



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

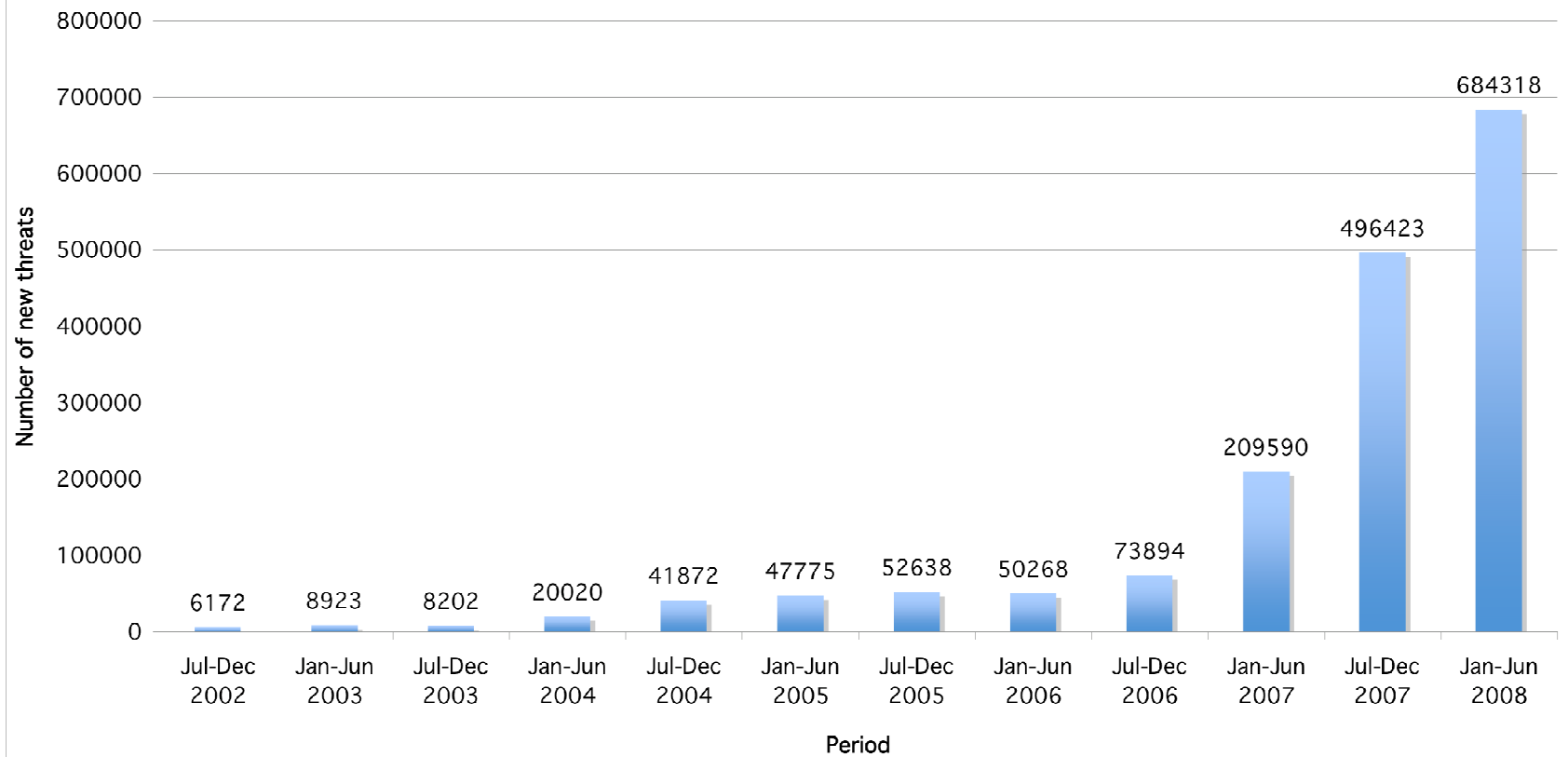
Information Protection

Threat Triggered Actions

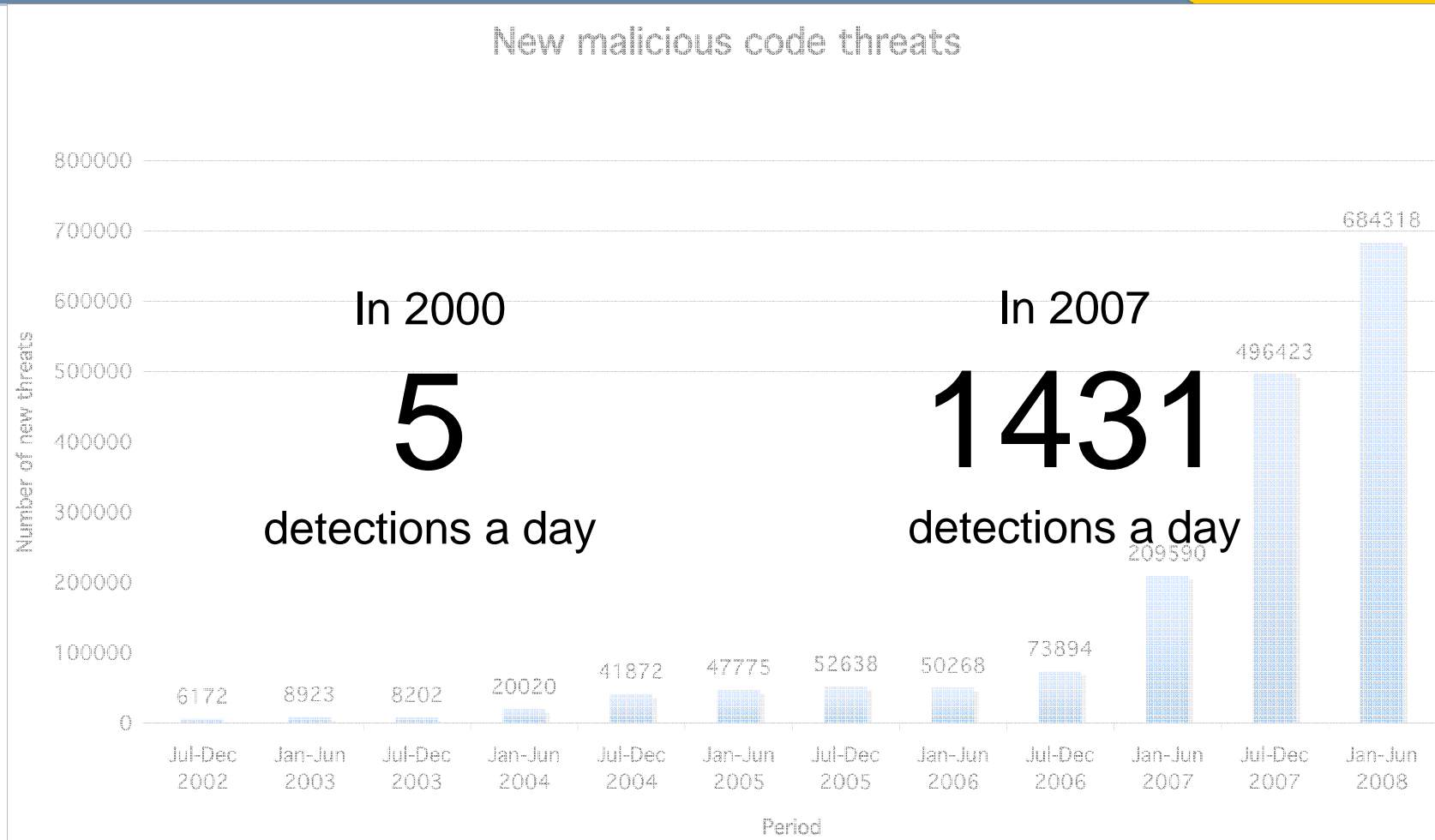
Malware Explosion



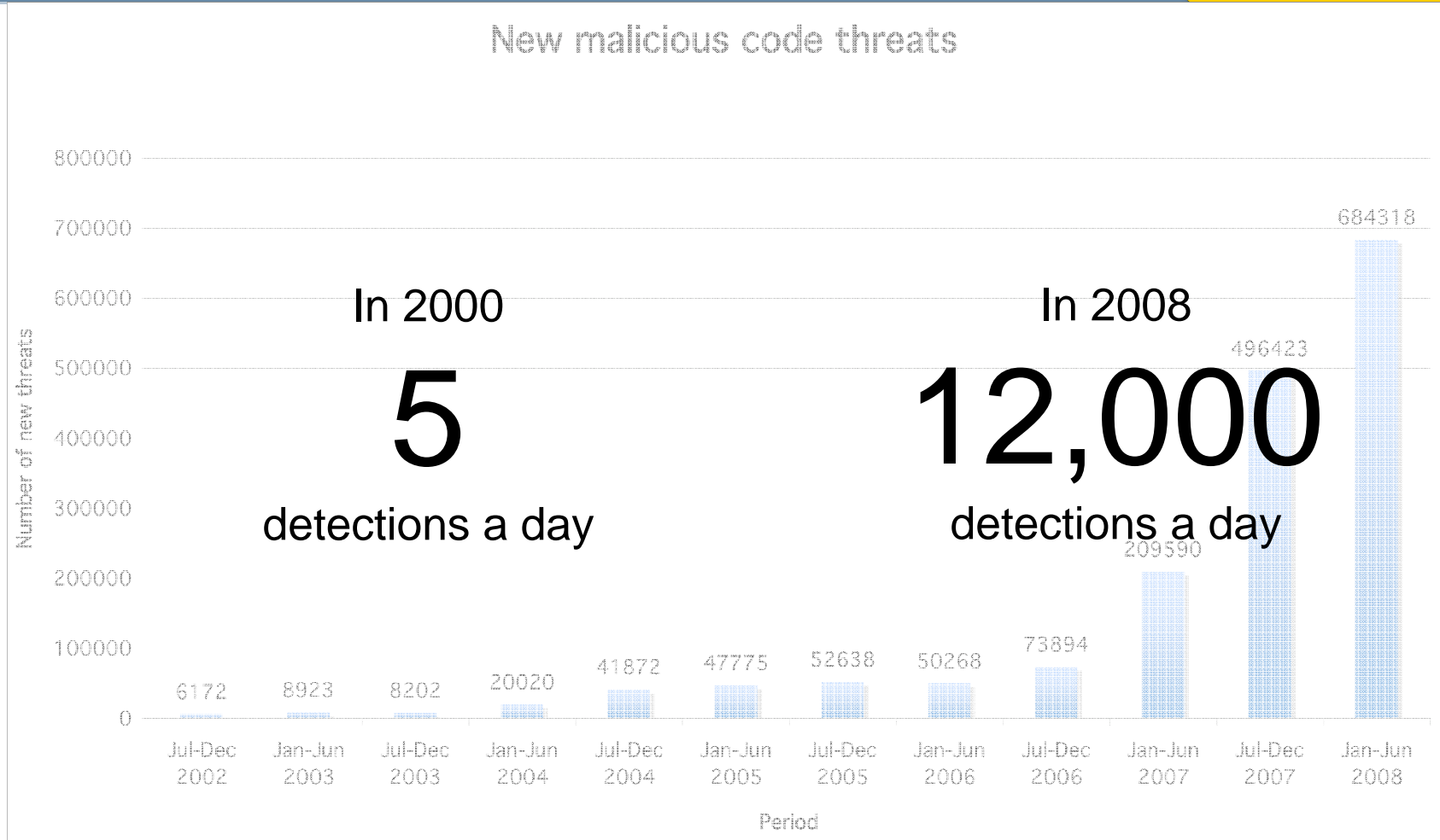
New malicious code threats



Malware Explosion



Malware Explosion



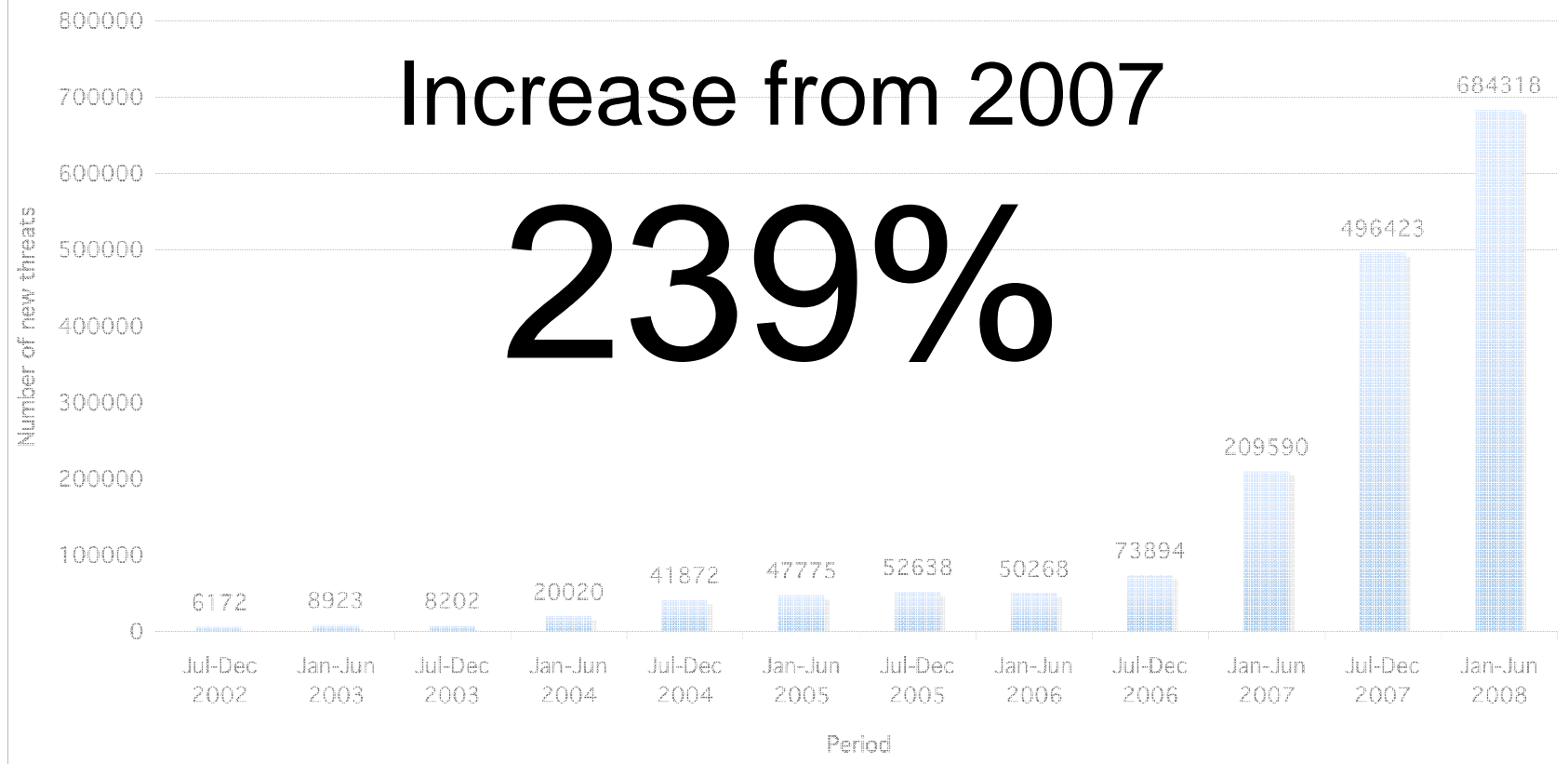
Malware Explosion



Malware Explosion



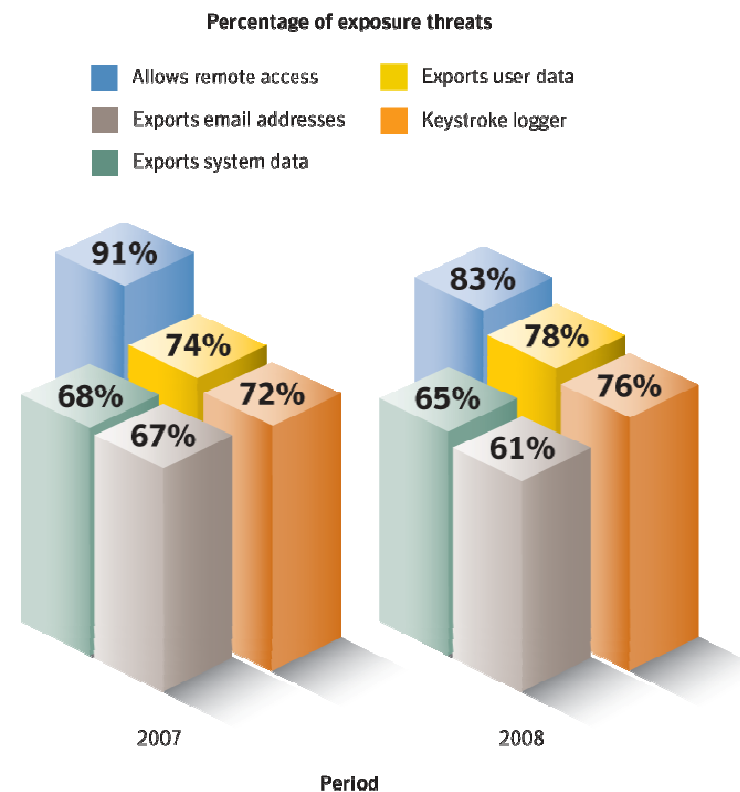
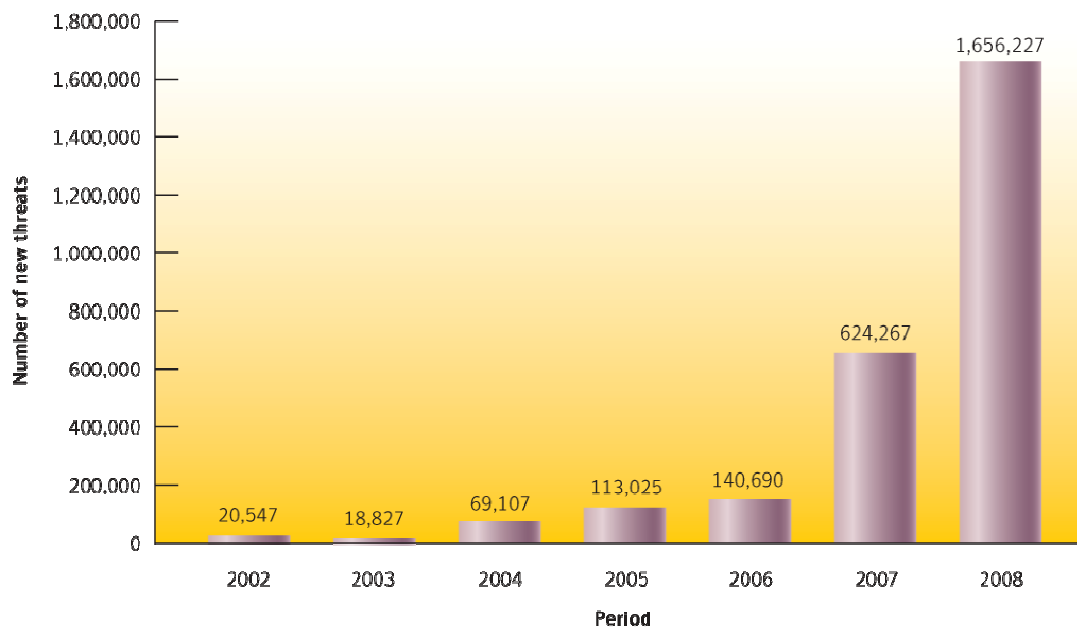
New malicious code threats



Malicious code is installed



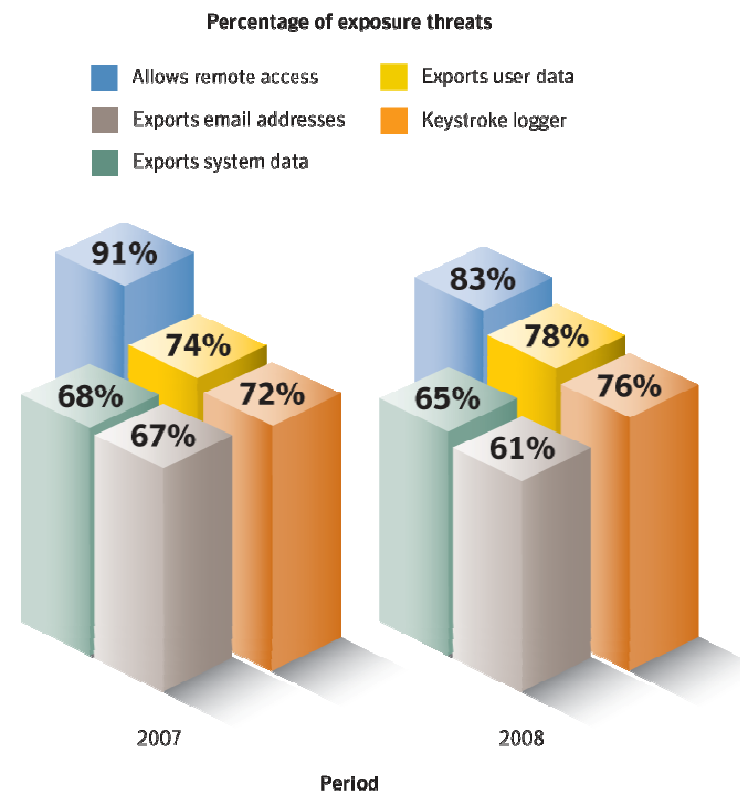
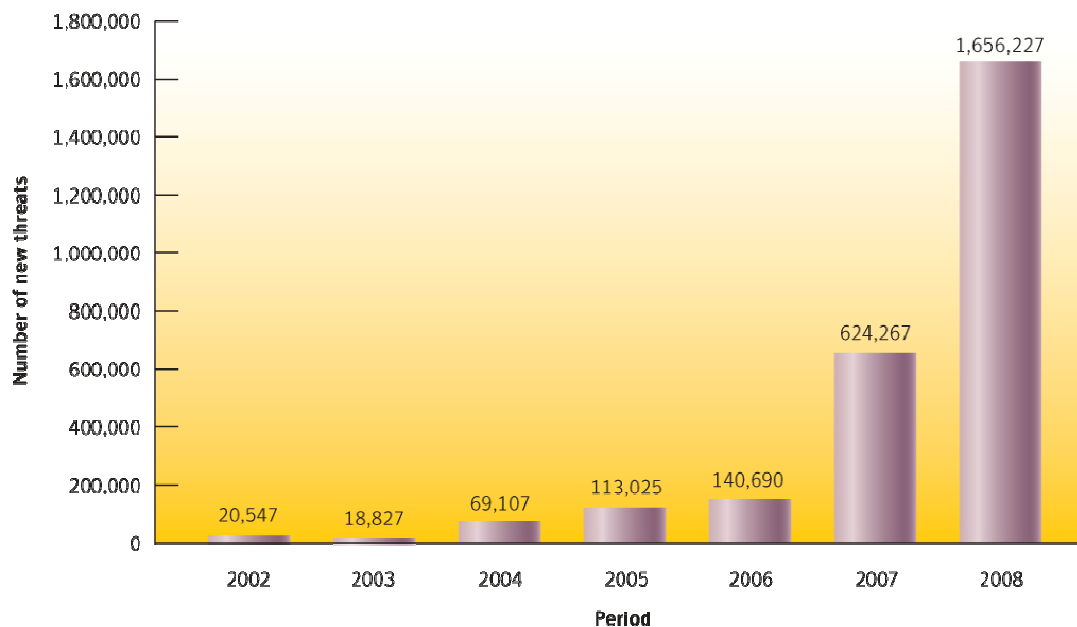
- 245 000 000 károkozó havonta
- 60%-a 2008-ban keletkezett
- 90% adatlopásra kihegyezve ...



Malicious code is installed

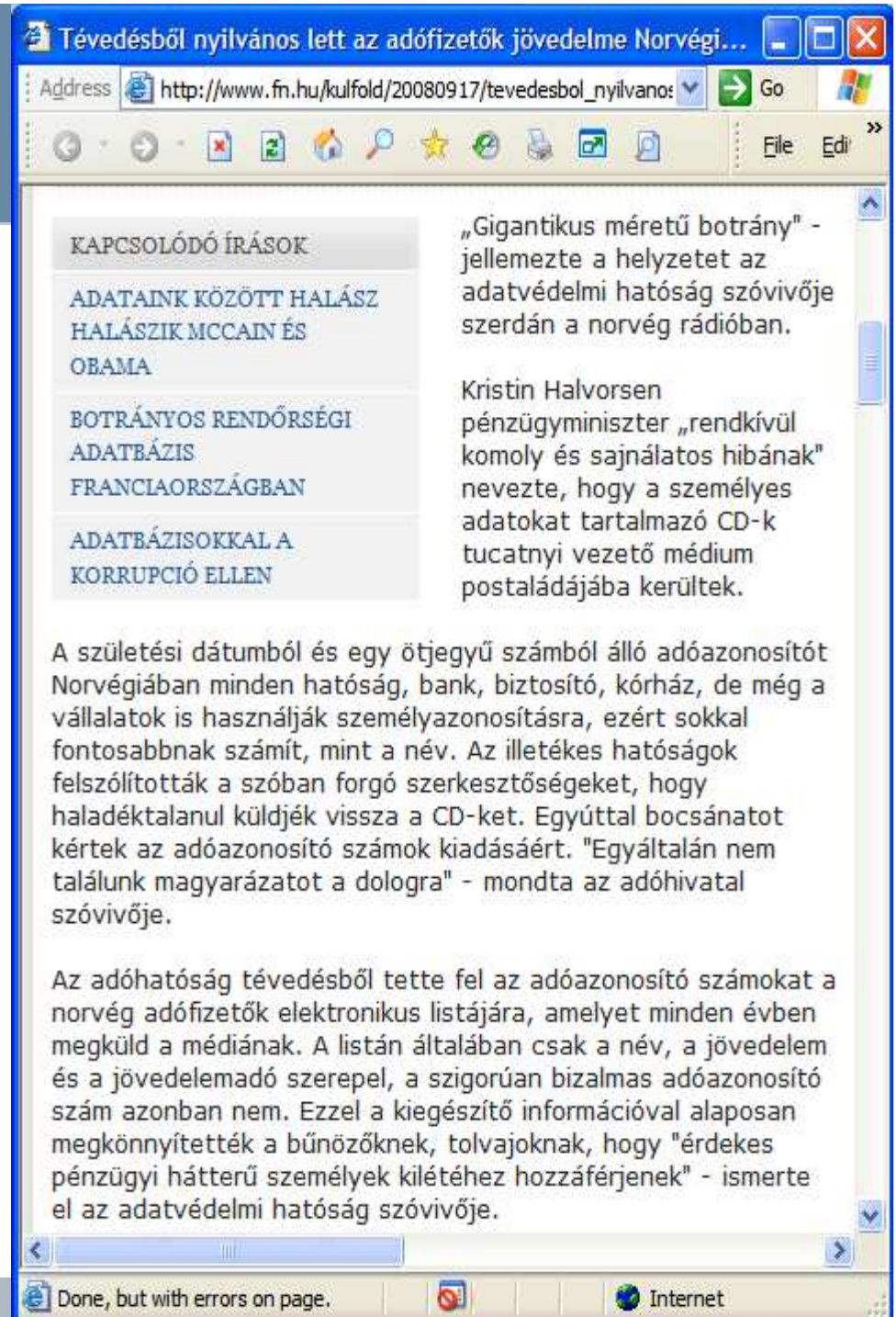


- 245 000 000 károkozó havonta
- 60%-a 2008-ban keletkezett
- 90% adatlopásra kihegyezve ...



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.



Tévedésből nyilvános lett az adófizetők jövedelme Norvégiában

Address http://www.fn.hu/kulfold/20080917/tevedesbol_nyilvano Go

KAPCSOLÓDÓ ÍRÁSOK

- [ADATAINK KÖZÖTT HALÁSZ HALÁSZIK MCCAIN ÉS OBAMA](#)
- [BOTRÁNYOS RENDŐRSÉGI ADATBÁZIS FRANCIAORSZÁGBAN](#)
- [ADATBÁZISOKKAL A KORRUPCIÓ ELLEN](#)

„Gigantikus méretű botrány” - jellemezte a helyzetet az adatvédelmi hatóság szóvivője szerdán a norvég rádióban.

Kristin Halvorsen pénzügyminiszter „rendkívül komoly és sajnálatos hibának” nevezte, hogy a személyes adatokat tartalmazó CD-k tucatnyi vezető médium postaládájába kerültek.

A születési dátumból és egy ötjegyű számból álló adóazonosítót Norvégiában minden hatóság, bank, biztosító, kórház, de még a vállalatok is használják személyazonosításra, ezért sokkal fontosabbnak számít, mint a név. Az illetékes hatóságok felszólították a szóban forgó szerkesztőségeket, hogy haladéktalanul küldjék vissza a CD-ket. Egyúttal bocsánatot kértek az adóazonosító számok kiadásáért. "Egyáltalán nem találunk magyarázatot a dologra" - mondta az adóhivatal szóvivője.

Az adóhatóság tévedésből tette fel az adóazonosító számokat a norvég adófizetők elektronikus listájára, amelyet minden évben megküld a médianak. A listán általában csak a név, a jövedelem és a jövedelemadó szerepel, a szigorúan bizalmas adóazonosító szám azonban nem. Ezzel a kiegészítő információval alaposan megkönnyítették a bűnözőknek, tolvajoknak, hogy "érdekes pénzügyi háttérű személyek kilétéhez hozzáférjenek" - ismerte el az adatvédelmi hatóság szóvivője.

Done, but with errors on page. Internet

Adatlopás, betörés: valóság



NewsBlog

Recent posts on technology, trends, and more

September 14, 2007 12:52 PM PDT

TD Ameritrade's 6 million customers hit by security breach

Posted by Dawn Kawamoto

Online trading company TD Ameritrade alerted more than 6 million customers that a security breach occurred with its client information database.

McLaren fined \$100 million in Formula One spying scandal

By Brad Spurgeon

Published: September 14, 2007

SPA-FRANCORCHAMPS, Belgium: McLaren Mercedes, the leading team in the Formula One championship, has been fined \$100 million and excluded from the constructors' title in the spying scandal that has plagued the sport all summer.

- E-Mail Article
- Listen to Article
- Printer-Friendly
- 3-Column Format
- Translate
- Share Article
- Text Size - +

TJX, Visa Agree to \$40.9 Million Payout for Data Breach Pending Deal Also Calls for TJX to Promote PCI Standard

The TJX Companies, Inc. (NYSE: TJX) and Visa have announced that TJX has agreed to fund up to \$40.9 million for payments to certain financial institutions following the much-publicized data breach of their systems.

International Federation, the sport's governing body, is investigating by using data obtained from Ferrari, McLaren's own car, the federation said in a statement released on Thursday in Paris.

InfoWorld

HOME NEWS TECHNOLOGIES BLOGS/COLUMNS TESTS

Gap contractor blamed for data breach

Two laptops containing personal data on job applicants at the clothing retailer have been stolen, which Gap blames on an unnamed contractor

By Robert McMillan, IDG News Service
September 28, 2007

An unnamed contractor is being blamed for a data breach that affected 800,000 people who applied for jobs with the clothing retailer.

Boeing laptop stolen -- 382,000 IDs lost Past and present employees at risk of being targeted

By AMY ROLPH
P-I REPORTER

A laptop with personal information on hundreds of thousands of Boeing employees was stolen earlier this month, and the aerospace giant says that the information could be used to target past and present employees.

U.K. data breach could cost banks \$500M, says Gartner Computer disks with bank account info on 25 million people were lost

Jaikumar Vijayan Today's Top Stories or Other Security Stories

Comments (3) Recommendations: 103 — Recommend this article


„Tegnap történt”



Official Google Docs Blog: On yesterday's email - Microsoft Internet Explorer

File Edit View Favorites Tools Help Back Forward Stop Home Search Favorites Print

Address http://googledocs.blogspot.com/2009/03/on-yesterdays-email.html Go



The Official
Google Docs Blog
News & notes from the Google Docs team

On yesterday's email

Saturday, March 07, 2009 11:34 AM

Yesterday we contacted some of our users to let them know about an issue that affected their Google Docs accounts. We believe the issue affected less than 0.05% of all documents, but, in the interest of transparency, we wanted to share the details more broadly.

As we noted in the [Google Docs Help Forum](#) yesterday, we've identified and fixed a bug where a very small percentage of users shared some of their documents inadvertently. The inadvertent sharing was limited to people with whom the document owner, or a collaborator with sharing rights, had previously shared a document. The issue affected so few users because it only could have occurred for a very small percentage of documents, and for those documents only when a specific sequence of user actions took place.

For this small percentage of documents, the bug (now fixed) occurred when the document owner, or a collaborator with sharing rights, selected multiple documents and presentations from the documents list and then changed the sharing permissions. The bug did not affect spreadsheets.

As part of the fix, we used an automated process to remove collaborators and viewers from the documents that we identified as having been affected. We then emailed the document owners to point them to their affected documents in case they need to re-share them.

We're sorry for the trouble this has caused. We understand our users' concerns (in fact, we were affected by this bug ourselves) and we're treating this very seriously. We hope this explanation provides greater clarity.

Posted by: Jennifer Mazzon, Google Docs Product Manager

powered by Google™

Archives

Archives ▾

Site Feed

 **10916** readers
BY FEEDBURNER

We Love Feedback

Have a story to tell? [Let us know](#) how you're using Docs.

Visit our [Google Group](#) to discuss Google Docs.

Useful Links

[Google Docs Home](#)
[User Support Group](#)

Message (1) processing took 297 ms Internet

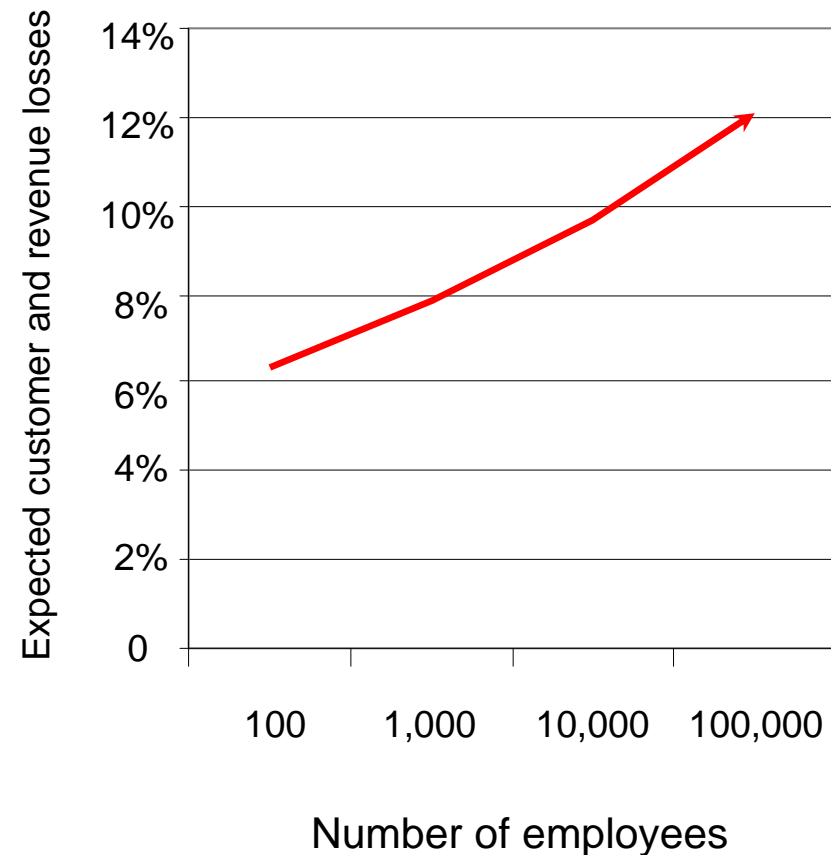
start [Taskbar icons: Internet Explorer, Outlook, Word, PowerPoint, etc.] 100% 13:51

... 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 vesztese.
 - Jogi eljárások, bírság
 - Részvény vagy árbevétel csökkenése



*July 2007, IT Policy Compliance Group

Az adatvesztés, -szivárgás növekvő aggodalmat szül.

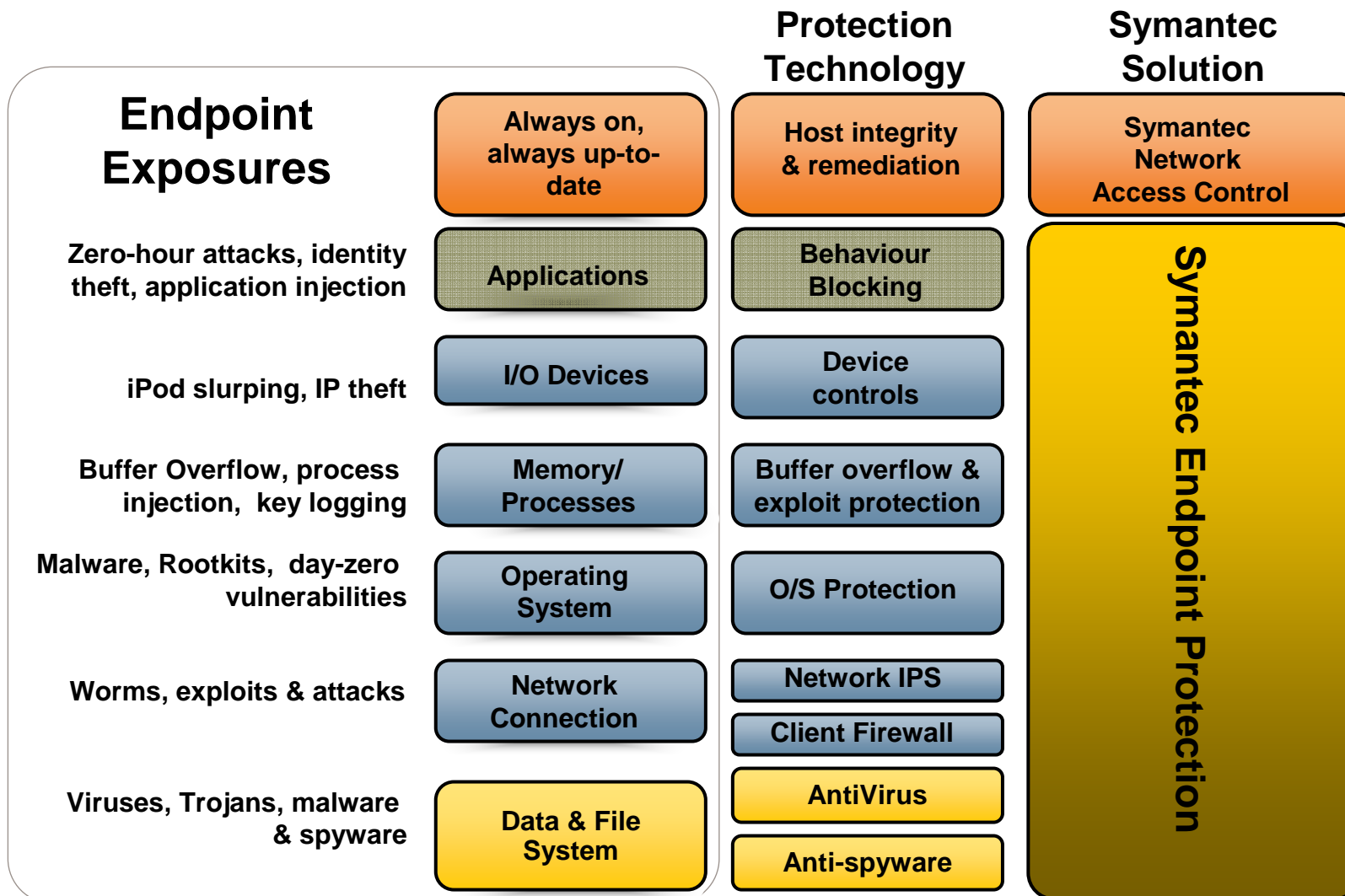


A biztonsági vezetők TOP gondjai

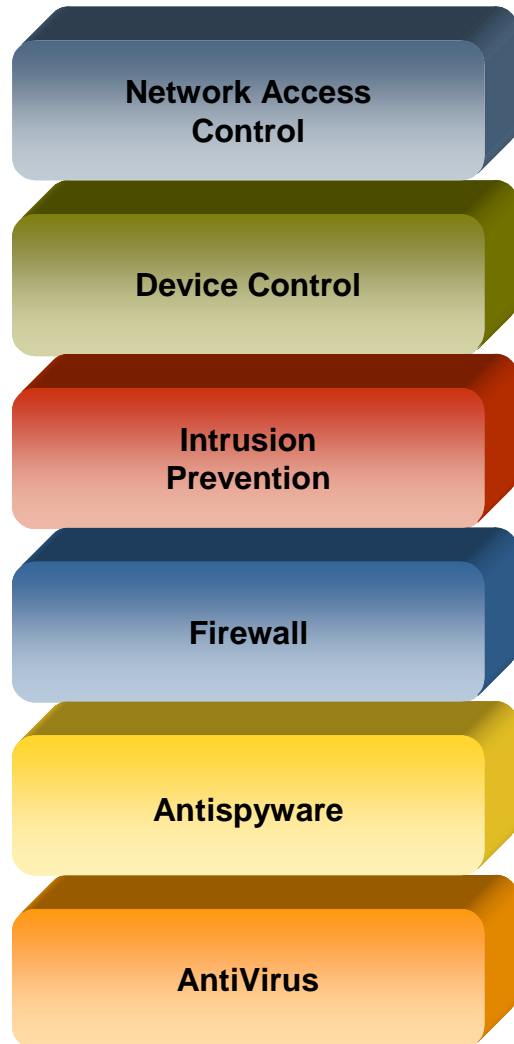
- 52% of CISOs gondolja hogy DLP meghatározó, markáns eleme lesz a biztonsági büdzsének¹
- 85% jelentett legalább egy olyan biztonsági eseményt, incidenst, amely adatszivárgással összefüggő volt – tavaly²
 - 63% esetében észleltek 6-20 biztonsági eseményt, ami személyes információkat is érintett.
- 216 millió személyes adatot ért támadás 2005 óta
- 2007-ben az incidensek 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 sérülékenységek 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



Milyen típusú 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%

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, segédprogramok	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%

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 címére küldte	38%
Elhatározta, hogy nem törli azokat, amelyek az otthoni gépén találhatóak már.	35%
Más hordozható 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%

Q5c. Ugy érzi, hogy helyes ezeket az információkat megtartani?	Total%
Mindenki más megtartotta ezeket az információkat	54%
Ezek az információkat hasznosak a jövőm szempontjából	53%
Eszköz voltam az információk létrehozásában	52%
Munkaadóm nem tudja megállapítani hogy én voltam ...	49%
A vállalat nem érdekli 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

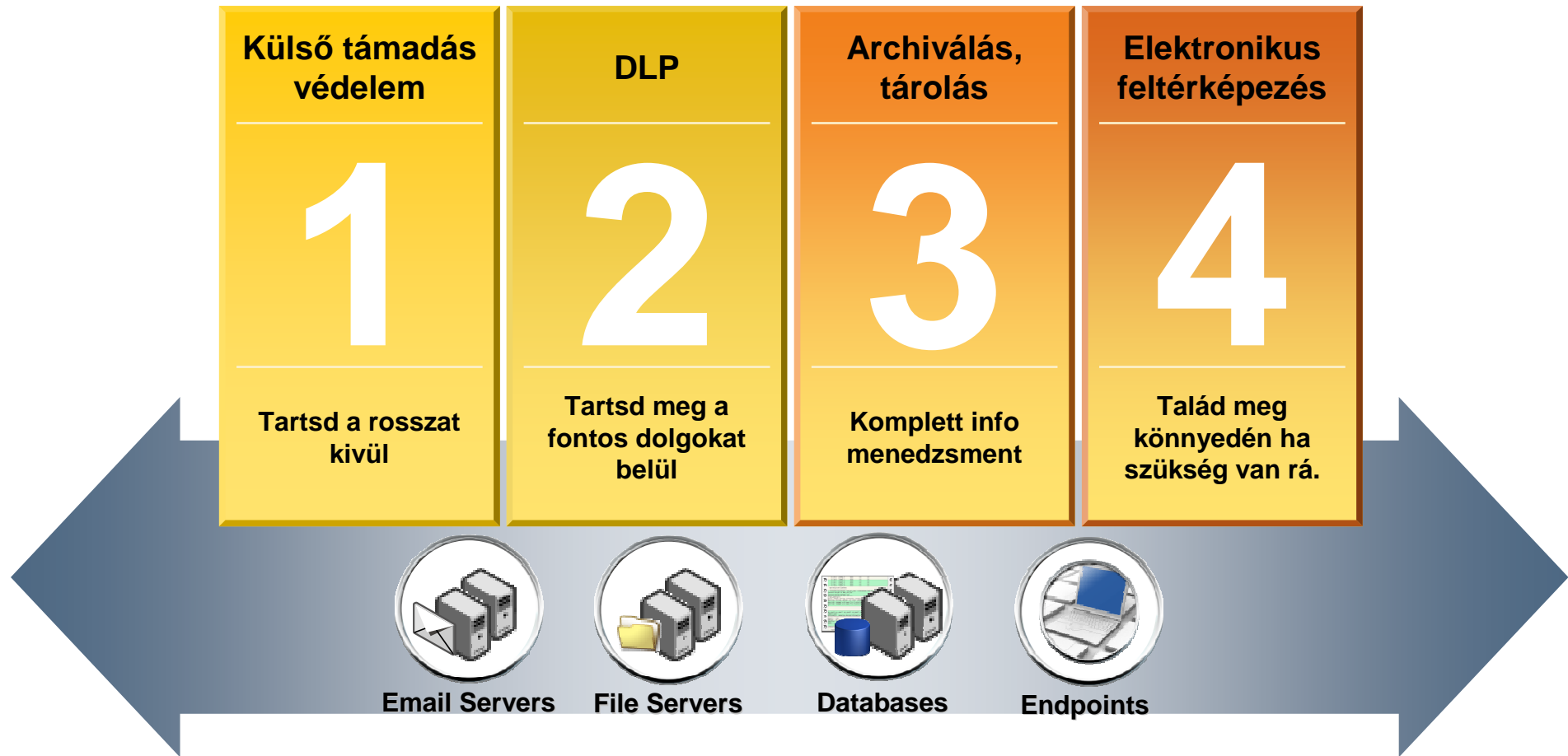


Q8a. Sikerült új állást találnia?	Pct%
Igen	69%
Nem	31%
Total	100%

Q8b. Használt fel az előző munkahelye fontos, bizalmas információiból, anyagaiból hogy az új munkahelyen megrótsítse pozícióját?	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%

- A kérdőívre 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 ellenőrizték az elektronikus vagy papír alapú dokumentumokat, mielőtt elhagyták a munkahelyeiket
- 24%-uk azután is rendelkezett hozzáféréssel a hálózathoz, számítógéphez hogy már elhagyta a vállalatot.



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 (ILDPA), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) or Extrusion Prevention System by analogy to [Intrusion-prevention system](#).

- 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 működő 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 „elvesztését”, 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

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, specifikáció
- Gyártási technológia
- árazás



Vállalati bizalmas adatok

Hírnév

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

Felfedez

Hol vannak az értékes információk tárolva?



Felügyel

Hogyan vannak az értékes adatok felhasználva?

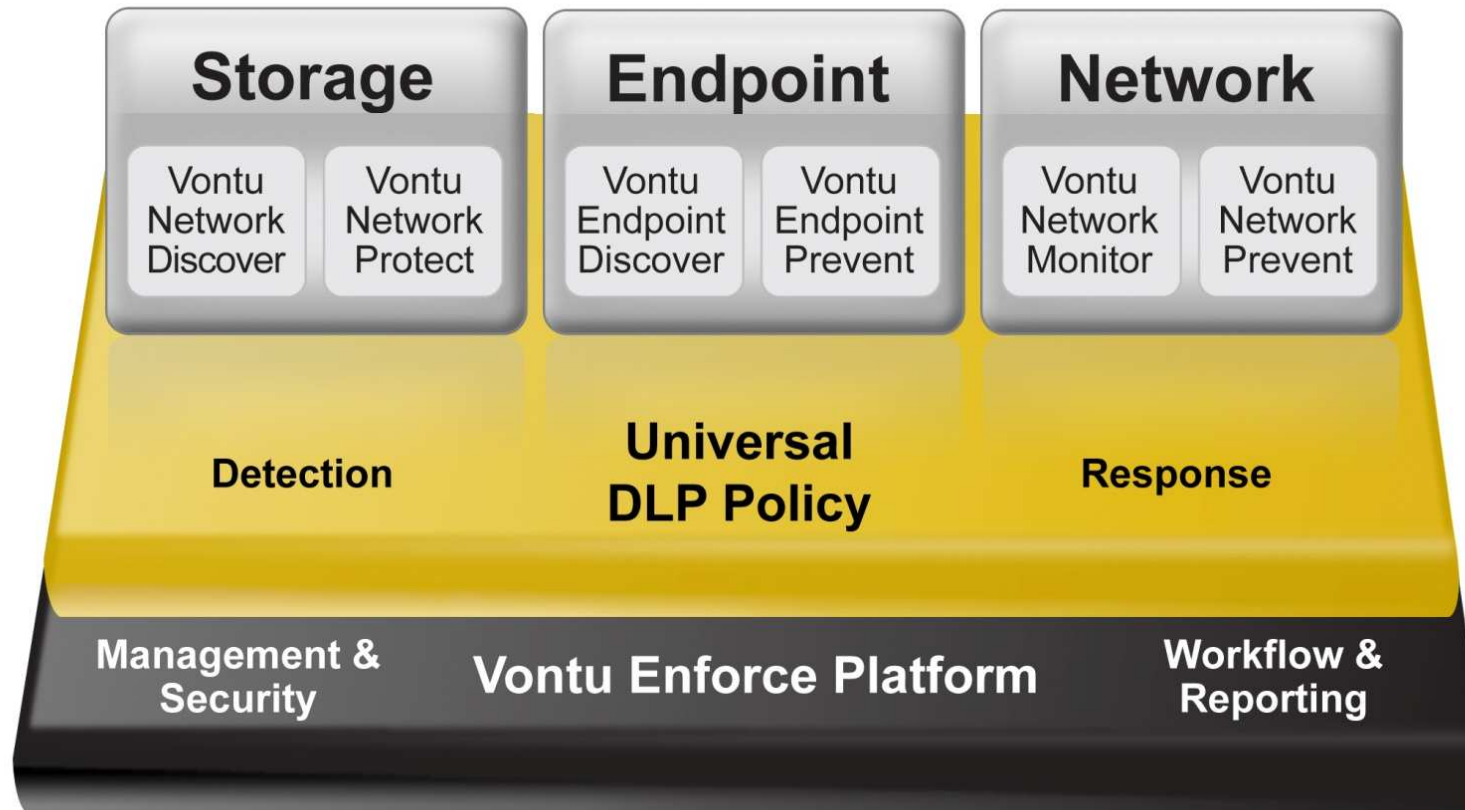


Kényszerít

Hogyan tudom megvédeni az értékes adataimat és megelőzni elvesztésüket?



Symantec DLP Architectura



Pontos megbízható felismerés az összes adattípuson



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



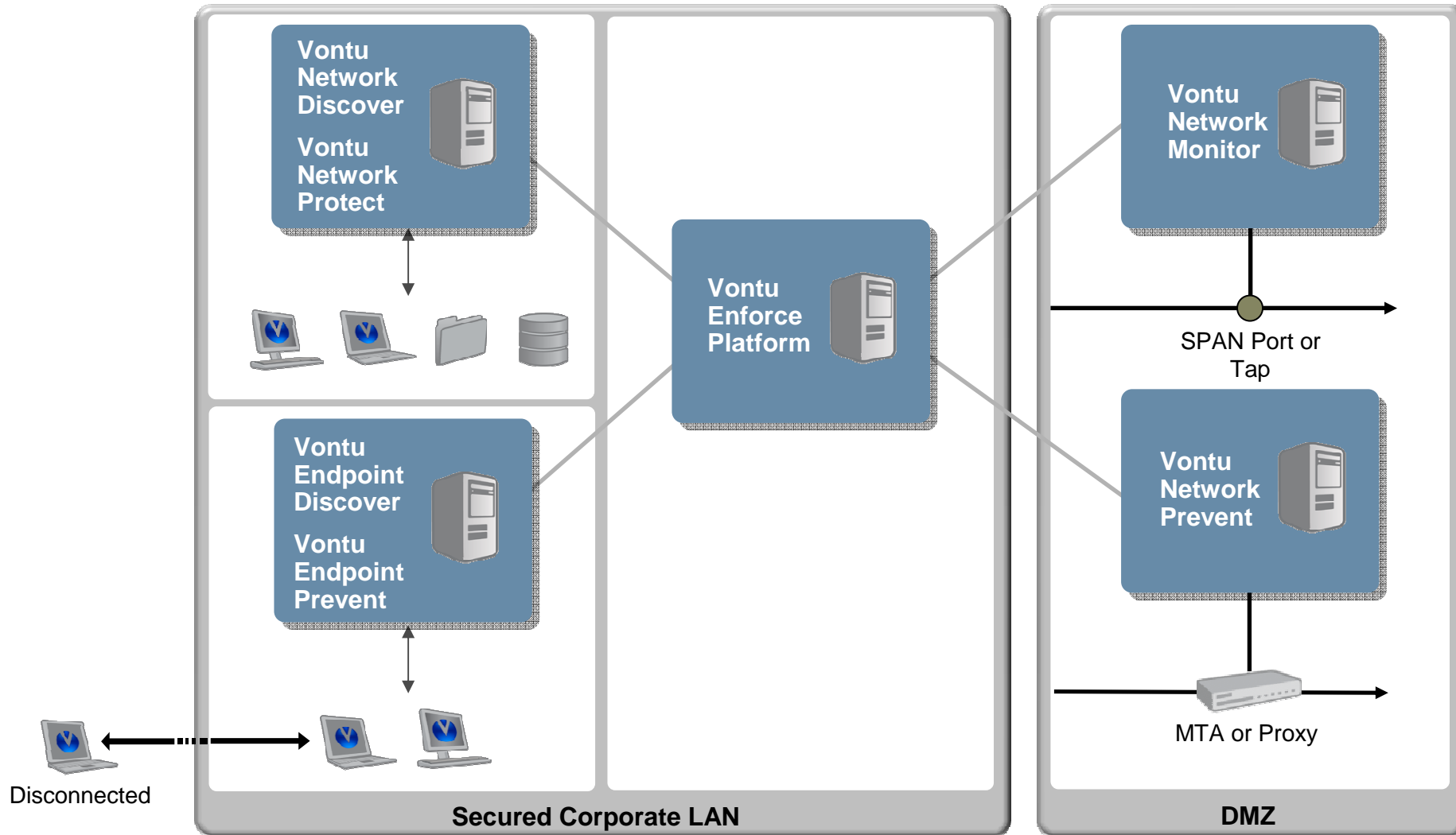
- <100ms latency
- Gb+ throughput

Storage

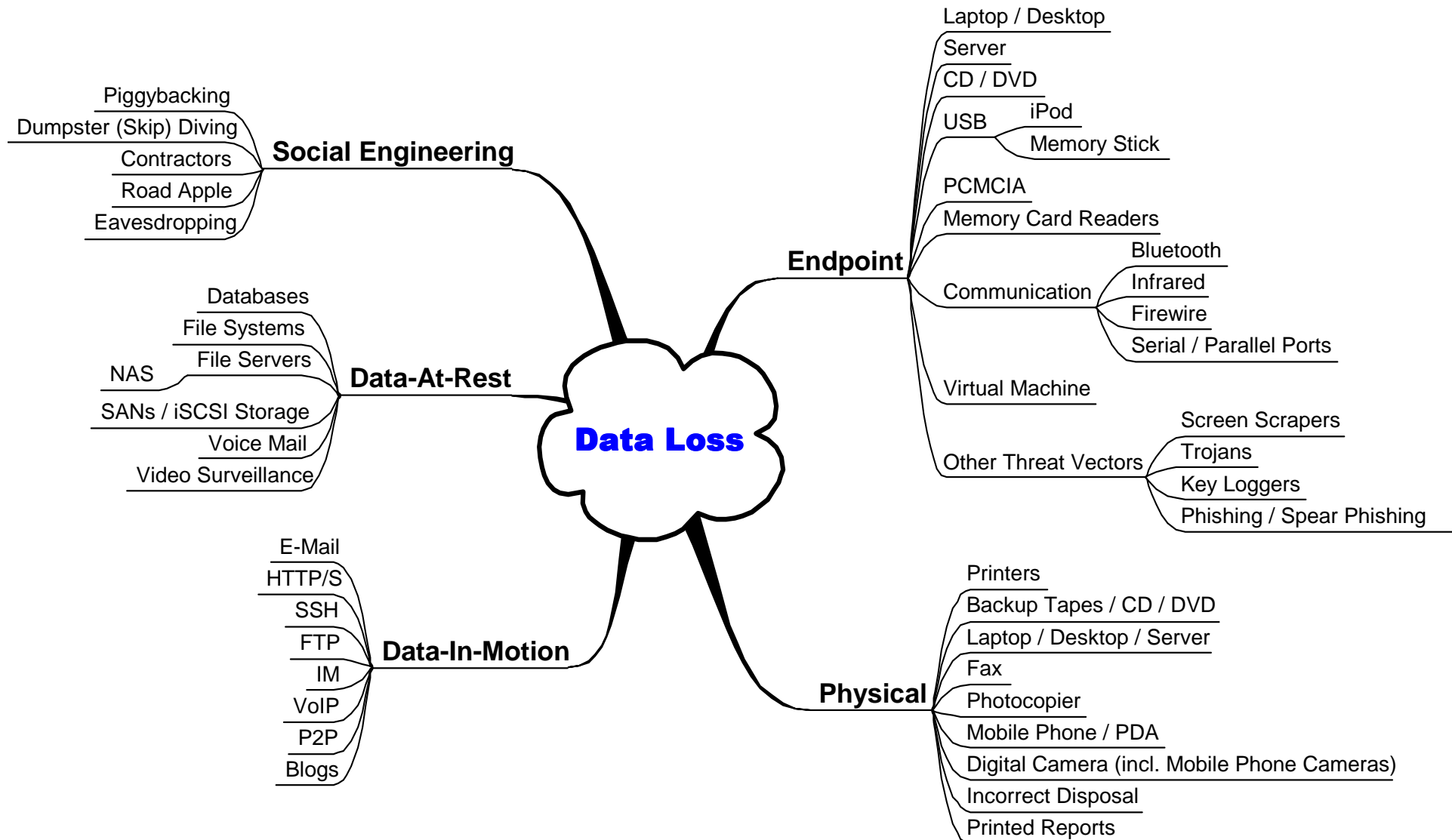


- Scan TBs per day
- 1000's of endpoints

Symantec DLP 8 Architectura



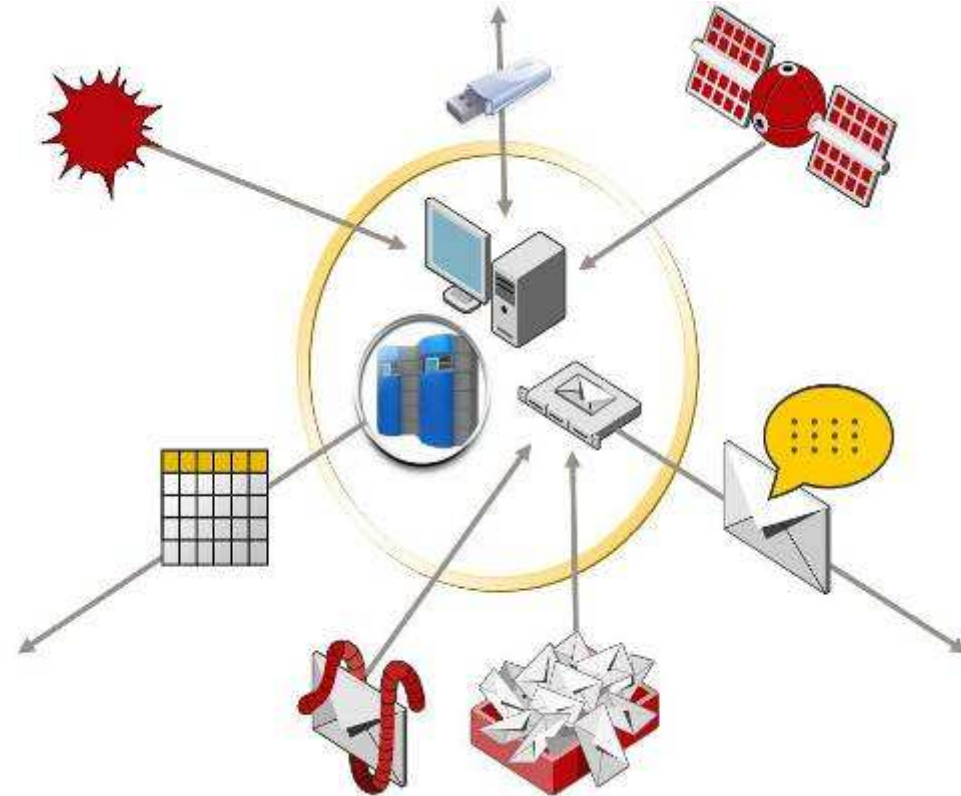
DLP – Minden szemszögből biztonságban?



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
 - PI. 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? Titkosítás!
 - Adatok CD-n küldve? Titkosítás
 - USB kulcs? Eszköz kontroll

Complimentary coverage at each essential layer



Policy Enforcement

Universal Policy, Single Console, Workflow, Reporting

Discovery & Protection

e-Discovery, Classification

Monitoring & Prevention

Inadvertent Mistakes, Malicious Users

Enforce Platform



IT Compliance

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



Confidence in a connected world.

Köszönöm!

© 2007 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.