



Endpoint ProtectorTM

Preveniți furtul de date în companii

Versiune client 32bit: 1.2.7.0
Versiune server 32bit: 2.0.3.0

Integritatea datelor dumneavoastră depinde de modul în care le protejați. Dacă nu vă protejați porturile USB, datele dumneavoastră pot fi furate și/sau compromise. Dispozitivele USB cu capacitate de stocare de tip flash, iPod-uri, Mp3 Playere, camere digitale, HDD-uri portabile, telefoane mobile etc. prezintă cele mai mari riscuri de compromitere a datelor în ziua de azi.

Aplicația Endpoint Protector vă permite să controlați aceste dispozitive într-un mod eficient, prevenind astfel infecțiile, intenționate sau accidentale de Spyware/Malware.

Porturile USB sunt protejate printr-un firewall cu administrare centralizată

Endpoint Protector funcționează ca un firewall pentru calculatoare și pentru porturile USB. Administratorul rețelei are posibilitatea de a autoriza dispozitivele conectate la PC. Orice alt dispozitiv ce nu a fost autorizat de către administrator nu va funcționa.

Controlați utilizarea:

- Dispozitivelor USB Flash
- iPod-urilor / Mp3 Playerelor
- Cititori de card-uri
- Hard diskurilor portabile
- Camerelor digitale
- Telefoanelor mobile
- etc.

Protejarea porturilor pentru Notebook-uri și Desktop-uri

Aplicația protejează calculatoarele companiei împotriva furturilor de date, scurgerii de informații, pericolelor implicate de utilizarea dispozitivelor USB flash, a Mp3 playerelor, iPodurilor etc., dar și a altor riscuri ce decurg din utilizarea acestora.

Administrarea centralizată a dispozitivelor

Aplicația permite controlarea dispozitivelor de către administrator, printr-un browser Web. Dispozitivele, fiind autorizate devin Dispozitive Autorizate (Trusted Devices). Orice alt dispozitiv ce nu a fost autorizat de către administrator nu va funcționa.

Înregistrarea dispozitivelor

Toți clienții și dispozitivele conectate la calculator, sunt înregistrați într-o bază de date ce se poate verifica oricând.

Funcționalitatea "Offline"

În cazul în care temporar nu aveți acces la Internet, protecția calculatoarelor se va menține activă, iar E-mailurile de notificare se vor înregistra și vor fi trimise în momentul în care se va restabili conexiunea la Internet.

Mențineți siguranța companiei știind ce date se copiază de pe calculatoarele companiei și pe ce dispozitiv(e).

CERINȚE DE SISTEM

Client

- Windows Vista (32 bit) (toate versiunile)
- Windows XP (SP2) (32 bit)
- Windows 2000 (SP4)
- Framework .Net 2.0
- min. 32 MB liber pe HDD

Server

Sisteme de operare suportate:

- Windows 2003 Server sau
- Windows XP (SP2) sau
- Debian (și alte distribuții Linux)

Servere Web suportate:

- Apache Server (Versiunea 5 sau mai recentă)

Baze de date suportate:

- MySQL (Versiunea 5 sau mai recentă)

Alte cerințe pentru server:

- PHP (Versiunea 5) cu suport de SOAP
- OpenSSL Versiunea 0.9.8

Configurare intuitivă cu ajutorul mecanismelor de instalare MSI.

Serverul Endpoint Protector este compatibil cu alte platforme de server integrându-se astfel ușor în infrastructura existentă.

Interfața administrativă foarte intuitivă permite o administrare eficientă în vederea unui ROI mult mai rapid.

Endpoint Protector vă permite să lucrați într-un mediu protejat, fără riscuri și nu restricționează eficiența utilizatorilor deoarece orice dispozitiv autorizat (TrustedDevice) poate fi folosit fără întrerupere pe calculator.

Prin implementarea dispozitivelor autorizate (TrustedDevice), utilizatorul este obligat să-și salveze datele criptate pe un dispozitiv autorizat, prevenind astfel scurgerea de informații în cazul în care se pierde dispozitivul.

Interfața Endpoint Protector este disponibilă în limba engleză. La cerere, vă stau la dispoziție și alte limbi.

Pentru mai multe informații, descărcați Foia Albă "Secure Passage through a World of Technological Threats - A Guide to Meeting Emerging Security Requirements by Employing Endpoint Security Solutions" de [aici](#).

Endpoint Protector - Reporting and Administration Tool

Endpoint Protector - Administration and Reporting Tool

Management Settings Rights Reports and Analysis EPP Parameters

Devices Machines Machine Groups Client Users Client User Groups

List of devices

Filter

Device Name (Identification):

Device Type:

Vendor ID:

Product ID:

Serial Number:

Apply filter Reset

Owner	Device Type	Device Name (Identification)	Description
Edi	USB Memory Device	UT161 / USB2FLASHSTORAGE	First time used: Edi/EDINA
	USB Memory Device	MEMOREX / TD_CLASSIC_003C	First time used: Edi/EDINA
Edi	USB Memory Device	Unknown device: Edi/EDINA	First time used: Edi/EDINA
	USB Memory Device	UT176 / USB2FLASHSTORAGE	First time used: Cipri/CIP1
	USB Memory Device	SMI / ATTACHE_PRO	First time used: Cipri/CIP1
	USB Memory Device	TOSHIBA / MK2006GAL	First time used: Cipri/CIP1

Endpoint Protector - Reporting and Administration Tool

Endpoint Protector - Administration and Reporting Tool

Management Settings Rights Reports and Analysis EPP Parameters

Device Types Rights Events File Types Administrators License

List of events

Id	Event name	Description	Logg
1	Connected	Device Connected	✓
2	Disconnected	Device Disconnected	✓
3	Enabled	Device Enabled	✓
4	Disabled	Device Disabled	✓
5	Online	Machine Online	✓
6	Offline	Machine Offline	✓



© Copyright 2004-2007 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin and Endpoint Protector are trademarks of CoSoSys SRL. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

Contact: **CoSoSys Ltd.**
 E-mail: sales@cososys.com
 Phone: +40-264-593110
 Fax: +40-264-593113