



Varovanje informacij in odtekanje podatkov v poslovnem okolju

Rok Jerman
Sophos d.o.o.



Vsebina

- Zakaj potrebujemo varovanje podatkov
- Kje so možna mesta za odtekanje informacij
- Priprava načrta vzpostavitve sistema varovanja podatkov
- Načini varovanja s pomočjo Sophos rešitev
- Vprašanja

Naraščanje stopnje izgubljenih/ukradenih zaupnih informacij

*70% of all company data is stored
redundant on endpoints (notebooks,
desktops, USB Memory sticks),
not only on servers*

Ponemon Institute: Confidential Data at Risk



*52% of large organizations have
lost confidential data through
removable media such as USB
drives in the past 2 years*

Forrester



*Worldwide 7m.
notebooks stolen or lost*

Computer Security Institute



Odmevnost primerov izgube podatkov

Digital Defences

Missing: 25 million child b

Portland VA hospital mistakenly posts s' personal data online

Michael Milstein, The Oregonian

seattlepi.com

Local US/World Sports Business A&E Life Comics Photos Opinion

BUSINESS

Last updated November 24, 2008 7:34 p.m. PT

Missing laptop puts Starbucks at risk

Company says

By DAN RICHMAN
P-I REPORTER

Starbucks Co information o

The informati numbers, acc employees.

"We are writ involved a bre was posted a Starbucks sp

"The private including your indication that the private information f said.

Security breach co Consumer Affairs

By **Malcolm MacLachlan**

The state Department employees, contractor that has compromised

The breach occurred o improperly transmitted spokesman Russ Heim titles of everyone on t information.

"The thing that is trou social security number

Hacker compromises data on 11,000 at U. of Indy

HOME PAGE MY TIMES TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

The New York Times

U.S.

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION

POLITICS WASHINGTON EDUCATION

Georgia Patients' Records Exposed on Web for Weeks

By BRENDA GOODMAN
Published: April 11, 2008

ATLANTA — A company hired by the State of [Georgia](#) to administer health benefits for low-income patients is sending letters to notify tens

SIGN IN TO E-MAIL OR SAVE THIS

PRINT

Posledice

- Izguba poslov
- Zmanjšanje zaupanja strank
- Negativno pojavljanje v medijih
- Javna opozorila, globe, tožbe





Ključne vrste podatkov

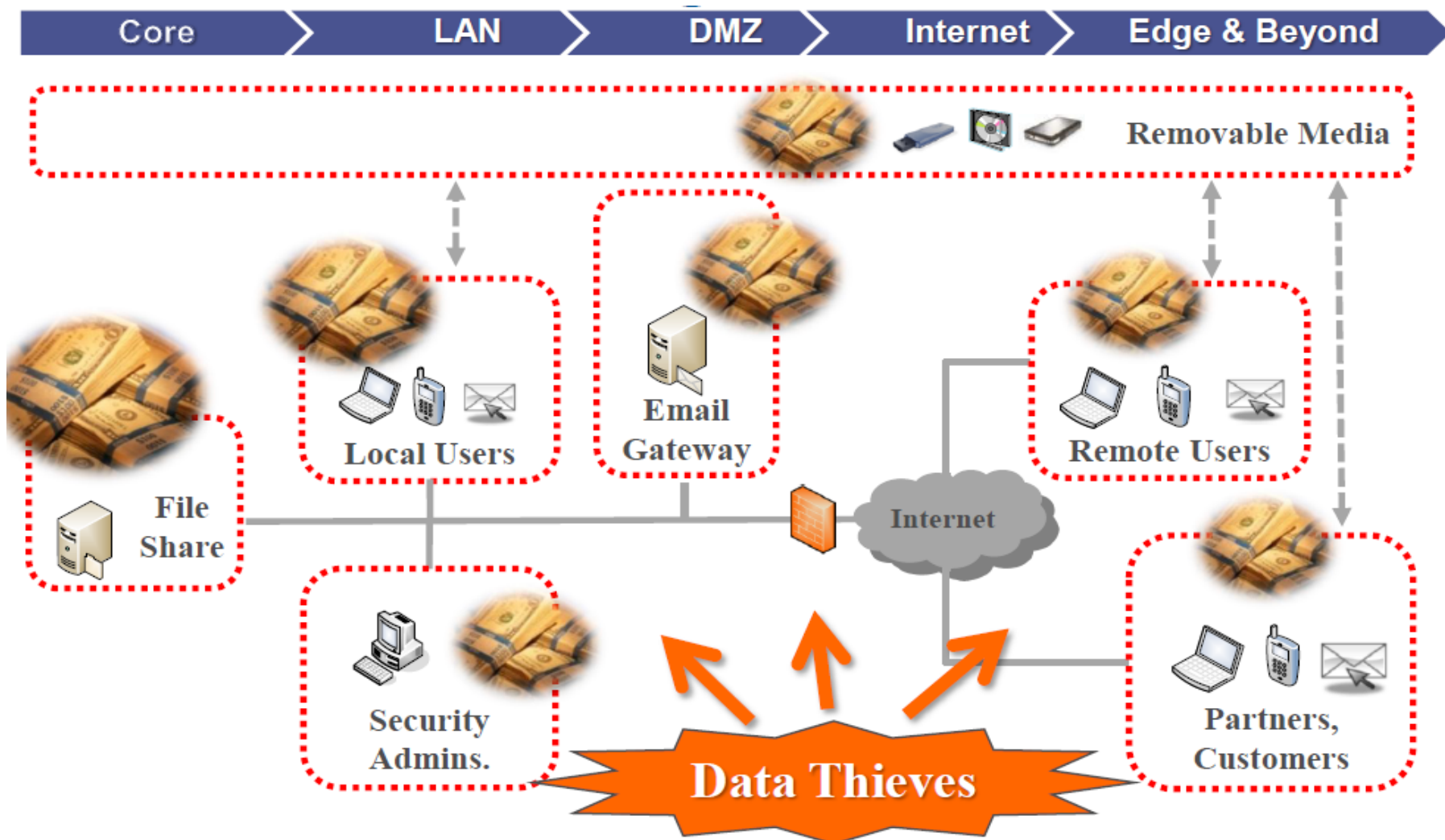
Osebni podatki

Baza strank
Baza zaposlenih
Zdravniške
evidence/kartoteke

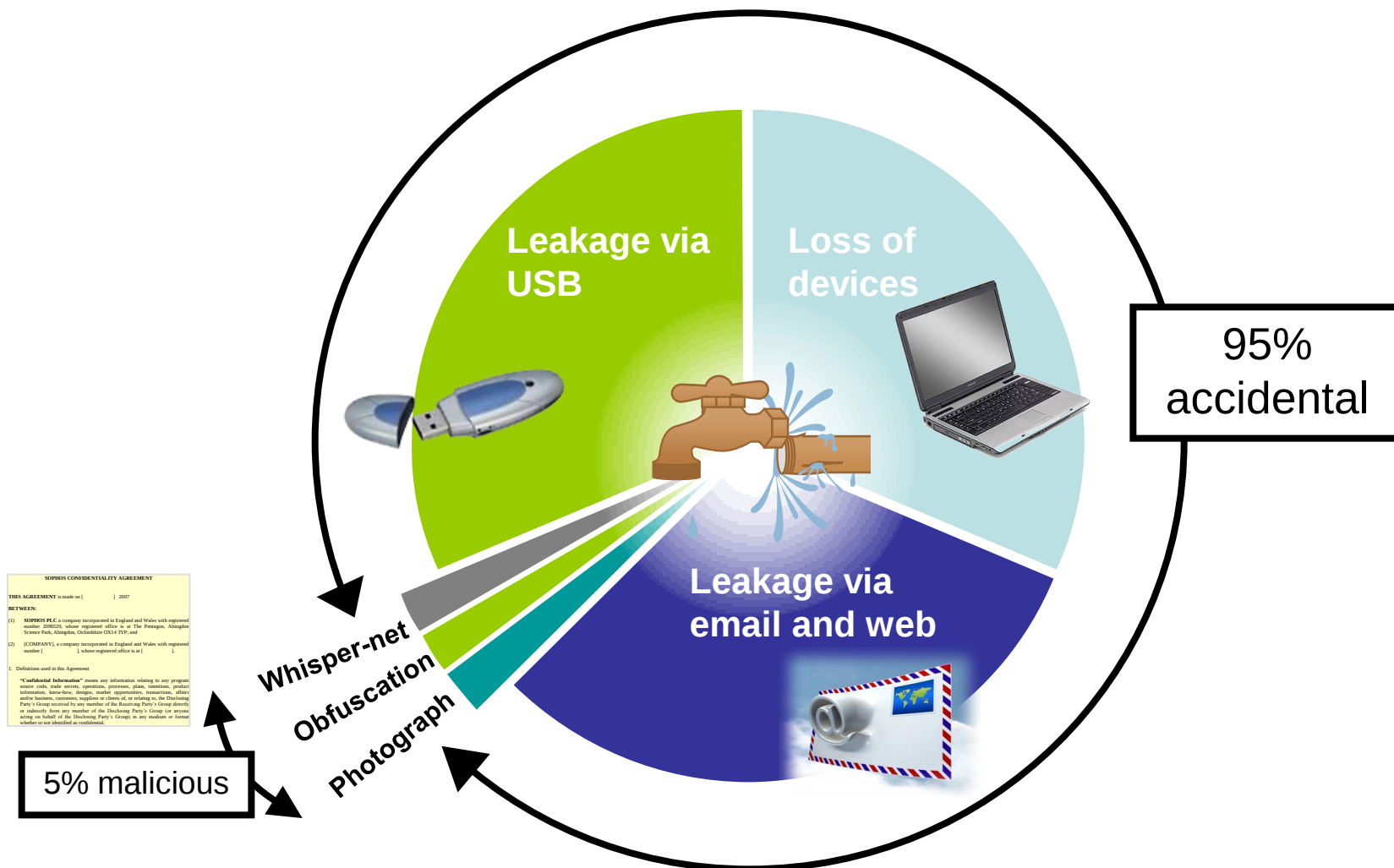
Intelektualna lastnina

Programska koda
“kuharski recepti”
Tehnološki načrti/scheme
Ferrari/McLaren

Poslovne okolje – možna mesta odtekanja informacij



Najpogostejši načini izgube podatkov



Načrt sistema varovanja podatkov - predpriprava

- **Indetifikacija zaupnih/pomembnih podatkov**

- Osebni podatki (strank, zaposlenih...)
- Finančni podatki
- Intelektualna lastnina

- **Določitev projektne skupine – definicija politike**

- IT – skrbniki sistemov / varnost - experti
- Skrbniki podatkovnih baz – razumejo proces
- Pravna služba - mnenja



Načrt sistema varovanja podatkov – določitev podatkov

- **iskanje podatkov v sistemu glede na stanje dosegljivosti**
 - Podatki v uporabi – na sistemih uporabnikov, kopije na USB ključih, podatki na spletnih straneh...
 - Podatki v arhivih – arhivi na sistemih uporabnikov, podatkovni strežniki, email arhivi, SharePoint portali ipd.
 - Komunikacijski podatki: mrežni promet, dostop do podatkovnih baz, VPN, SMTP, HTTP, IM...

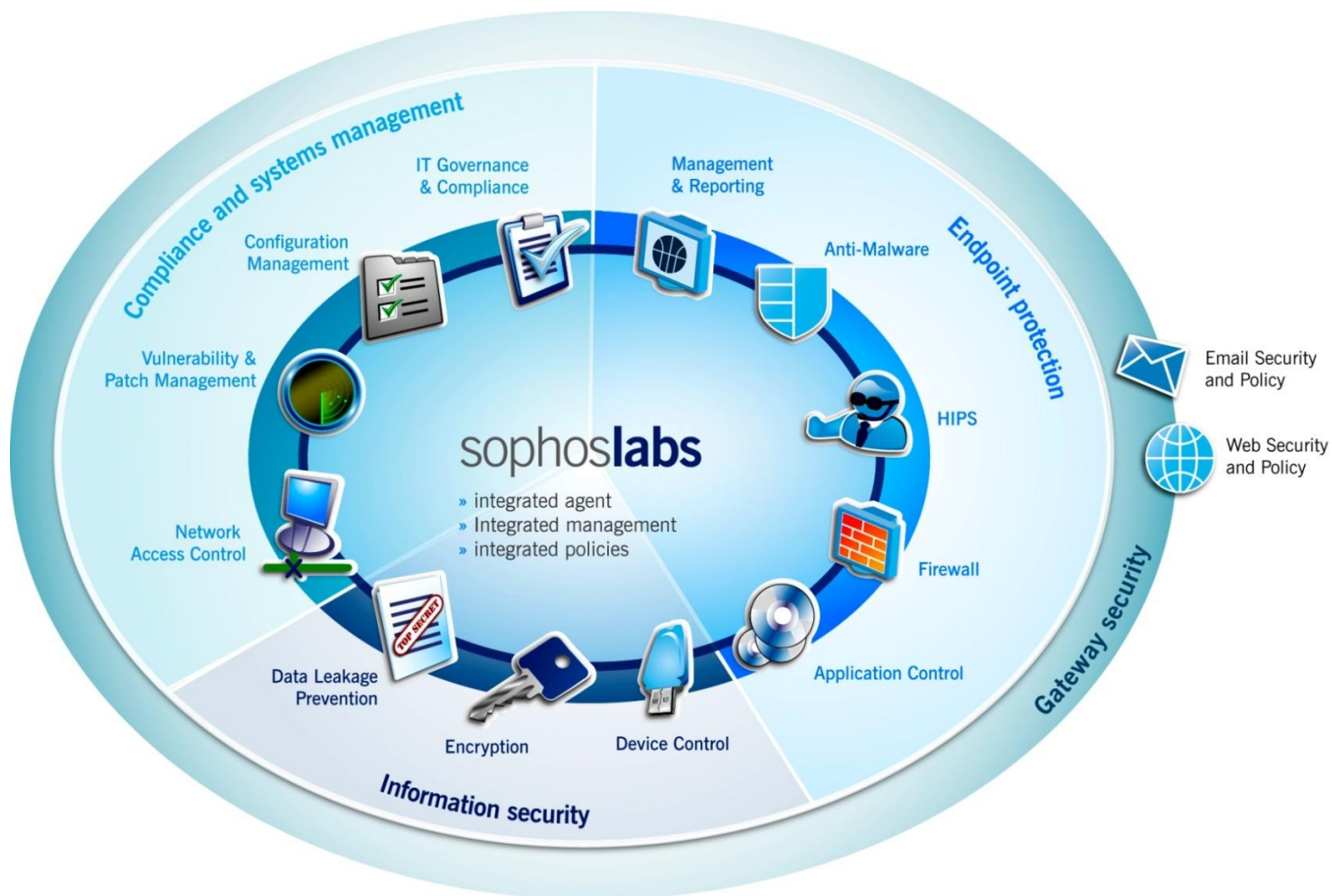


Preventiva – izobraževanje uporabnikov!

- Izdelava varnostne politike ni samo izdelava dokumentacije
- Uporabniki morajo biti vključeni v proces implementacije
- Odgovornost uporabnikov za izgubo podatkov
- izobraževanje:
 - Povečuje razumevanje uporabnikov do varnostne politike
 - Seznanja uporabnika s pričakovanji varnostne politike in njegovo vlogo pri varovanju podatkov



Načini varovanja s pomočjo Sophos rešitev



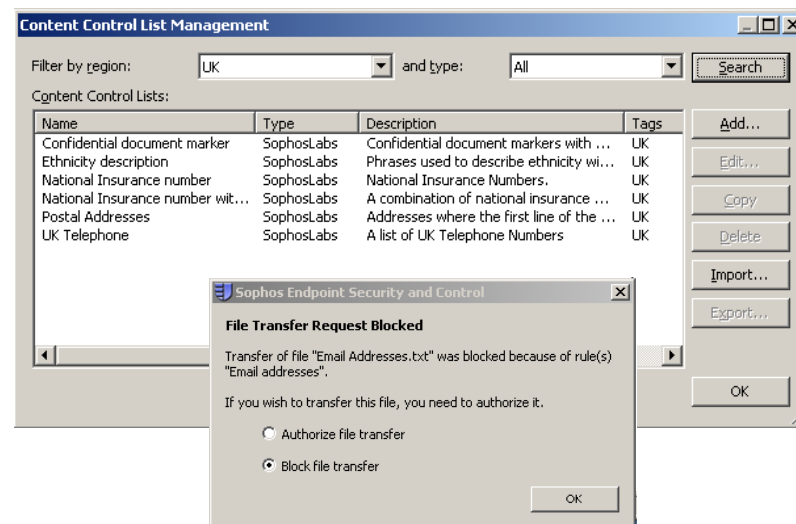
Nadzor vsebine

Področje:

- ✓ Nosilci podatkov: USB ključi, CD, DVD
- ✓ Internet aplikacije: IM, P2P, browsers

Pristop:

- ✓ Pregled vsebine, ki se prenaša na nosilce podatkov ali preko interneta
- ✓ Uporaba podrobnih politik
- ✓ Blokiranje, opozarjanje in poročanje v zvezi s posredovanjem OP



Nadzor vsebine

Edit Rule - Credit or debit card numbers with qualifying terms

1. Rule name:

Credit or debit card numbers with qualifying terms

2. Rule description (optional):

Identify documents containing over ten credit or debit

3. Select the rule's conditions:

- ☒ Where the file contains
- ☒ Where the destination is

4. Select the action to take if the rule is matched (all actions are performed):

- ☒ Allow file transfer
- ☐ Allow transfer on acceptance by user
- ☐ Block transfer

5. Select files to exclude:

- ☐ Where file name matches
- ☐ Where the file type is

6. Rule content:

For any file
where the file contains:

[10 or more matches](#) of Credit or debit card numbers with qualifying terms [Global],
and where the destination is
[Removable Storage](#)
[or Optical Drive](#)
[or Floppy Drive](#),
Allow file transfer.

Content Control List Management

Filter by region:

Global

and type:

All

Search

Content Control Lists:

Name	Source	Description
☐ Bank account details ...	SophosLabs	Bank account detail...
☐ Bank routing numbers...	SophosLabs	A combination of ba...
☐ Confidential documen...	SophosLabs	Confidential docum...
☐ Credit and debit card ...	SophosLabs	Credit and debit car...
☒ Credit or debit card n...	SophosLabs	A combination of cr...
☐ Credit or debit numbe...	SophosLabs	Credit or debit card...
☐ Email addresses [Global]	SophosLabs	Email address format...
☐ International Bank Ac...	SophosLabs	International Bank ...
☐ National identification...	SophosLabs	National identity or ...
☐ National identification...	SophosLabs	National identificati...

OK

File transfer blocked by Sophos

Transfer of file "test.txt" was blocked because of rule(s) "test file match".



Nadzor vsebine - Email

Advanced Data Control:

- ✓ “out-of-the-box” nastavitve politik za nadzor vsebine kot na endpoint klientu
- ✓ Uvoz lastnih politik iz EC



Advanced data control for Email Appliances



Nadzor vsebine - Web

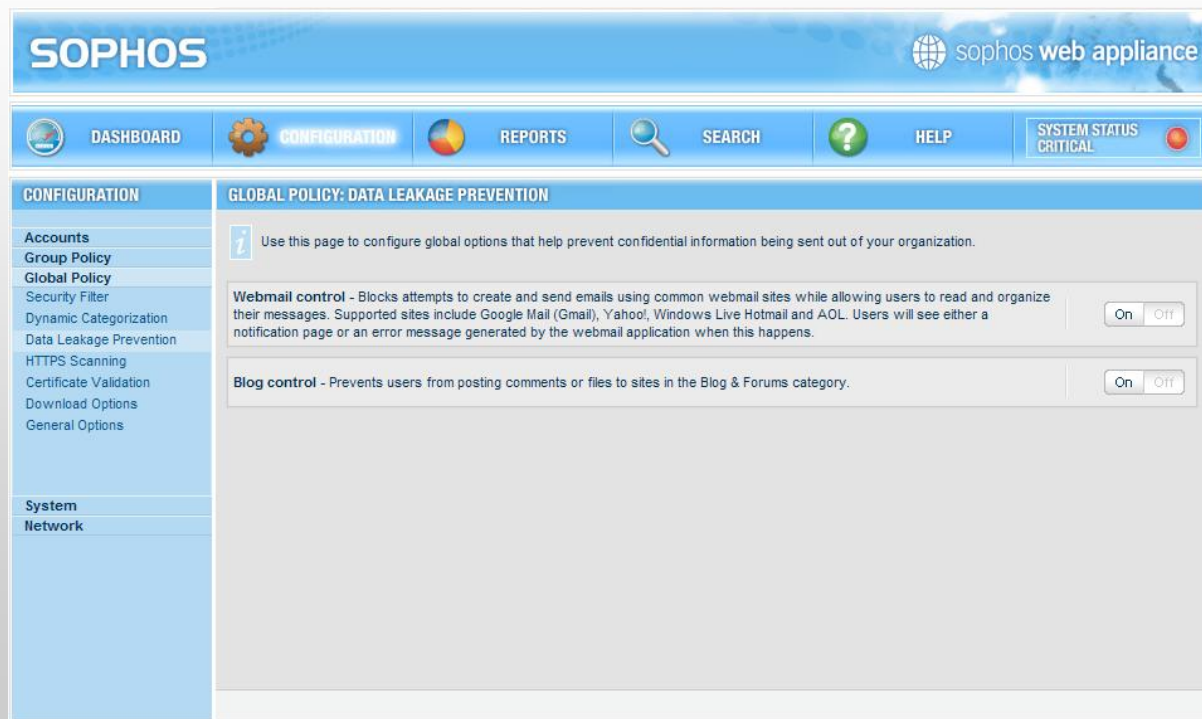


Outbound Content Control

- Allows reading/viewing but prohibits posting/sending
- Ensures sensitive data cannot leave the organization

Categories controlled:

- Blogs
- Forums
- Webmail
 - Gmail, Yahoo, Hotmail, AOL
 - Generic HTML webmail systems



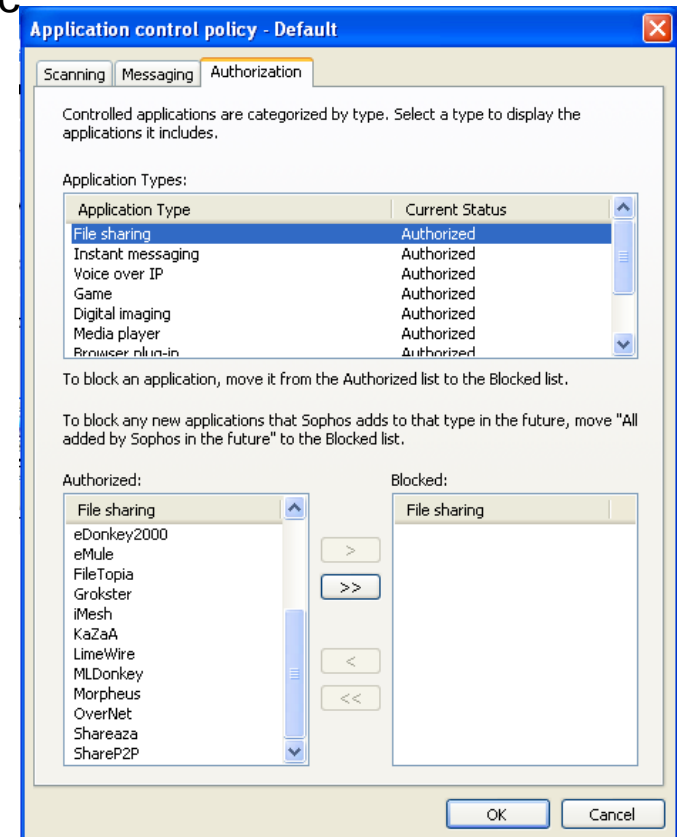
Nadzor nad uporabo nezaželenih aplikacij

Področje:

- ✓ P2P; IM clients; web browsers; mobile sync
- ✓ proxies; security tools
- ✓ remote management, virtualization tools
- ✓ Web 2.0: Facebook, Google docs

Pristop:

- ✓ Allow list – only allow authorized applications
- ✓ Block list – block specific categories of applications



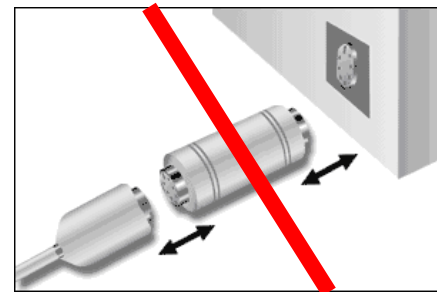
Nadzor priključenih naprav

Področje:

- ✓ Izmenjivi nosilci(USB ključ, removable drives)
- ✓ Optical media (CD/DVD)
- ✓ Diski
- ✓ Mobilne naprave
- ✓ Modemi

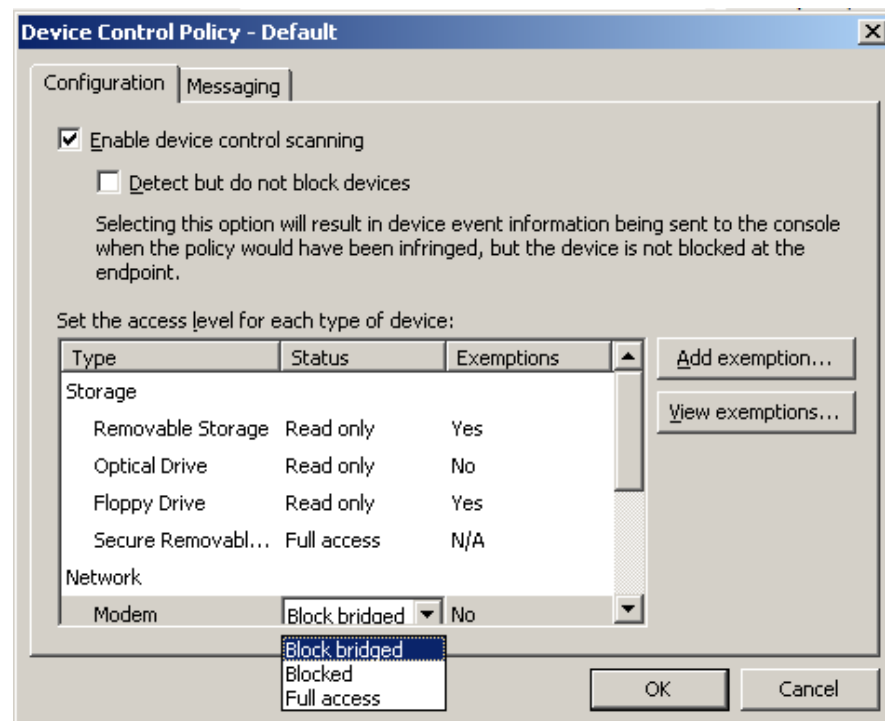
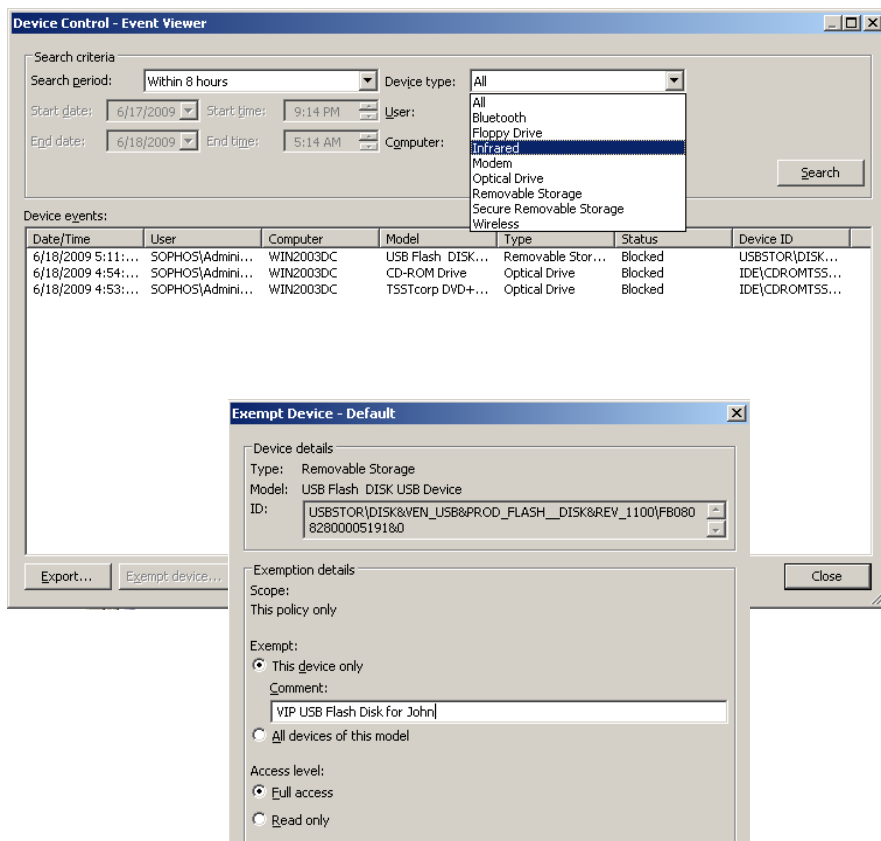
Pristop:

- ✓ Izjeme za individualne naprave
- ✓ Dovoljena raba kriptiranih naprav / ostalo blokirano
- ✓ Dovoljen read-only dostop





Nadzor priključenih naprav



Kriptiranje podatkov

Področje:

- ✓ Nenamerna izguba naprav/nosilcev podatkov
- ✓ Nezaščitena komunikacija

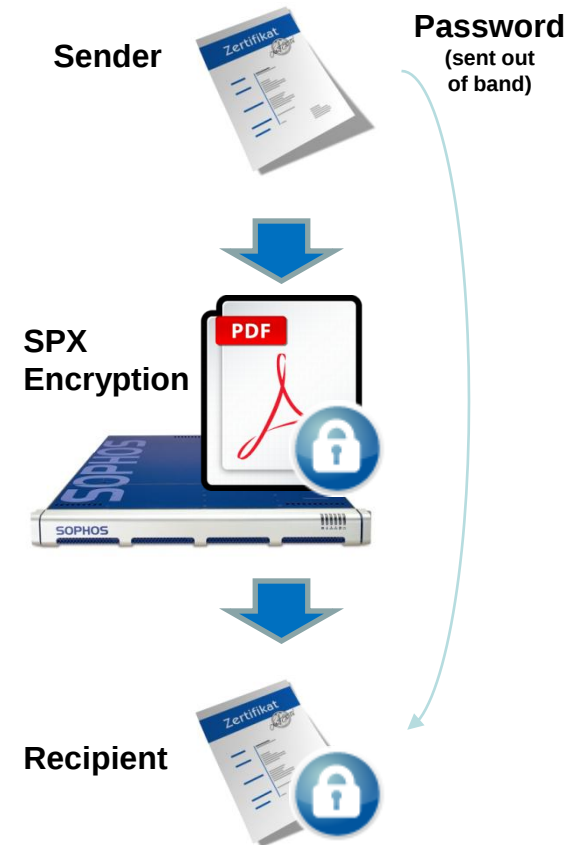
Pristop:

- ✓ Full disk encryption
- ✓ USB, CD and removable media encryption
- ✓ Policy based email encryption
- ✓ Central key management and back up
- ✓ Ability to audit encryption status



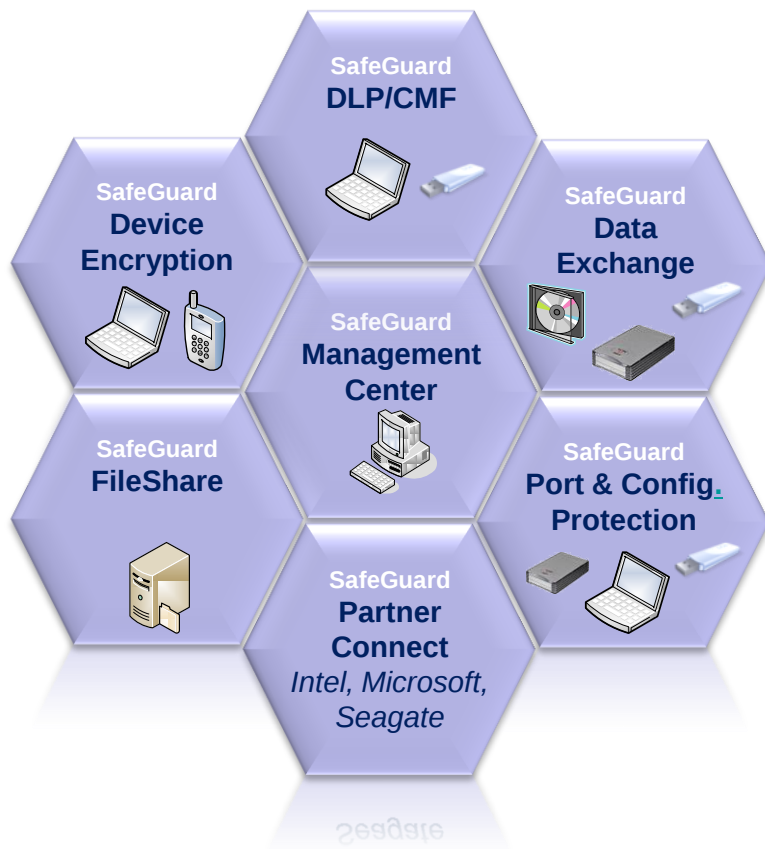
Email Security and Data Protection

- Sender
 - Sends email through their normal email client as usual
 - Sends password out-of-band
- Sophos Email Appliance with SPX Encryption
 - Policy determines encryption requirements
 - Email/Attachments encrypted into a PDF container
 - Password returned to sender
- Receiver
 - Receives email with encrypted PDF attachment
 - Opens/views by entering supplied password
 - Responds by clicking a link in the email





SafeGuard Enterprise





Sophos rešitve

Endpoint Security and Control 9

SES&C Client 9

Anti-Malware, HIPS
Anti-Spyware/Adware
Application control
Device control
Data control

Enterprise
Console

Sophos Client
Firewall

Sophos NAC

Sophos Mobile
Security

Endpoint Security and Data Protection 9

Endpoint
Security
and
Control

SafeGuard
Disk Encryption

SafeGuard
PrivateCrypto

SafeGuard Enterprise 5

SafeGuard
Management
Center

Device
Encryption

Data
Exchange

Configuration
Protection

Bitlocker client



Vprašanja