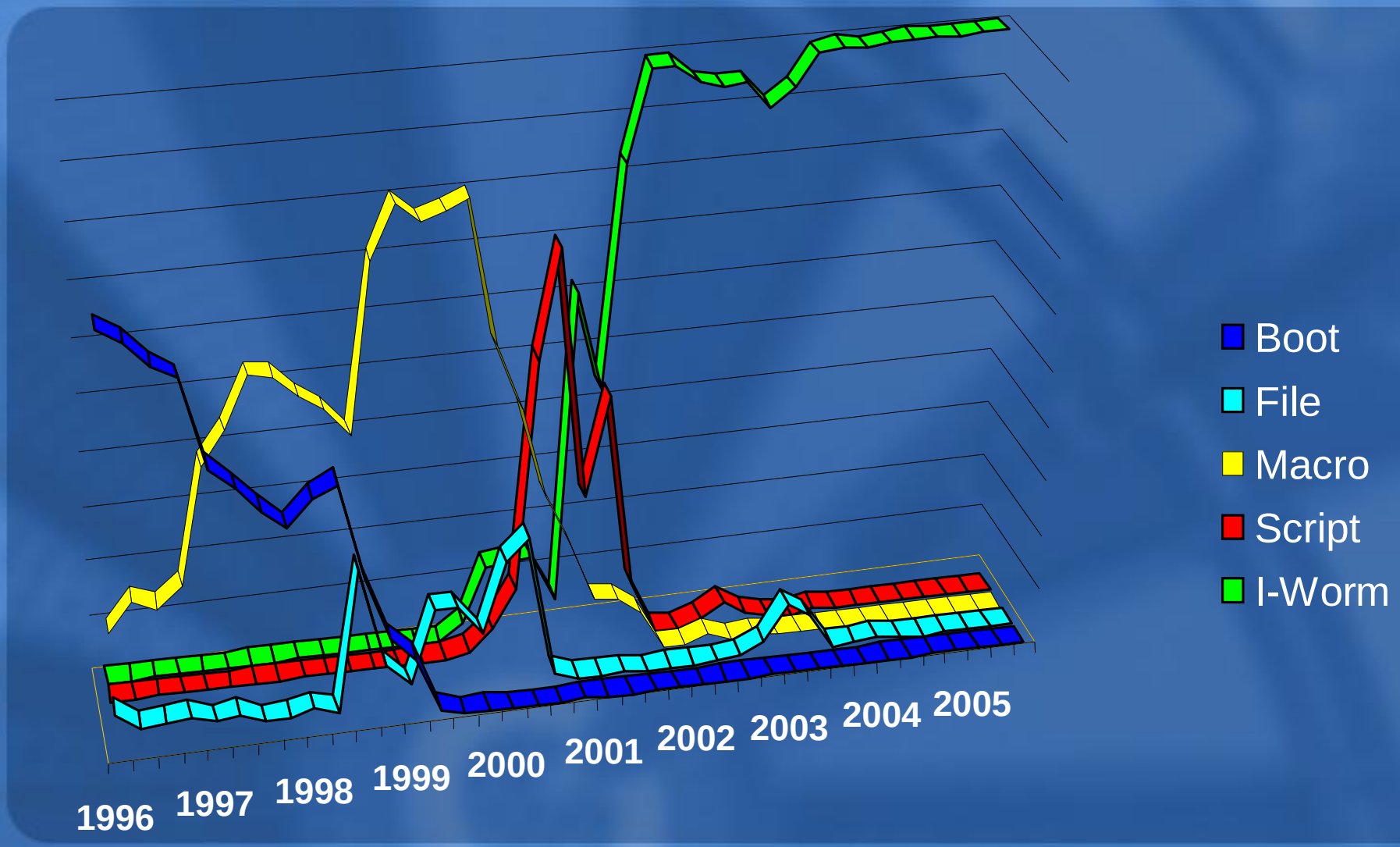

VirusBuster
www.virusbuster.hu
Károkozók és SPAM-védelmi megoldások tapasztalatai
a felsőoktatási intézményekben
XXI. Századi megoldások

Gyurik Csaba
Szolgáltatási Osztályvezető

- Rövid helyzetkép
- Egyetemi környezet kihívásai, nehézségei
- Megvalósítási lehetőségek
  - **VirusBuster egyetemi környezetben**
  - **Mit nyújthatunk a terméken kívül**

Tartalom

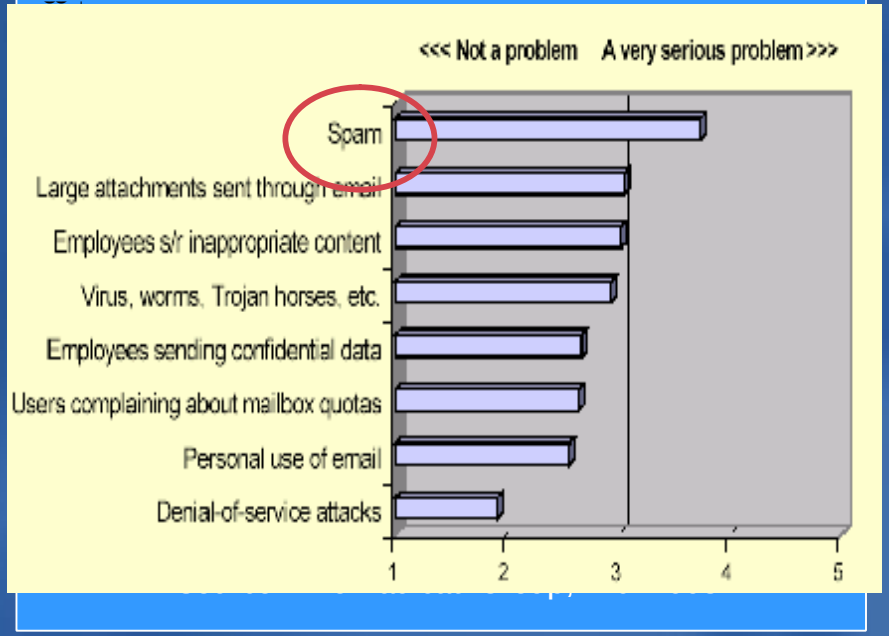
Vírusok eloszlása



Helyzetkép

1. A SPAM levelek száma folyamatosan nől
2. Profibb SPAM küldők jelennek meg
3. A SPAM gazdasági vonzatai növekszik
4. A „jó hogy van” megoldásoktól el kell jutni a MEGOLDÁSig
5. Többszintű, többtechnológiás SPAM szűrők lehetősége

Osterman Research: Spam is the biggest problem in today’s security market



Levelezési tulajdonságok

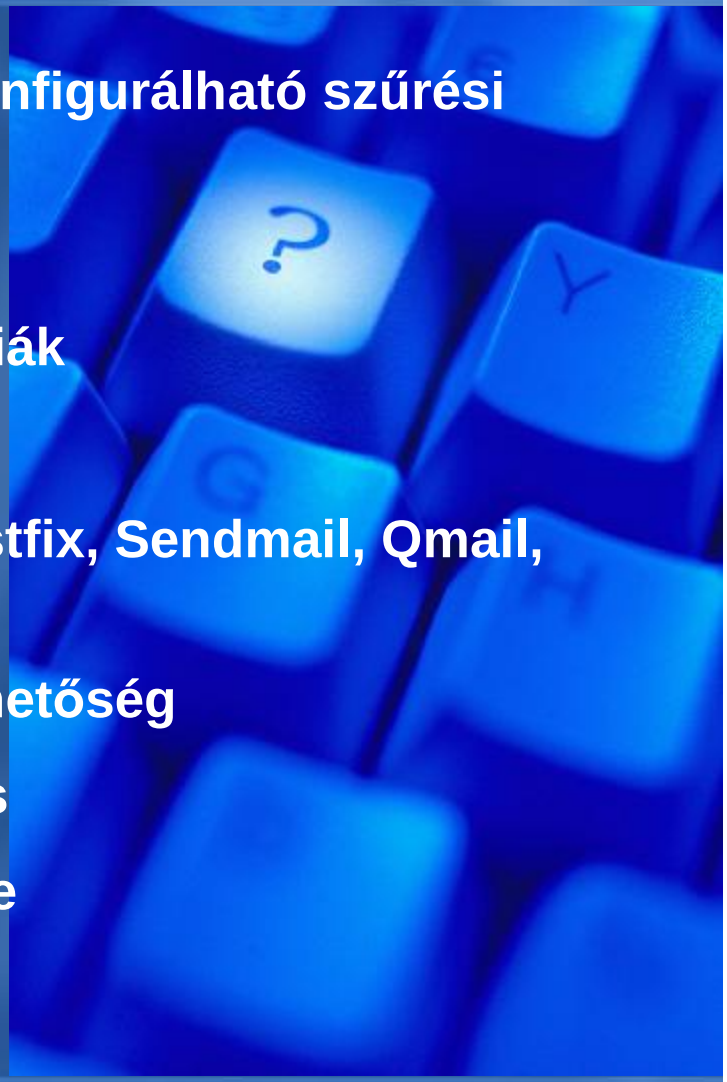
- Egyetemi levelezés igen heterogén és nagymennyiségű
  - A levelek majdnem 90%-a SPAM
  - Viszonylag állandó vírusbeáramlás van (célpont)
  - Sok levelező szerver, nem minden esetben egy átjárón kommunikálnak
  - A sok levelező szerver különböző platformokon üzemel (Windows, Linux, AIX, Solaris...)
  - A karok „önálló” egységként üzemelnek, ezért a saját védelmük a legtöbb esetben egyénileg megoldott, esetenként központilag biztosított termékkel
  - Nagy levelezési mennyiség a világ minden része felé
  - Gyártói támogatás mellőzése

Átlag levelezési statisztika

```
Uptime                  7 days 09:28:51   CFG updated           7 days 07:19:58
================================================================ 2007-03-26 18:00:01 =
Smtp Receiver [ 8110]:    0 / 32 / 32     Received:           957453 /  26.60G
Hook Scanner  [ 8106]:    0 /  6 /  6     Sent:               414762 /  22.41G
Smtp Sender   [ 8112]:    0 / 22 / 32     System load average:              1.02
Total connections:             957793     Queue status (R/S):     0 /         0
Dropped connections:                0     Resend spool:           0 /   25 sec
Checked mails:                 989115
Blocked mails:                 575616     Warning message sent:              216
------------------------------------------------------------ Virus and file filter -
Virus found:           4870 /  989115     Virus killed:                        0
IWorm found:                      3541     Modified attachments:                0
ZH virus found:         182 /  912920     Deleted attacments:                111
Infected mails                    3652     File filtered:                      15
------------------------------------------------------------------- SPAM Filter -
Spams found:         826274 /  985489     Total spams found:   872416 /  989109
ESP spams found:     375419 /  912920
------------------------------------------------------------ Blocked connections -
RBL:                                0     Domain blacklist:                    0
IP blacklist:                       0     Rcpt blacklist:                      0
------------------------------------------------------------------------ Errors -
5xx transmit.errors:                0     ZH comm. errors:                    27
4xx transmit.errors:                0     ESP comm. errors:                    6
Processing error:                   0
```

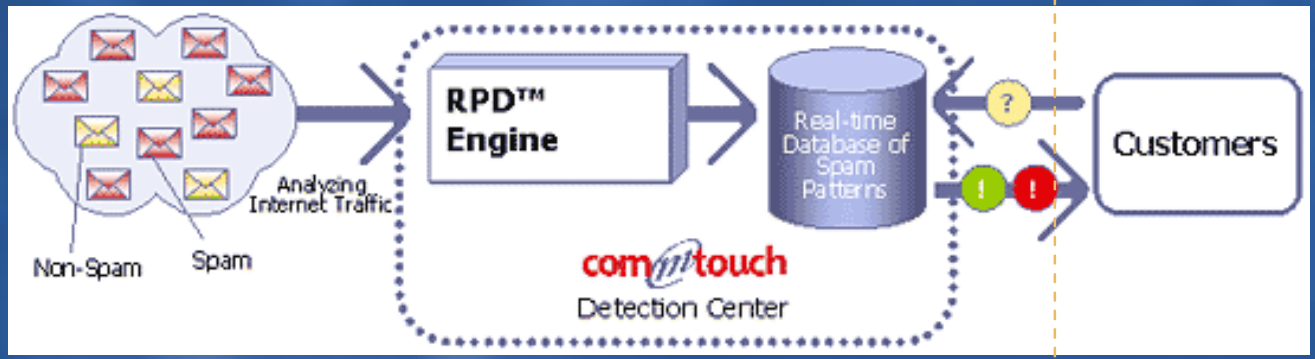
Meg lehet oldani?

- Több szintű és akár mailcímenként konfigurálható szűrési megoldások
- Kedvező terhelési mutatók
- Hatékony szűrések, egyedi technológiák
- Könnyű beilleszthetőség
- Gateway és integrált formában is (Postfix, Sendmail, Qmail, Groupwise)
- Távüzemeltetési, távmenedzsment lehetőség
- Folyamatos magyarországi támogatás
- Felhasználói igények figyelembevétele

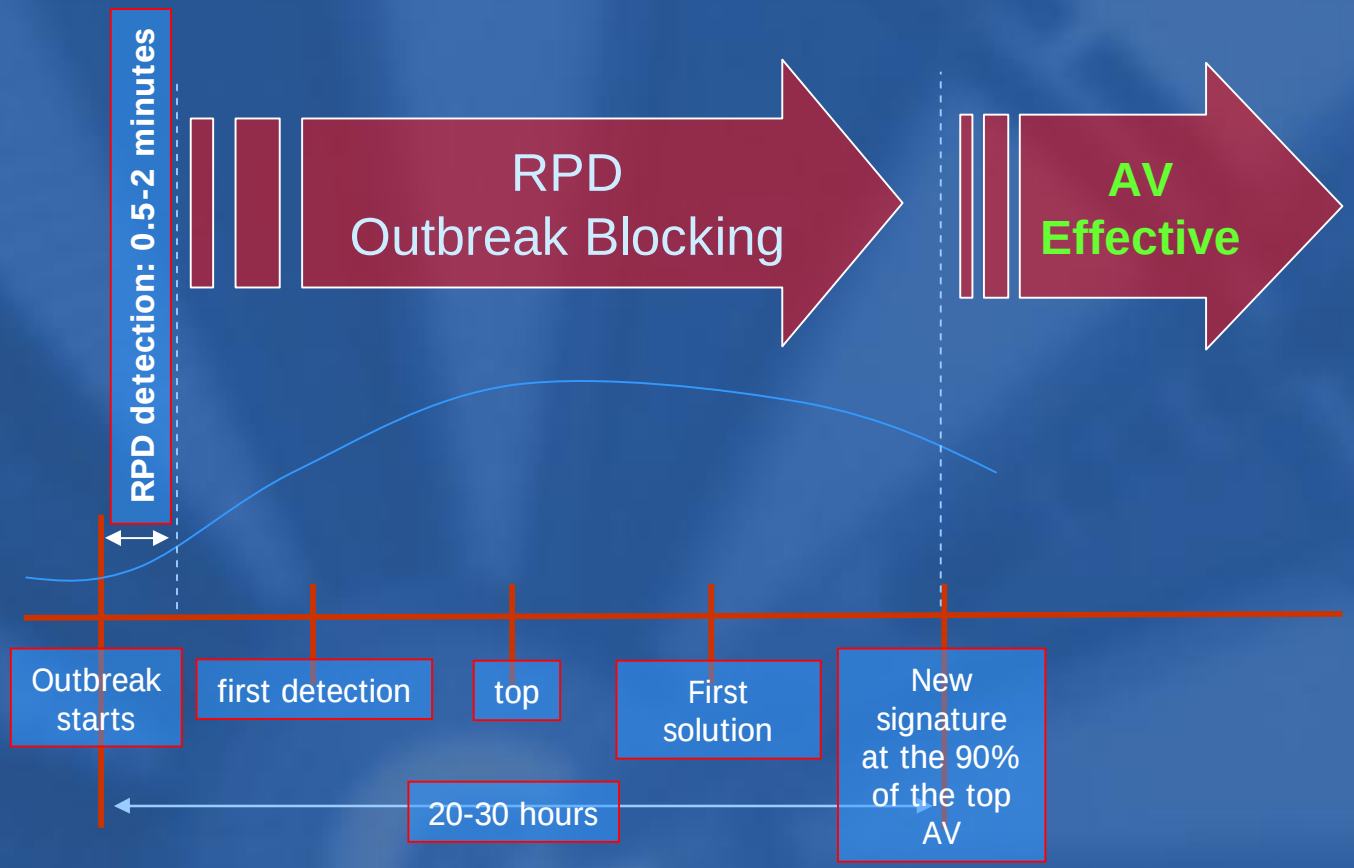


RPD™ szűrő

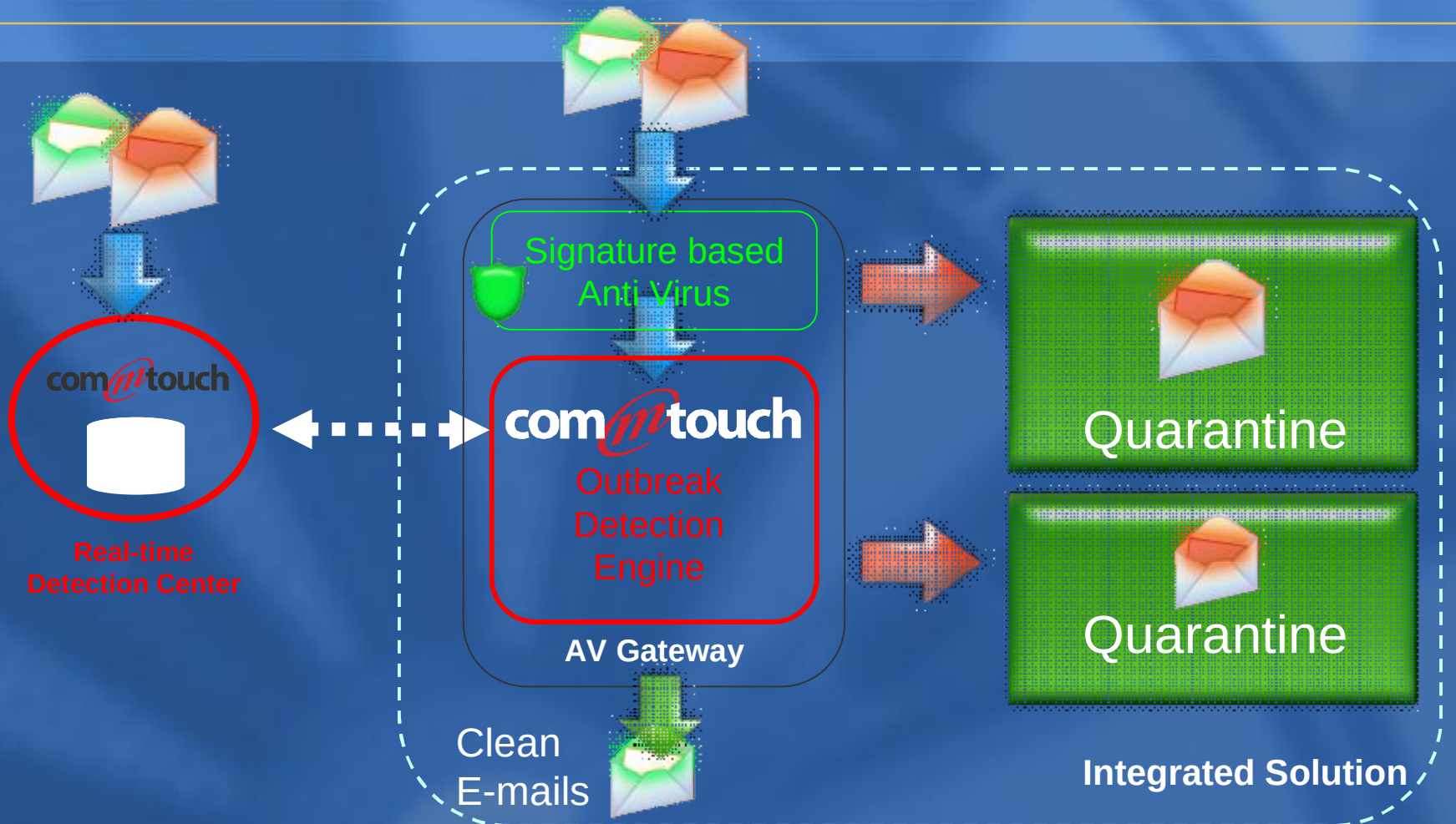
- **Recurrent Pattern Detection Technológia**
  - **Ismétlődő Minta Keresés**
  - Gyors
  - Pontos
  - Világra kiterjedő
  - Központilag karban tartott „Felejts el” alkalmazás
  - Nyelvfüggetlen



Reakció idő

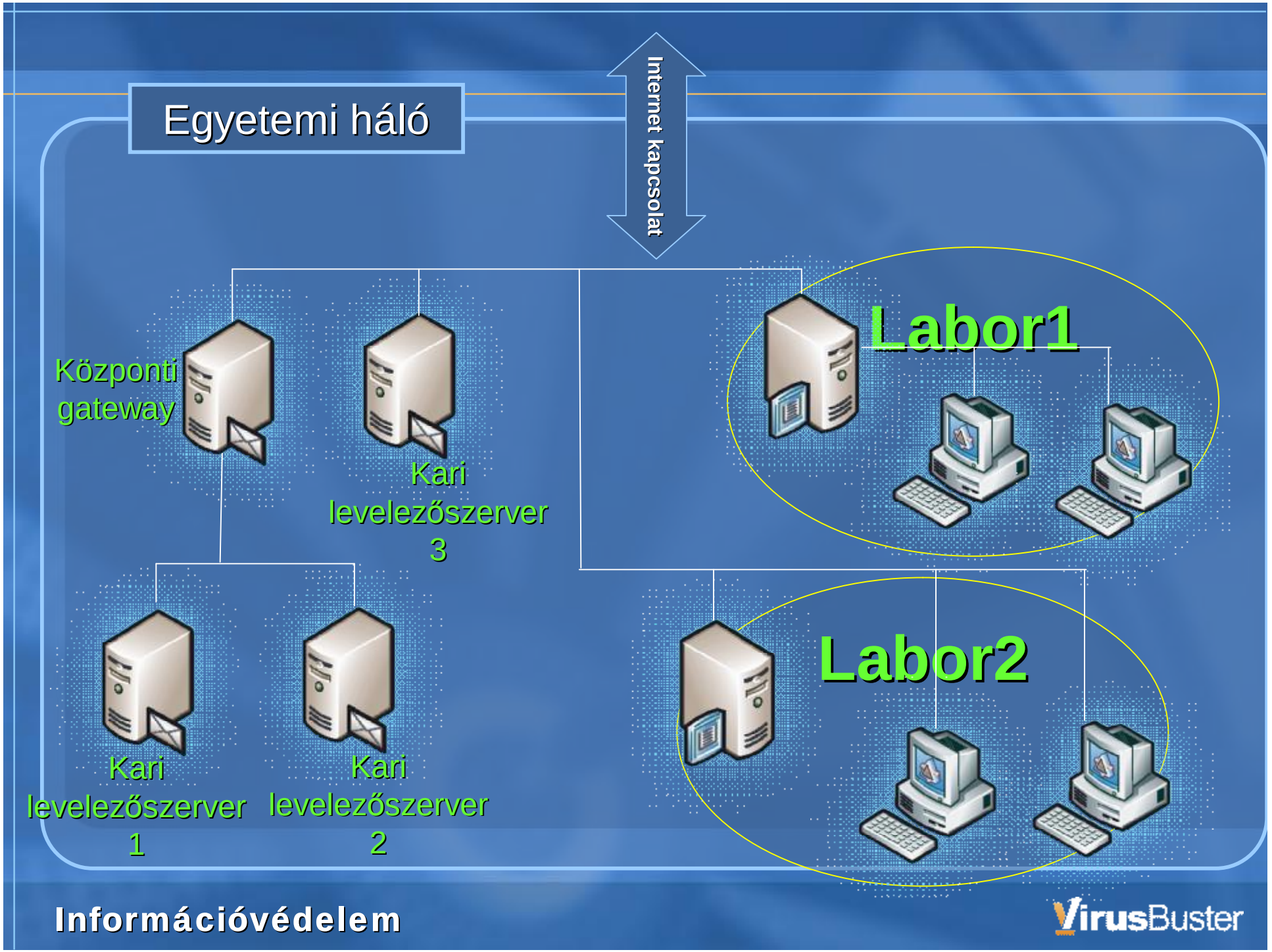

RPD detection: 0.5-2 minutes
RPD
Outbreak Blocking
AV
Effective
Outbreak starts
first detection
top
First solution
New signature at the 90% of the top AV
20-30 hours

Zero-Hour vírus felismerés

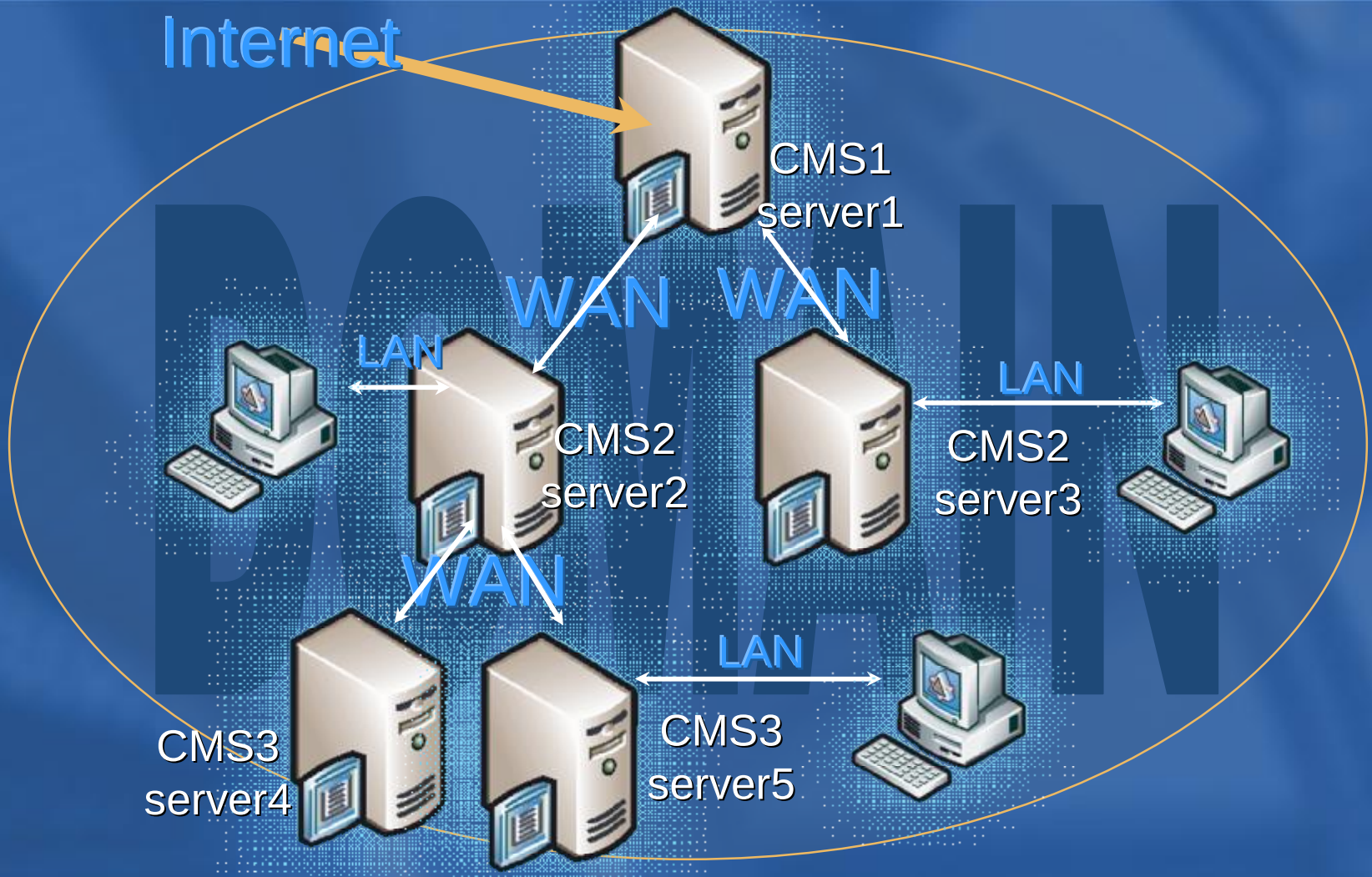


Védelmi megoldások fájlszinten

- Az egyetemi környezet ezen a területen is heterogén és tagolt
  - **Kari szinten a legtöbb esetben szétválasztva, akár laboronként is**
  - **Jogosultság kezelés lokalizált szinten megoldott, ezért menedzsmentje szintén lokalizált (helyi domain kontrollerek, több workgroup)**
  - **Pull technológiák működése sikeresebb a jogosultsági problémák miatt**
  - **Legtöbb esetben nem szeretnek támogatást igénybevenni**
  - **Szerver védelem és kliens védelem nem minden esetben megoldott**
  - **Heterogén hardver környezet**
  - **Egyéni programok és egyéni megoldások élnek az alkalmazott rendszerben**
  - **Gyártói támogatás mellőzése**

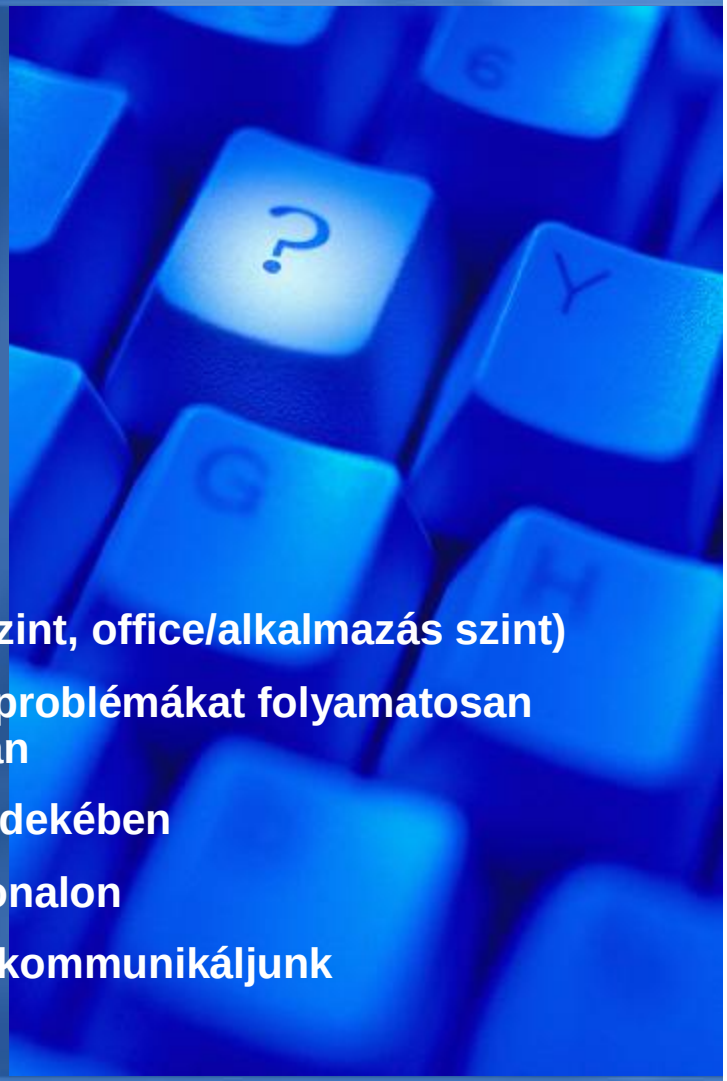

Egyetemi háló
Internet kapcsolat
Központi gateway
Kari levelezőszerver 3
Kari levelezőszerver 1
Kari levelezőszerver 2
Labor1
Labor2

Central Management Solution



Meglehet oldani?

- **Windows védelem**
  - Push & pull technológiák támogatása
  - Domain és workgroup támogatása
  - Időzített telepítések
  - Csak besorolt gépek telepítése
  - Eltérő konfigurációs beállítások
  - Optimalizált kommunikáció
  - Idegen szoftver eltávolítás
- **Megoldás Windows, Unix, Novell rendszerekre**
- **Többszintű szűrés (Fájlszint, kommunikációs szint, office/alkalmazás szint)**
- **Egyedi programoknál/rendszereknél felmerülő problémákat folyamatosan figyelemmel kísérjük és segítünk a megoldásban**
- **Folyamatos fejlesztések a hatékony védelem érdekében**
- **Tapasztalt, segítőkész kollégák a támogatási vonalon**
- **VirusBuster oldalról igény, hogy folyamatosan kommunikáljunk**



VirusBuster termékcsalád

Szerver

- VirusBuster for Windows Server NT4/2000/2003
- VirusBuster for Novell 4.11 or higher
- VirusBuster for SAMB

Kliens

- VirusBuster for DOS
- Buster for Windows Client E/NT4/2000/XP/Vista (Q2)
- d

Menedzsment

Central Management Solution

Plug-inek

- VirusBuster for MS Outlook Outlook98 vagy magasabb
- VirusBuster for MS Office Office 2000 vagy magasabb
- Tartalomszűrő

ise megoldások

- er Mailservers for SMTP
- BSD, Sun, AIX
- irusBuster Mailserver for Groupwise, Sendmail, Qmail, Postfix
- VirusBuster Enterprise Firewall 2004
- ZeroHour protection
- Extended Spam Protection

Információvédelem

VirusBuster

Szolgáltatások

Személyes szakmai támogatás

Kiemelt támogatás+ lekötött támogatási idő,
rendszerfelügyelet, folyamatos kapcsolat, naprakészség

Kiemelt támogatás

Alap támogatás+ dedikált szakember (helyi rendszerismeret)
Folyamatos rendelkezésre állás, emelt reakció idő (akár 2ó)

Alap támogatás

Szoftver és adatbázis frissítések biztosítása, telefonos és
e-mailes támogatás 48 órás reakció idő

VirusBuster
www.virusbuster.hu

KÉRDÉSEK ?

support@virusbuster.hu

https://SUPPORT.VIRUSBUSTER.HU

Microsoft CERTIFIED Partner