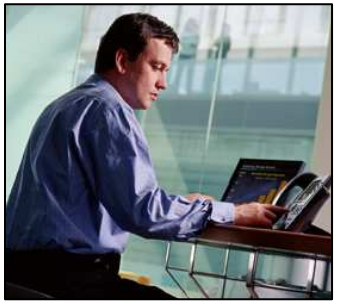
Cisco hozzáférés felügyelet és eseménykezelés

Hétpecsét Szakmai Fórum

HIRSCH GÁBOR
Cisco Magyarország
gahirsch@cisco.com

Általános piaci igények

A felhasználók három fontos elvárása



EGYSZERŰSÍTÉS

- Scale
- Cost
- Staffing
- Integration and systems management

ALKALMAZÁSOK OPTIMALIZÁLÁSA

- Enablers
- Awareness
- App management
- Performance/optimization
- Resilience

HÁLÓZATBIZTONSÁG FOKOZÁSA

- Threats
- Theft
- Loss
- Response time

Security = Still a Top Business Issue

Top Business Trends

	Ranking
Security breaches/business disruptions	**1**
Operating costs/budgets	**2**
Data protection and privacy	**3**
Need for revenue growth	4
Use of information in products/services	5
Economic recovery	6
Single view of customer	7
Faster innovation	8
Greater transparency in reporting	9
Enterprise risk management	10

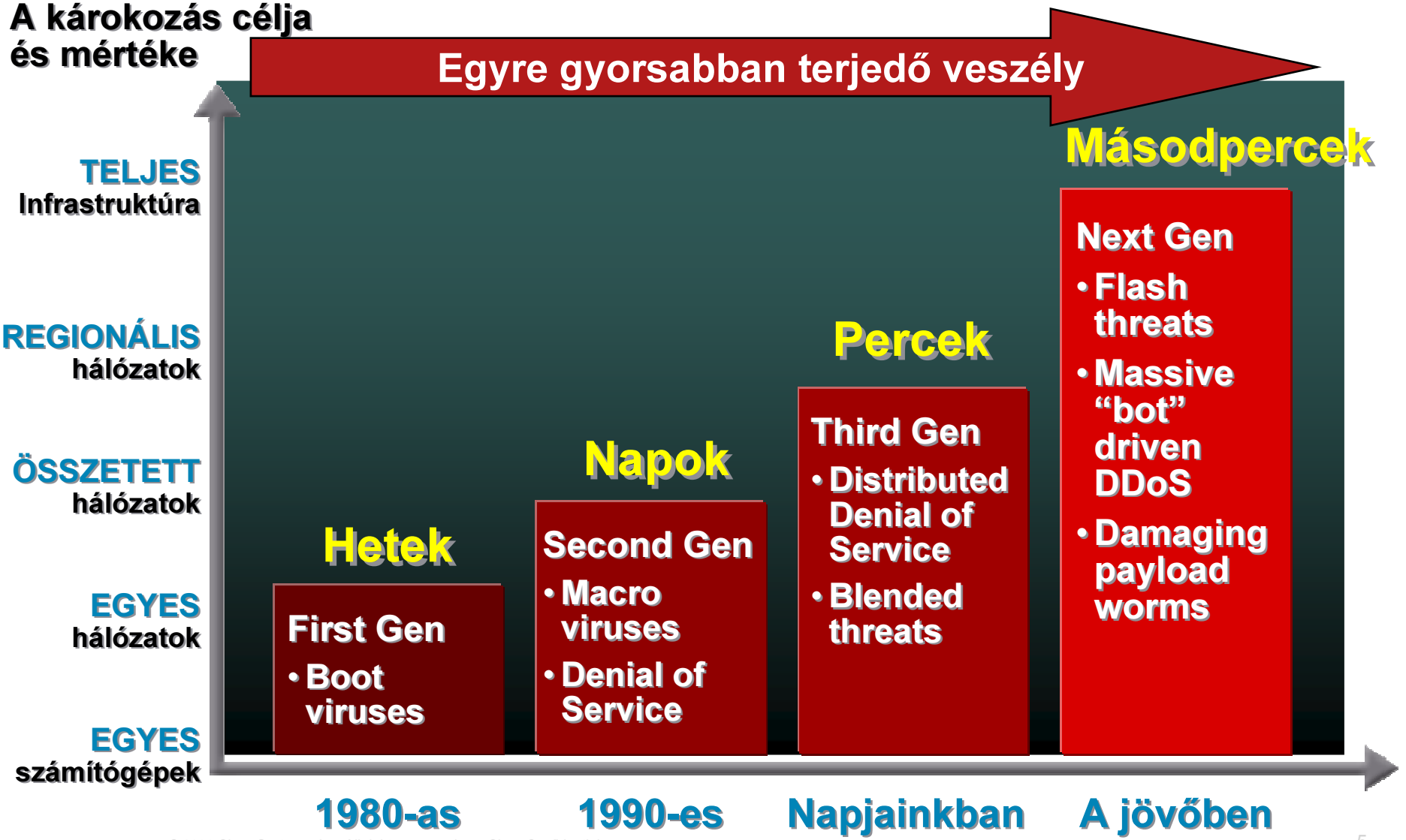
Source: Gartner Group, 2004

Top Security Challenges

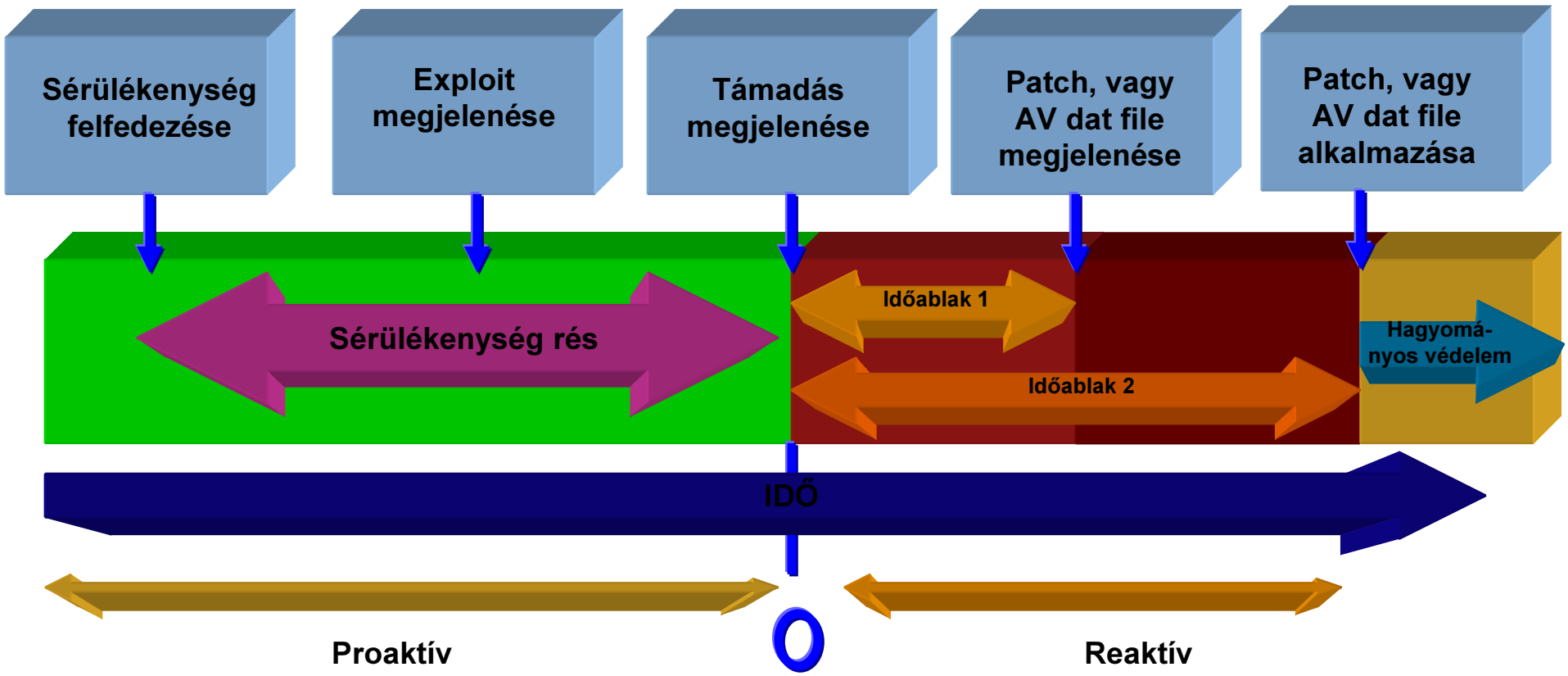
Ranking	
1	**Limited budget**
2	**Regulatory compliance**
3	**Educating executives on risks**
4	**Scope, volume and proliferation of data/devices**
5	**Not enough security staff**
6	Wireless LANs
7	Mobile clients
8	Company growth
9	Volume and complexity of network traffic
10	Lack of key security skills

Source: CSO/Cisco Proprietary Research, April 2006

A biztonsági kihívások evolúciója



Sérülékenységi rés – zero-update védelem



Konvergencia … D / V / V / M

Integrált és Átfogó Biztonság

Hozzáférés védelem

Authentication, Authorization and Accounting (AAA)

- Ki vagy? Mit csinálhatsz? Mit csináltál?
- Hogyan kapcsolódhat?
  - Standard hálózati hozzáférés
    - központban
    - telephelyen
  - Remote access hozzáférés
    - othonról
    - idegen hálózatból
  - Wireless hozzáférés
- Ki kapcsolódhat?
  - Alkalmazott
  - Partner
  - Contractor
  - Supporter
  - Vendég

Eddigi megoldások veszélye

1. A szervezet biztonsági szabályzatával nem egyező végpont megpróbál kapcsolódni

2. A kapcsolat engedélyezett

3. A támadás szétterjed a végpontok veszélyben vannak

Ahogy a Network Admission Control működik

Cisco Network Admission Control (NAC)

- A NAC a Cisco vezette iparági program, melynek célja az egyre inkább elterjedő biztonsági veszélyek (férgek, vírusok) által okozott károk csökkentése
- A NAC által az üzemeltetők a hálózati hozzáférést a hiteles végpontok (PDA, PC, szerver) számára engedélyezni tudják, míg a nem megfelelő eszközöket korlátozzák
- Ez a fejlesztés nagy mértékben javítja a hálózat képességét, hogy azonosítsa, megelőzze a veszélyeket és adaptálódjon hozzájuk

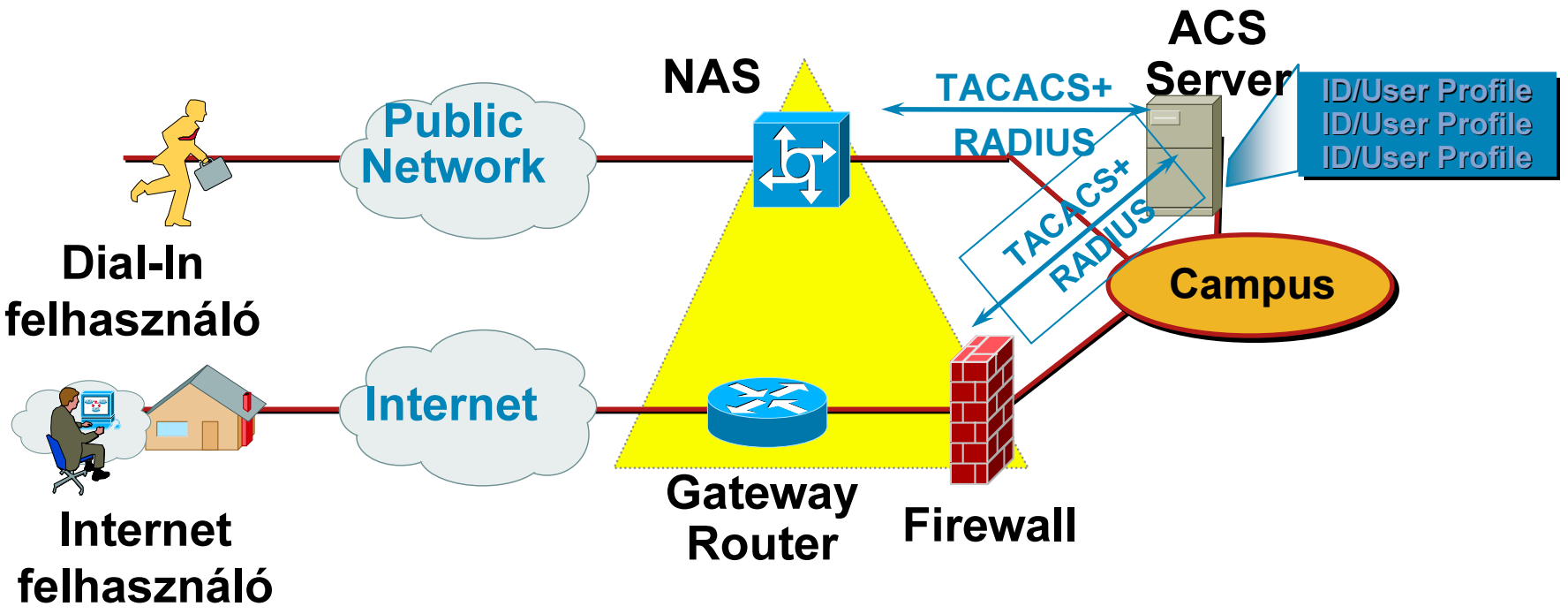
AhnLab
netForensics
SENFORCE
secure elements
infoexpress
CITADEL SECURITY SOFTWARE
BIGFIX

TREND MICRO
symantec.
Network ASSOCIATES
YOUR NETWORK. OUR BUSINESS.
IBM
ca
Microsoft

Erős NAC Partner Program

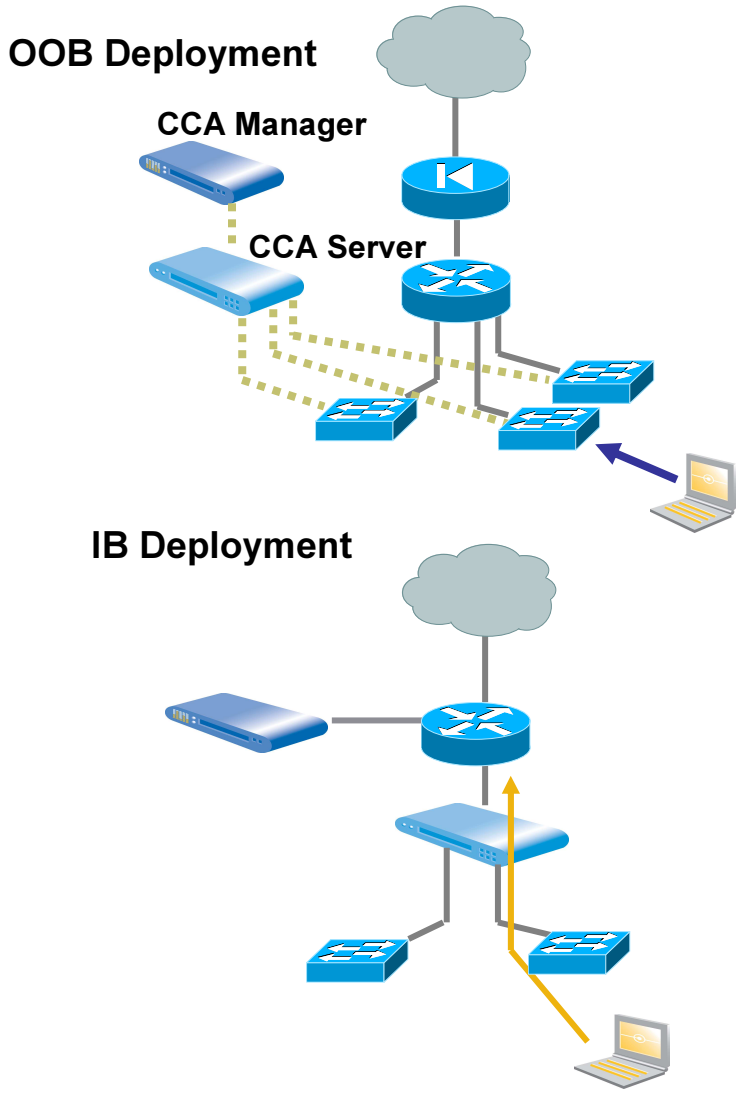
http://www.cisco.com/en/US/partners/pr46/nac/partners.html

ACS architektúra

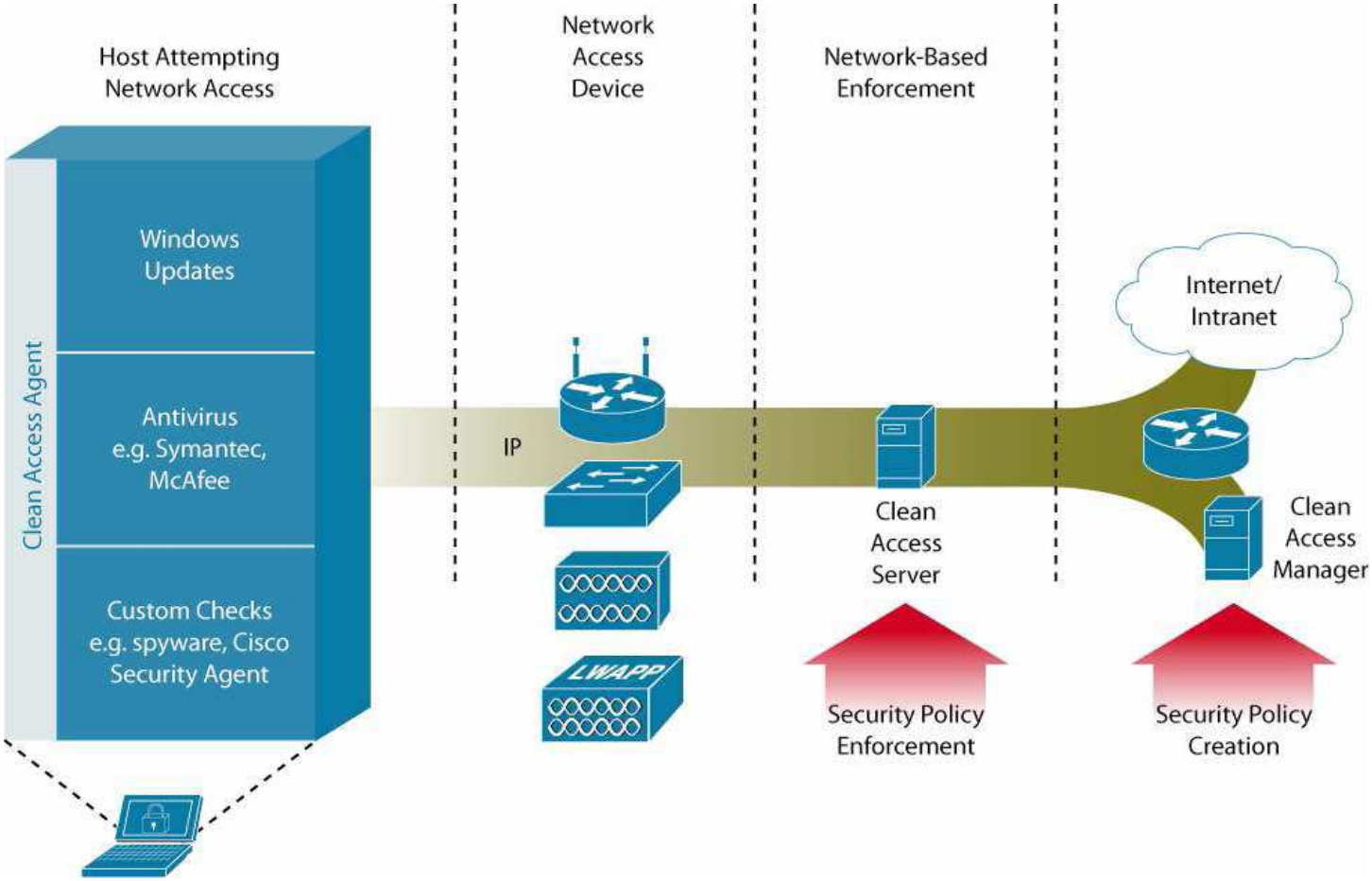


Cisco NAC Appliance

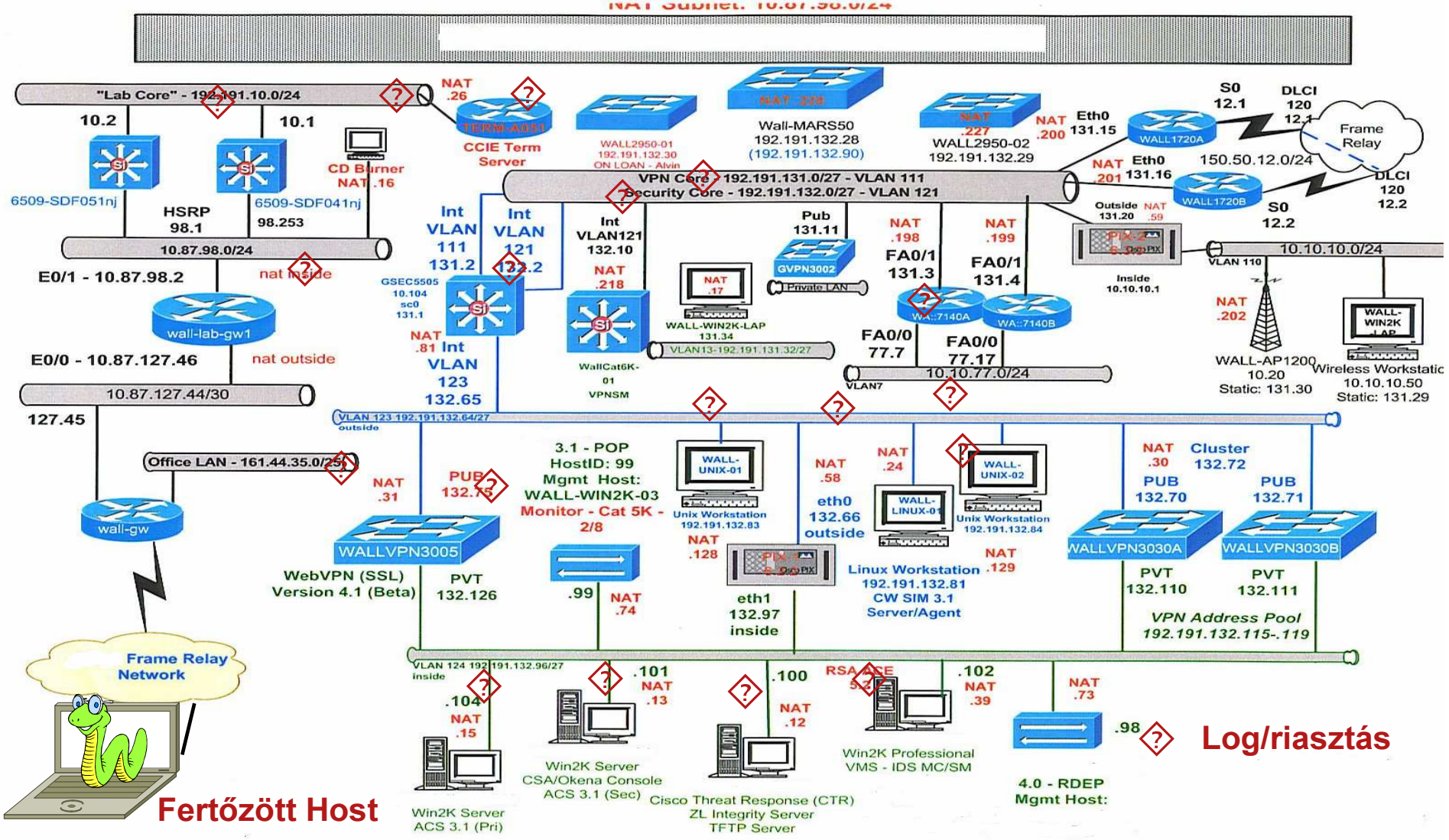
- User and posture validation for LAN and WLAN
- Unmanaged endpoints, straightforward network designs
- Out-of-band, VLAN-based quarantining via SNMP
- In-band option, bridge or first L3 hop (must see MAC address)
- 802.1x independent
- Key considerations
  - Location of CCA server (VLAN reach)
  - Remediation load scaling
  - Access layer complexity (IP phone, hub)



NAC appliance alkalmazása Wi-Fi környezetben



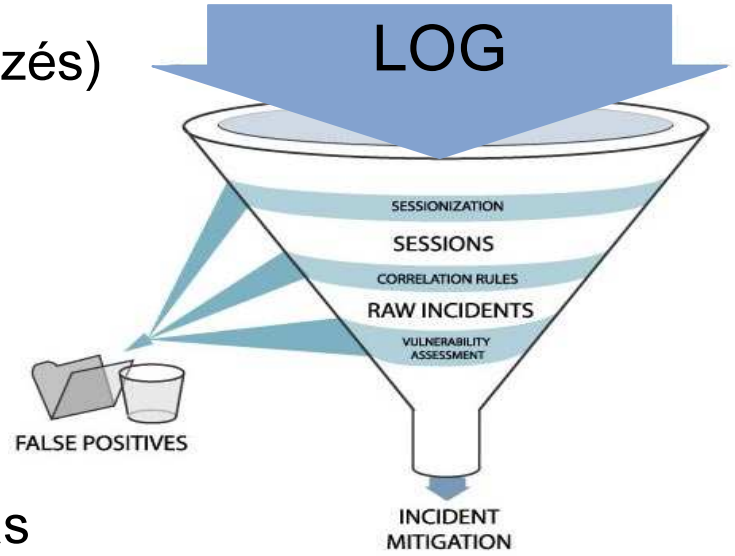
Mélységi védelem = komplexitás



Eseménykezelés (SIEM)

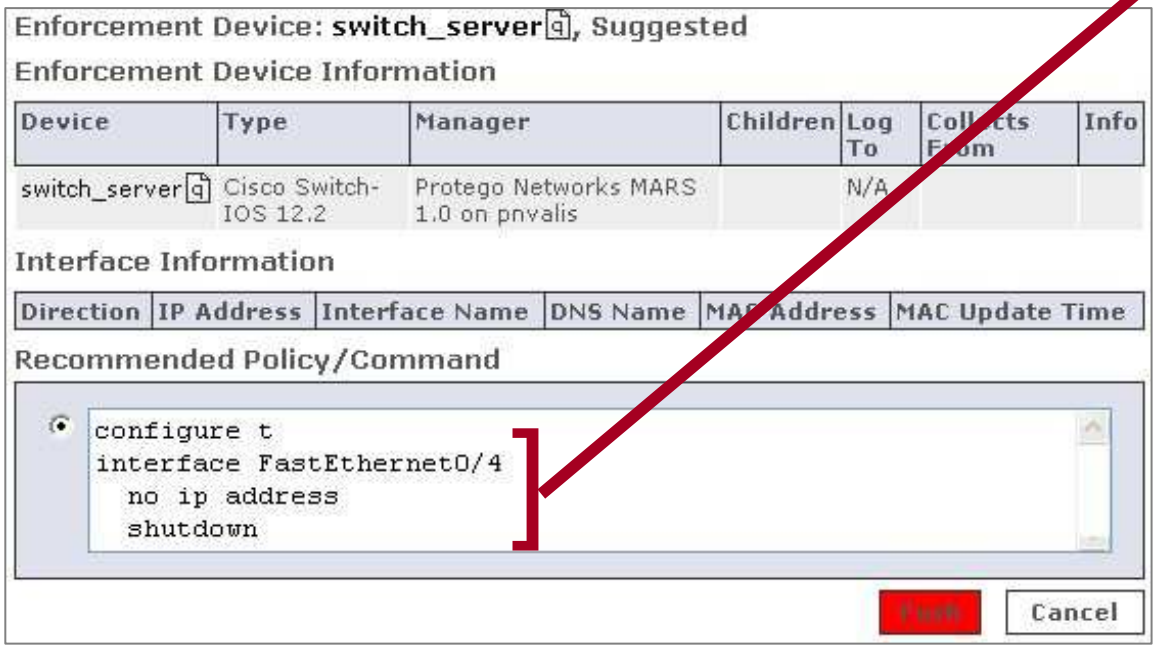
Hogyan működik?

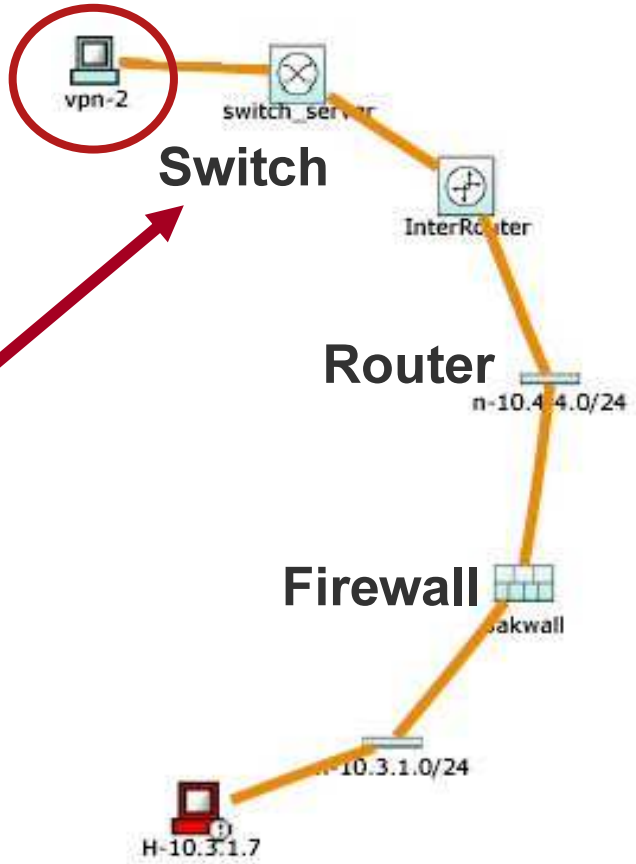
1. Eszközök/alkalmazások naplóállományainak (események) összegyűjtése
2. Események elemzése, értelmezése
3. Események normalizálása (session képzés)
4. Korreláció
5. Szabályok futtatása
6. False Positive analízis
7. Gyanús host-ok kiszűrése
8. Forgalom viszgálat, anomália azonosítás



CS-MARS - alkalmazott védelem

- Vezérlési lehetőségek
  - Layer 2/3 támadási út világosan látható
  - A kivédési eszközök definiálhatók
  - A pontos kivédési parancs megadható





CS-MARS előnyök

- Fejlett funkcionalitás, legalacsonyabb TCO
- Azonnali eredmények
  - Gyors installációs, out-of-box használat, web-based HTML console
  - Agentless capture, embedded Oracle®, no dba necessary
  - Az elterjedt hálózati és biztonsági eszközök támogatása …
    Cisco, NetScreen, McAfee, Nokia, Extreme, Checkpoint, ISS, Enterasys, Foundstone, Snort, eEye, Windows, Solaris, Linux, Oracle, Web, Cacheflow, Cisco Netflow…

- Optimalizát teljesítmény és skálázhatóság
  - Gyors in-line processzálás
  - ~ több, mint 10,000 EPS minden szolgáltatással együtt
  - Nagy kapacitású RAID tároló, folyamatos NFS archive
  - A Global Controller elosztott CS-MARS menedzsmentet támogat

További információ

Cisco Self Defending Network Strategy
www.cisco.com/go/selfdefend

Cisco Threat Defense System
www.cisco.com/go/tds

Cisco Security and VPN Solutions
www.cisco.com/go/security

Cisco SAFE Blueprints
www.cisco.com/go/safe

Cisco Security Partners
www.cisco.com/go/securitypartners

- Performance of Cisco IOS Routers, PIX and VPN 3000
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/netbr09186a00801f0a72.html
- Remote Access and SSL VPN demo
  http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/prod_presentation0900aecd8015029c.html

Q and A