# AddNet
# Integrovaná správa sítě - jako základ kybernetické bezpečnosti organizace


**Jindřich Šavel**

**14.4.2015**

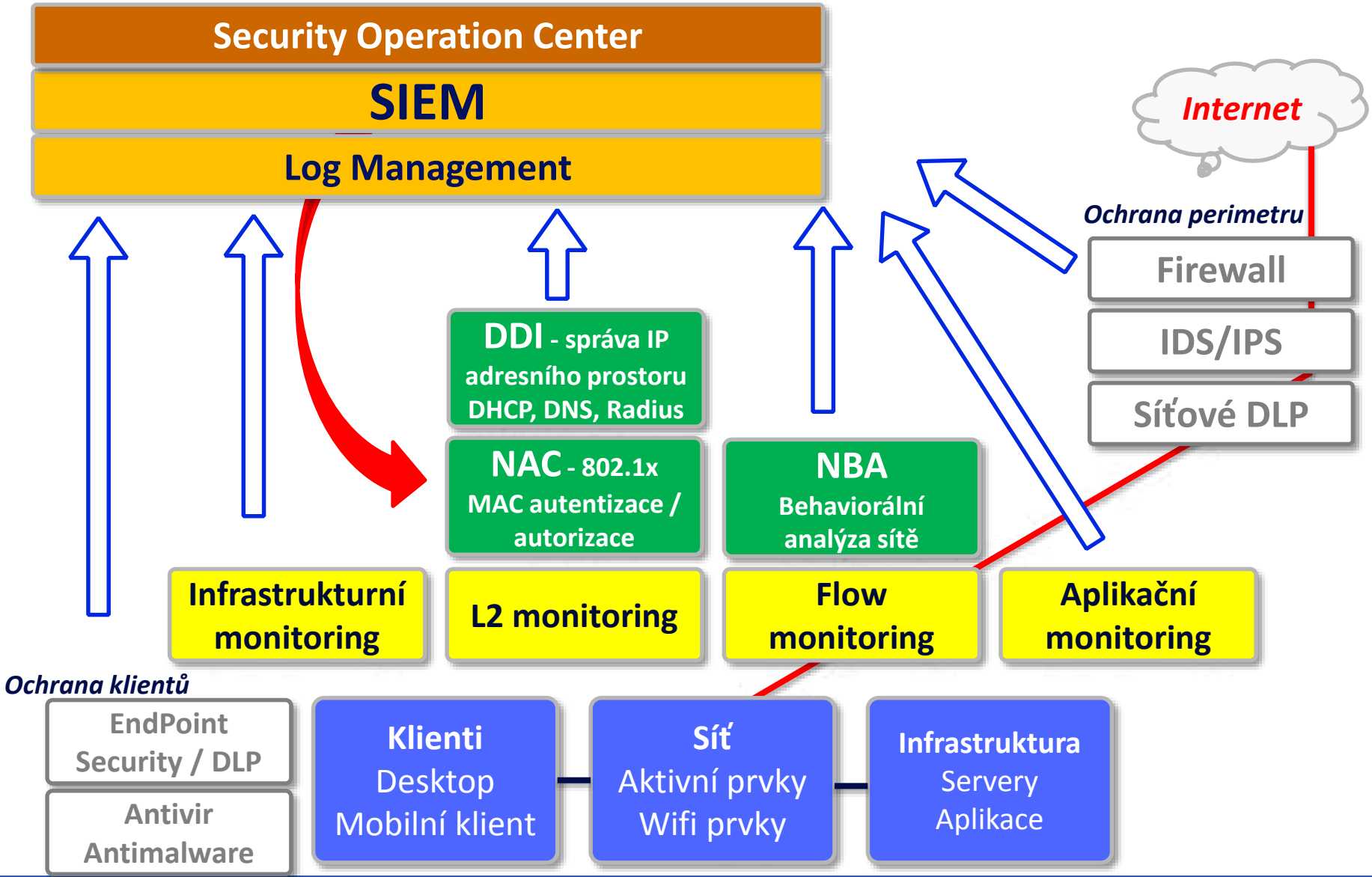
# Představení společnosti Novicom

- **Česká společnost zabývající se**
  - **vývojem,**
  - **dodávkami**
  - **a provozem**

  systémů pro
  - **správu sítí**
  - **monitoring**
  - **bezpečnost**
  - **a komunikace**


- **Orientace na střední a velké zákazníky a na dále na všechny vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých systémů**
- **Společnost s historií - 20 let českém trhu**

# Aktivní bezpečnost sítě



# Centrální monitoring a IP správa sítě
## Funkční přehled

novicom

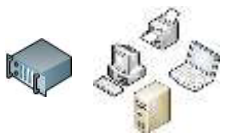
inveaTECH

**MoNet** ⟵ **AddNet** ⟶ **FlowMon**

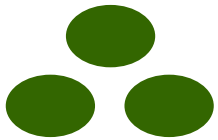
- Aplikace
- Aplikační servery
- Databáze
- Operační systémy
- Virtualizace
- Hardware
- Síťové prvky
- Prostředí

Univerzální Monitoring

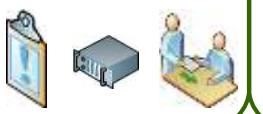
**Nezávislý monitoring**



**Distribuovaný monitoring**



**Otevřený monitoring**



**SLA Reporting**

### IPAM
- Správa IP adresního prostoru
- L2 Monitor – historie IP/MAC/port

### DDI – Základní síťové služby
- High Performace & distribuované DHCP
- Flexibilní & distribuované DNS

### Bezpečnost
- 802.1x & MAC Autentizace
- Autorizace – VLAN přiřazení
- Distribuovaný RADIUS
- Krizové plánování

### BYOD and mobilní zařízení
- Automatizovná správa IP & NAC
- Samoobslužný management portal

### Aktivní prvky
- Repository
- Port utilizace monitor
- Zálohování konfigurací

### Sběr provozních dat
- NetFlow v5/v9/IPFIX
- L3/L4/I4 visibility
- Network performance monitoring
- On-demand packet capture

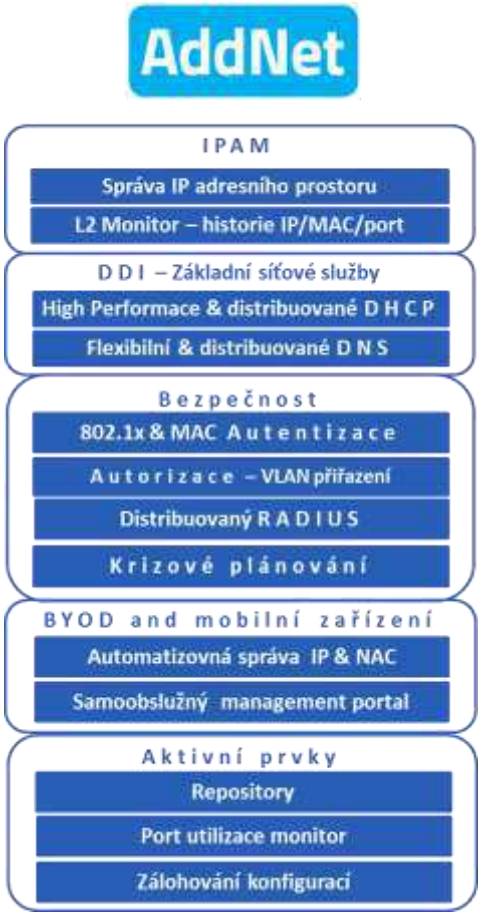
### Provozní statistiky
- Objemové and provozní statistiky
- Drill down a datová analýza
- Vlastní profily a Reporting

### Behaviorální analýza
- Útoky, Malware, APTs
- Síťové anomálie, porušení politik
- Konfigurační a provozní problémy

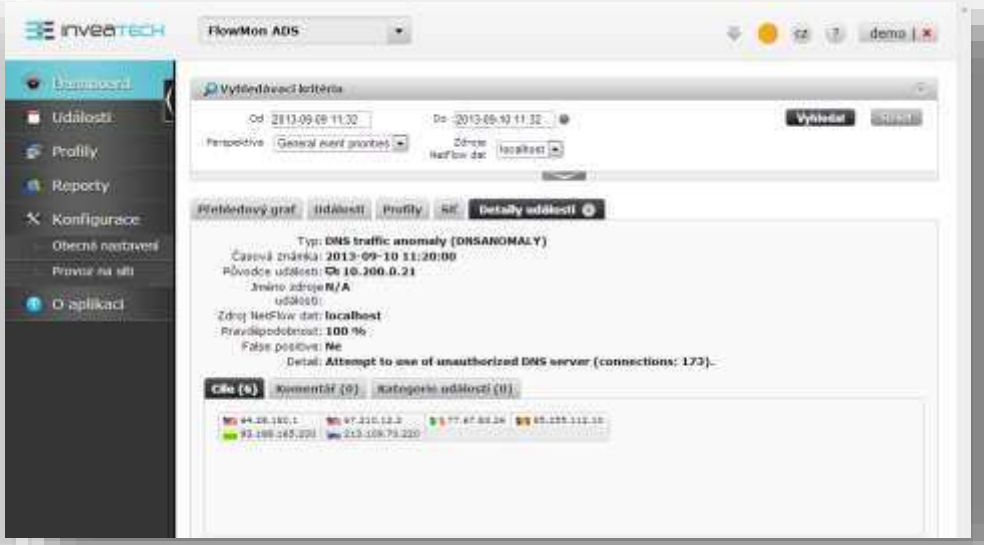
### Dashboard
- Top and traffic statistics
- Bezpečnostní incidenty

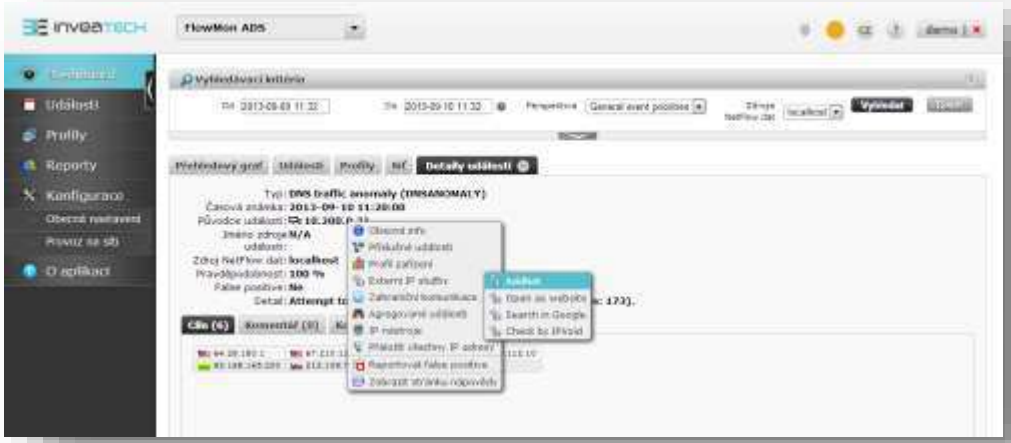
# Představení pojmů IPAM / L2M / DDI / NAC

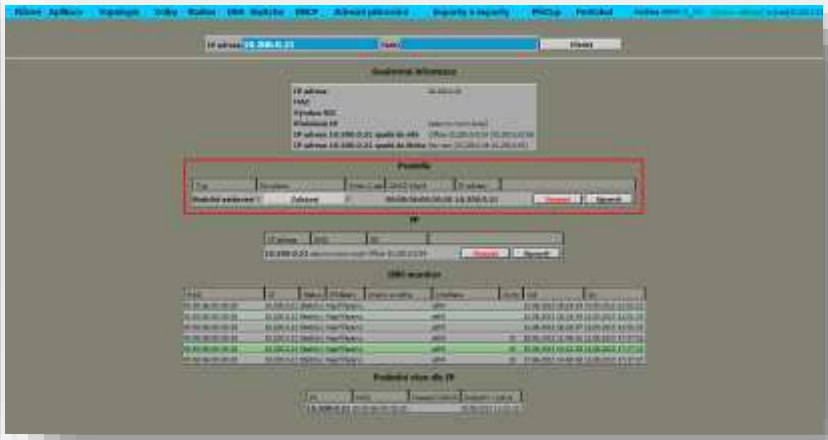
- **IPAM**
  - Správa IP adresního prostoru
- **L2 Monitoring**
  - Monitoring výskytu zařízení v síti (IP/MAC - lokalita/port)
  - Monitoring v reálném čase, úplná historie výskytu
- **DDI**
  - Integrovaná správa IP adresního prostoru a základních síťových služeb
  - DHCP a DNS
- **NAC – řízení přístupu zařízení do sítě**
  - Autentizace zařízení (802.1x / MAC s ochranou)
  - Autorizace zařízení – dynamické řízení přidělování do VLAN



# ZoKB v praxi - §22 vyhlášky 316



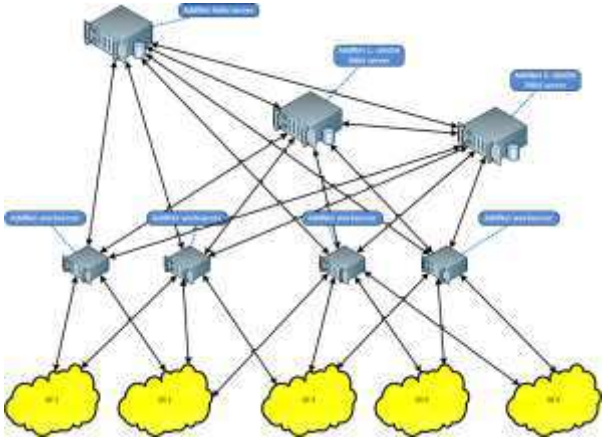



# Z vyhlášky č. 316 ze dne 15.12.2014

- **Dočtete se např.**
- **§22 Nástroj pro detekci kybernetických bezpečnostních událostí**
  - *(2)„… dále používá nástroj pro detekci kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace*
  - *a) v rámci vnitřní komunikační sítě a*
  - *b) serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.“*

# V čem je AddNet jiný?

- **Využití vlastních technologií**
  - **Novicom SGP** – Secure Grid Platform
  - **Novicom SDP** – Secure Delivery Protocol
  - **Novicom FireBox appliances**
- **Flexibilní podpora topologie nasazení**
  - Centralizované nasazení
  - Plně distribuovaného nasazení
  - Kombinované nasazení



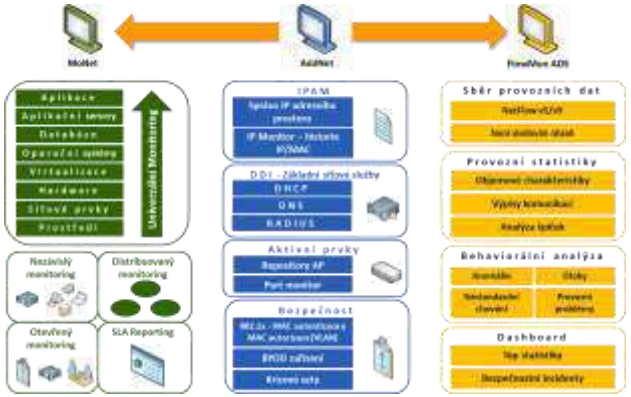
- **Nadstandardní provozní spolehlivost a škálovatelnost**
  - Provoz v distribuovaných lokalitách i při nedostupnosti řídící lokality
  - Podpora aktivního clusteringu na všech úrovních
  - Nadstandardní bezpečnost dat (appliance, datový přenos, architektura)
- **Unikátní spojení DDI a NAC**
  - DDI nástroj pro rozsáhlé distribuované sítě je doplněný o NAC - řízení přístupu zařízení s využitím integrovaných Radius služeb

# Klíčové přínosy AddNetu

- **Řádová úspora práce síťových administrátorů**
- **Standardizace činností a centralizace správy v rozsáhlých a distribuovaných sítích**
- **Zavedení řízení bezpečnosti přístupu do sítě formou 802.1x**
  - 802.1x/MAC autentizace a autorizace (přiřazování do VLAN)
- **Plně automatizovaná správa BYOD a mobilních zařízení**
- **Jednoznačná identifikace BYOD a mobilních zařízení v síti**
- **Podstatné zvýšení provozní spolehlivosti DNS, DHCP, Radius díky N+1 redundanci a nadstandardní škálovatelnosti**
- **Úspora nákladů díky dlouhodobému sledování utilizace aktivních prvků**
- **Bezproblémová spolupráce se síťovými technologiemi Microsoft a Cisco**

# Bezpečnost na 4 kliknutí - Co pro to potřebujete?

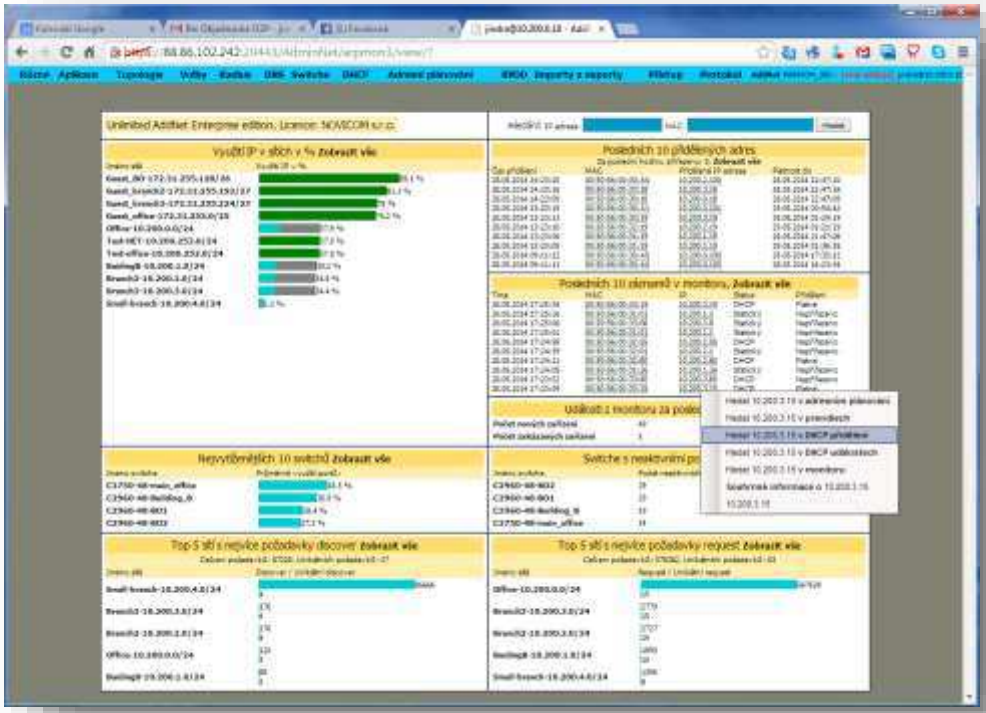
- **Monitoring vnitřní sítě**
  - **L2 monitoring** (**která IP/MAC kde** a **kdy** byla v síti)
  - **Flow monitoring** (**která IP/MAC s kým** a **jak** komunikovala)
  - **Infrastrukturní monitoring** (**které zařízení/služba** je afektována)
- **Pokročilé nadstavby monitoringu**
  - **NBA** – behaviorální analýza sítě (**kdo a jak** se chová neobvykle)
  - **DDI** – nástroj správy IP adresního prostoru **(IPAM)** a základních síťových služeb **(DHCP / DNS)**
  - **NAC** – řízení přístupu zařízení do sítě
    - 802.1x / MAC Autentizace
    - Autorizace – řízení přidělování VLAN




***Mějte vaší síť plně pod kontrolou!***

# AddNet?

- *Zahoďte excelové evidence IP adres*
- *Rozhodujte, která zařízení mohou komunikovat ve vaší síti*
- *Zaveďte si pořádek a bezpečnost v síti*



- *Zvyšte provozní spolehlivost sítě*
- *Radikálně snižte pracnost síťové administrace*

# Další informace

- **Novicom s.r.o.**
  - Koněvova 67
  - 130 00 Praha 3
  - www.novicom.cz
  - sales@novicom.cz
- **Jindřich Šavel**
  - obchodní ředitel
  - jindrich.savel@novicom.cz
  - +420 271 777 231
  - +420 777 222 961