



# Endpoint Data Protection



## Overview

Unrestricted data transfer to removable devices like USB and CD/DVD drives, or through web, mail, IM, P2P applications and more is resulting in rising security breaches. While organizations are struggling to define their data loss prevention needs comprehensively, endpoint data protection has emerged as the critical immediate step. Simultaneously, presence of branch offices, rise in sophisticated attacks and the resultant bugs and vulnerabilities are necessitating centralized, automated asset management at the endpoint.

Hence, organizations need security that moves with users to protect data and assets in endpoint devices. While gateway security solutions secure the organizations' perimeter, endpoint solutions are needed to secure the weakest link in organizations - the end user.

## Cyberoam - Endpoint Data Protection

Available in downloadable form, Cyberoam offers enhanced Endpoint Data Protection with policy-driven data and asset management over the endpoint. The easy-to-manage enhanced Endpoint Data Protection provides seamless control with logging, reporting, encryption and policy-driven controls. It prevents data loss, enhances security, employee productivity and efficient management of IT assets while retaining business flexibility. In addition, organizations can meet regulatory and security compliance requirements.

## Benefits


**Prevent Endpoint Data Leakage** - Control files transferred over removable devices, instant messengers, emails, network sharing and printers, preventing data leakage over endpoints.


**Remote Data Control through Encryption** - Eliminate the risk of data loss through device and file encryption. Decryption requirement prevents data leakage in case of lost devices.


**Rapid and Simple Deployment** - Automatic and centralized installation of robust, tamper-proof agents over multiple end points ensures seamless and transparent deployment.


**Reduce Total Cost of Ownership of IT and Security** - Hardware and software asset management with inventory, patch, update management and remote deployment of Microsoft Software Installation (MSI) packages, allow organizations to control hardware and software costs while meeting security compliance requirements.

**Reduce Malware Penetration, Legal Liabilities, Business Losses** - Centralized hardware and software management prevents legal liabilities arising out of unauthorized and illegal application deployment by users. Automated patch management reduces malware penetration, lowering incidences of network outage. Prevention of data leakage across distributed offices and mobile workforce further lowers legal liability and business losses.

 Data Protection & Encryption

 Device Management

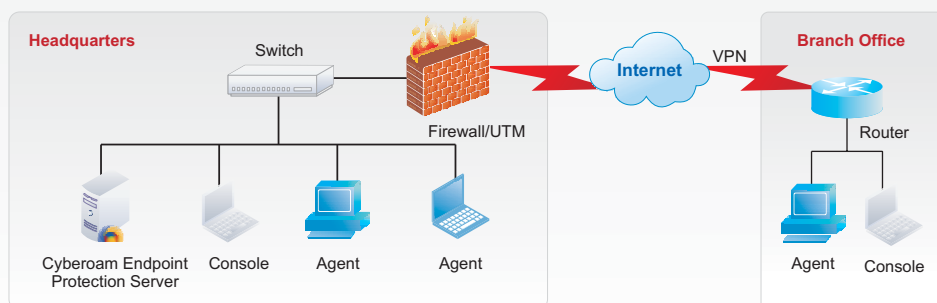
 Application Control

 Asset Management

## Solution Components

The Cyberoam Endpoint Data Protection consists of 3 components:

- Server - Database storage and agent management
- Console - Audits, controls and monitors the computers
- Agent - Collects and forwards the data to the server



Deployment Diagram

## Feature Specifications

 Data Protection & Encryption

## Document Control

- Policy creation based on
  - Disk types - Fixed, Floppy, CD-ROM/DVD, Removable, Sharing
  - File name and extension
  - Application type
- Logging and search: Local and Shared files based on
  - Access, modify, delete, copy, create, restore, rename
  - Source, destination path
  - File name, extension, size
  - Application, disk type

## Encryption over Removable Devices

- Support USB-based storage devices
  - Pen drives
  - Hard drives (indicative list only)
- Add, classify storage devices by
  - Black List & White List
  - Hierarchy / Group-based
  - Encryption
- Policy-based control for
  - Read & Write
  - Encryption on Write; Decryption on Read
- Encryption based on files, devices
- Removable storage logs by

- Device description
- Plugin / plugout record with time stamp

## Email Control

- Policy creation based on
  - Sender, recipient
  - Subject
  - Attachment: File name, extension, size
- Email logs
  - Email content, attachment
  - Protocols: SMTP / POP3
  - Applications - Exchange®, Lotus Notes®
  - Webmail - Hotmail®, Yahoo Mail®
  - Search email by
    - Application, sender / recipient
    - Subject
    - Attachment - File name, extension, size

## Instant Messaging (IM) Control


- Applications supported - MSN, Yahoo, Skype, ICQ, QQ, Google Talk, UC, Popo, RTX, LSC, ALI, Fetion, TM
- Policy creation based on
  - File name, extension, size
- IM Logs
  - Chat conversation logs
  - File upload, download
  - Search on
    - Content of chat conversation
    - UserId / nickname

## Printer Control

- Printer access: Local, network, shared and virtual printers
- Printer name
- Application-based printing
- Print logs by
  - Printer type, name, time
  - Number of pages
  - File / Task, application name

## Shadow Copy

- Backup of files transferred over:
- Removable, fixed and shared devices based on
    - Modify, cut / copy to, delete activity
    - File name, extension and size range
  - Instant Messaging (Files transferred / blocked)
    - File name, extension and size range
  - Email based on
    - Sender / recipient
    - Email size range
  - Printer based on
    - Print records / logs
    - Record printed file / task image

 Device Management

## Access policy for

- Storage Device
  - Floppy, CDROM, Burning Device, Tape, Movable Device
- Communication Device
  - COM, LPT
  - USB, SCSI, 1394 Controller
  - Infrared, PCMCIA
  - Bluetooth, Modem, Direct Lines

- Dial-up Connection
- USB Device
  - USB Keyboard, Mouse, Modem, Image Device
  - USB CDROM
  - USB Storage and Hard disk
  - USB LAN Adapter and other USB Devices
- Network Device
  - Wireless LAN Adapter
  - PnP Adapter (USB, PCMCIA)
  - Virtual LAN Adapter
- Other devices - Audio & Virtual CDROM

 Application Control

- Application access policy for: Games, IM, P2P (indicative list only)
- Add, classify applications based on hierarchy and role
- Create white list / black list of classified applications
- Granular, policy-based application access controls
- Application usage logs
  - By application
  - Start / stop, timestamp, path

 Asset Management

- Automatic collection of endpoint information
  - Hardware configuration
  - List of installed applications
- Inventory tracking of hardware assets
  - CPU, memory, network adapter, disks, motherboard, integrated peripherals
- Inventory tracking of software assets
  - Anti-virus information
  - Application name, version, manufacturer, installed path
  - OS information - Name and version, license number

- Install date, service pack
- Microsoft® patch information
  - Security update
  - Hotfix
  - Microsoft® application updates
- Historical information
  - Track addition and deletion of hardware and software
- Add custom tags to software and hardware assets
- Add custom assets such as printers, routers, switches, and more

## Patch Management

- Microsoft® patch management by listing of patches
- Microsoft® patch management by nodes
- Auto download of patch at nodes
- Centralized installation of patches

## Alert Policy

- Monitors hardware and software changes

## Remote Deployment

- Creation and installation of packages
- Deployment of packages based on node or group

## Administration

- Role-based granular administration
- Role-based access to computer, user groups
- Multiple administrators, user levels
- Multiple console support
- Robust, tamper-proof agents
- Centralized deployment of agents
- Auto agent installation on multiple endpoints
- Automatic installation of agent in domain controller environment

## Alerts &amp; Warning Messages

- Policy violation alerts to administrator
- Alert level - Low, Important & Critical
- Customized warning message to end user
- Warning - Pop-up dialog box

## General Policy Control

- Control Panel, Computer Management
- System (Task Manager, Registry Editing, Command Prompt)
- Network, IP/MAC Binding and ActiveX controls
- Printscreen key stroke

- Lock computer on policy violation
- Policy enforcement for offline endpoints
- Temporary policy creation: Set expiry, date, time

## Logging &amp; Reporting

- Logging and search based on date, time, endpoint range
- Graphical, real-time and historical monitoring
- Basic endpoint logging
  - Endpoint startup
  - User logon & logoff
  - Patch installation
  - Dialup logs & IP Address/MAC Address information

## System Requirements

Module	Operating System	Database	Recommended Hardware
Server	Win2000 SP4/XP SP2/2003 SP1/Vista & Win 7*	SQL Server 2000 SP4 or above / SQL Server 2005 SP1 or above MSDE SP4 / SQL Server 2005 Express	Pentium IV 2GHZ/512MB Memory/50GB HDD space
Console	Win2000 SP4/XP/2003/2008/Vista & Win 7*	NA	Pentium III 1GHZ/256MB Memory/4 GB HDD space
Agent**	Win 2000/XP/2003/2008/Vista & Win 7*	NA	Pentium III 500 MHZ/128MB Memory/1 GB HDD space

\*Supports 32 bit version for Vista and Win 7 \*\*Licensing is based on number of Agents.

## Toll Free Numbers

Thailand : +66-2-331-6491, Fax: +66-2-331-648

USA : +1-877-777-0368 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958

Copyright © 1999-2010 Elitecore Technologies Ltd. All Rights Reserved.  
Cyberoam and Cyberoam logo are registered trademarks of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice. 1.0-20100128