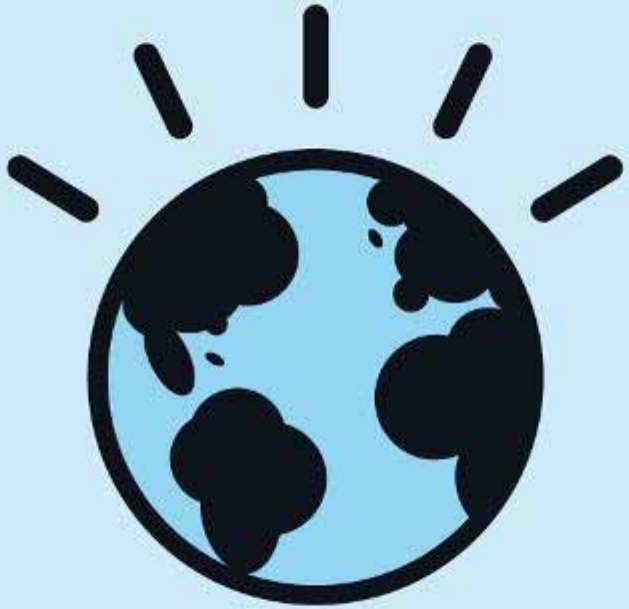
# Detekce anomálií v síťovém provozu, systémy prevence průniku

Jan Vaněk, IT Security & Business Continuity Services



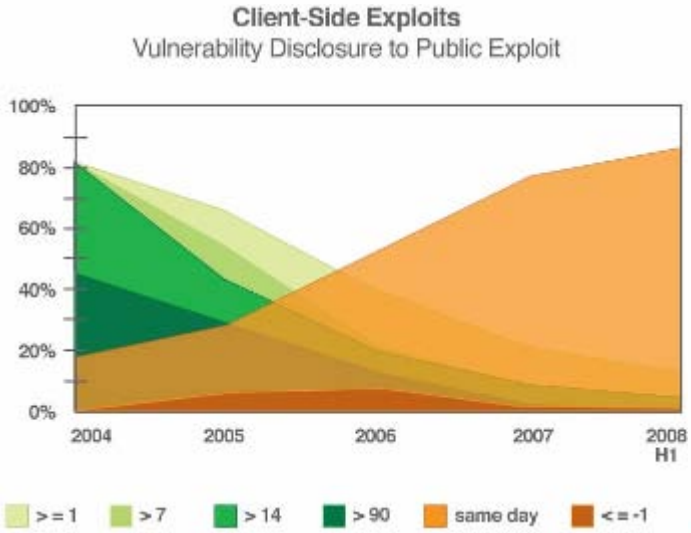
A smarter planet means
a brighter future.

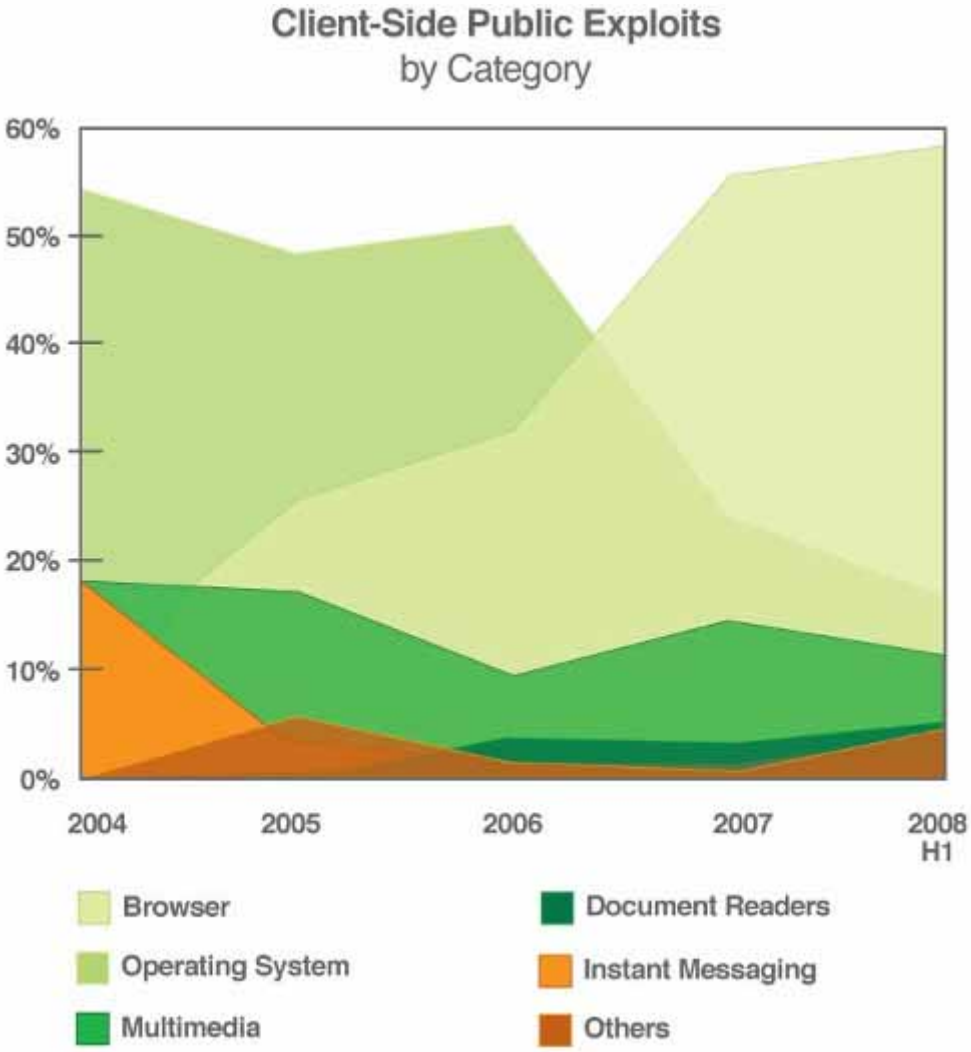
# Internet Security Systems

- Založena v r.1994, ústředí USA Atlanta, akvizice ISS v roce 2006
- Orientována čistě na bezpečnost, průkopník a vedoucí společnost na trhu síťové bezpečnosti IDS/IPS systémy a vulnerability skenování (core produkty)
- Vlastní výzkumný a vývojový team X-Force

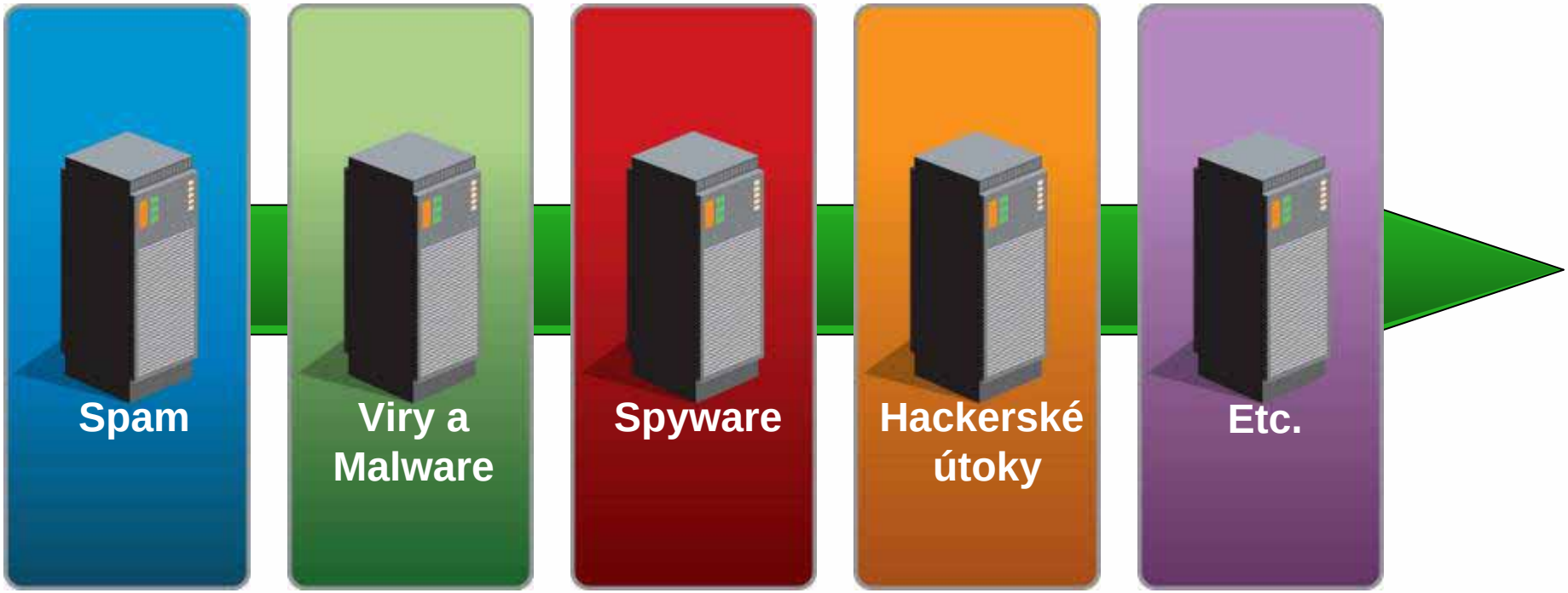
# Zranitelnosti na koncových stanicích

- Zvyšuje se dostupnost exploitů
- Více než 80% veřejných exploitů je vytvořena ve stejný den, kdy je publikována zranitelnost
- Většina exploitů je směrována vůči prohlížečům a ne proti OS, jak tomu bylo v minulosti.



# Problémem je efektivní ochrana před dnešními komplexními hrozbami

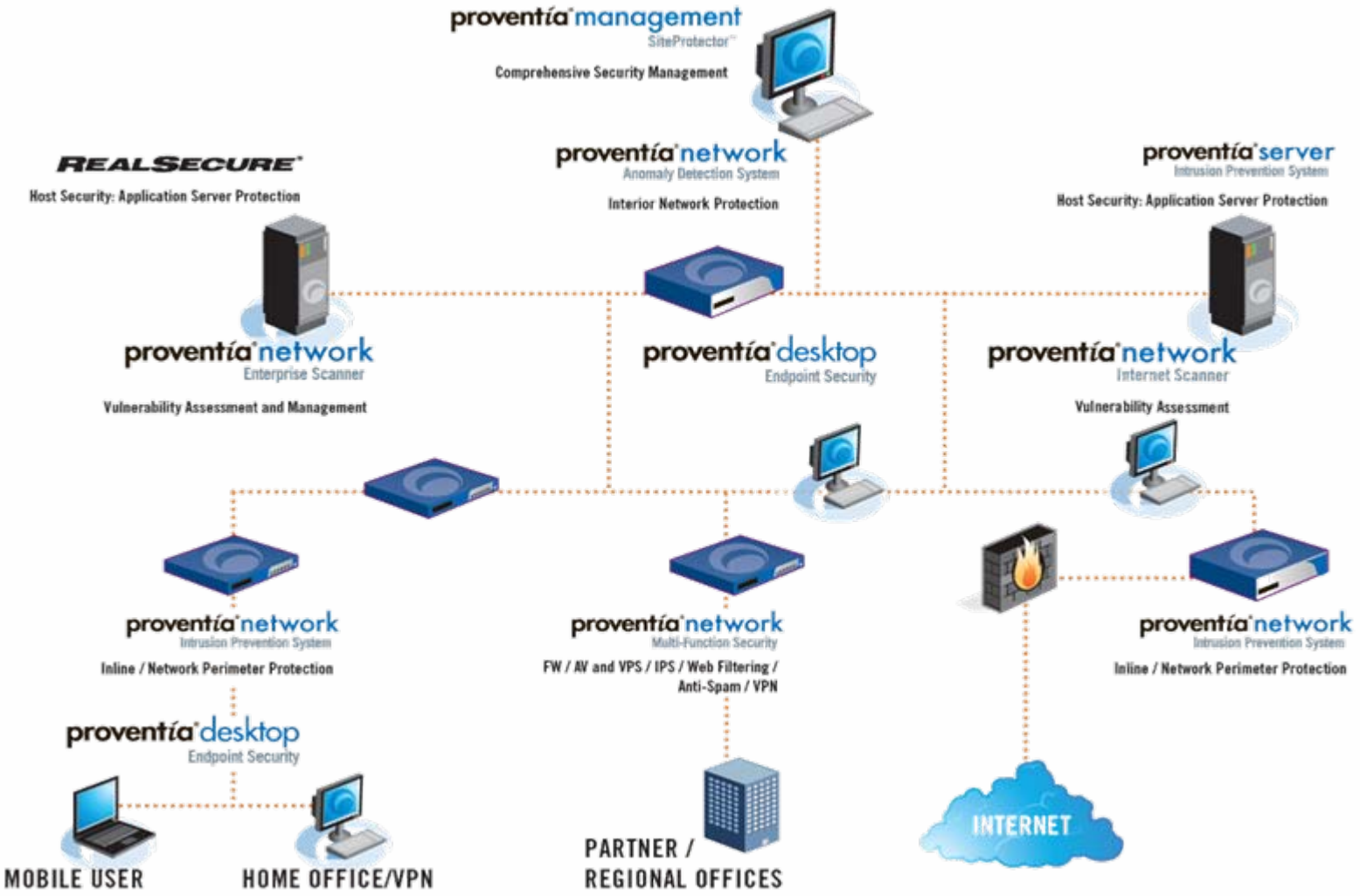



Issue of:

- Complexity, Scalability, Reporting
- No longer addresses complex security issues

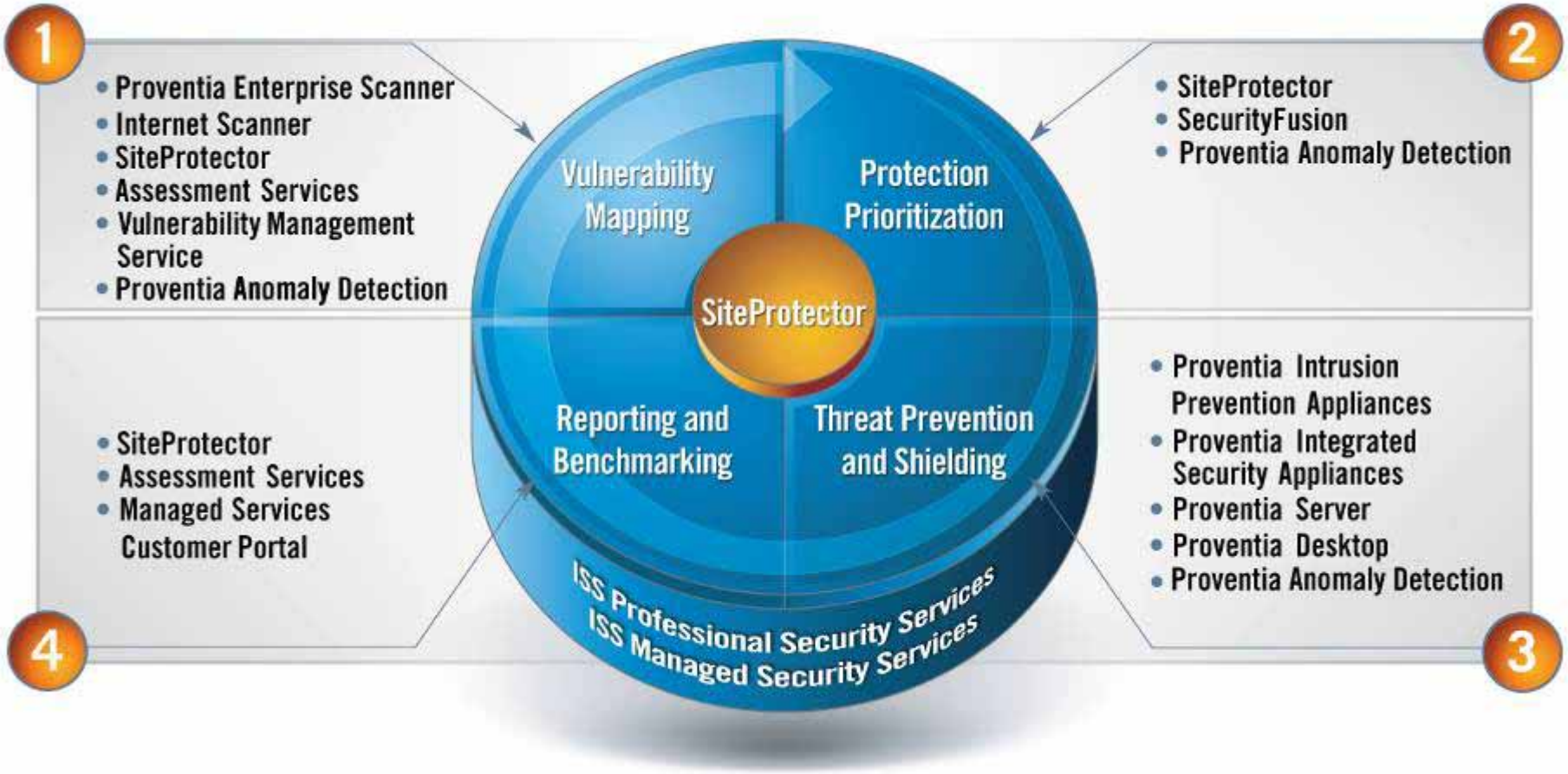
# Ochrana od Perimetru až po Desktop

*Preventivní hloubková ochrana*

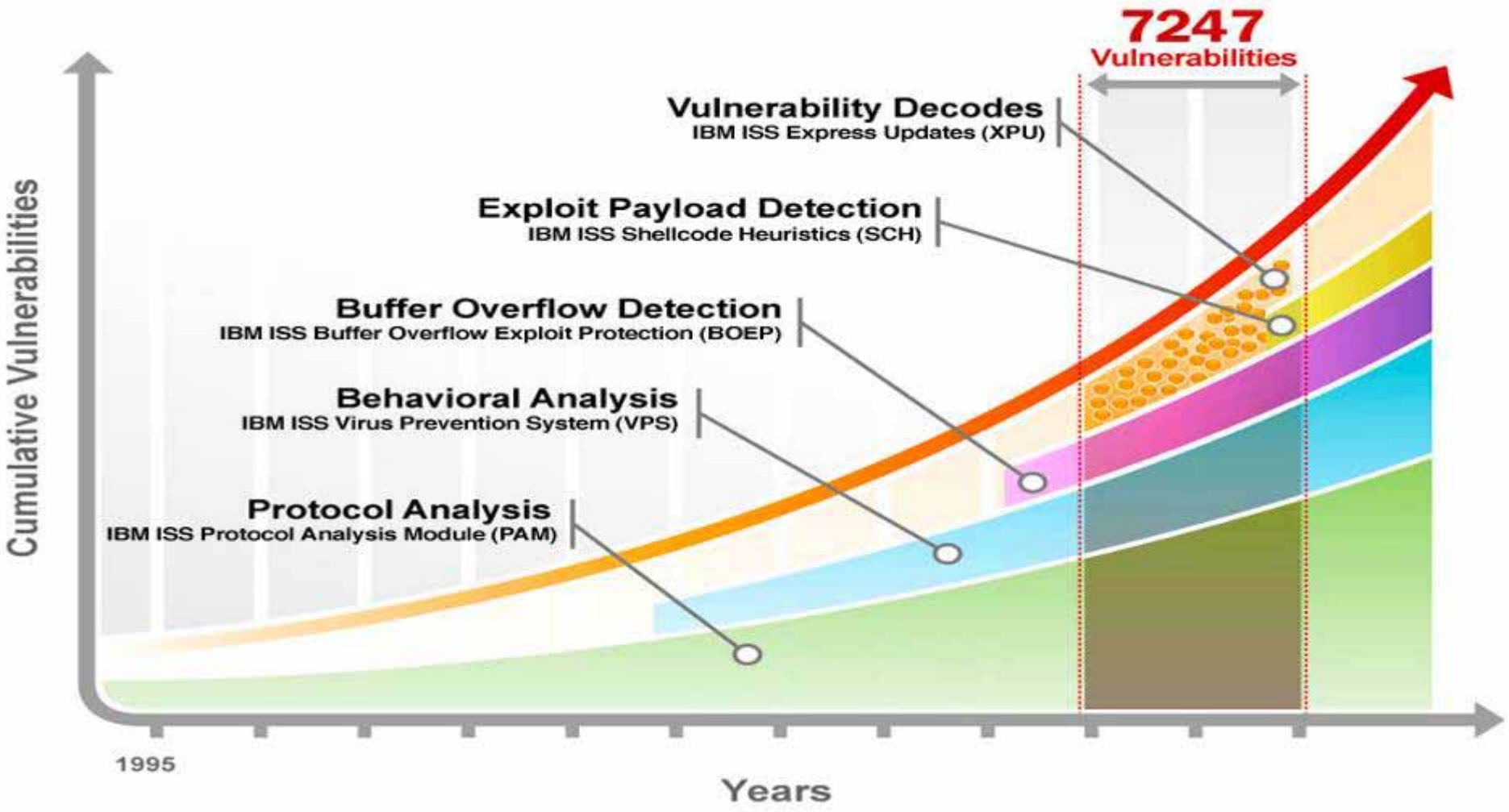


# ISS - Koncept řízení bezpečnosti

The Proventia® ESP – a framework for ISS' products and services

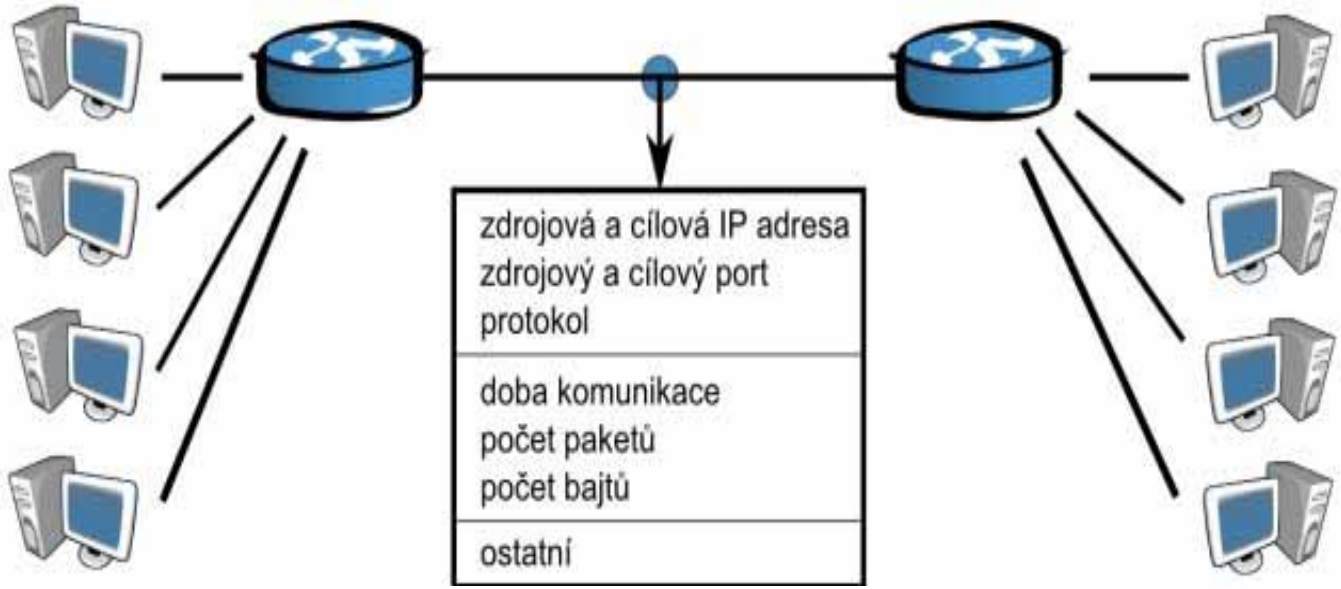


# Metody detekce škodlivých kódů/útoků



# NetFlow

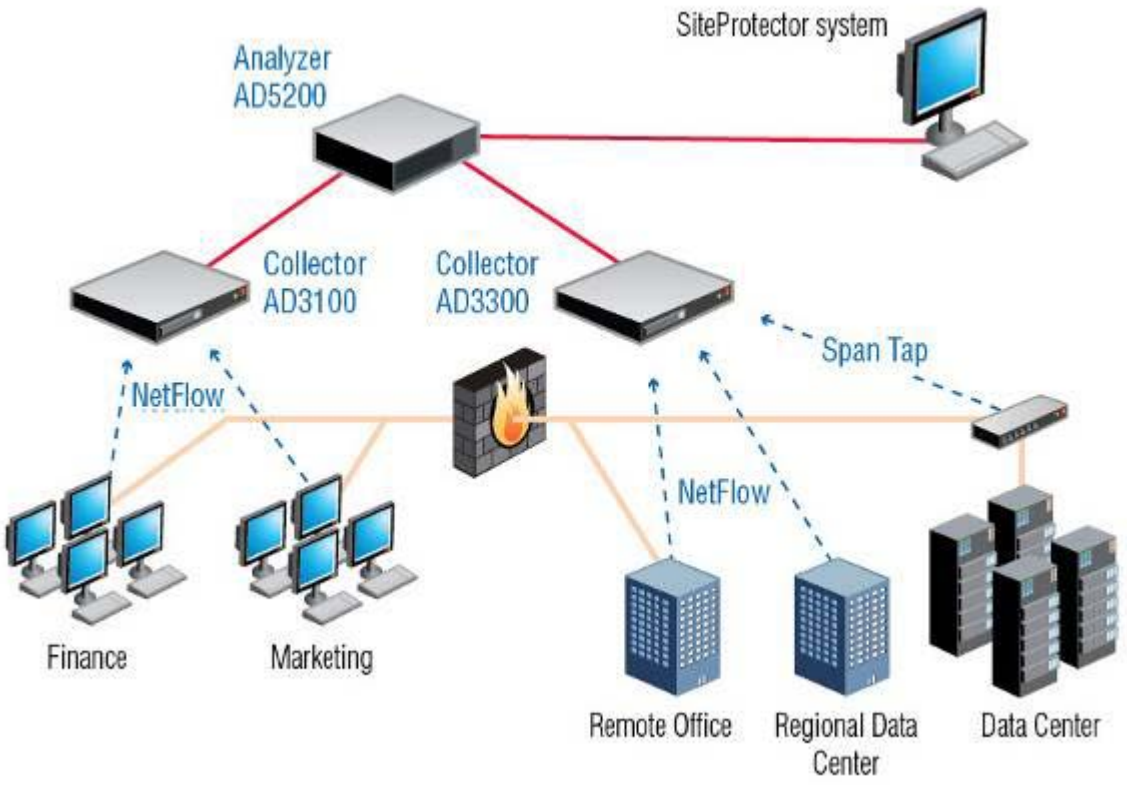
- NetFlow je v současnosti nejrozšířenější průmyslový standard pro měření a monitorování počítačových sítí na základě IP toků.



# Architektura Anomaly detection systému

**IBM Proventia® Network Anomaly Detection System (ADS) is a two-tier, appliance-based system that:**

- Delivers industry-leading network behavior analysis to support network protection, regulatory compliance and network management
- Incorporates global research to facilitate up-to-date network protection and analysis with Active Threat Feed and ATLAS global threat portal
- Complements existing security and network protection strategies by integrating with the IBM Internet Security Systems™ protection platform
- Works with the IBM Proventia Management SiteProtector™ system, which helps streamline network management through centralized command and control

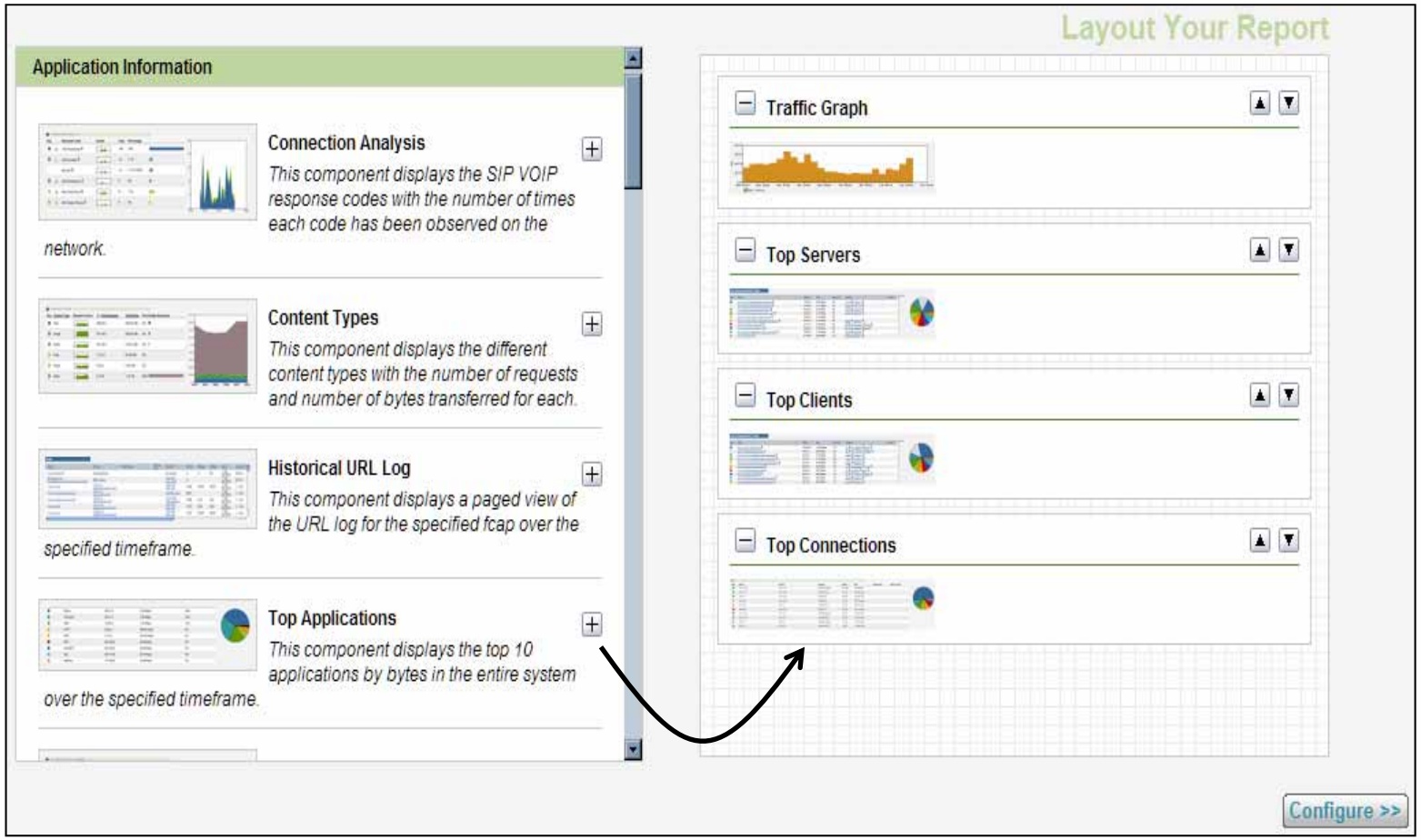


# Hlavní přínosy anomaly detection systému

- **Bezpečnostní přínosy**
- Detekce Botnetů, Zero-day síťových červů armies and phishing
- Ochrana před útoky z řad interních uživatelů – detekce nezvyklých aktivit
- Možnost korelace s událostmi z dalších bezpečnostních komponent
- Vysledování nevhodného využívání zdrojů (Skype, YouTube, 2TP, atp.)

- **Další přínosy**
- Monitoring využívání zdrojů
- Kapacitní plánování (trendování, historické statistiky využití aplikací)
- Forenzní – (vysledování příčin chyb, identifikace nedostatečného výkonu atp.)

# Customizovatelný Reporting



# Proventia Network IPS

- Zařízení, které umožňuje ochranu před útokem a škodlivými kody, které nejsou odhalitelné standardními bezpečnostními mechanismy
- Další vrstva ochrany vedle firewallu a antivirových systémů
- V závislosti na typu zapojení funguje buď v IDS  modu /detekce útoků a obsluha rozhodu o následné akci/ nebo IPS modu – dochází automaticky k zablokování útoku
- Široká škála modelů, které se liší propustností, počtem portů, latencí, redundancí.
- Možnost dékodovat přes 190 protokolů a datových formátů
- Virtuální patching, (ochrana zranitelných – neopatchovaných systémů) využívá X-Press updaty
- Ochrana před známými i neznámými útoky. Reakce na útok: Block, Quarantine, Ignore, Log Evidence, Email SNMP, User-Specified
- Jednotný management použitelný nejen pro síťové IPS, ale i vulnerability skenery, host IPS pro servery a desktopy a další ISS produkty.

# Proventia Network IPS

| | Network | | | | | | |
|---|---|---|---|---|---|---|---|
| | Remote Segments | | Perimeter | | | Core | |
| Model | GX3002 | GX4002 | GX4004 | GX5008 | GX5108 | G2000 | GX6116 |
| Protected Throughput | 10 Mbps | 200 Mbps | 200 Mbps | 400 Mbps | 1.2 Gbps | 2 Gbps | 6 Gbps |
| Protected Segments | 1 | 1 | 2 | 4 | 4 | 4 | 8 |


**Better Protection**
- Protect each segment of the network
- Consistent Naming for Attacks
- Simple Reporting – 1 System
- Automated Updates – XPU's

**Lower Cost**
- Fewer Resources for a Single Management System to handle all devices
- Automation (Updates, Trust X-Force)
- Single Reporting System
- Single process to manage security alerts

**EZ Implementation**
- Same GUI throughout
- Single System to Manage
- Deployment Services
- Managed Security Services
- Certified Technical Support

# Internet/Enterprise Scanner

- Vyhledávání a klasifikace zranitelností uvnitř šítě
- Možnost plánování automatizovaných skenů a pravidelného reportingu
- Vizualizace prostřednictvím centrální správy SiteProtector
- Možnost nastavení workflow pro odstranění zranitelnosti
- ES1500 umožňuje skenovat až 5 segmentů sítě současně s různou politikou
- Existuje v SW variantě „Internet Scanner“ i jako specializovaná appliance„EnterpriseScanner“

# Serverová ochrana

- **Proventia Server for Windows/Linux**
- **RealSecure Server Sensor**

Supports Windows and Unix platforms (AIX, HP-UX and So

**Nejširší podpora platforem na trhu!**


- **Ochrana serveru před známými i neznámými útoky**
- **Možnost kotroly šifrovaného SSL spojení**
- **Ochrana před Buffer overflow útoky**
- **Řízení přístupu k serveru dle nastavené politiky, možnost vynucení politiky**
- **Personální firewall, kontrola spouštěných aplikací**
- **Kontrola integrity registrů, souborů, auditování OS**
- **Logování podezřelých aktivit a kontrola shody s nastavenou politikou**

# Přehled funkcionalit centrální správy

# SiteProtector SP 1001 Management Appliance

- **Připraveno k nasazení do stávající infrastruktury, bez nutnosti pořizovat další HW,SW**
- **HW specifikace: 2U rack, CPU Dual Xeon 2.8 GHz, RAM 4 GB, Disk Space Dual 74 GB**
- **Windows Server 2003, Database SQL Server 2005, Quarterly OS Security Updates, Server protection Proventia Server for Windows**
- **Umožňuje zpracování až 1mil. Událostí za den**
- **Robustní centrální správa, která umožňuje dohled a správu všech ISS produktů**

NSS approved

SC MAGAZINE GLOBAL AWARDS 2005

Security Company Of The Year


Gartner

Magic Quadrant Leader

TOLLY Up to Spec CERTIFIED

IDC Analyze the Future

#1 Market Share

# Dotazy?

WEST COAST LABS CHECK MARK SEE YOUR SAFEGUARDS AT www.check-mark.com

2005 FROST & SULLIVAN Market Leadership Award

METAGROUP

Leader

2005 Network Computing WELL-CONNECTED AWARDS FINALIST

SCP SUPPORT CENTER PRACTICES - CERTIFIED -