COSOSYS

Endpoint
Protector 2009

Secure Endpoint Management

CoSoSys Product Presentation

Overview

- New Features in 2009 Version
- Endpoint Security Challenge
- Difficulties of Policy and Regulatory Compliance
- Endpoint Protector as Solution
- How it Works
- How Endpoint Protector Integrates
- Conclusion

New Features in Endpoint Protector 2009

Overview of New 2009 Features

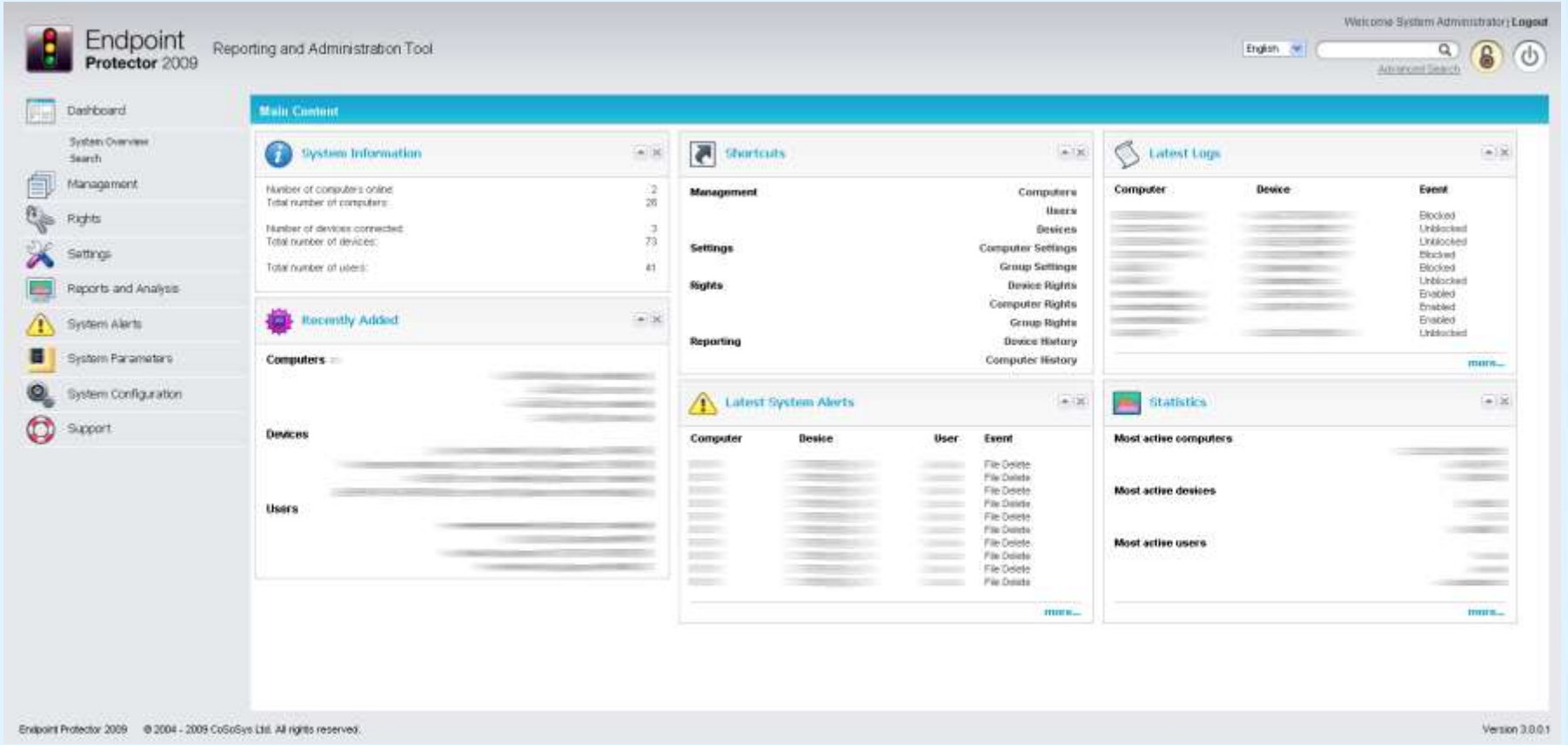
- File Whitelisting
- Completely updated and improved web-based Administration & Reporting Tool Interface
- Improved Client Self Defense
- More Controlled Device Types
  (ExpressCard SSD, Printers, Bluetooth,…)
- Endpoint Lockdown mode
- Wizard for simplified Device Management
- Improved Active Directory Sync
- System Snapshots
- Multilingual Interface
- and more

File Whitelisting

- Only authorized (whitelisted) files are allowed for transfer to authorized portable devices
- All attempts to transfer unauthorized files are stopped and traced
- Security that only whitelisted files leave the network
- All file transfers are traced

New Admin & Reporting Interface

- Completely updated web-based Administration and Reporting Tool



New 2009 Features

Improved Client Self Defense

- Extended protection for Client Service to be stopped
- Even user with Administrative privileges require a password to uninstall or stop Endpoint Protector Client

Endpoint Lockdown mode

- One click instantly locks down all endpoints and stops ongoing data transfers and device use

Wizard for simplified Device Management

- Allows faster/more intuitive device right management

System Snapshots

- Previous Settings/Policies Snapshots can be restored

Multilingual Interface

- (English, German, French, Romanian, Hungarian…)

Endpoint Security Challenge

Risks of Data Loss

- Data Loss, Data Theft and Data Leakage results in:
  - Loss of Revenue
  - Competitive Losses (Trade Secrets)
  - Loss of Intellectual Property
    (Proprietary Information, Designs, Plans, Source Code)
  - Loss of Reputation
  - Loss of Customer Confidence and Credibility
  - Noncompliance > possible lawsuits or fines
  - Bad Press
  - Federal charges

Podslurping (iPod Friend or Foe)

160 GB

40.000 Songs / Pictures

or
- Your entire CRM
- Confidential Files, PPTs, EXLs, DOCs, Construction Plans, Designs, AutoCAD Files, Layouts, Patient Data, etc..
- Entire databases with credit card info
- **All company secrets leaked or stolen**
- **Possible loss of millions in IP or Revenue**

8 GB

2.000 Songs / Pictures

or
- Entire customer database
- Confidential PPTs, EXLs, DOCs, etc...
- **Company secrets compromised**

1 GB

240 Songs

or
- Customer database
- Confidential PPTs, EXLs, DOCs, etc...
- **Company secrets leaked or stolen**

Why Endpoint Protector

darkREADING
RISKY BUSINESS

13-Nov-2007

Korean Execs Stole $1.8B in Trade Secrets

According to a report by Korea Times, two top execs from a Korean company stole key data and trade secrets worth of more than 1.8bn (!). The confidential data was stolen using those common USB drives you all know where they transferred more than 900 documents while working at the office.

Guardian Unlimited

21-Nov-2007

Astonishment over data security

Security experts have expressed astonishment that the missing child benefit data discs which could leave 25 million people at risk of ID fraud were not encrypted before being copied on to CDs and put in the post.

The Register®

04-Jan-2008

NATO secrets USB stick lost in Swedish library

The discovery of a USB memory stick containing classified NATO information (material on NATO's ISAF peace-keeping force in Afghanistan, as well as an intelligence report on the attempted assassination of Lebanon's defense minister and the murder of Sri Lanka's foreign minister) in a library in Stockholm has prompted a meeting between the Swedish Military Intelligence and Security Service and foreign defence officials.

SC MAGAZINE

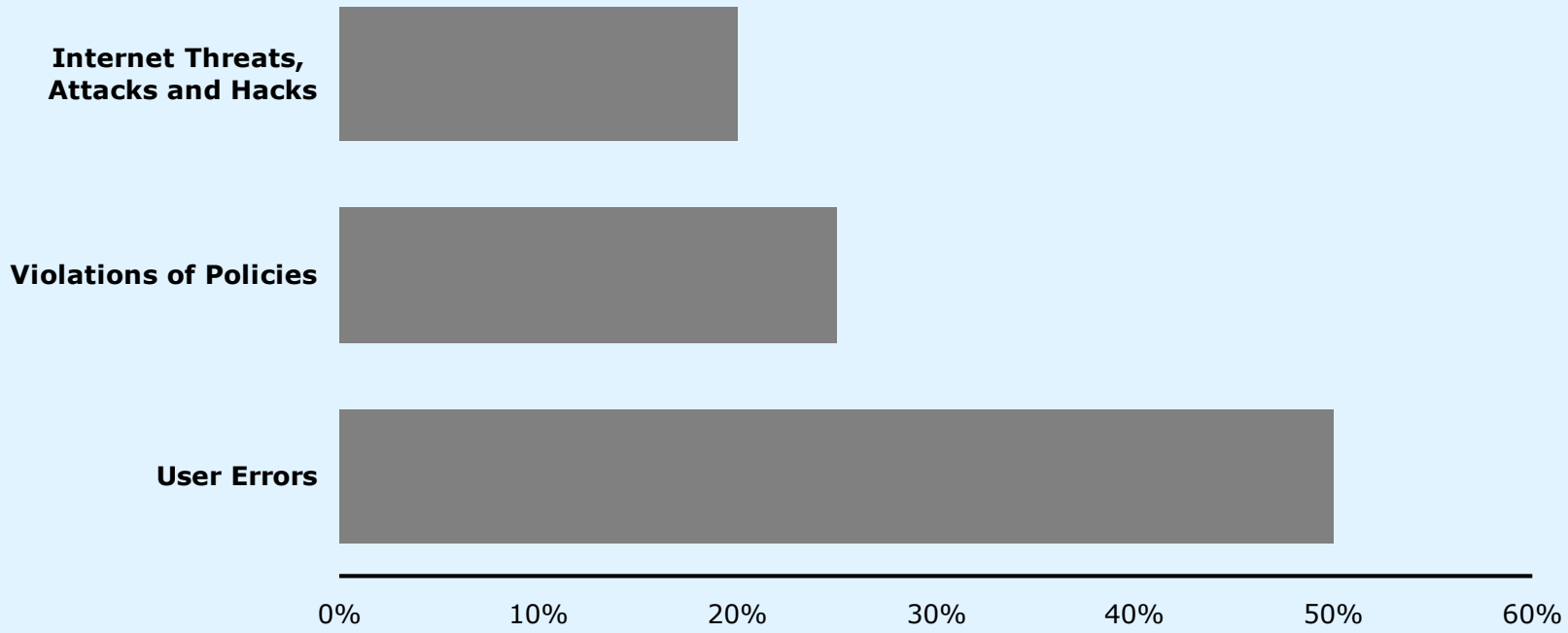
17-Jul-2007

Energy Department hits university with fine over Los Alamos breach

The U.S. Department of Energy has imposed a $3.3 million fine against the current and former operators of the Los Alamos National Laboratory following an incident last year in which a subcontractor's employee stole classified documents by storing them on a USB stick.

Causes of Data Loss

Causes of Data Losses by Number of Events



Source: ITPolicyCompliance.com
Feb-2007

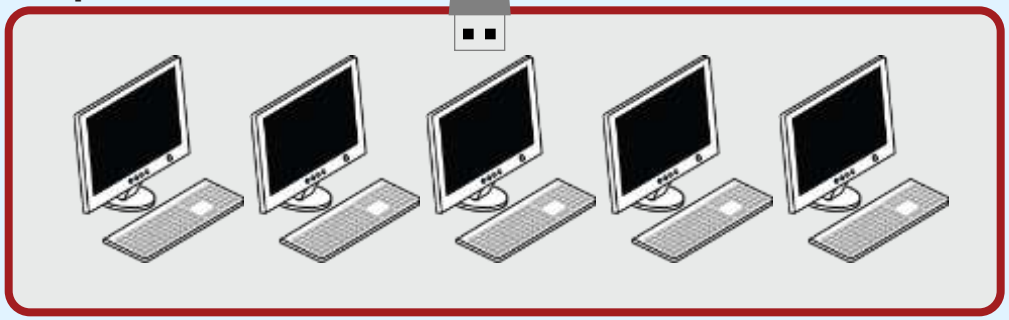
The Threat Within

Portable devices:

Threats by legitimate users:

- Theft of data
- Loss of data
- Add viruses/malware in network
- Sharing of illegal content
- Abuse of corporate IT equipment

Corporate Network:



# of Threats = Portable Devices x Users x Workstations

Why Endpoint Protector

- Primary concerns for company networks
  - Data Leakage
  - Data Loss
  - Data Theft
  - Data Manipulation
  - Regulatory Non-Compliance
  - Uncontrolled use of devices
  - Increasing adaptation of USB and other connectivity
  - Malware intrusion through portable devices
  - Introduction of illegal data (music or other pirated content)

Difficulties of Policy and Regulatory Compliance

Social Engineering, the USB Way

USB Drives can turn external threats into internal ones

Example:

- **20** USB drives are loaded with a Trojan that collects documents, passwords, logins
- The USB drives are plated (smoking areas, parking) around targeted company
- Employees show up for work and find USB Drives and plug them immediately in their work computer when they reach their desk
- Trojan e-mails the findings back
- **From 20 drives, 15 were found** and all where plugged into company computers
- The possible data to obtain this way could include all vital company secrets

June-2006 darkREADING RISKY BUSINESS

Regulatory Compliance Requirements

Sarbanes Oxley

- 105 Protection against violation of confidentiality
- 302 Prevents unauthorized modification, destruction of data
- 404 Safeguards against unauthorized and improper use of data
- 409 Real-time reporting and event-driven alerts

GLBA

- Gramm-Leach-Bliley Act
  501 (a) Privacy Obligation Policy. It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information

HIPAA

- 55% of all Required Implementation Specifications (11/20)
- 64% of all Addressable Implementation Specifications (14/22)
- 60% of all Implementation Specifications together (25/42)

Basel II

- Basel II requires, organizations to identify, assess, monitor and control their operational risk, much of which occurs at the endpoint

more

- PIPED (Canada)
- SB 1386 (California, US)
- 95/46/EC (Europe)
- EU Data Protection Directive
- DPA (UK)
- PCI DSS (UK)

Removable Drive Threats

- Since 2007 malware was infecting PCs increasingly using removable devices
  - Organizations better protect against E-mail (viruses, malware)
  - → Hackers are looking for less well-defended backdoor routes
- Malicious tools for removable Drives become more and more:
  - USB Dumper
  - USB Hacksaw
  - USB Switchblade
- Malware examples seen so far are USB drive worms:
  - Downadup / Conficker (infected 6% of PCs worldwide) Source: Computerworld
  - RavMon, LiarVB-A, Hairy worm, etc.
- Infected USB drives use auto-run and other functionality to execute malicious code on USB drives, iPods, digital cameras etc.

USB threats are definitely on the rise!

Endpoint Protector as Solution

3 Pillar Security Architecture

- Protects Data on PCs
- Prevents Data loss
- Identifies Data theft
- Prevents Malware intrusion
- Maintains Productivity

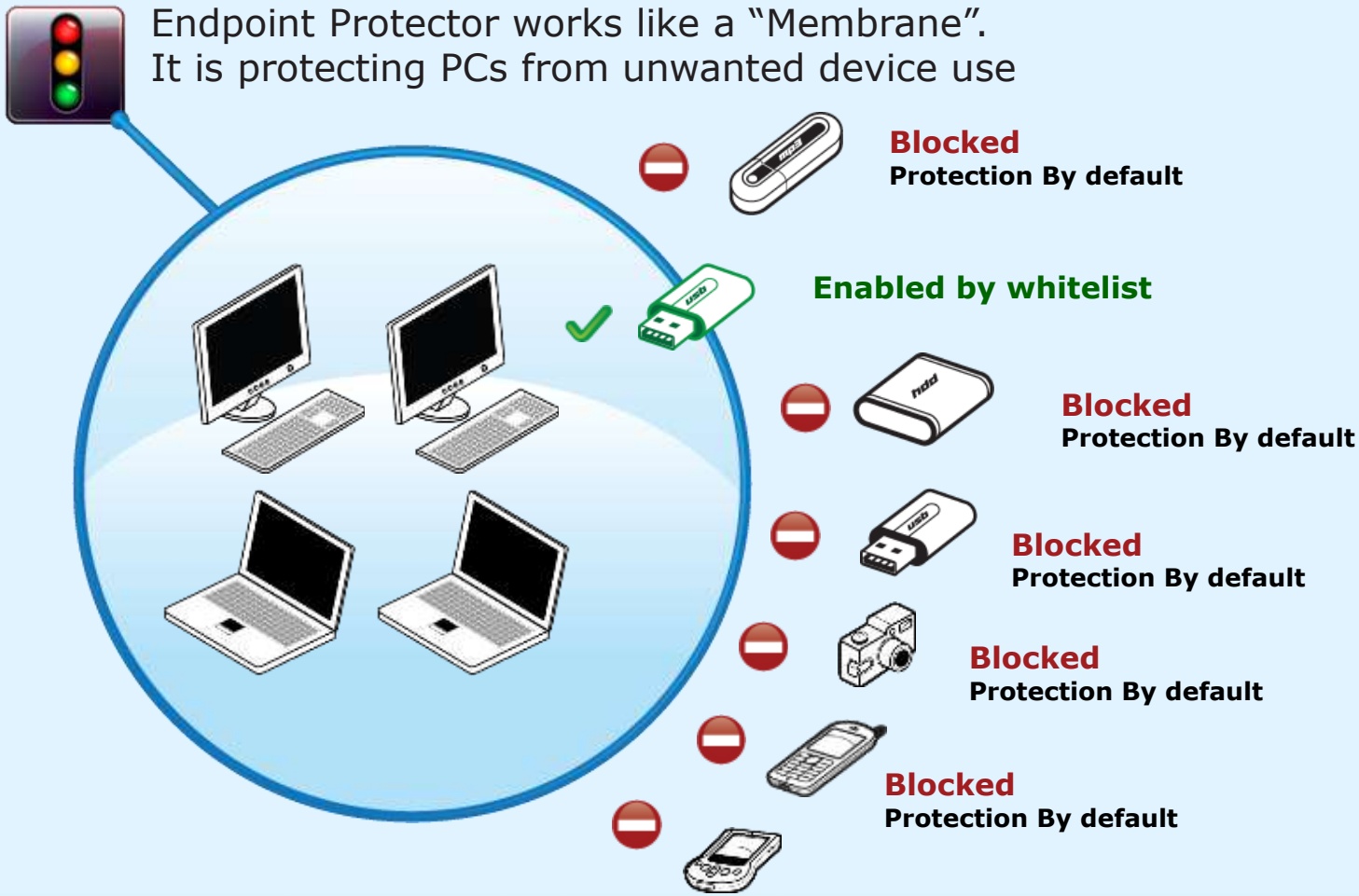
- Data read and write/delete is monitored and traced/ shadowed
- Auditable trail is recorded

- Protecting data in transit
- Portable data is encrypted
- In case of portable device loss data is useless to finder or thief

Local Data Protection | **File Tracing/Shadowing** | **Portable Data Encryption**

Endpoint Protector 2009

Protection for your PCs



Controlled Devices

- USB Sticks
  (normal Flash Drives, U3 and other Autorun Drives)
- Wireless USB
- Memory Cards
  SD Cards, MMC Cards, Compact Flash Cards, etc.)
- Card Readers (internal and external)
- Floppy Drives
- CD/DVD-Player / Burner (internal and external)
- Digital Cameras
- Smartphones / Handhelds / PDAs
- iPods
- MP3 Player / Media Player Devices
- external HDDs / portable hard disks
- Firewire Devices
- PCMCIA Devices
- ZIP Drives
- Biometric Devices
- Bluetooth
- ExpressCard SSD
- Printers
- etc..

File Tracing / File Shadowing

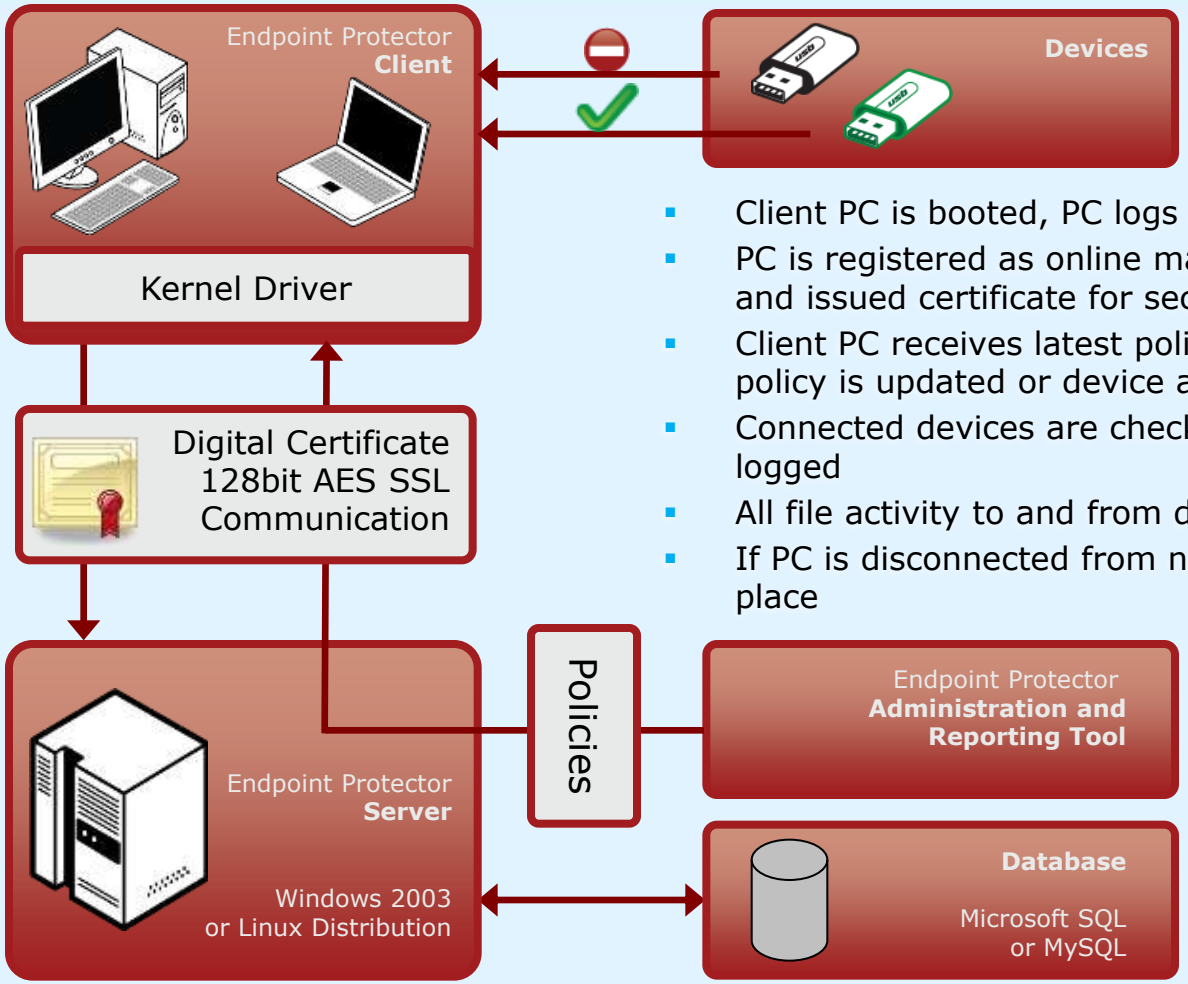
- Monitoring what files were copied to and from pre-approved storage devices
- Creates an audit trail of what data is transferred in and out of the organization, including:
  - File names
  - File types
  - File time stamps
  - Complete File is recorded (shadowed)
- Gain the freedom not to restrict usage of storage devices altogether while keeping close track over potential abuse

TrustedDevices

- Enforcing Encryption by using TrustedDevices
- Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen
- Strong data encryption with 128bit or 256bit AES encryption
- TrustedDevices with Hardware or Software based Encryption are available

How Endpoint Protector Works

How Endpoint Protector Works



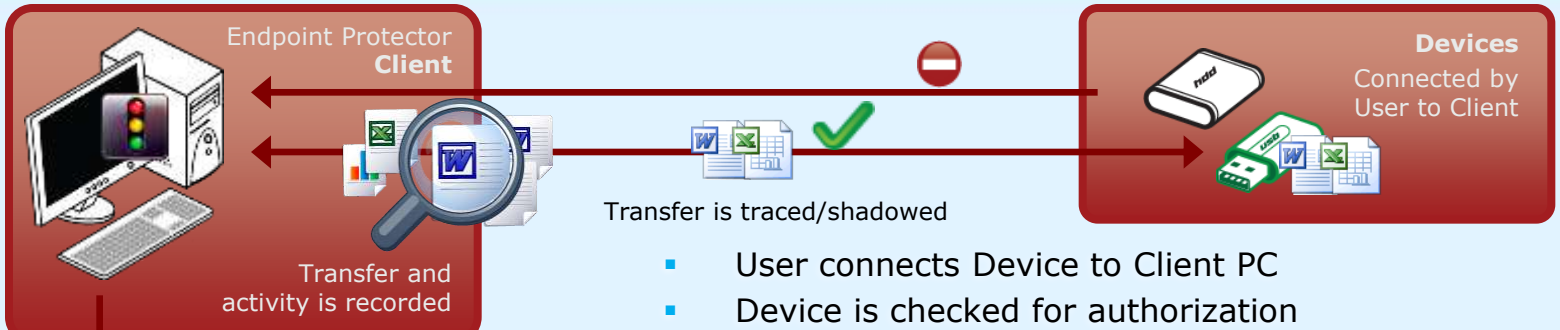
- Client PC is booted, PC logs on
- PC is registered as online machine in Endpoint Protector Server and issued certificate for secure communication
- Client PC receives latest policies and stores them locally until policy is updated or device activity is registered
- Connected devices are check for permissions and activity is logged
- All file activity to and from device can be traced/shadowed
- If PC is disconnected from network the latest policies remain in place

Policy based Management

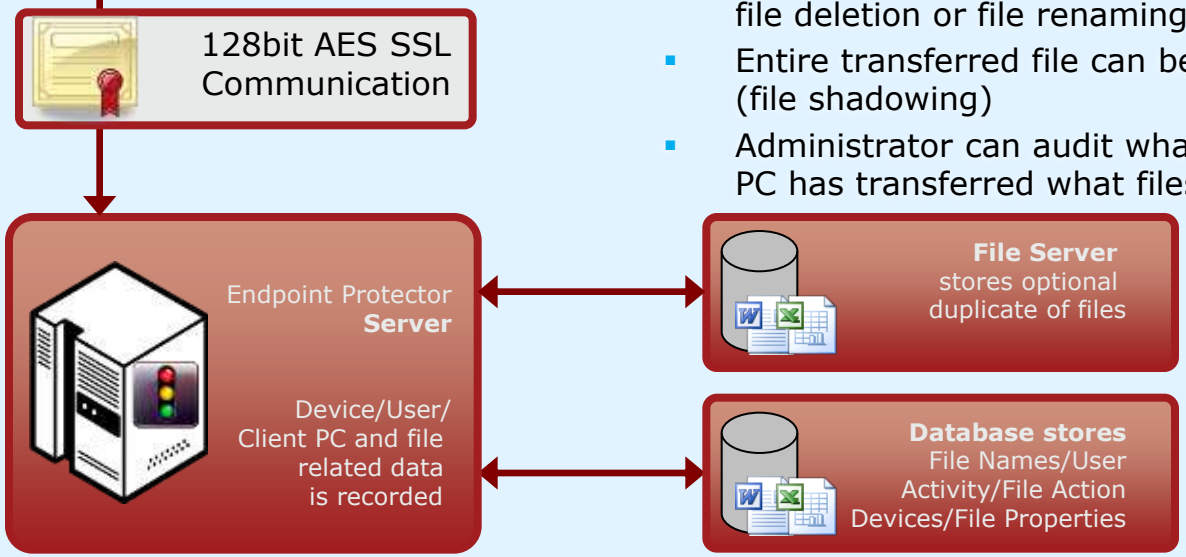
- Control which user can use what device
- Monitor what data is accessed and transferred
- Manage what files are allowed to be transfer (file whitelisting)

	Device use								Data monitoring		
	iPod/ MP3 Player	USB Flash Drive	CD/ DVD-R/W	Digital Camera	Smart-Phone Sync	External HDD / Firewire	Floppy Drive	Trusted Device	File Tracing	File Shadow	File Whitelist
Default User	⛔	⛔	⛔	⛔	⛔	⛔	⛔	⛔	✓	✓	✓
Finance Dept.	⛔	⛔	⛔	⛔	⛔	⛔	⛔	✓	✓	✓	✓
R&D Dept.	⛔	✓	✓	⛔	✓	⛔	⛔	✓	✓	✓	✓
IT Dept.	✓	✓	✓	✓	✓	✓	✓	✓	⛔	⛔	⛔
Home Worker	⛔	⛔	⛔	⛔	✓	⛔	⛔	✓	✓	✓	✓
General Administration	⛔	⛔	⛔	✓	✓	⛔	⛔	✓	✓	✓	✓
Management	✓	⛔	✓	✓	✓	⛔	✓	✓	⛔	✓	✓

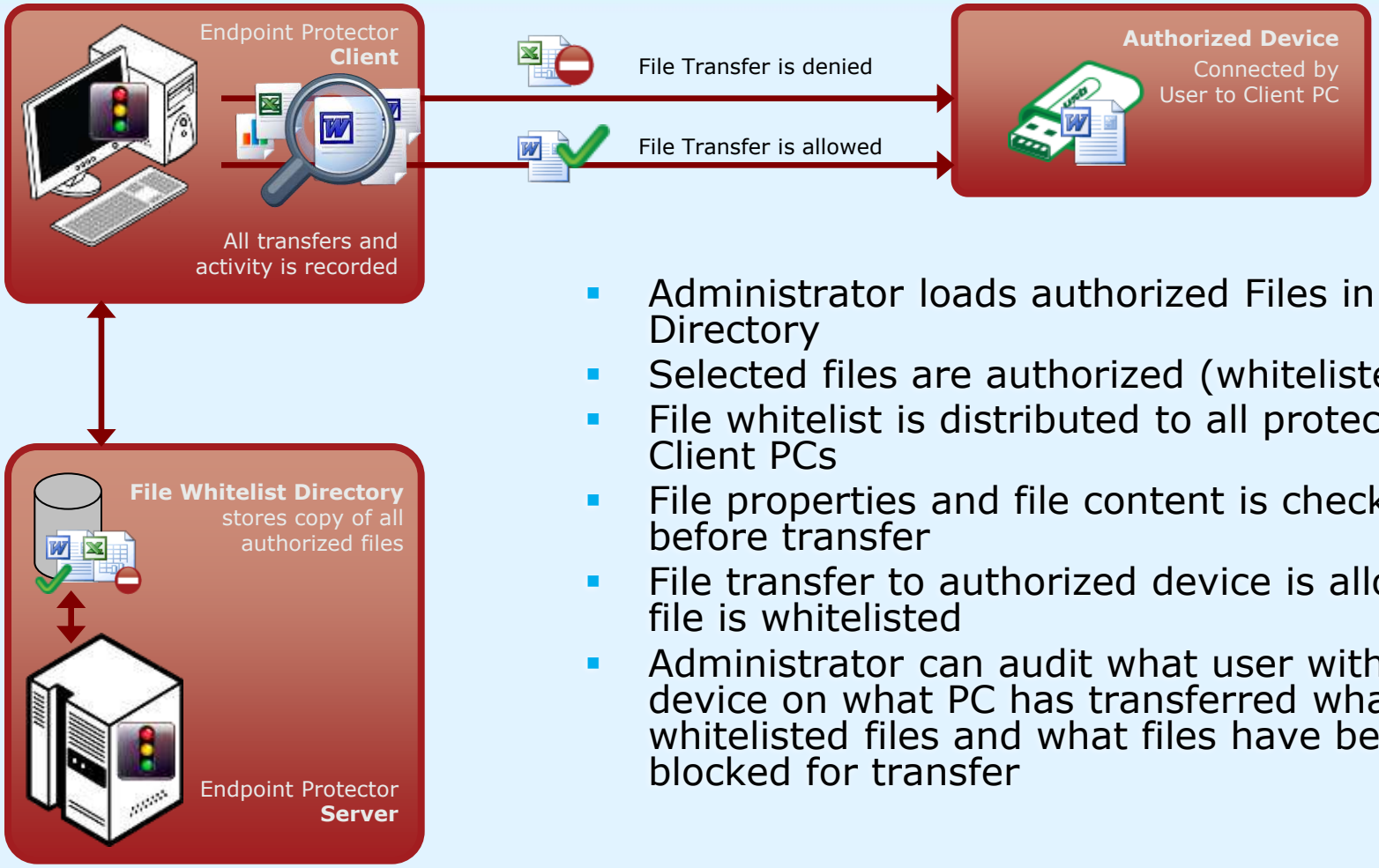
How File Tracing/Shadowing Works



- User connects Device to Client PC
- Device is checked for authorization
- Files can be transferred to authorized device
- File transfer to and from device is recorded. Actions such as file deletion or file renaming are recorded as well
- Entire transferred file can be recorded to File Server (file shadowing)
- Administrator can audit what user with what device on what PC has transferred what files



How File Whitelisting Works



- Administrator loads authorized Files in specific Directory
- Selected files are authorized (whitelisted)
- File whitelist is distributed to all protected Client PCs
- File properties and file content is checked before transfer
- File transfer to authorized device is allowed if file is whitelisted
- Administrator can audit what user with what device on what PC has transferred what whitelisted files and what files have been blocked for transfer

How Endpoint Protector Integrates

Your Choice of Server Platform

- **Two server platforms** for seamless integration in existing network infrastructure
- Endpoint Protector is also available as hosted Server (SaaS)

Windows based Endpoint Protector **Server**

- Server Platform
  - Windows 2003
- Web Server
  - IIS
- Database
  - SQL 2005 (Express)

Fast integration into existing IT infrastructure

or

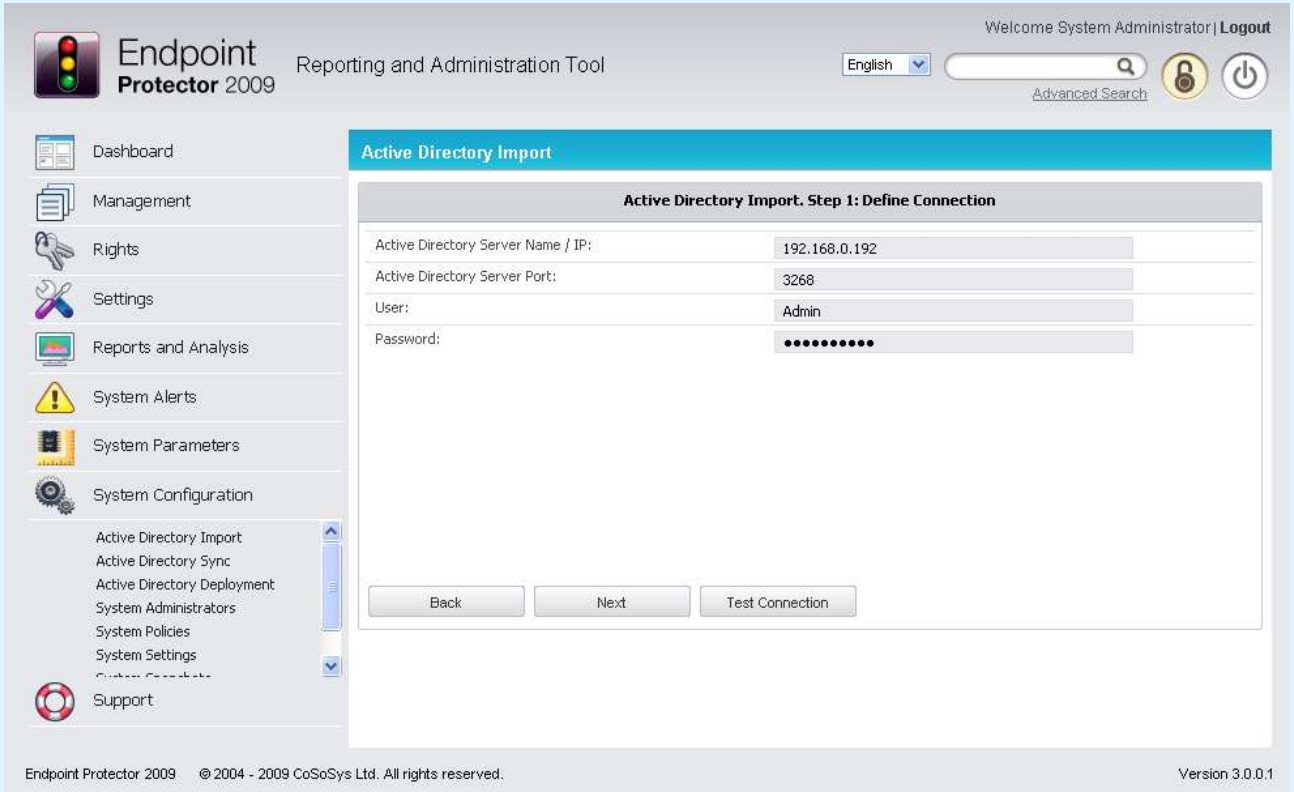
Linux based Endpoint Protector **Server**

- Server Platform
  - Red Hat
  - Debian is recommended or other Linux Distribution
- Web Server
  - Apache
- Database
  - MySQL

Lower Total Cost of Ownership (TCO)

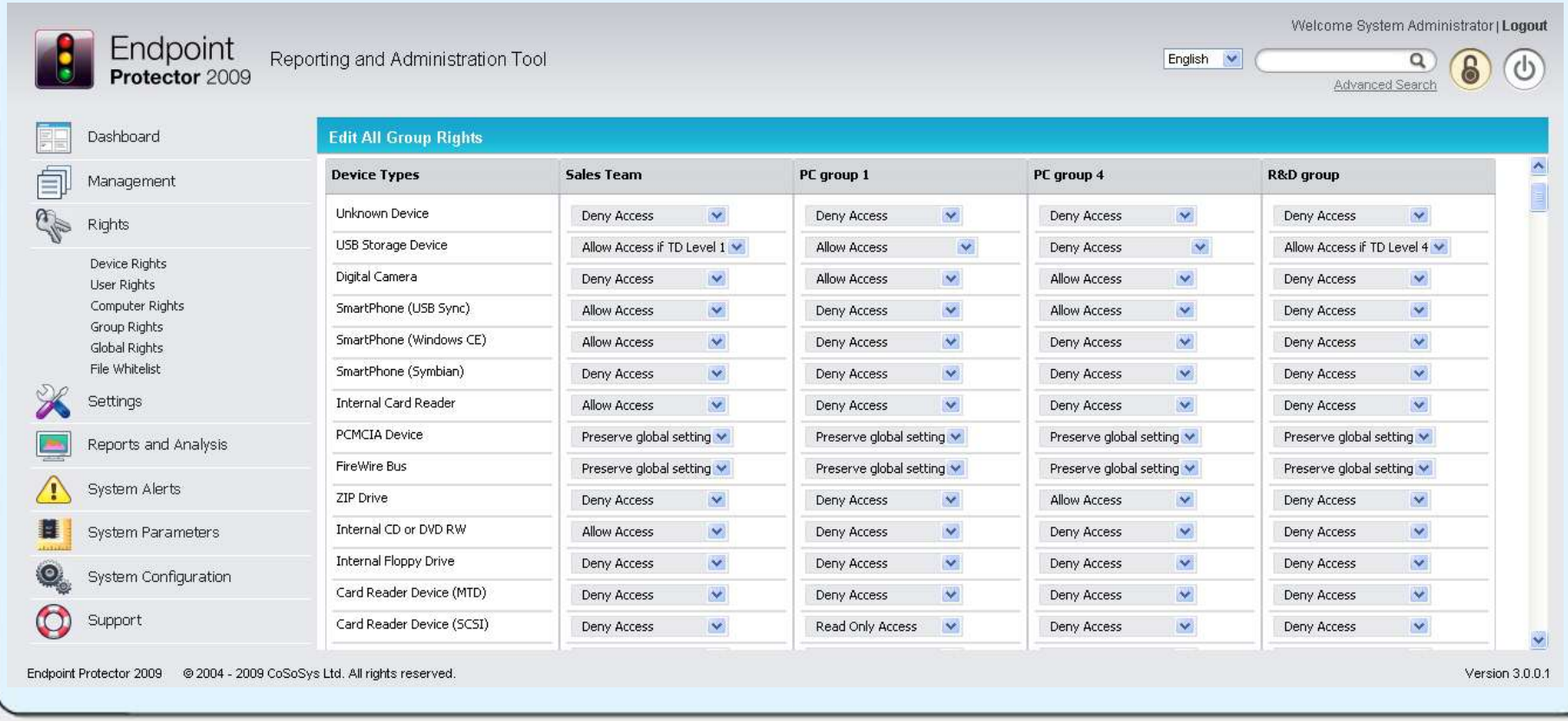
Active Directory Integration

- Endpoint Protector works with Active Directory (Import / Sync)
- Fast and efficient integration in existing infrastructure

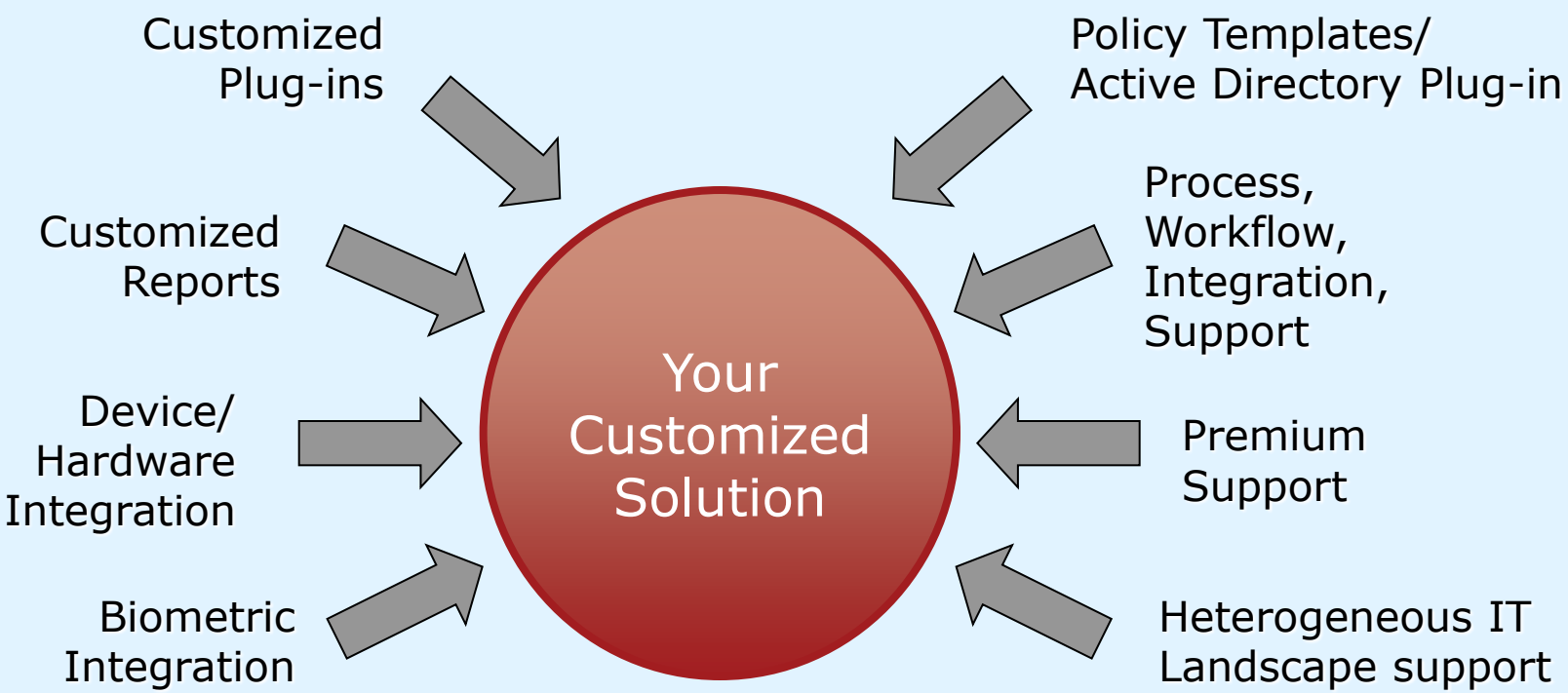


Group Policy Builder

- Building Group Policies at ease
- Policy changes are immediately distributed to protected clients



We Build your Solution



We Make Solutions for you!

Conclusion

Conclusion

Your Data is only as safe as your Endpoints are!

Control

Monitor

Protect & Enforce

Thank You!

Endpoint
Protector 2009

For further information about CoSoSys Software please visit our website at www.endpointprotector.com or www.cososys.com
or just contact us directly.

	CoSoSys Ltd.	CoSoSys Security NA	CoSoSys Germany
E-Mail:	sales@cososys.com	sales.us@cososys.com	sales.de@cososys.com
Phone:	+40-264-593110	+1-408-239 4727	+49-177-555 6435
Fax:	+40-264-593113	+1-209-578 6494	+49-721-151 497421

To Protect

Desktop PCs / Workstations

Notebooks / Netbooks

Servers

COSOSYS

Enforced Encryption with TrustedDevices for Secure Endpoint Management

CoSoSys Product Presentation

March 2009

Enforced Encryption

How Does it Work?
What are TrustedDevices?

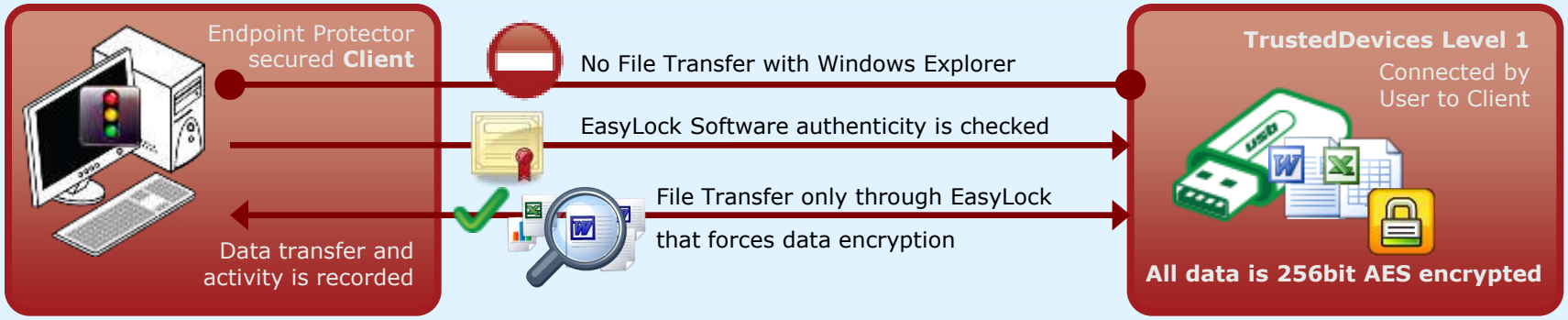
TrustedDevice Functionality

- Enforce Encryption by using TrustedDevices
- TrustedDevices are available in different Security Levels (to fit every budget)
- Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen
- Strong data encryption with 128bit or 256bit AES encryption (Software or Hardware based)

TrustedDevice Levels

Level	Security Level Explained	Devices/Hardware
1	▪ Minimum security for office and personal use with a focus on software based encryption for data security ▪ Offers companies already regulatory compliance	▪ Any USB Flash Drive and most other portable storage devices can be turned into a TrustedDevice Level 1 with **EasyLock Software** ▪ Fits any budget ▪ No hardware upgrade required
2	▪ Medium security level with biometric data protection or advances software based data encryption	▪ Requires special hardware that includes security software and that has been tested for TrustedDevice Level 2 ▪ Hardware is widely available
3	▪ High security level with strong hardware based encryption that is mandatory for sensitive enterprise data protection for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC	▪ Requires special hardware that includes advanced security software and hardware based encryption and that has been tested for TrustedDevice Level 3
4	▪ Maximum security for military, government and even secret agent use. Level 4 TrustedDevices include strong hardware based encryption for data protection and are independently certified (e.g. FIPS 140). These devices have successfully undergone rigorous testing for software and hardware	▪ Requires special hardware that is available primarily through security focused resellers

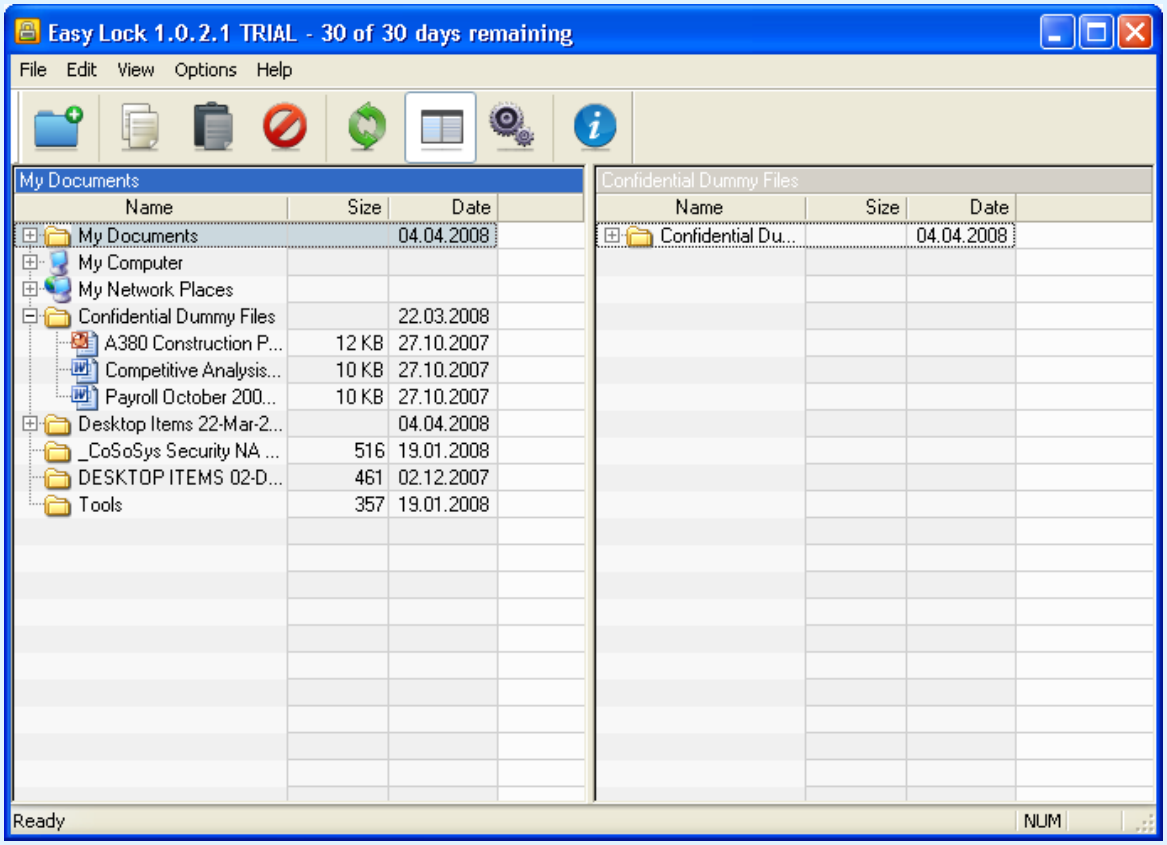
How a Level 1 TrustedDevice Works



1. User connects Device to EPP protected Client PC
2. Device is checked for authorization
3. If device is an authorized TrustedDevice Level 1, the EasyLock software on Device will automatically open
4. User can transfer files via Drag & Drop in EasyLock
5. Data transferred to devices is 256bit AES encrypted
6. User cannot access the device using Windows Explorer or similar applications (e.g. Total Commander)
7. User does not have the possibility to copy data in unencrypted state to the TrustedDevice
8. All File transfer to and from the device is recorded. Actions such as file deletion or file renaming are recorded as well.
9. Administrator can audit what user, with what device, on what PC, has transferred what files.

EasyLock Software for TD Level 1

- Government-approved 256bit AES CBC-mode Encryption
- Secure Password
- Intuitive Drag & Drop Interface
- Enforced Encryption on Endpoint Protector secured PCs, Notebooks and Server
- Turns existing hardware like USB Flash Drives into a TrustedDevice Level 1



TrustedDevice Level 2 to 4

- Data Encryption is enforced by special hardware
- Data Encryption can be Software (Level 1 and 2) or hardware based (Level 3 and 4)
- TrustedDevice Level is checked by Endpoint Protector Client
- Security Software on TrustedDevice (all Levels) is checked for authenticity by Endpoint Protector Client

Conclusion

Conclusion

Enforced Encryption is better than relying on people to remember it!

Control

Monitor

Protect & Enforce