symantec™

Confidence in a connected world.

Az adatszivárgás megelőzése

Global Intelligence Network

Identifies more threats + takes action faster + prevents impact

Worldwide Coverage | **Global Scope and Scale** | 24x7 Event Logging

Rapid Detection

Attack Activity
- 240,000 sensors
- 200+ countries

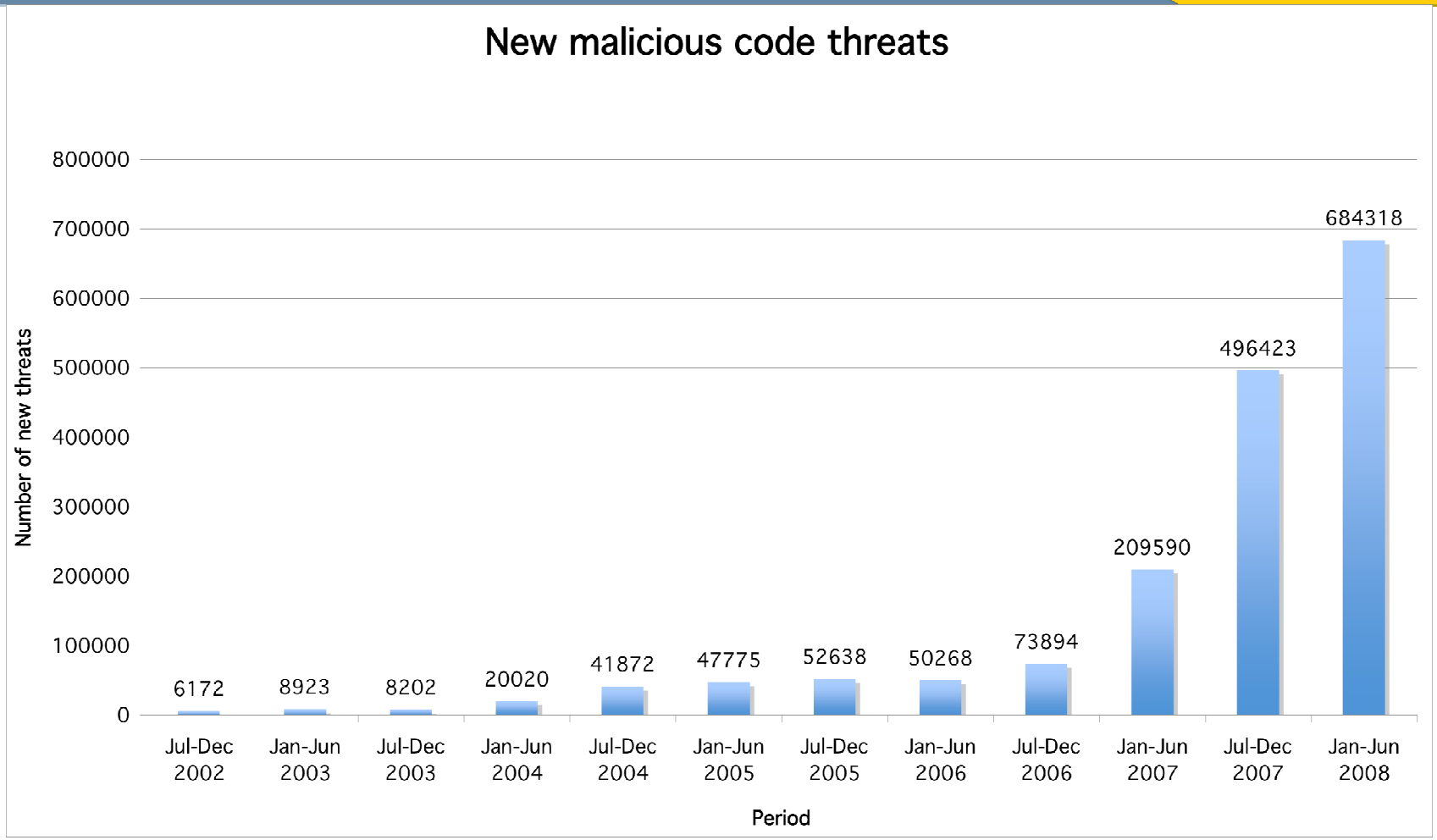
Malcode Intelligence
- 130M client, server, gateways
- Global coverage

Vulnerabilities
- 32,000+ vulnerabilities
- 11,000 vendors
- 72,000 technologies

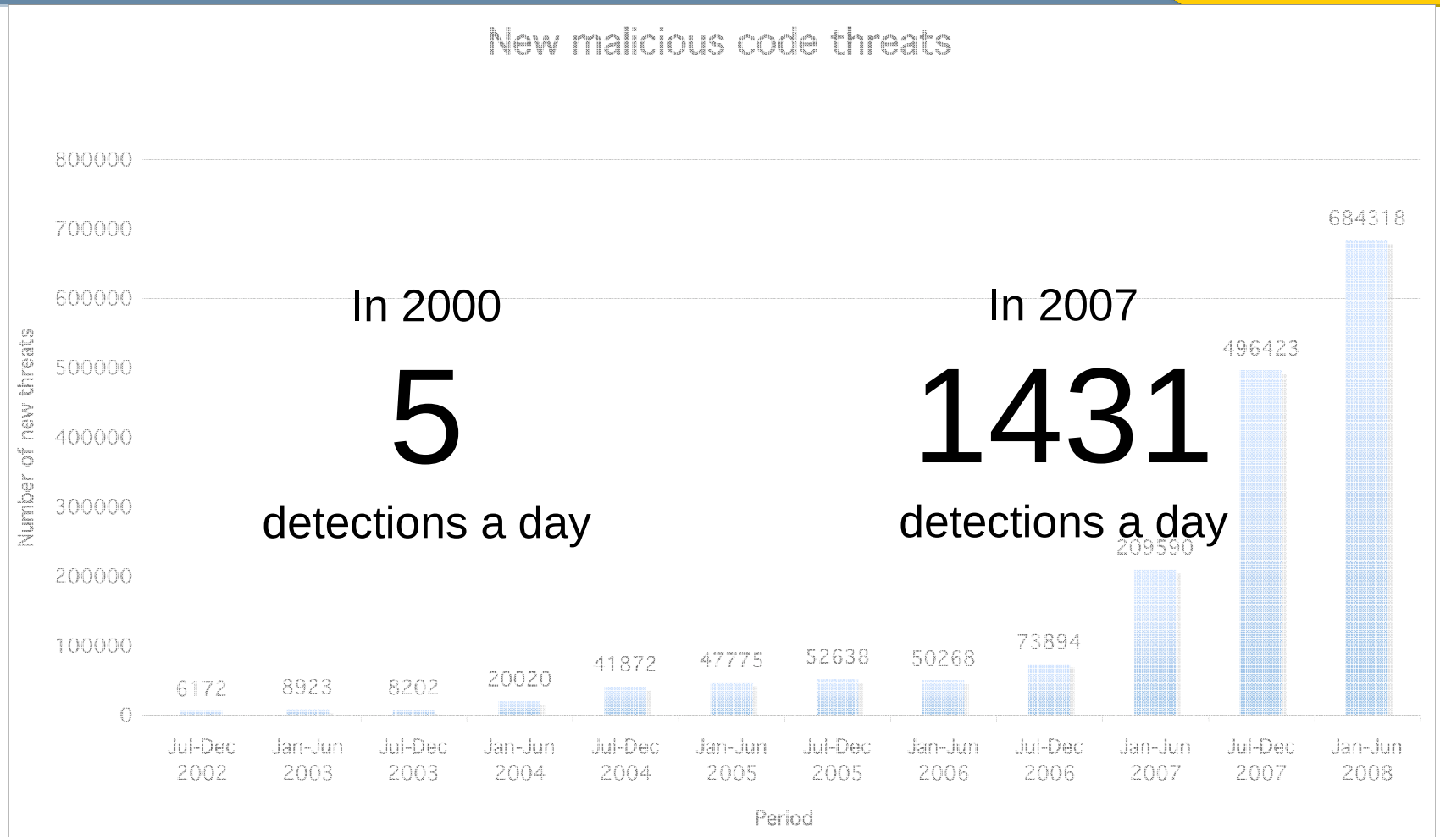
Spam/Phishing
- 2.5M decoy accounts
- 8B+ email messages/daily
- 1B+ web requests/daily

Preemptive Security Alerts | **Information Protection** | Threat Triggered Actions

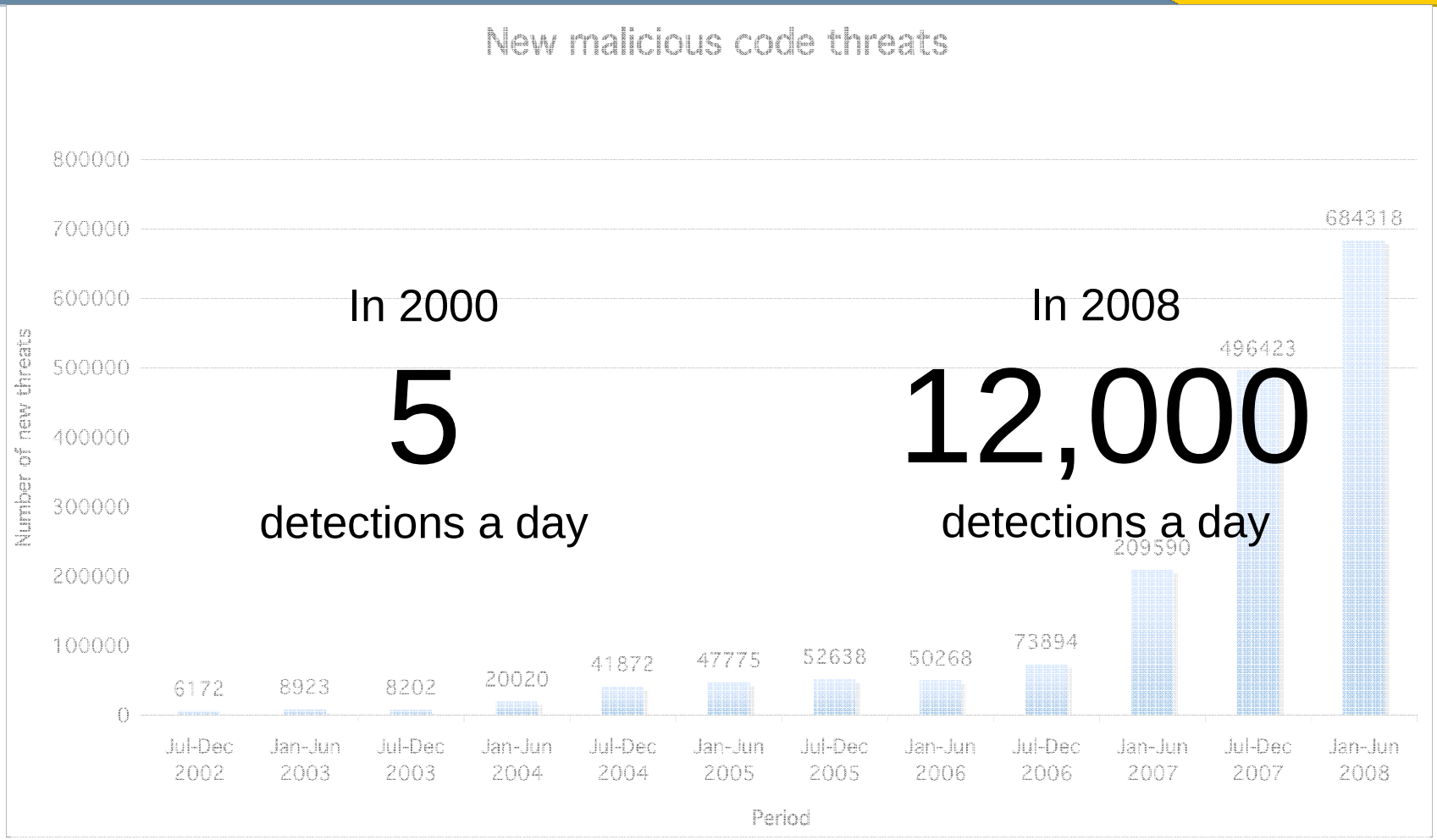
Malware Explosion



Malware Explosion

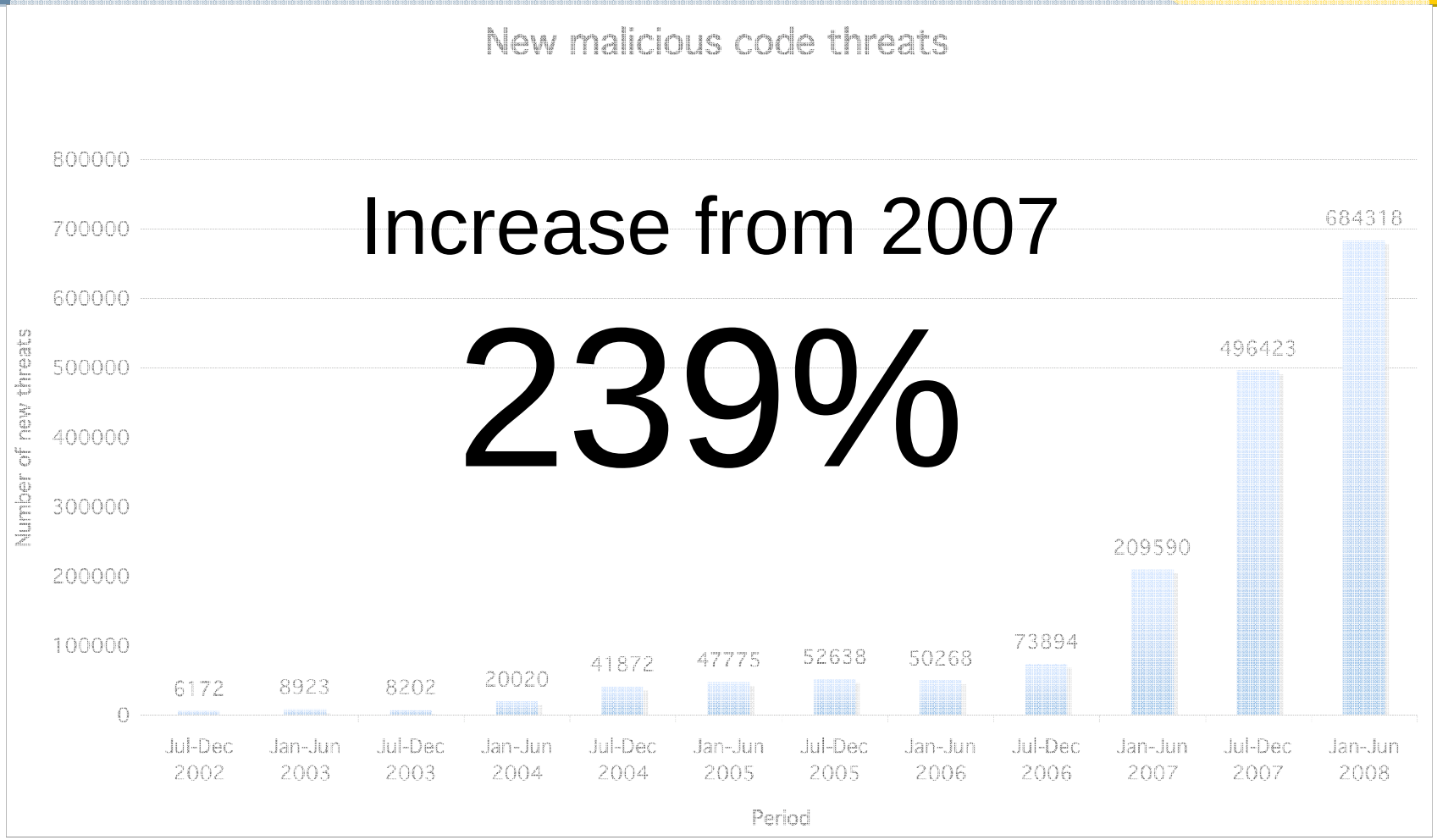


Malware Explosion



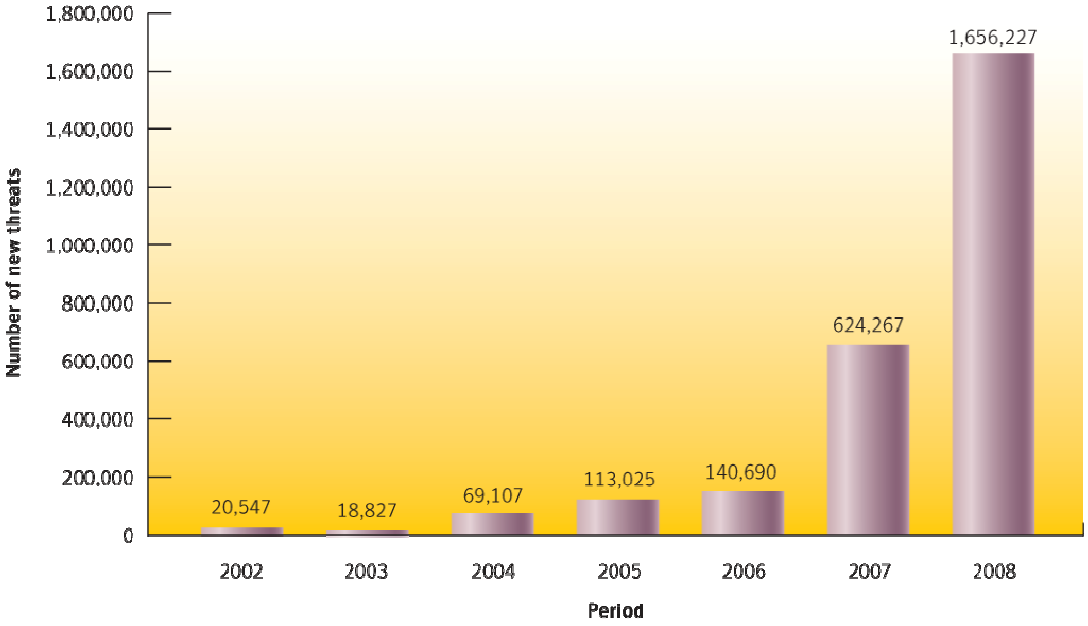
Malware Explosion

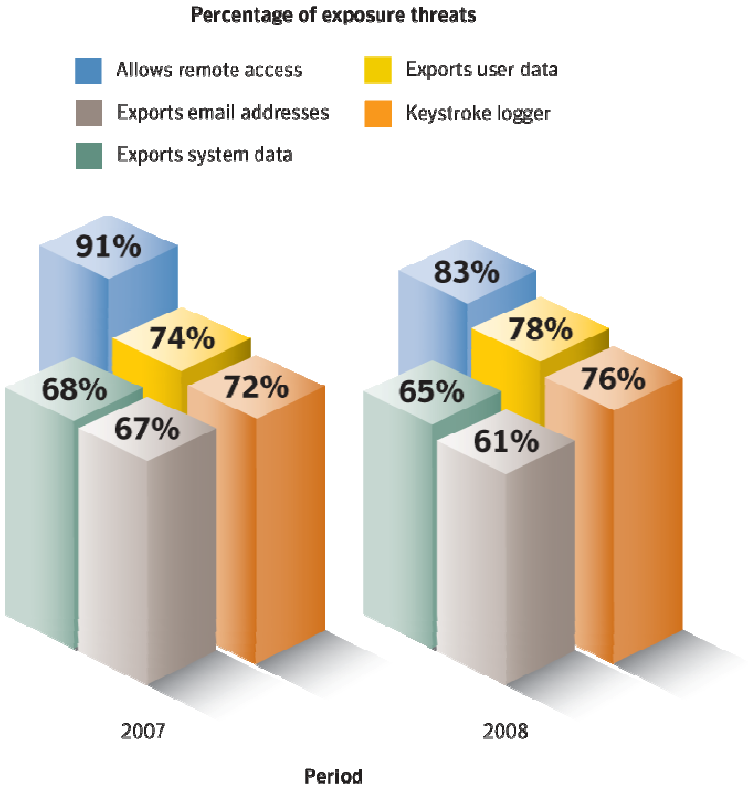
Malware Explosion



Malicious code is installed

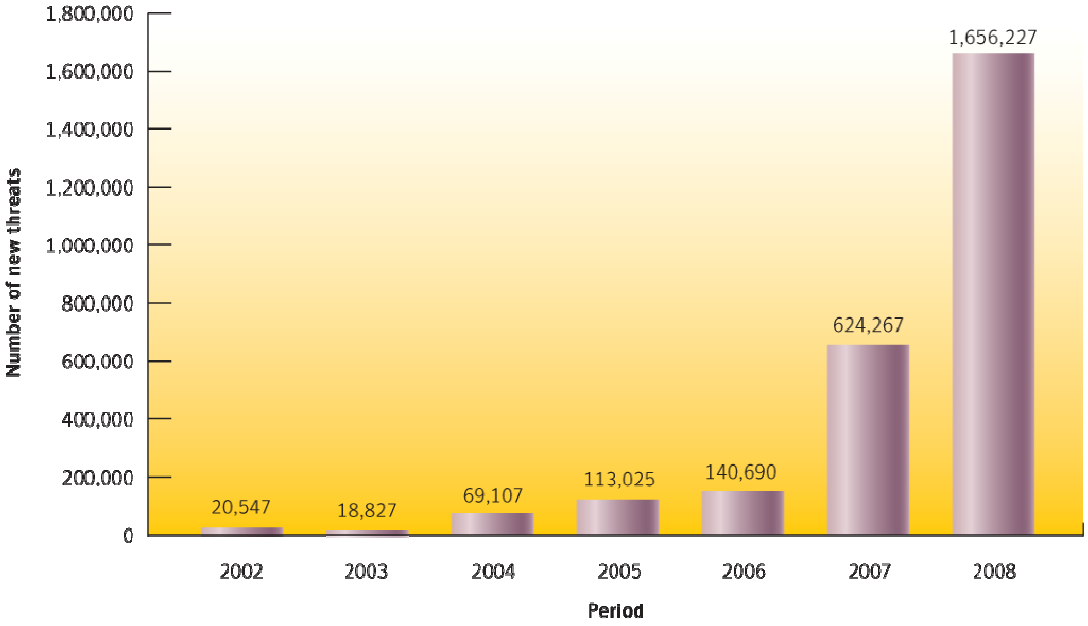
- 245 000 000 károkozó havonta
- 60%-a 2008-ban keletkezett
- 90% adatlopásra kihegyezve ...

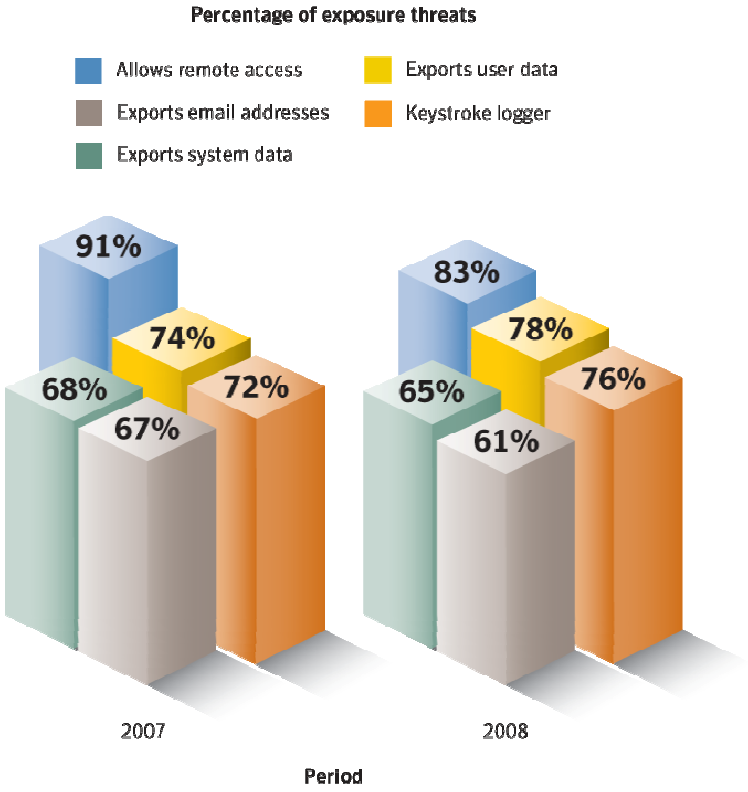




Malicious code is installed

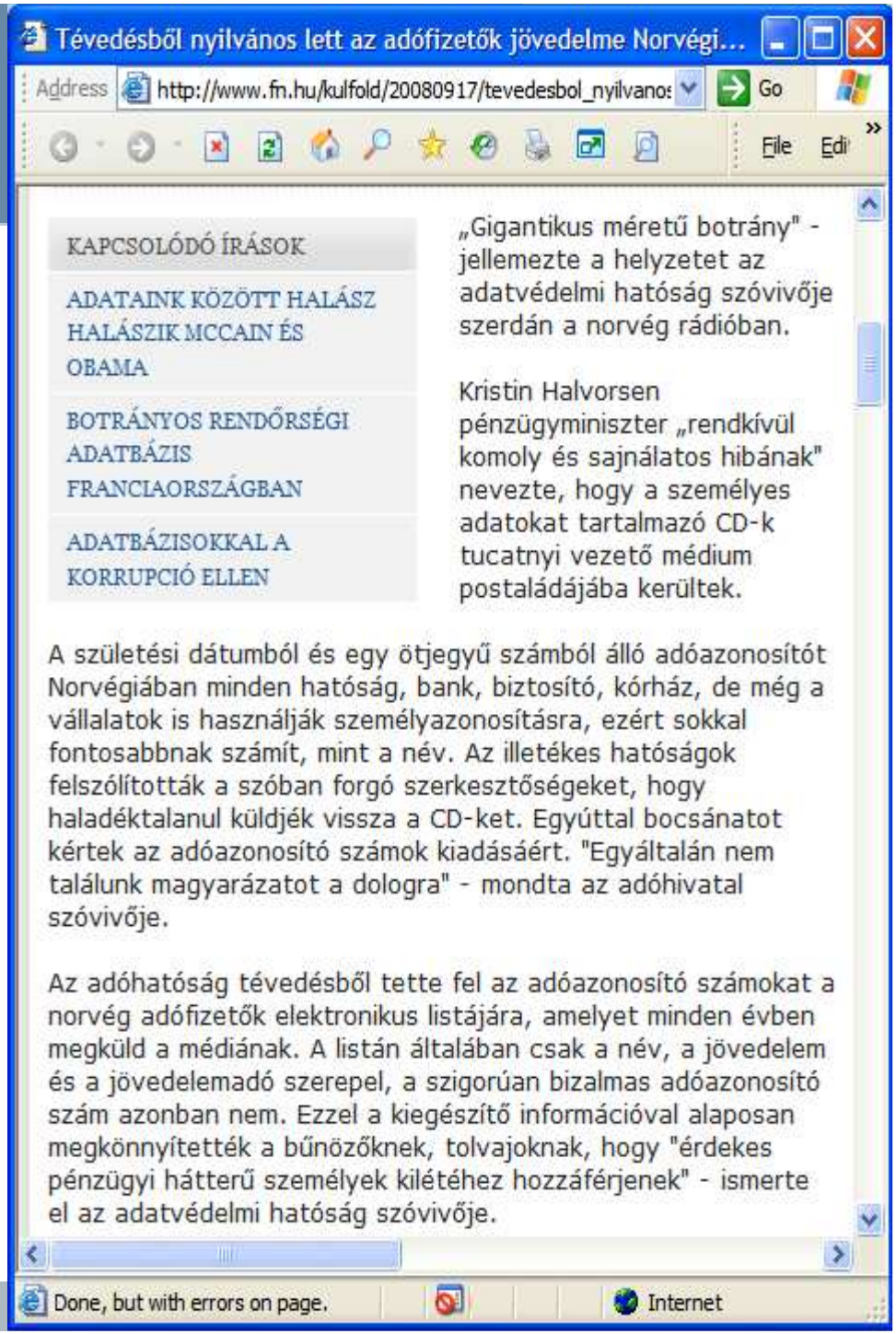
- 245 000 000 károkozó havonta
- 60%-a 2008-ban keletkezett
- 90% adatlopásra kihegyezve ...



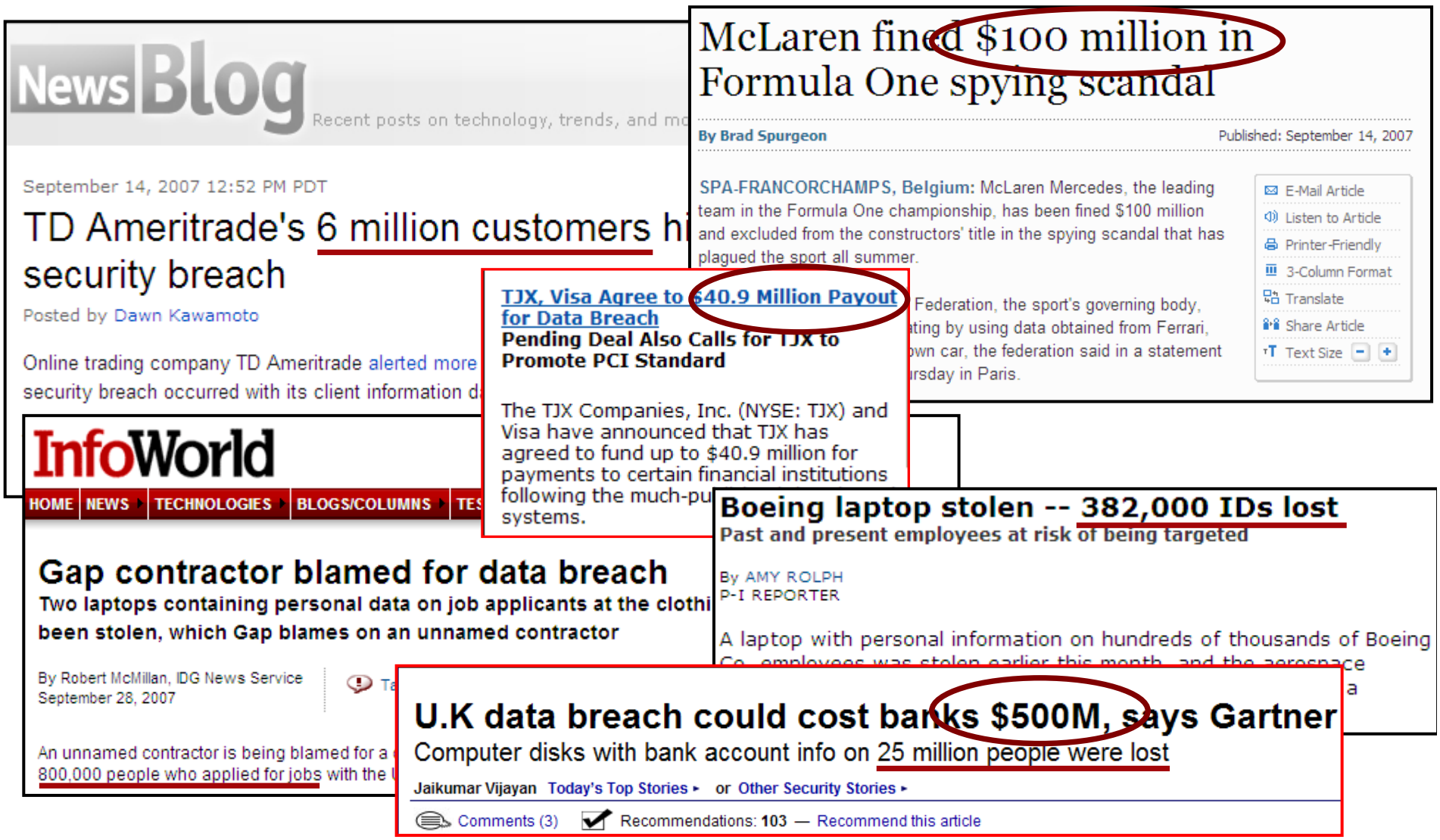


Tévedésből nyilvános lett az adófizetők jövedelme Norvégiában

- Adatbotrány borzolja a kedélyeket Norvégiában: az adóhatóság mind a négymillió adófizető azonosítására alkalmas személyes információkat, beleértve jövedelmüket is, tévedésből vezető újságok szerkesztőségeibe postázta.



Adatlopás, betörés: valóság

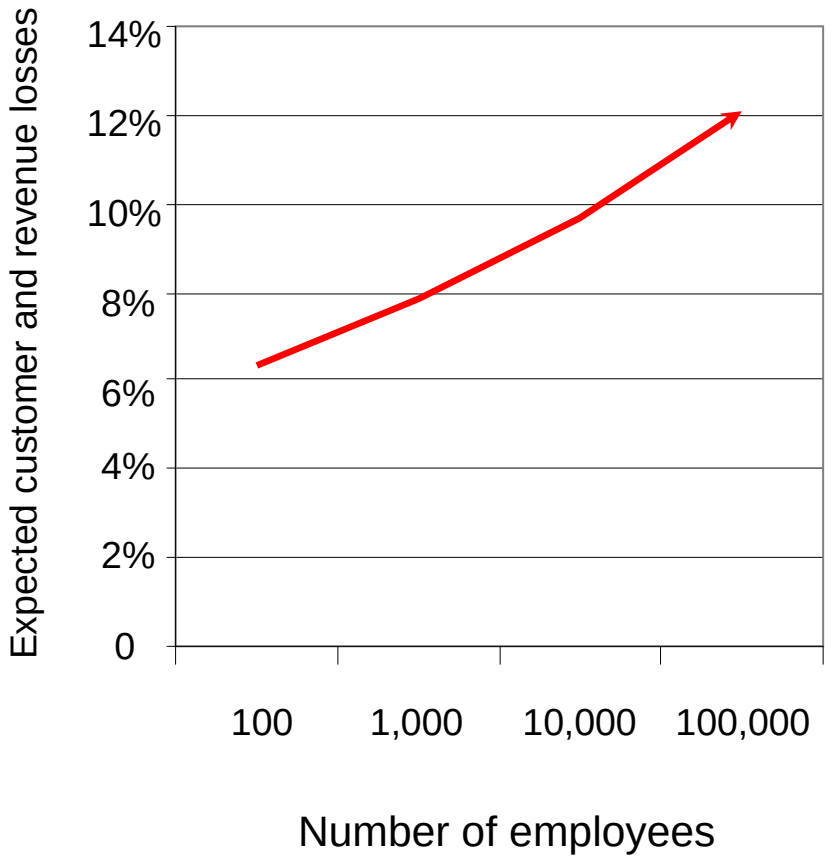


„Tegnap történt”

… és a betörések költségesek

Közvetett és közvetlen költségek a nyilvánosan jelentett adat betörések kapcsán

- Kárelhárítási folyamat költsége $100 - 300 elveszített személyes adatként*
  - Felhasználó értesítése
  - Hitel monitorozás
  - Rendszer helyreállítás
  - Nyomozati költségek
  - Audit költségek
  - Hitelkártyák letiltása, újabbak készítése
- Jelentős közvetett költségek*
  - A márka értékének, piacnak illetve a felhasználók bizalmának vesztése.
  - Jogi eljárások, bírság
  - Részvény vagy árbevétel csökkenése



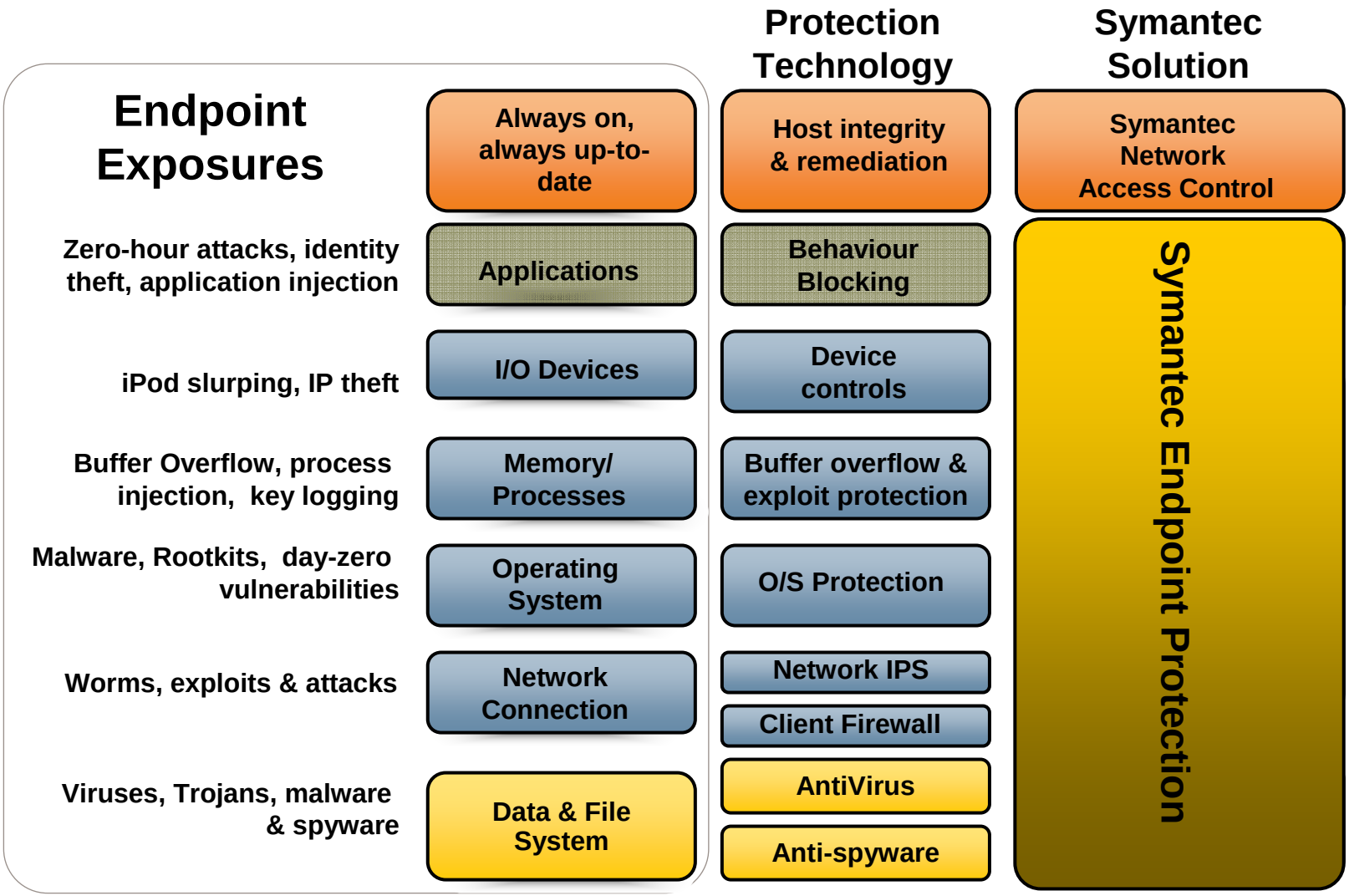
*July 2007, IT Policy Compliance Group

Az adatvesztés, -szivárgás növekvő aggodalmat szül.

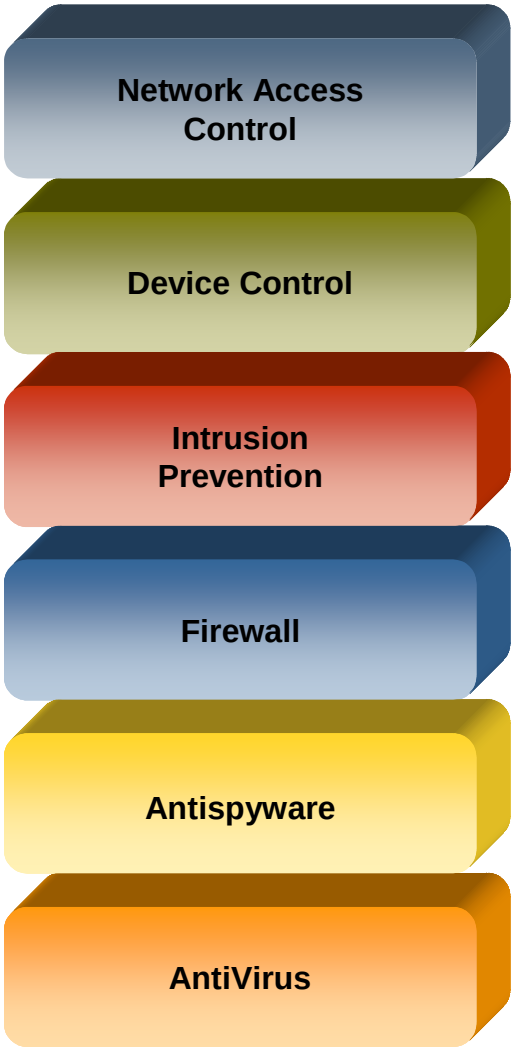
A biztonsági vezetők TOP gondjai

- 52% of CISOs gondolja hogy DLP meghatározó, markáns eleme lesz a biztonsági büdzsének[1]
- 85% jelentett legalább egy olyan biztonsági eseményt, incidenst, amely adatszivárgással összefüggő volt – tavaly[2]
  - 63% esetében észleltek 6-20 biztonsági esemény, ami személyes információkat is érintett.
- 216 millió személyes adatot ért támadás 2005 óta
- 2007-ben az incidenesek következtében 6.3mrd dollár költség keletkezett – 2006-ban ez 4.8 mrd volt ...
- az esetek 40%-ában a betörés „kiváltója” 3. fél, -vállalat, szervezet, outsource vagy szerződött partner.[3]

Anatomy of Layered Endpoint Protection



Symantec Endpoint Protection 11



- A kliens program „NAC Ready”
- Compliance funkciót biztosít a végpontok számára

- Device control megakadályozza az adatszivárgást
- Védelmet nyújt mp3 lejátszók, USB tárolók, stb

- Viselkedési mintán alapuló IPS funkció
- A hálózati forgalom analizálása védelmet nyújt a sérlükénységek ellenen

- Iparág legjobb és legjobban menedzselhető tűzfala.
- „Location Awareness” szabályrendszer, automatikus felismeréssel és alkalmazott szabályrendszerrel

- Best anti-spyware, kiváló rootkit felismerés és eltávolítás
- VxMS scanning technology (Veritas) – Raw disk scan

- A világ vezető antivirus megoldása
- A gyártók közül a legtöbb folytonos Virus Bulletin minősítéssel rendelkezik (41) - 1999 óta egyetlen teszten sem hibázott

Ponemon Survey

Adobe Acrobat Document

Ponemon – DLP Survey

Milyen tipusú bizalmas, fontos vállalati adatokat, információkat tartott meg miután elhagyta a vállalatot.	Total%
Email cimlisták	65%
Nem pénzügyi üzleti információk	45%
Ügyfél információ, beleértve kontakt info	39%
Dolgozói adatok	35%
Pénzügyi adatok	16%
Más	1%

Engedélyezte a munkadója hogy ezeket a fontos, bizalmas adatokat megtartsa, birtokolja?	Pct%
Igen	16%
Nem	79%
Nem biztos	5%
Total	100%

Ponemon – DLP Survey

Milyen elektronikus vagy papir alapú információt tartott meg miután elhagyta a vállalatot	Total%
Elektronikus levelezés, archive is	64%
Nyomtatott dokumentációkat	62%
Word vagy más word alapú dokumentumok.	48%
Digitális fotók, jpeg, gif állományok	41%
Excel vagy más táblázatok, dokumentumok.	39%
Szoftverek, segédpogramok	32%
Vállalati adatbázisok extractja vagy dumpja	16%
PowerPoint vagy hasonló dokumentációk	13%
PDF állományok	9%
Access vagy hasonló adatbázisok	8%
Forráskód	3%
Egyéb	3%
Total	338%

Ponemon – DLP Survey

Hogyan juttatta ki a fontos, bizalmas vállalati adatokat a volt vállalatának rendszereiből vagy hálózatából.	Total%
Elvitette a papirokat vagy mappákat	61%
CD/DVD médiára rögzítette	53%
USB memory stick-re töltötte le	42%
A dokumentumokat mellékletként a privát email cimére küldte	38%
Elhatározta, hogy nem törli azokat, amelyek az otthoni gépén találhatóak már.	35%
Más hordoható eszközre továbbította (PDA, Blackberry, iPod, telefon vagy más mobile device)	28%
Megtartotta a vállalati gépet, notebookot vagy egyéb hordozható eszközt	13%
Az adatokat Zip drive-ra töltötte	3%
Más módon	2%
Total	273%

Ponemon – DLP Survey

Q5c. Ugy érzi, hogy helyes ezeket az információkat megtartani?	Total%
Mindenki más megtartotta ezeket az információkat	54%
Ezek az információkat hasznosak a jövöm szempontjából	53%
Eszköz voltam az információk létrehozásában	52%
Munkaadóm nem tudja megállapítani hogy én voltam …	49%
A vállalat nem érdemli meg ezeket az információkat	47%
Nincs különösebb okom	39%
Az információ az enyém, megtartom	34%
Az információ nem értékes a vállalat számára	33%
Véletlen “baleset volt” (elvinni)	13%
Total	375%

Ponemon – DLP Survey

Q8a. Sikerült új állást találnia?	Pct%
Igen	69%
Nem	31%
Total	100%

Q8b. Használt fel az előző munkahelye fontos, bizalmas információból, anyagaiból hogy az új munkahelyen megrősítse pozicióját?	Pct%
Igen	67%
Nem	33%
Total	100%

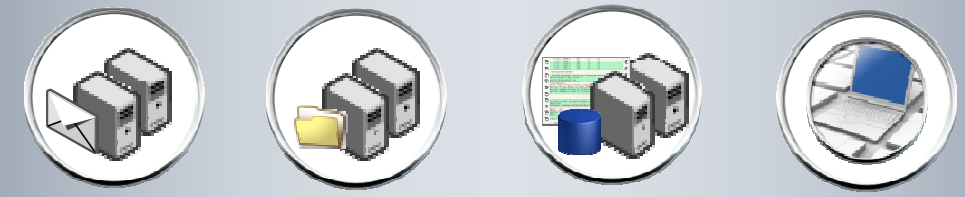
Q8d. Milyen jellegű információkat, adatokat használt vagy tervez felhasználni az előző munkadó tulajdonából ?	Pct%
Email listák	63%
Felhasználói adatok, kapcsolattartók információi	39%
Dolgozói adatok	34%
Szoftverek	32%
Nem pénzügyi üzleti információk	28%
Más szellemi vagyon	5%
egyéb	3%
Forráskód	2%
Pénzügyi információk	1%
Total	207%

Ponemon – Kulcs megállapítások

- A kérdőivre válaszolók 53%-a töltött le információt CD-re vagy DVD-re. 42% USB drive-ra és 38% küldte csatolt állományként a saját email címére.
- 79%-a válaszolóknak vitt el adatot a munkaadó engedélye nélkül.
- 82%-a válaszolóknak állítja, hogy munkaadóik nem auditálták vagy ellenőrzték az elektronikus vagy papír alapú dokumentumokat, mielőtt elhagyták a munkahelyeiket
- 24%-uk azután is rendelkezett hozzáféréssel a hálózathoz, számitógéphez hogy már elhagyta a vállalatot.

Information Risk Management

Külső támadás védelem	DLP	Archiválás, tárolás	Elektronikus feltérképezés
1	2	3	4
Tartsd a rosszat kivül	Tartsd meg a fontos dolgokat belül	Komplett info menedzsment	Talád meg könnyedén ha szükség van rá.



Data Loss Prevention - Wikipedia

Data Loss Prevention (**DLP**) is a computer security term referring to systems that **identify, monitor, and protect data** *in use* (e.g., endpoint actions), *data in motion* (e.g., network actions), and *data at rest* (e.g., data storage) **through deep content inspection and with a centralized management framework**.

The systems are designed to detect and prevent the unauthorized use and transmission of confidential information.

It is also referred to by various vendors as Data Leak Prevention, Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) or Extrusion Prevention System by analogy to Intrusion-prevention system.

Adatszivárgás?

- Ráismer a saját vállalatára a példákban, elképzelhető hogy elbocsátott alkalmazottaik hasonló képpen cselekedtek?
- Valóban meg tudja akadályozni az adatok illetéktelen felhasználását; hogyan?
- Biztos benne, hogy alkalmazottai csak azokhoz az információkhoz férnek hozzá, amelyek a munkájukhoz elengedhetetlenül szükségesek?
- A müködő eljárások, munkafolyamatok biztonsági szempontból is megfelelőek, személyes információ nincsen veszélyeztetve

Top 5: Mi a DLP és mi nem az ...

A DLP:

- **Integrált megoldás** mely megelőzi a fontos, bizalmas adatok „elveszítését”, tekintet nélkül azok tárolási helyére vagy használati módjára
- Mély tartalom elemző megoldás, összefüggéseket is vizsgál.
- A teljese vállalati struktrúrára kiterjedő üzleti megoldás amely a felső vezetői kihívásokra is választ adhat
- Az üzletmenetet lehetővé tevő, felszabadító technologia
- Munkavállalók oktatása

A DLP nem:

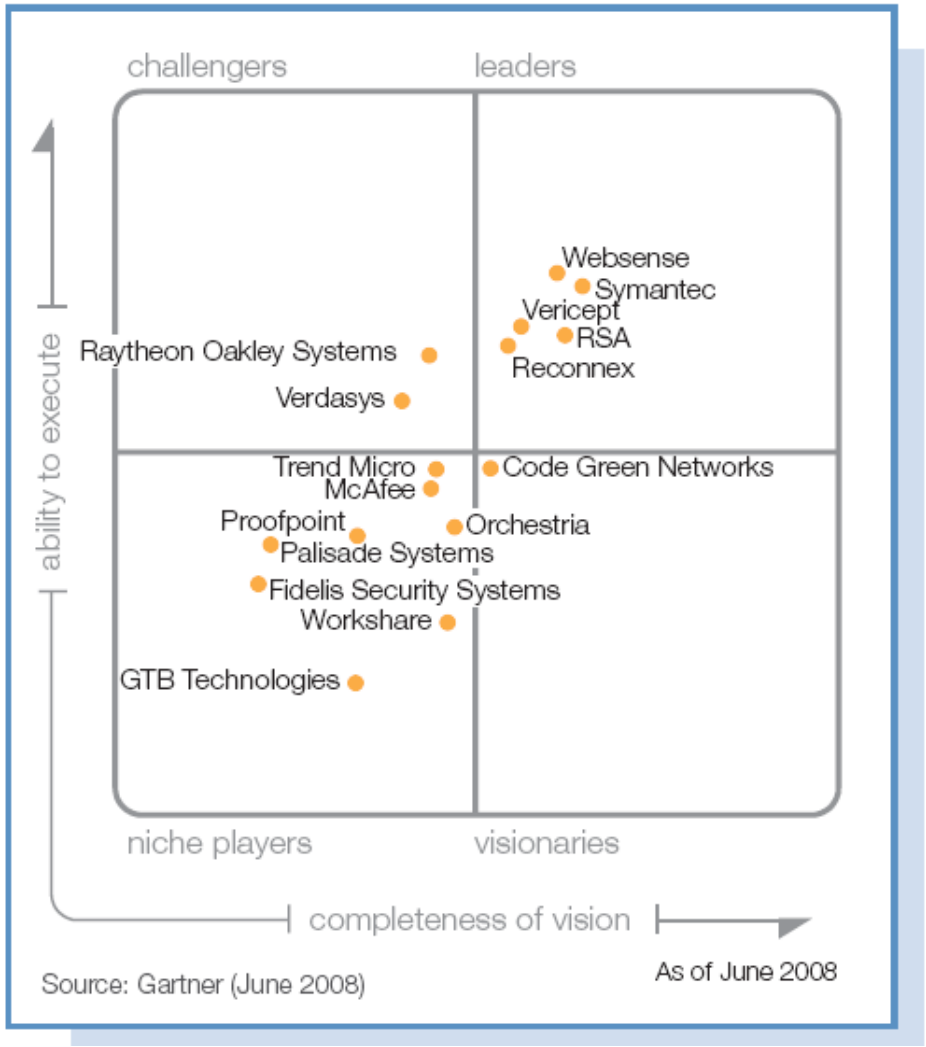
- titkosítás, eszközvezérlő vagy „tartalom vak” megoldás
- Nem központi tároló, amely a fontos adatokat tárolja
- Csak végponti megoldás
- „csak” szabályozói igény
- csodaszer

DLP megoldás


www.StrangeCosmos.com
www.StrangeCosmos.com

Gartner MQ 2008,Jun

Figure 1. Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention



Minden az adatról, az információról szól ...

Felhasználó, Dolgozó Ügyfél adatok

Szabályozói megfelelőség

- Személyi számok
- Bankkártya számok
- Személyes adatok
- Egészségügyi információk

„szellemi tulajdon”

Verseny

- Szoftver forráskód
- Műszaki tervezés, specfikáció
- Gyártási technológia
- árazás

Vállalati bizalmas adatok

Hírnév

- Negyedéves pü. eredmények
- Felvásárlási és egyesülési stratégia
- Vezetők belső levelezése
- Belső kommunikáció

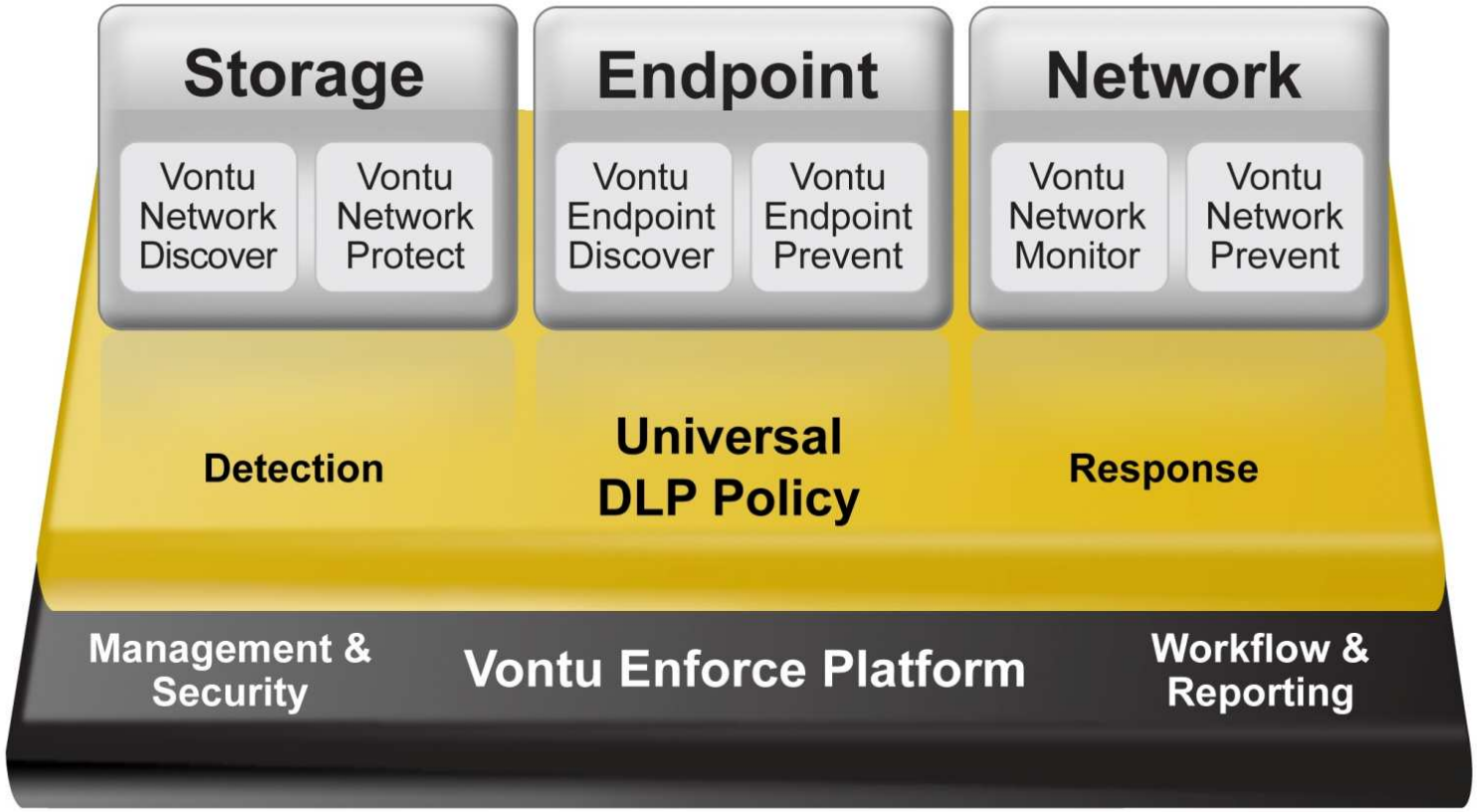
Data Loss Prevention

Felfedez — Hol vannak az értékes információk tárolva?

Felügyel — Hogyan vannak az értékes adatok felhasználva?

Kényszerít — Hogyan tudom megvédeni az értékes adataimat és megelözni elvesztésüket?

Symantec DLP Architectura



Pontos megbizható felismerés az összes adattipuson

Policy

Policy Builder

- Boolean logic
- Response rules
- Best practice policy templates
- Group based policies

Detection Technologies

DCM
Described Content Matching

Described Data

- Non-indexable data
- Lexicons
- Data identifiers

EDM
Exact Data Matching

Structured Data
Customer Data

- Customer/Employee/ Pricing
- 300M+ rows per server
- Partial row matching
- Near perfect accuracy

IDM
Indexed Document Matching

Unstructured Data
Intellectual Property

- Designs/Source/ Financials
- 5M+ docs per server
- Derivative & passage match
- Near perfect accuracy

Minimális false positive

Content

Structured

- PHI
- PII
- Inventory

Unstructured

- Design documents
- Source code
- Media files
- Financial results

Described

- Credit Cards
- SSNs
- Dictionaries
- Keywords

+

Context

People

- Departments
- Partners
- Contractors

Location

- Country
- Department
- Branch office

Language

- European
- Asian

Container

- Document type
- Network protocol
- Encrypted

+

Scale

Volume

- Billions of records
- Millions of documents

Network

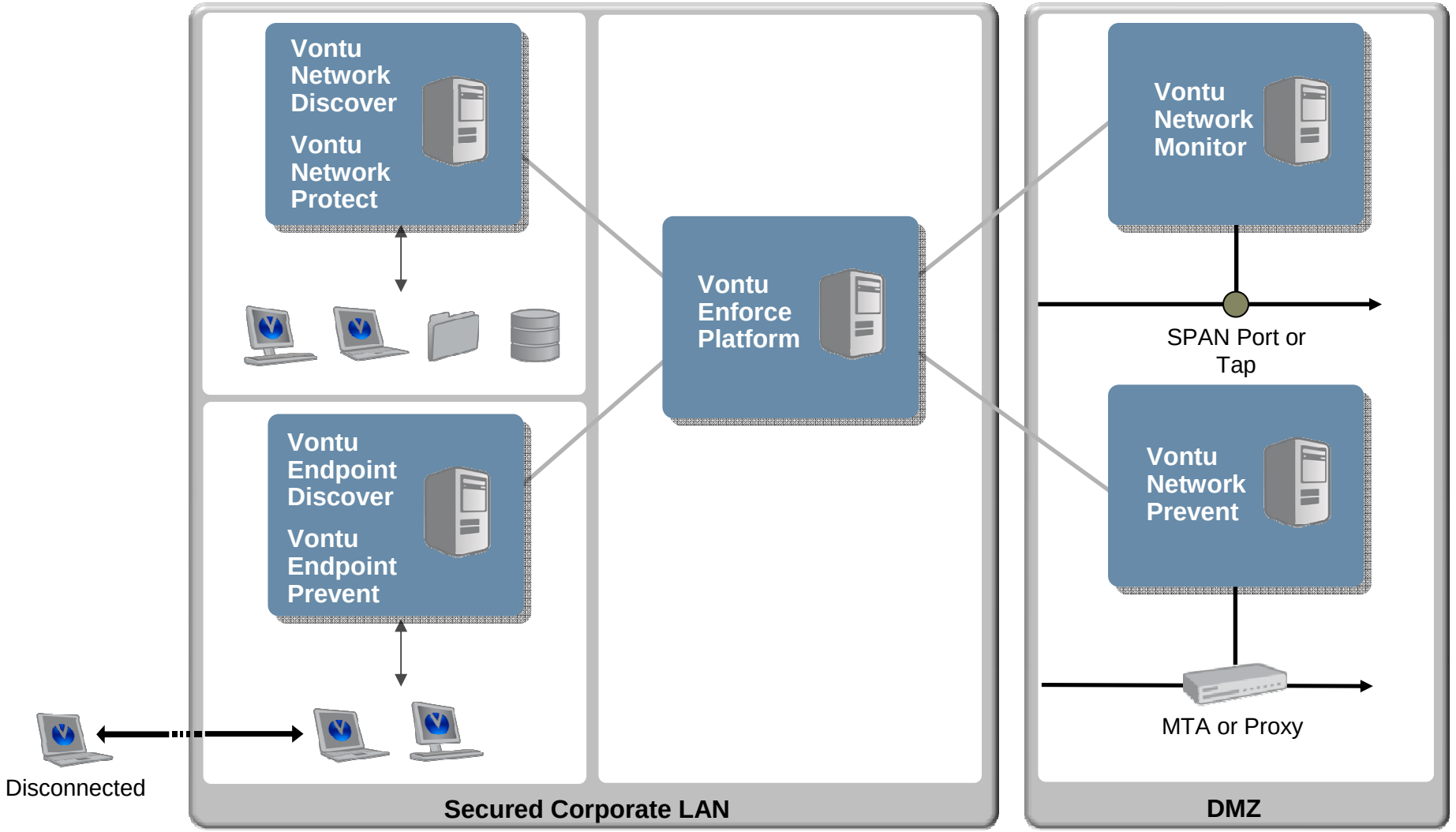
- <100ms latency
- Gb+ throughput

Storage

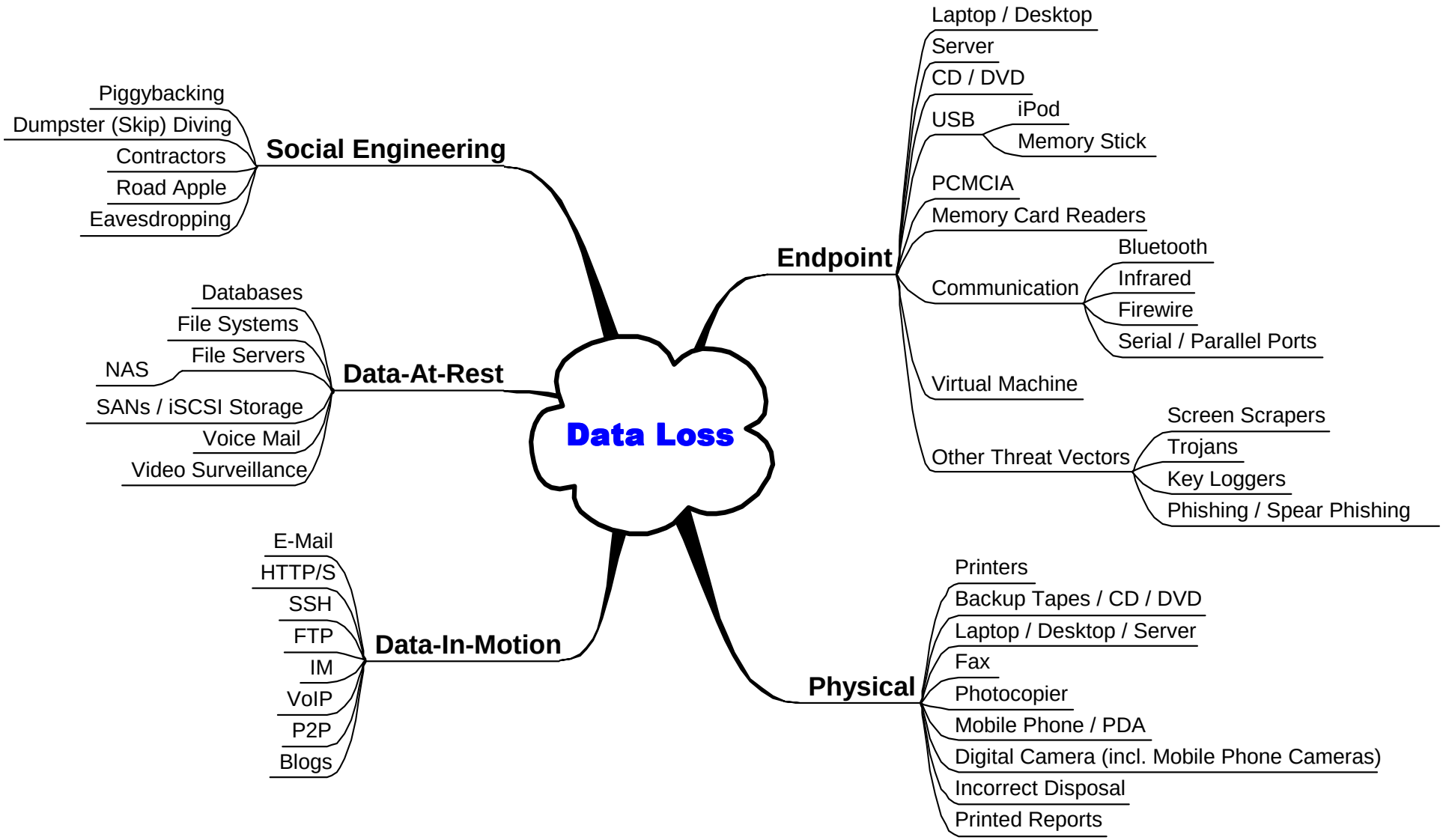
- Scan TBs per day
- 1000’s of endpoints

35

Symantec DLP 8 Architectura

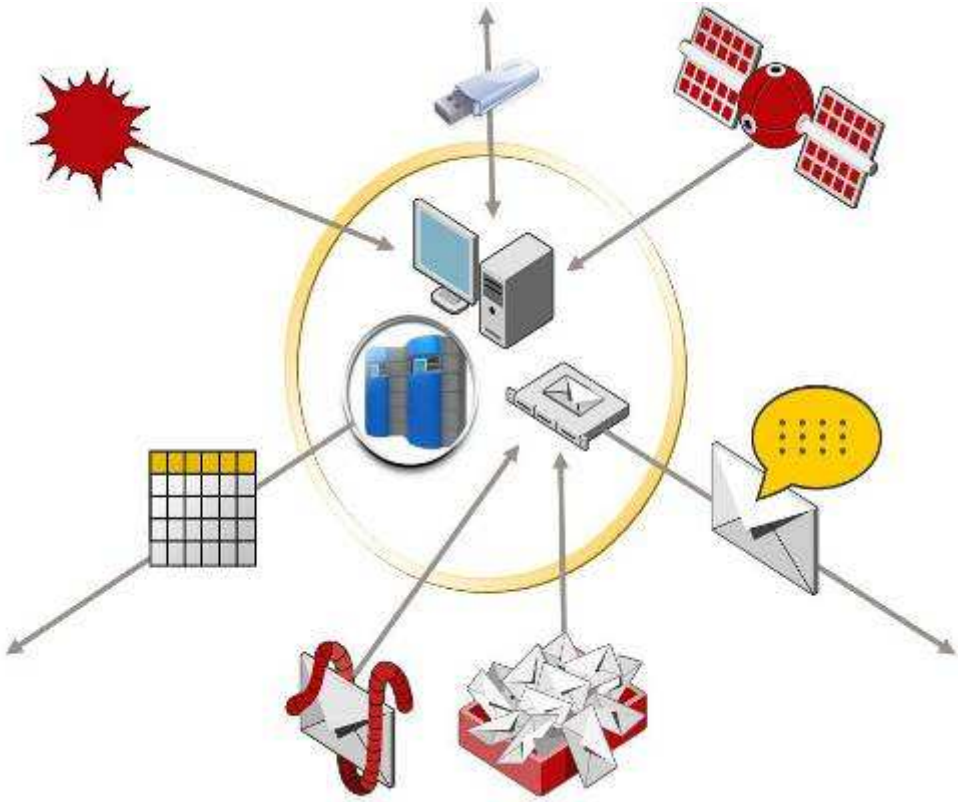


DLP – Minden szemszögből biztonságban?



Itt az idő hogy ne többet, de okosabbat tegyünk.

- Vizsgáljuk meg az adatforrásokat…
  - Laptop, desktop, server, fiók hálózat
  - USB, iPod, CD ROM, DVD
  - Email, webmail, instant messenger, FTP
  - File server, database, collaboration tools (e.g. SharePoint)
- Új technológia: Automatikus keresés és tartalom osztályozás, minősítés
  - Szabályzat alapú felügyelet, megelőzés, megakadályozás az IT környezet minden pontján
  - Pl. Előzzük meg hogy kritikus levelek hagyják el a szervezeti egységet
- Bizonyosodjunk meg hogy a vállalati környezet nem veszélyeztetett
  - Tűzfalak, anti-spam, anti-malware
  - IDS / IPS
  - network access control



- Az adatkezelés folyamatos ellenőrzése…
  - Backup máshol tárolva? Titkositás!
  - Adatok CD-n küldve? Titkosítás
  - USB kulcs? Eszköz kontroll

Complimentary coverage at each essential layer

VONTU

symantec

Policy Enforcement Universal Policy, Single Console, Workflow, Reporting		Enforce Platform +	IT Compliance
Discovery & Protection e-Discovery, Classification	**Monitoring & Prevention** Inadvertent Mistakes, Malicious Users		
Endpoint Laptops, Desktops, Branch Offices, Mobile Devices		Endpoint Discover Endpoint Prevent +	Endpoint Security Endpoint Management
Network Email, Webmail, Blog Postings, SSL, Instant Messaging, FTP, TCP		Network Monitor Network Prevent +	IT Compliance Messaging Security
Storage Backup Storage, File Servers, Databases, Document Repositories, Mail Archives		Network Discover Network Protect +	Storage Management Backup and Recovery Archiving

39

Köszönöm!