TippingPoint

IDS vs IPS…

… nenechte muže zemřít !!

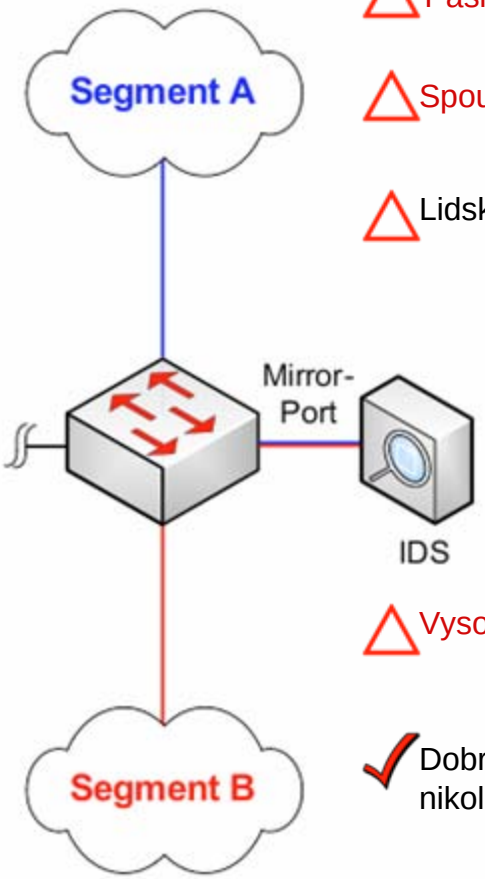
Miroslav Knapovsky – 3Com senior systems engineer EMEA

IDS proti IPS

TippingPoint

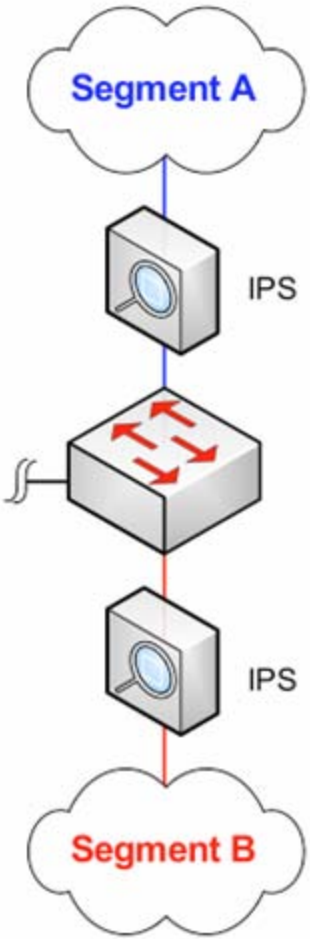
IPS SECURED NETWORKS

IDS



- Pasivní monitorování
- Spousta logů
- Lidský faktor
- Vysoké náklady na provoz
- ✓ Dobré řešení pro auditing, nikoliv pro reálný život

IPS



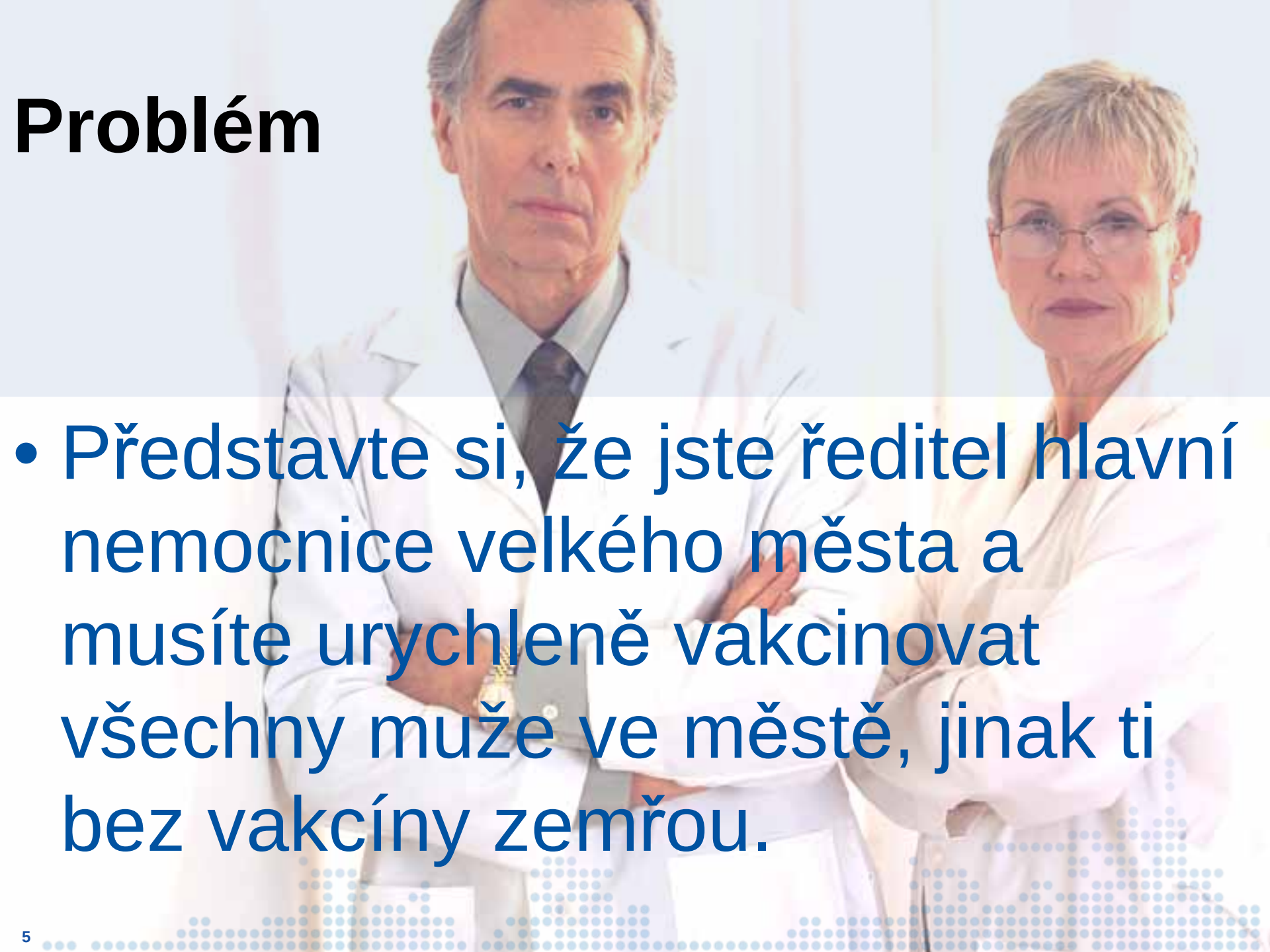
- ✓ Preventivní ochrana
- ✓ Zvyšuje bezpečnost bez vlivu na korektní aplikace
- ✓ Cenově efektivní oproti nákladům na obnovu a možnému výpadku . Minimalizuje rizika.
- ✓ Dává administrátorům čas K distribuci bezpečnostních a opravných balíčků.
- ✓ Nízké TCO

TippingPoint

IPS proti IDS

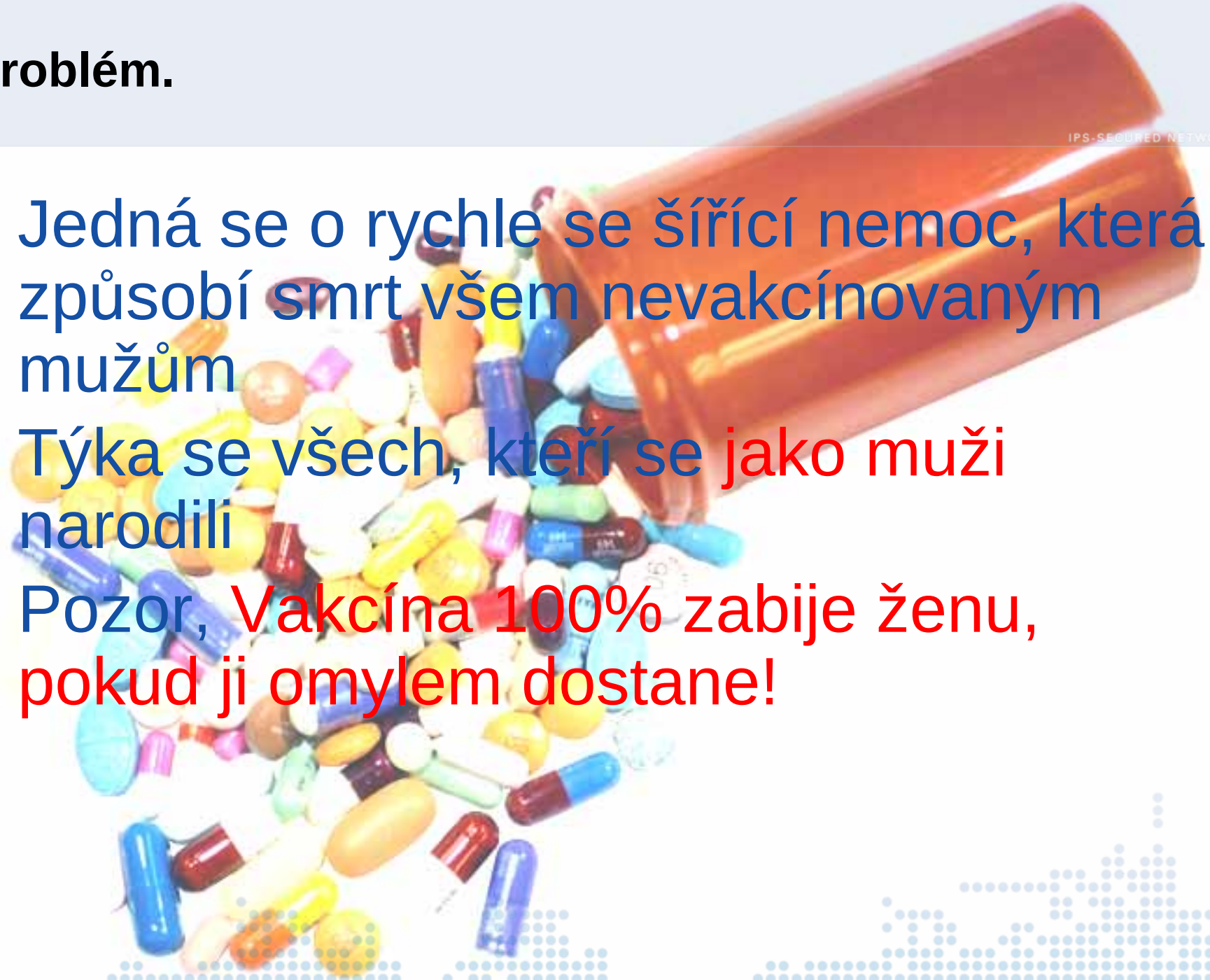
Nebo … jak zachránit všechny muže bez omylu.

Problém



- Představte si, že jste ředitel hlavní nemocnice velkého města a musíte urychleně vakcinovat všechny muže ve městě, jinak ti bez vakcíny zemřou.

Problém.



- Jedná se o rychle se šířící nemoc, která způsobí smrt všem nevakcínovaným mužům
- Týka se všech, kteří se jako muži narodili
- Pozor, Vakcína 100% zabije ženu, pokud ji omylem dostane!

- Na vakcinaci máte 24 hodin.

Jak budete při rozlišování postupovat?

TippingPoint

IPS-SECURED NETWORKS

- Podle jména či příjmení?
- Podle délky vlasů?
- Podle oblečení, naušníc, prstýnků?
- Podle make-up?
- Podle tetování?
- Podle anatomie (Jsou ty prsa mužská nebo ženská ☺)?
- …?
- …?

… Pamatujte – žádné omyly, nebo žena zemře. Tak kdo to vlastně je…

Řešení ?

TippingPoint

IPS SECURED NETWORKS

- **Čím více se budete ptát, tím déle rozbor zabere. Takže vám může dojít čas. Nevakcinovaní muži zemřou.**

- **Můžete omezit množství otázek? Méně dotazů = rychlejší analýza pohlaví.**
  - **…Ale také více omylů a více lidí zemře – obou pohlaví.**
  - **Což je mimoděk běžný přístup u většiny výrobců IPS.**

- **Pokud budete pracovat se statistikou, nevypadá to zle…**
  - **Někteří muži samozřejmě zemřou, ale zachráníte 95%**

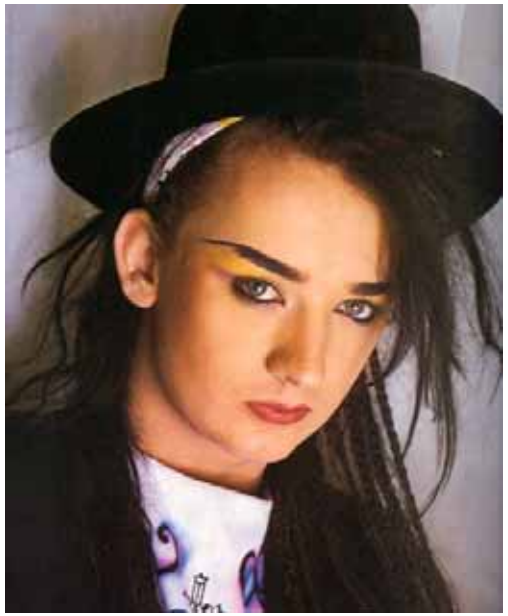
??? Ale existuje možnost, že na nevakcinovaných mužích virus zmutuje a napadne i ostatní vakcinované.

…Pokud by jste je již neviděli dříve

TippingPoint

IPS SECURED NETWORKS

- **Nechali by jste je zemřít?**



Jak tento problém efektivně vyřešit?

TippingPoint
IPS SECURED NETWORKS

- **Jak tento problém vyřešit s minimalizováním možného omylu?**
  - **Více specializovaných doktorů. (ASIC, FPGA, Paralelní zpracování!)**
  - **Základní kontrola je snadná, ale s některými lidmi je třeba strávit více času.**
  - **Vložit více do vývoje efektivnější kontroly**

    = přijít na rychlý a efektivní způsob rozpoznání Y genu v chromozónu rozborem dotyku prstu.

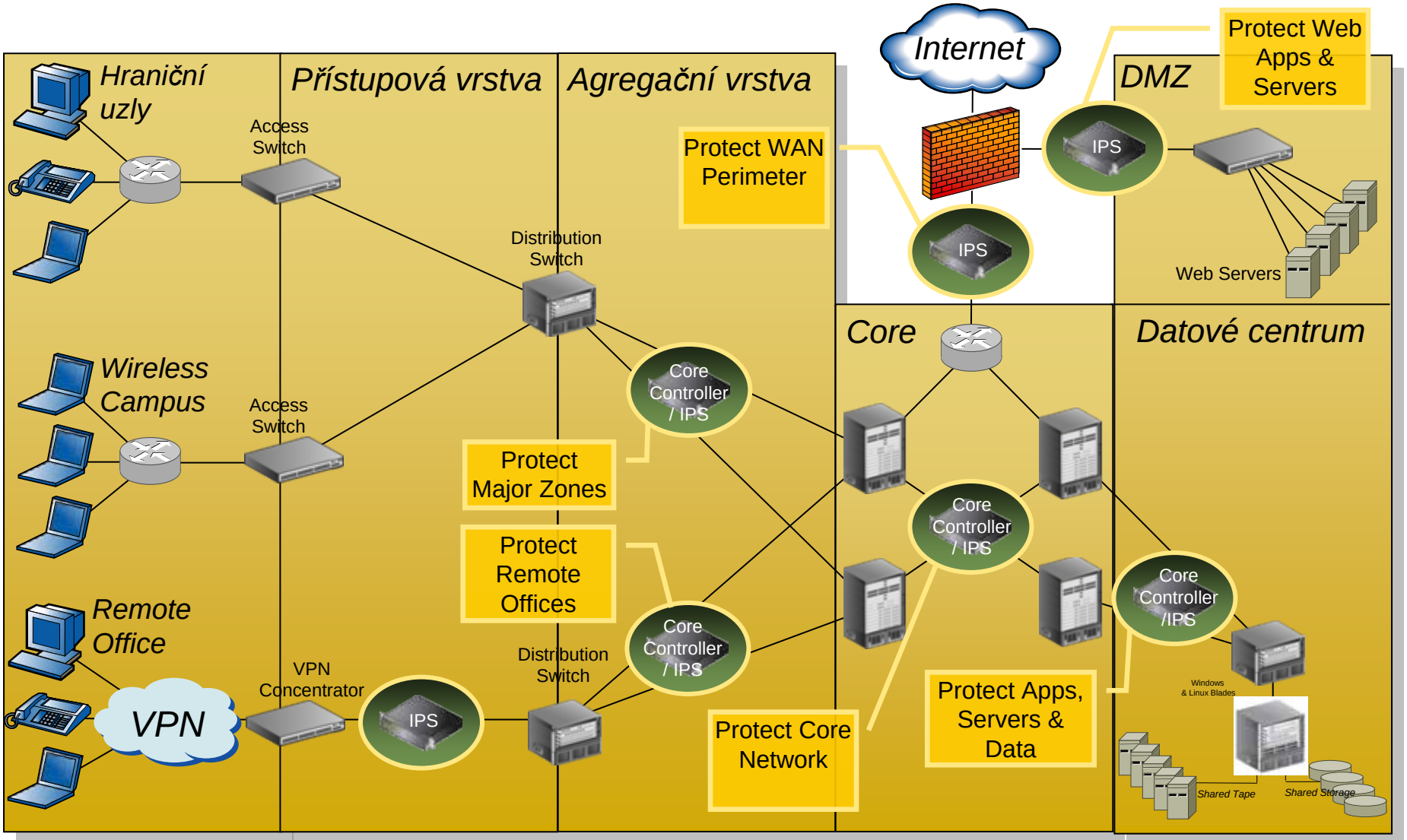
- **100% jistota. Žádná falešná pozitiva (nebo negativa)**
- **Tak jako Tipping Point IPS.**

TippingPoint IPS

- **Rozdílný přístup k IPS architektuře**
- **Minimální čas na instalaci.**
  - **Není komplikované.**
  - **Nepotřebuje týdny na ladění…vlastně není třeba ladit vůbec.**
  - **Žádné učící se módy.**
  - **Žádné zpoždění. Nezpomaluje aplikace.**
- **Žádná falešná pozitiva! (Boy George přežije taky!)**
- **Nevyžaduje tým odborníků ke správě.**
- **38% podíl na trhu.**

Flexibilní řešení od centra sítě až k hraničním uzlům

TippingPoint



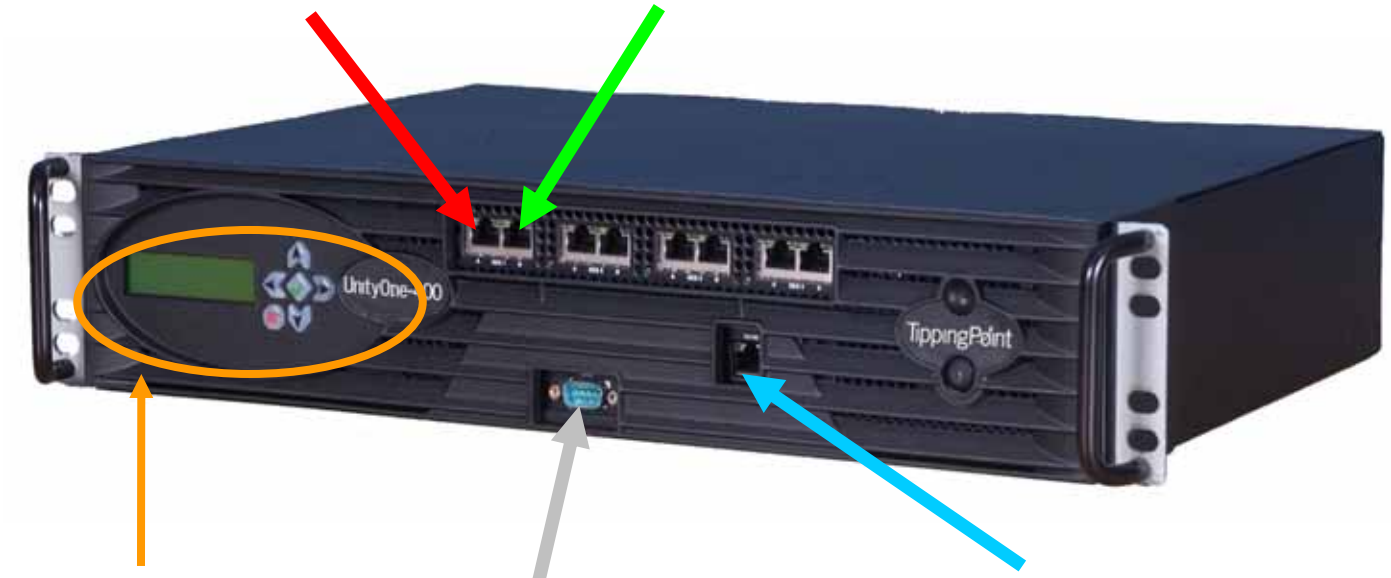
TippingPoint Unity-One IPS

TippingPoint

IPS SECURED NETWORKS

Segment 1 –
Ethernet port A

Segment 1 –
Ethernet port B



LCD

Console Port (DB9)
(115,200 BPS, 8, N, and 1)
Null Modem Cable

Out-of-Band Management
10/100 Ethernet Port

Popis TippingPoint technologie

TippingPoint

PROTECTS...
- Microsoft Applications & Operating Systems
- Oracle Applications
- Linux O/S
- oIP

FROM...
- Worms/Walk-in Worms
- Viruses, Trojans
- DDoS Attacks
- Internal Attacks
- Unauthorized Access
- Spyware

PROTECTS...
- Routers (e.g. Cisco IOS)
- Switches
- Firewalls (e.g. Netscreen, CheckPoint FW1)
- oIP

FROM...
- Worms/Walk-in Worms
- Viruses, Trojans
- DDoS Attacks
- SYN Floods
- Traffic Anomalies

PROTECTS...
- Bandwidth
- Server Capacity
- Missions-Critical Traffic

FROM...
- Peer-to-Peer Apps
- Unauthorized IM & other Apps
- DDoS Attacks

rol

- Constant update protection service
- Bi-weekly Digital Vaccine

In-line, Automated, Evergreen Attack Prevention

TippingPoint Intrusion Prevention Systems

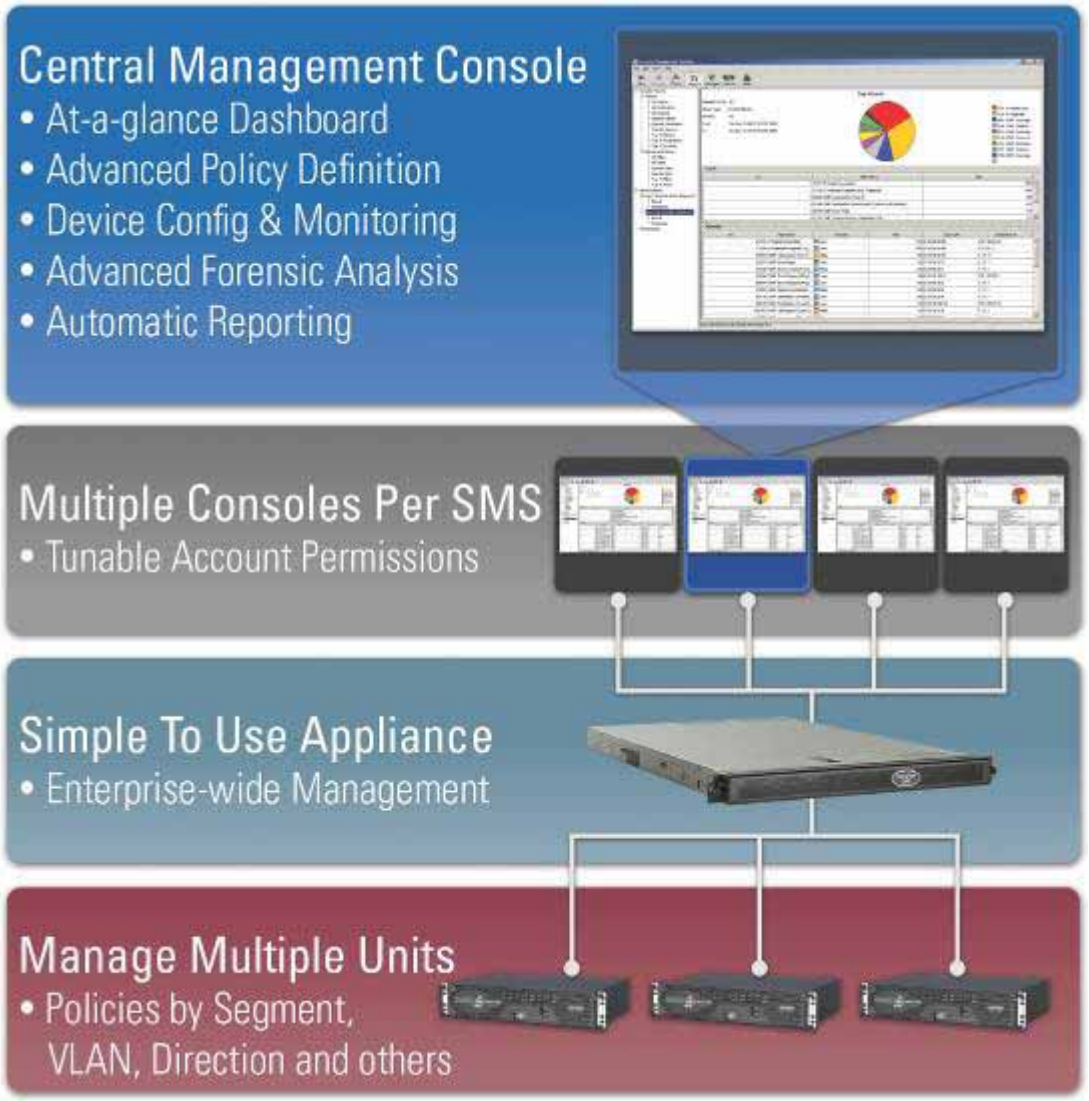
Application Protection

Infrastructure Protection

Performance Protection

Centrální správa, distribuované nasazení

- **Snadná instalace**
- **Snadná škálovatelnost a odolnost proti výpadku**
- **Vysoká dostupnost**
- **Distribuce politik**
  - **Na segment**
  - **Na virtuální segment**
  - **Na skupiny zařízení**

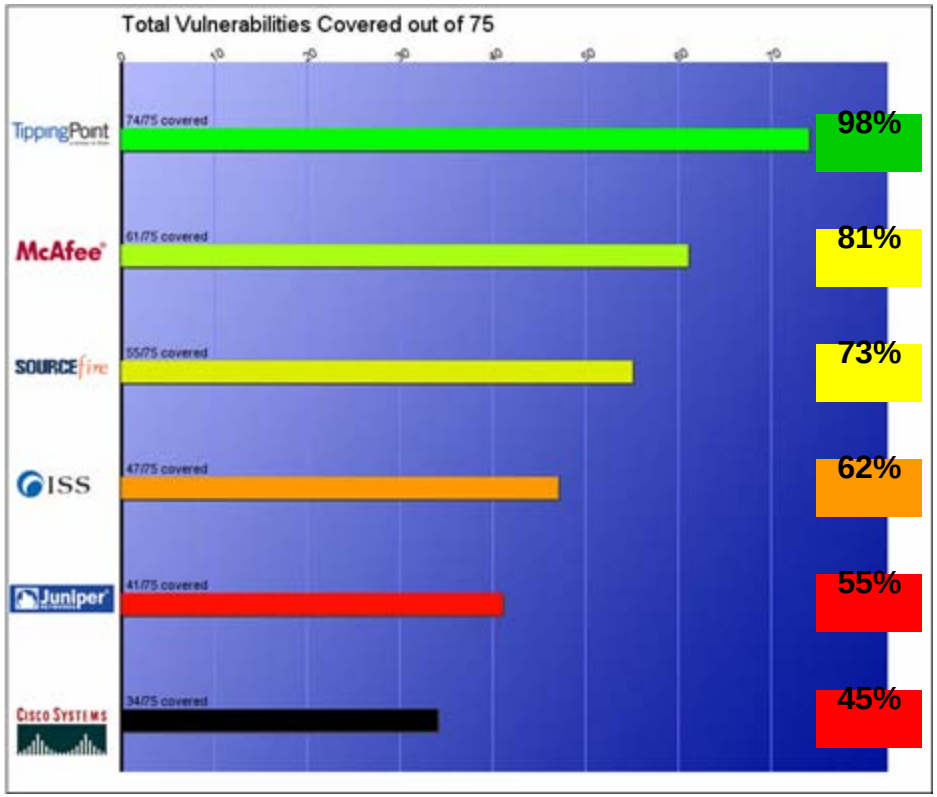


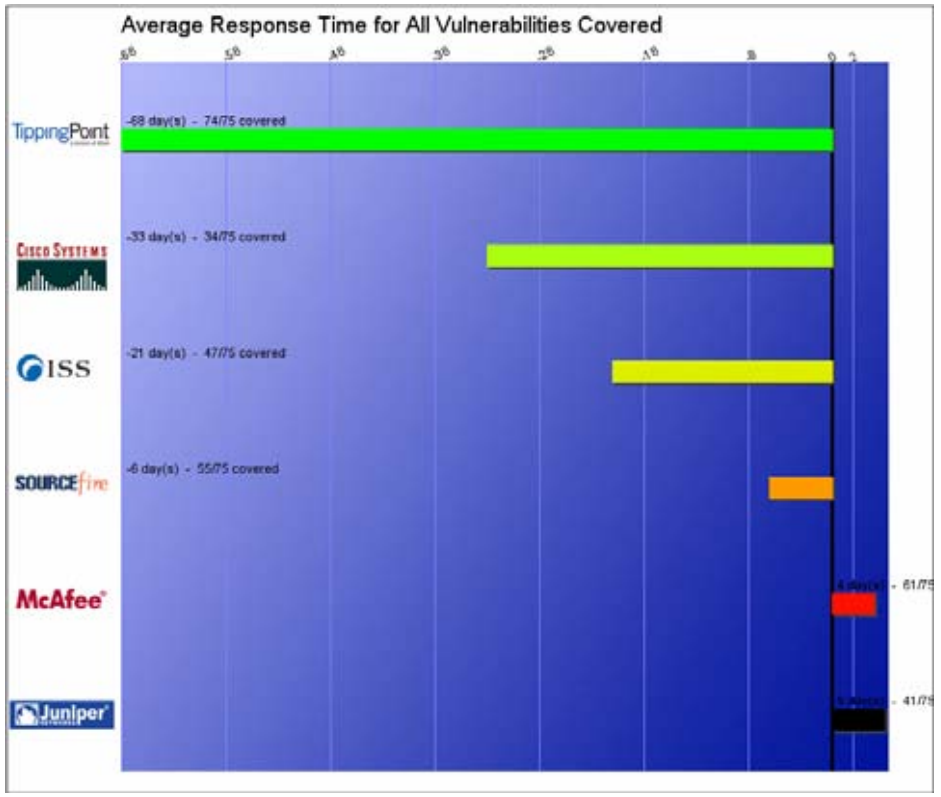
Digital Vaccine® – Rychlost pokrytí

TippingPoint

IPS SECURED NETWORKS

2008 Microsoft Vulnerability Coverage



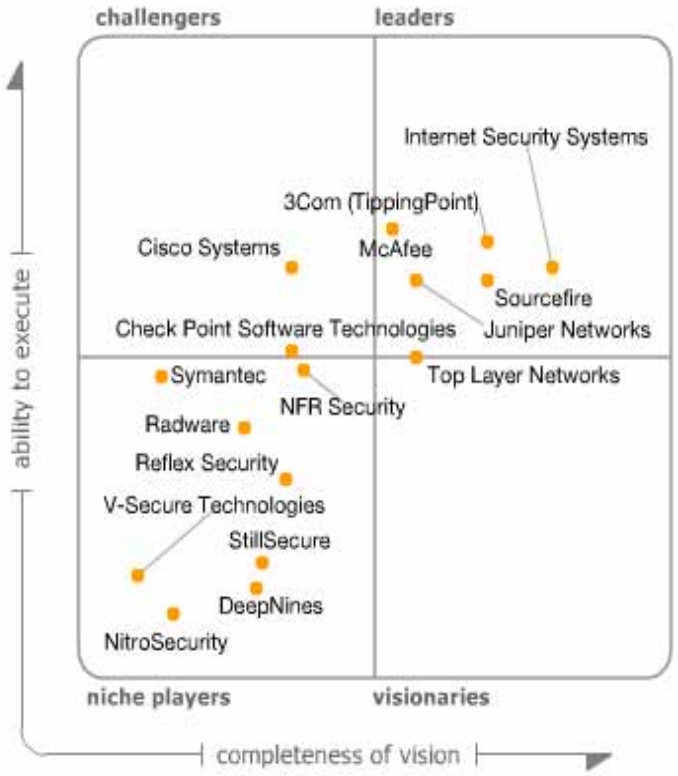


Unparalleled Security Coverage

- Greatest number of vulnerabilities covered
- Fastest to protect customers
- Leader in Microsoft coverage
- TP Research Team + ZDI = Best of Breed

The Usual Gartner.....- 2005 & 2006

TippingPoint

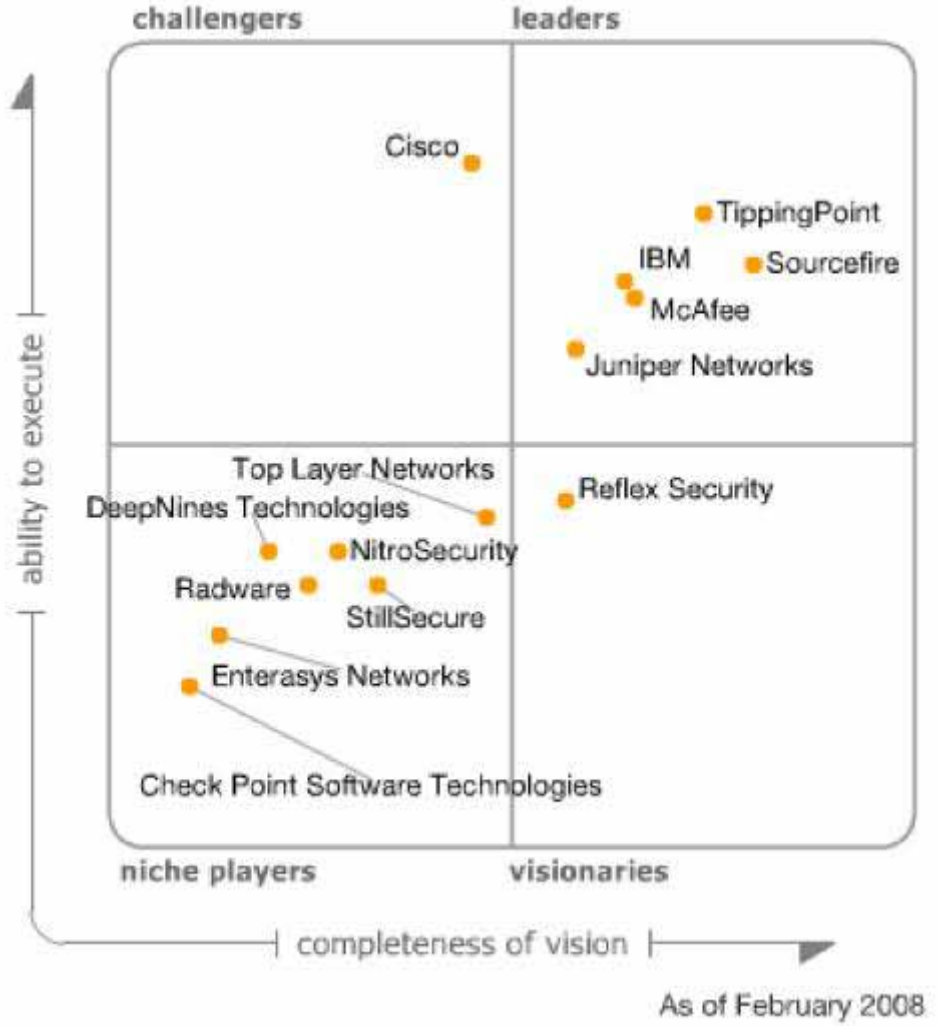


Quelle: Gartner (November 2005)

Source: Gartner (December 2006)

Gartner Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08

TippingPoint



Source: Gartner (February 2008)

- "This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from TippingPoint."

* Magic Quadrant Disclaimer
The Magic Quadrant is copyrighted February 14, 2008 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The "Magic Quadrant for Network Intrusion Prevention System Appliances, 1H05" was authored by Greg Young and John Pescatore February 14, 2008.

TippingPoint's Blue Chip Customer Base

TippingPoint

IPS SECURED NETWORKS

- 3,200+ customers worldwide, across every major industry and geography

Automotive

BMW, Volkswagen, Hyundai, Volvo, DaimlerChrysler, Bridgestone, Toyota

Education

The University of Texas Health Science Center at Houston, Texas State University, UCLA, Colorado College, University of Dayton, Wake Forest University, Boston College, Regis University, University of Miami, Ohio University

Financial

Fidelity Investments, T. Rowe Price, BancTec, ING, TSYS, Cannex, Archstone Smith, Countrywide Financial

Government

Los Alamos National Laboratory, NASA

Media

Discovery.com, cable onda, NBC, NCSOFT, Univision, dish Network, Viacom

Healthcare

GE, Blue Shield, The University of Texas MD Anderson Cancer Center, Galderma, Mission St. Joseph's, UW Health, American Cancer Society, WellStar Health System, BlueCross BlueShield of Tennessee

Retail

Overstock.com, Ross Dress for Less, Wal-Mart, Pier 1 Imports, Office Depot, Safeway, JCPenney

Technology

EarthLink, Hitachi Inspire the Next, LG, Texas Instruments, NCSOFT, Dell, Charter, NovAtel, mtm, hp invent

TippingPoint's Blue Chip Customer Base, Cont.

TippingPoint

IPS SECURED NETWORKS

- 3,200+ customers worldwide, across every major industry and geography

TippingPoint

Děkuji za pozornost

- Miroslav_Knapovsky@3com.com