



Endpoint Data Protection



Overview

Il trasferimento non regolato dei dati a dispositivi rimovibili USB o drive CD/DVD, oppure mediante applicazioni web, e-mail, di IM o P2P ha portato a un incremento del numero di violazioni alla sicurezza. Mentre le aziende cercano di definire le proprie esigenze di prevenzione di perdita di dati in maniera globale, la protezione dei dati stessi presso gli endpoint è divenuta un aspetto cruciale, cui dare immediatamente importanza. L'esistenza simultanea di filiali, di un maggior numero di attacchi complessi e dei conseguenti bug e vulnerabilità impone una gestione centralizzata e automatizzata degli endpoint.

Le aziende, quindi, hanno bisogno di una sicurezza che segua gli utenti, al fine di proteggere i dati e gli assetti presso i dispositivi terminali. Mentre le soluzioni per la sicurezza dei gateway rendono sicuro il perimetro delle aziende, le soluzioni per gli endpoint servono a rendere sicuro l'anello più debole di queste, ovvero l'utente finale.

Endpoint Data Protection di Cyberoam

L'Endpoint Data Protection di Cyberoam è disponibile in formato scaricabile e consente la gestione dei dati e degli assetti presso l'endpoint secondo policy specifiche. La soluzione Endpoint Data Protection, ottimizzata per la semplicità di gestione, permette un controllo continuo grazie alla possibilità di logging, reporting ed encryption e funzionalità basate su policy. Ciò consente di prevenire la perdita di dati, migliorare la sicurezza e la produttività dei dipendenti e di gestire in maniera efficace gli assetti IT, preservando la flessibilità del business. Inoltre, le aziende possono rispettare i requisiti di sicurezza e le norme di legge.

Benefici


Prevenzione della perdita accidentale dei dati presso gli endpoint: controllo dei file trasferiti a dispositivi rimovibili, sistemi per la messaggistica istantanea, e-mail, network sharing e stampanti al fine di prevenire la perdita accidentale dei dati presso gli endpoint.


Controllo remoto dei dati mediante codifica: eliminazione del rischio di perdita dei dati grazie alla codifica del dispositivo e dei file. La funzionalità di decryption impedisce la perdita di dati nel caso di smarrimento di un dispositivo.


Installazione rapida e semplice: l'installazione automatica e centralizzata attraverso moduli sicuri e a prova di manomissione su endpoint multipli avviene in maniera trasparente e senza rischi di interruzione.

Riduzione del costo totale di possesso (TCO) del comparto IT e della sicurezza: la gestione delle risorse hardware e software comprensiva di inventario, gestione patch e aggiornamenti e installazione remota di pacchetti Microsoft Software Installation (MSI) consente alle aziende di ridurre i costi per l'hardware e il software, conformemente ai requisiti di sicurezza.

Riduzione della penetrazione del malware, della responsabilità legale e delle perdite commerciali: la gestione centralizzata di hardware e software previene le responsabilità legali derivanti dall'utilizzo di applicazioni non autorizzate o illegali da parte degli utenti. La gestione automatizzata delle patch riduce la penetrazione del malware, abbattendo l'incidenza dell'indisponibilità della rete. La prevenzione della perdita di dati tra uffici distribuiti e utenti mobili riduce ulteriormente la responsabilità legale e le perdite per il business.

 Data Protection & Encryption

 Device Management

 Application Control

 Asset Management

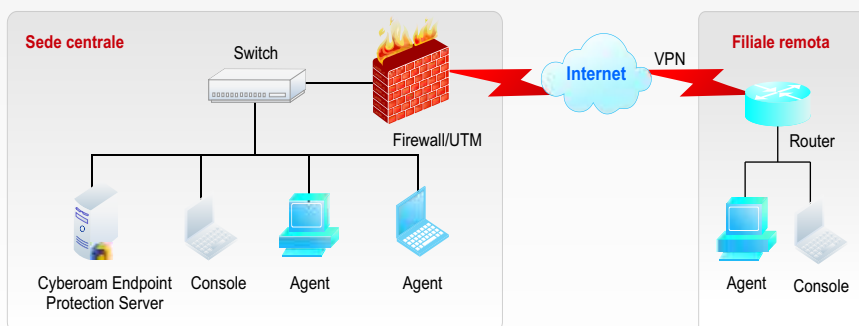
Composizione della soluzione

La soluzione Cyberoam per l'Endpoint Data Protection si basa su tre componenti:

Server – Storage del database e gestione dell'Agent

Console – Attività di audit, controllo e monitoraggio sui computer

Agent – Raccoglie e inoltra i dati al server



Schema d'installazione

Specifiche


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 & 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 & 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

Requisiti di sistema

Modulo	Sistema operativo	Database	Hardware raccomandato
Server	Win2000 SP4/XP SP2/2003 SP1/Vista	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	NA	Pentium III 1GHZ/256MB Memory/4 GB HDD space
Agent*	Win 2000/XP/2003/2008/Vista(32 bit only)/Win 7**	NA	Pentium III 500 MHZ/128MB Memory/1 GB HDD space

*Licensing is based on number of Agents. **In Roadmap

Numeri Verdi:

USA : +1-877-777-0368

India : 1-800-301-00013

APAC/MEA : +1-877-777-0368

Europa : +44-808-120-3958

Copyright © Elitecore Technologies Ltd. Tutti i diritti riservati.
 Il marchio e il logo Cyberoam sono marchi registrati della Elitecore Technologies Ltd. La Elitecore fa del proprio meglio per fornire sempre informazioni accurate, ma non assume alcuna responsabilità in caso di inaccuratezza o incomplettezza delle stesse, né considera la presente una dichiarazione vincolante. La Elitecore si riserva il diritto di cambiare, modificare, trasferire o rivedere la pubblicazione senza preavviso.

 horus
value added distributor

Distributore ufficiale per l'Italia:

Horus Informatica
 Tel: (+39) 02 33510135
 Fax commerciale: (+39) 02 33510199
 Email: commerciale@horus.it
 www.horus.it

 Cyberoam®