com)

