Aktivní bezpečnost sítě

Jindřich Šavel

27/11/2014

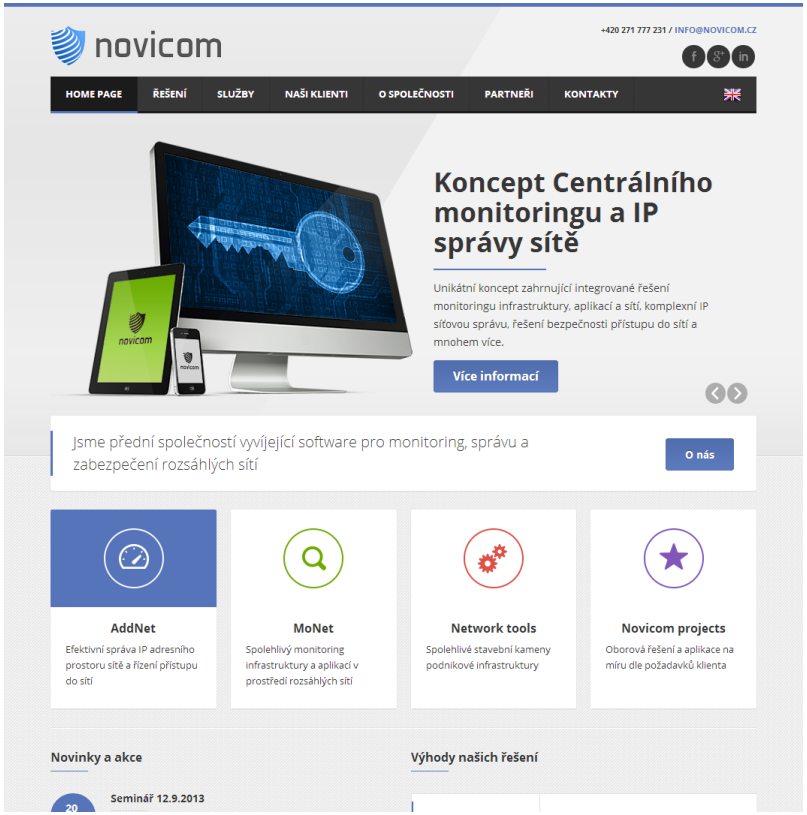
Program prezentace

- Představení společnosti
- Koncept aktivní bezpečnosti sítě
- Spolehlivé infrastruktura pro DDI/NAC řešení

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**

Novicom - nástroje pro monitoring a správu sítí

MoNet	*Řešení distribuováného monitoringu IT infrastruktury a aplikací*
AddNet	*Efektivní a správa IP prostoru a bezpečnost přístupu v rozsáhlých sítí*
Network tools	*Sada nástrojů pro vysoce efektivní a bezpečný provoz IT infrastruktury*
Projects	*Oborová a customizovaná řešení*

Novicom SGP – Secure Grid Platform

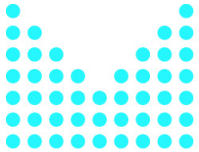
Novicom SDP – Secure Delivery Protocol

Původní Novicom technologie

- **Novicom SGP (Secure Grid Platform)**
  - technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2/infrastrukturní monitoring a základní síťové služby DHCP/ DNS/ Radius)
  - vícenásobná redundance typu Active-Active, podpora hierarchického a distribuovaného modelu v prostředí rozsáhlých sítí
- **Novicom SDP (Secure Delivery Protocol)**
  - vlastní komunikační protokol navržený pro zajištění spolehlivé komunikace v prostředí velice nekvalitní sítě
  - pracuje na linkách s chybovostí až 95%
  - garance maximálního zabezpečení přenášených dat (military grade security)
- **Novicom FireBox platforma**
  - systém HW a virtuálních appliancí, zvyšující bezpečnost, spolehlivost a servisní flexibilitu pro klíčové komunikační a bezpečnostní funkce SGP
  - je založené na OS Linux s bezpečnostními úpravami kernelu, s nezávislými prvky centrální správy a zálohování/obnovy

Významní zákazníci

novicom



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Univerzita Tomáše Bati ve Zlíně

Office DEPOT
Taking Care of Business

TOPTRANS

Česká pošta

OSTRAVA!!!

THOMAYEROVA NEMOCNICE PRAHA 4

ČESKÝ ROZHLAS

AUTODÍLY AUTO ŠTANGL

HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY

ozp 207 OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

wüstenrot

Aktivní bezpečnost sítě

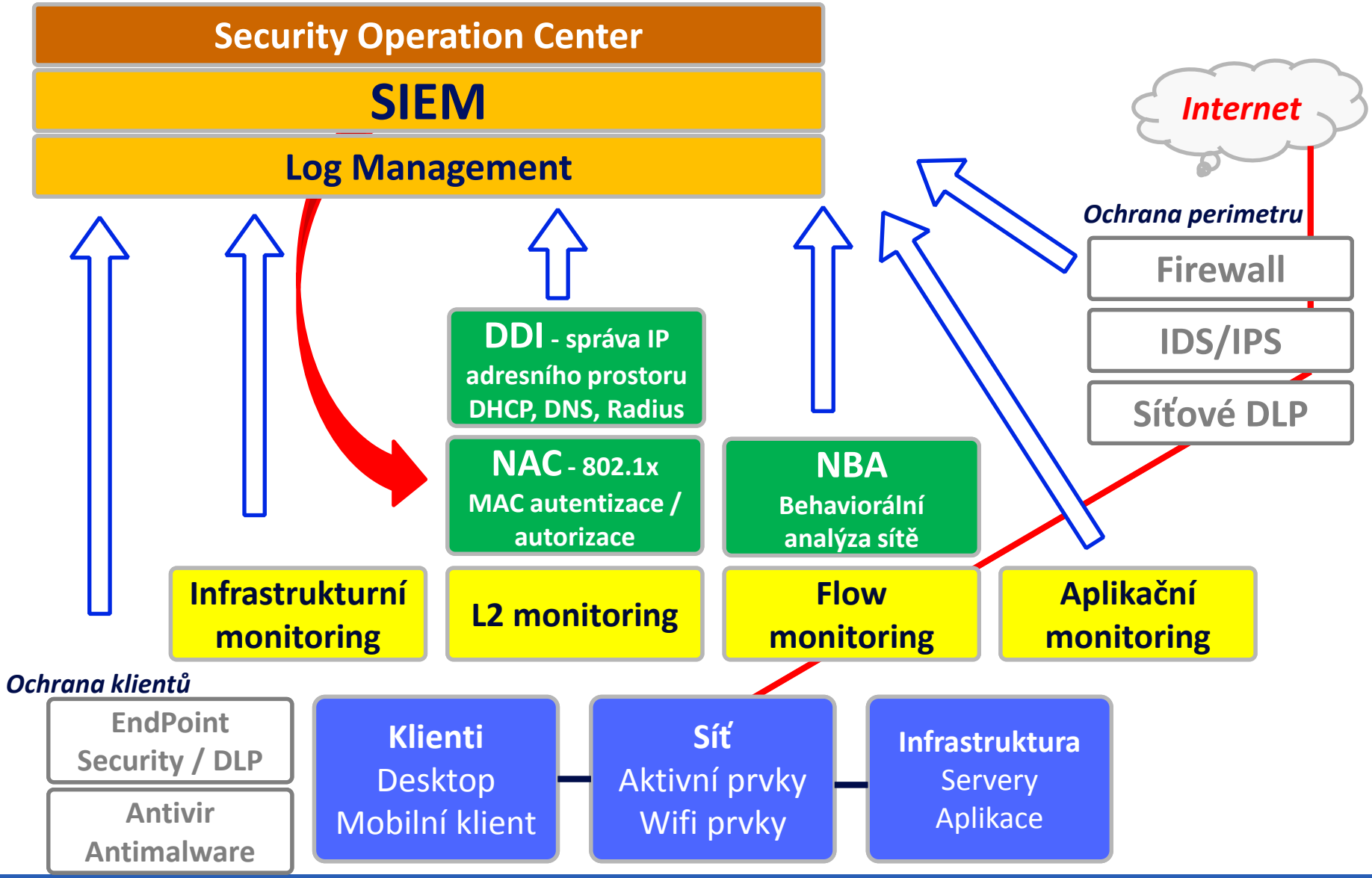
- **Koncept připravený na půdě NSMC**
- **Network Security Monitoring Cluster**
  - ***kooperační odvětvové uskupení zaměřené na oblast bezpečnosti počítačových sítí a bezpečnosti v ICT***
- **Aktivity klastru**
  - společné projekty
    - v oblasti technické infrastruktury inovačního charakteru,
    - aplikovaného výzkumu, vývoje a inovací
  - návrh a integrace komplexních řešení v oblasti monitorování bezpečnosti sítí
  - osvěta týkající se bezpečnosti počítačových sítí a informací, školení a vzdělávání
  - sdílení informací o aktuálních trendech v oblasti bezpečnosti sítí
  - návrhy úpravy právních norem v oblasti bezpečnosti ICT infrastruktury a jejího zabezpečení
  - komunikace s organizacemi a asociacemi zabývající se bezpečností počítačových sítí (např. ENISA, IT Security in Germany atd.)

NSMC NETWORK SECURITY MONITORING CLUSTER | Our Vision Your Security

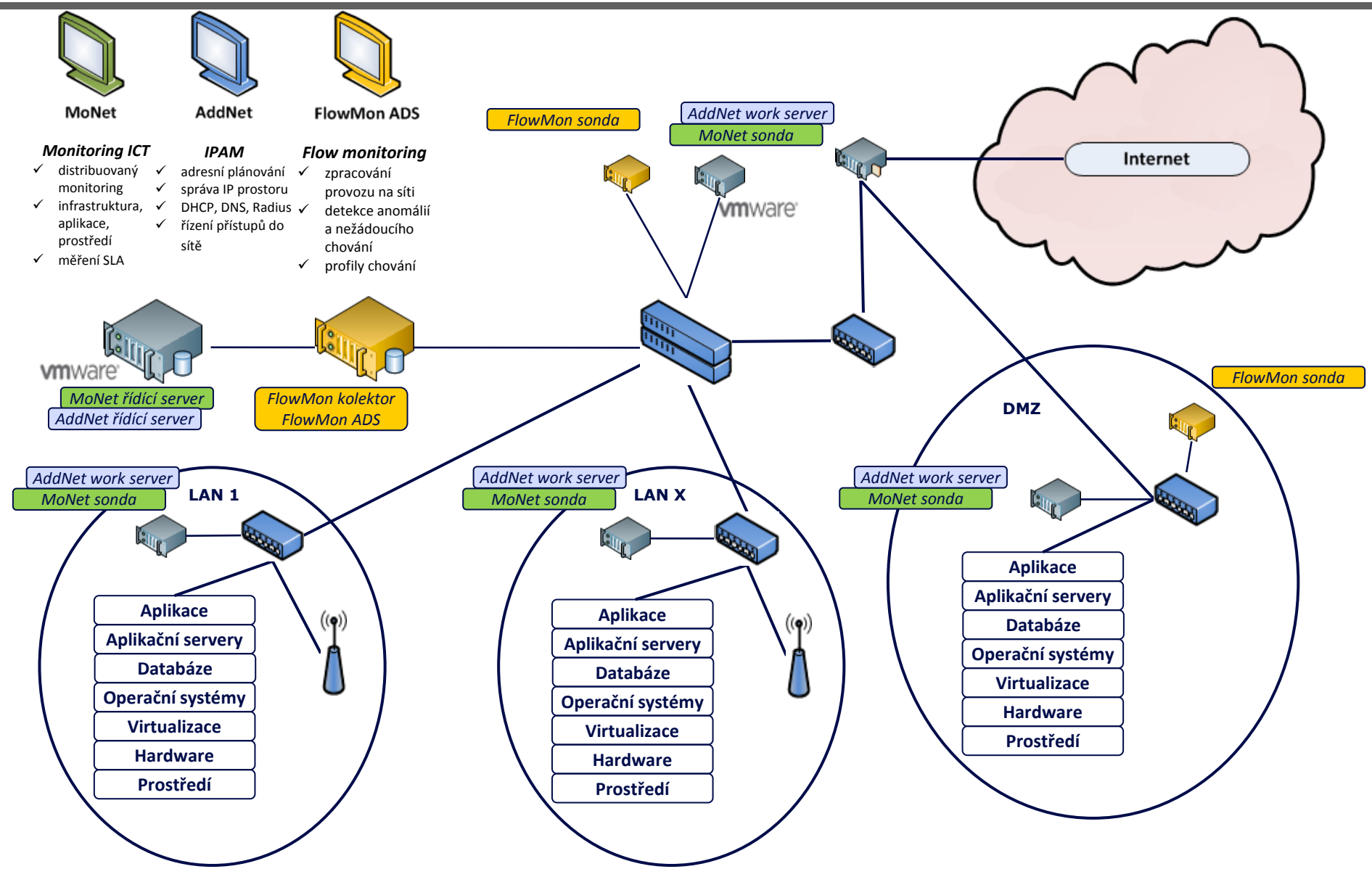
www.kybernetickabezpecnost.eu

- Pro vedoucí pracovníky a management organizací

Aktivní bezpečnost sítě



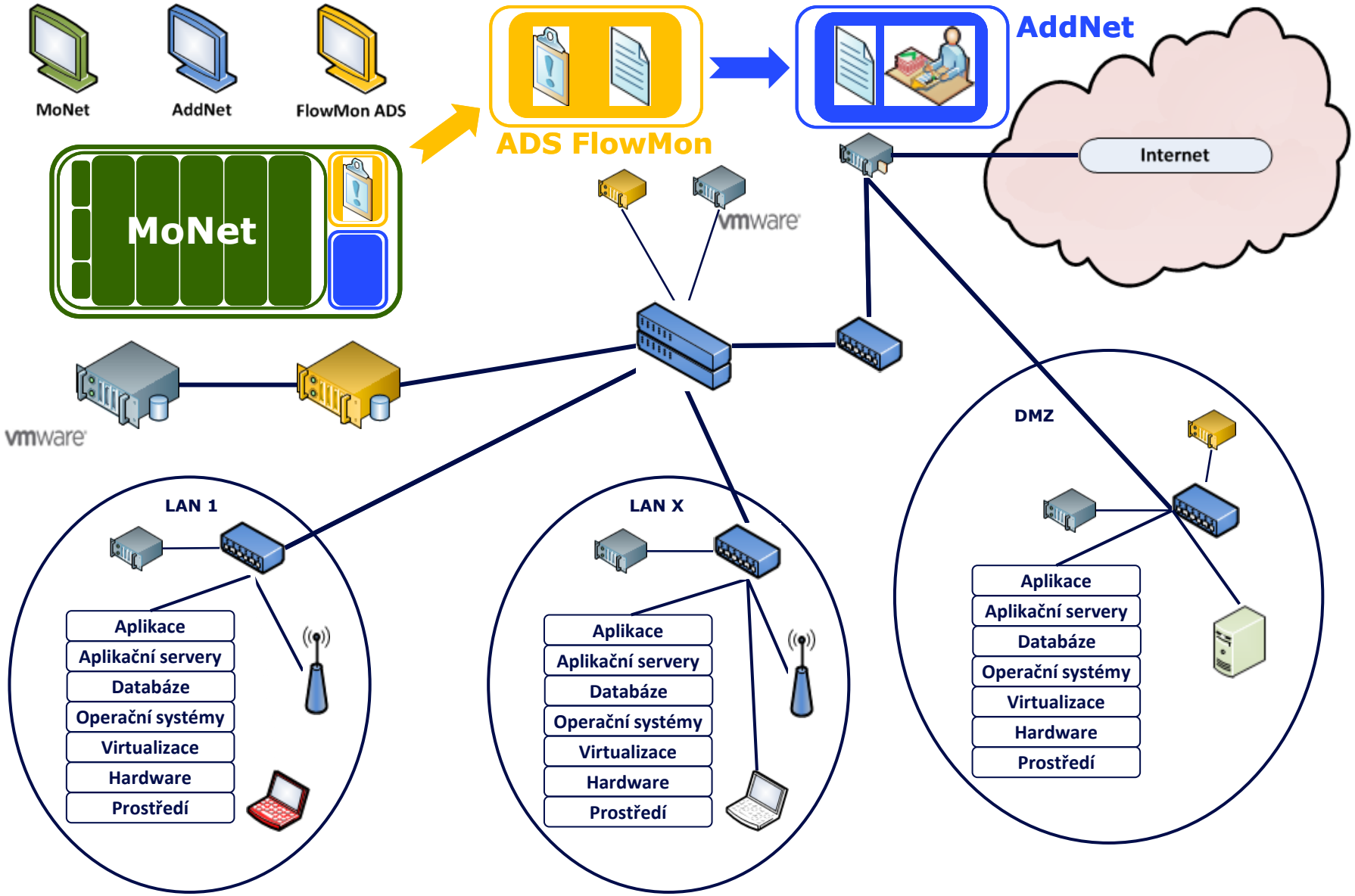
Centrální monitoring a správa sítě



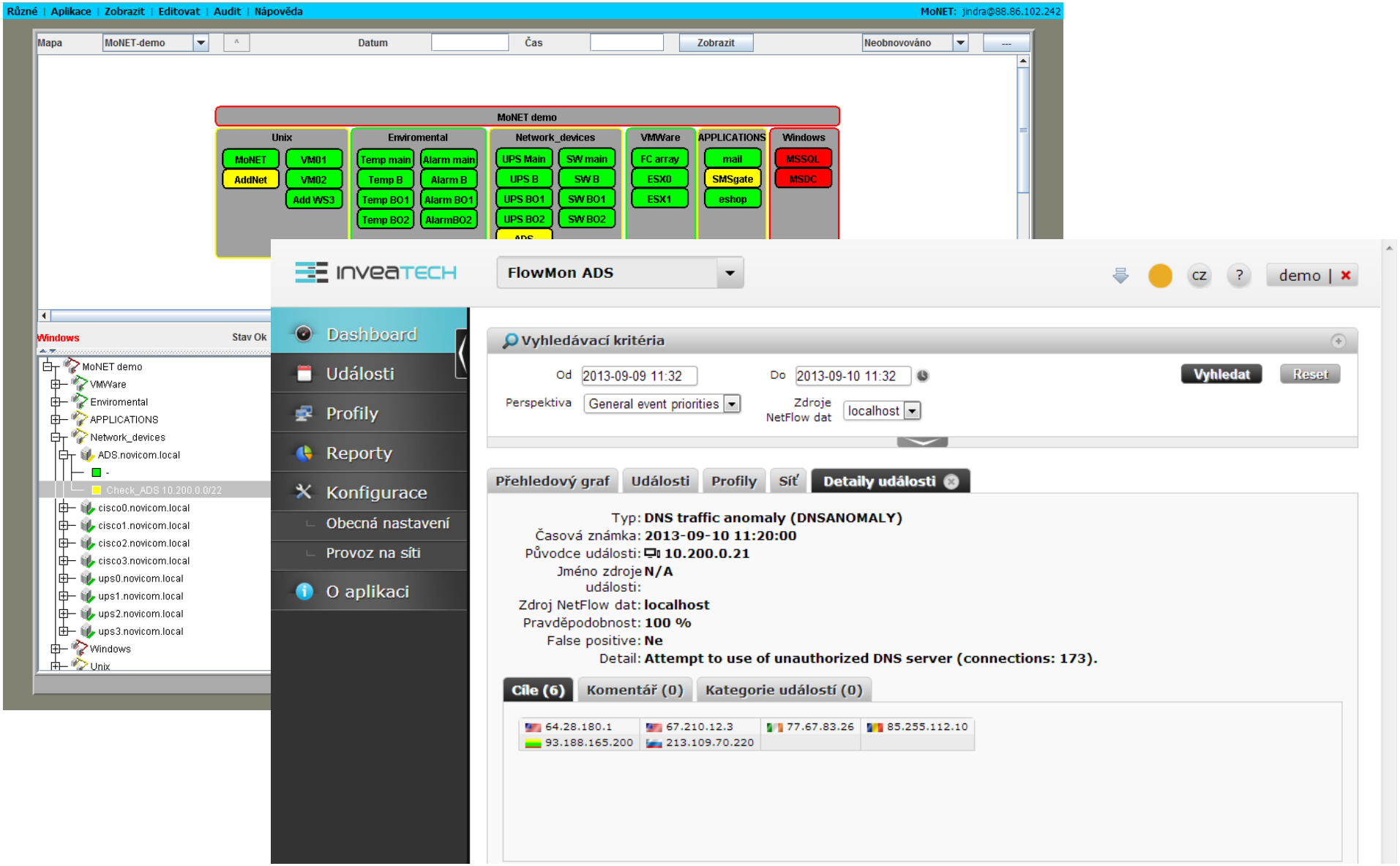
Síťová infrastruktura – podpora NAC

- **Základ pro spolehlivé a bezpečné fungování sítě**
- **Využití aktivních prvků s podporou 802.1x**
- **Při požadavku zařízení na síťovou komunikaci**
  - příslušný switch proved dotaz do integrovaného Radius serveru AddNetu, který dá informaci,
    - zda má zařízení povolenou komunikaci (802.1x & MAC autentizace)
    - případně zařadí zařízení do nastavené VLAN (autorizace)
- **Při požadavku na odpojení zařízení**
  - je tato informace opětovně distribuována přes Radius. Při opětovném dotazu (par. Positive time to live) je přístup odepřen a zařízení nemůže komunikovat na síti
- **Ověřeno s produkty**
  - Podpora heterogenních DDI a NAC řešení
  - Široké spektrum produktů
    - Switche, routery, wireless, multiservice access platformy a gatewaye,…

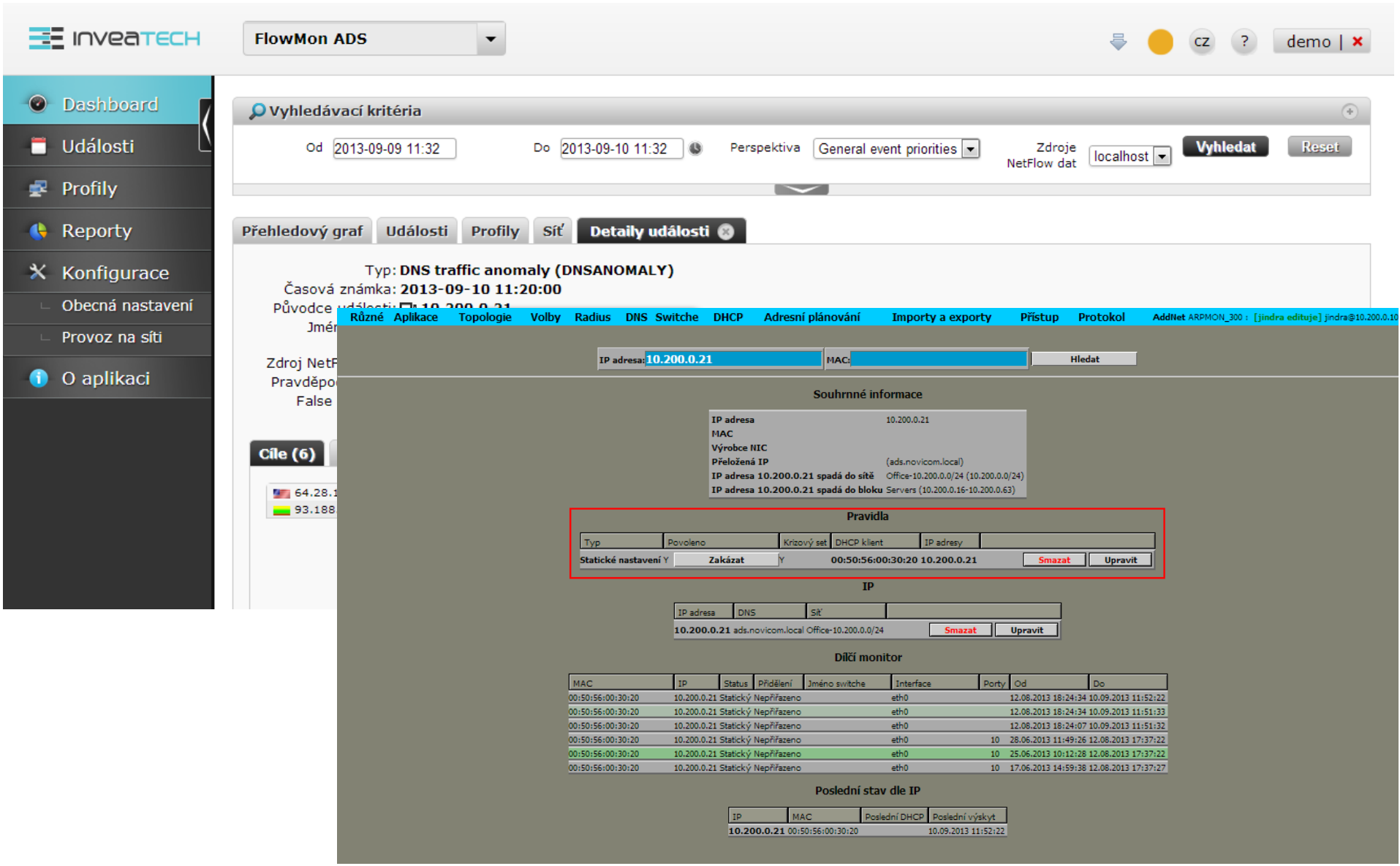
Integrované řešení monitoringu a správy



Koncept v detailu - MoNet => FlowMon ADS



Koncept v detailu - FlowMon ADS => AddNet



Centrální monitoring a IP správa sítě
Funkční přehled

novicom

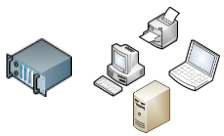
inveaTECH

MoNet ⟵ **AddNet** ⟶ **FlowMon**

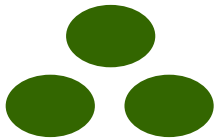
- Aplikace
- Aplikační servery
- Databáze
- Operační systémy
- Virtualizace
- Hardware
- Síťové prvky
- Prostředí

Univerzální Monitoring

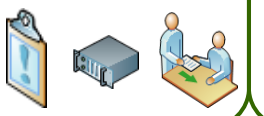
Nezávislý monitoring



Distribuovaný monitoring



Otevřený monitoring



SLA Reporting

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

DDI – Základní síťové služy
- 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/l4 visibility
- Network performance monitoring
- On-demand packet capture

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

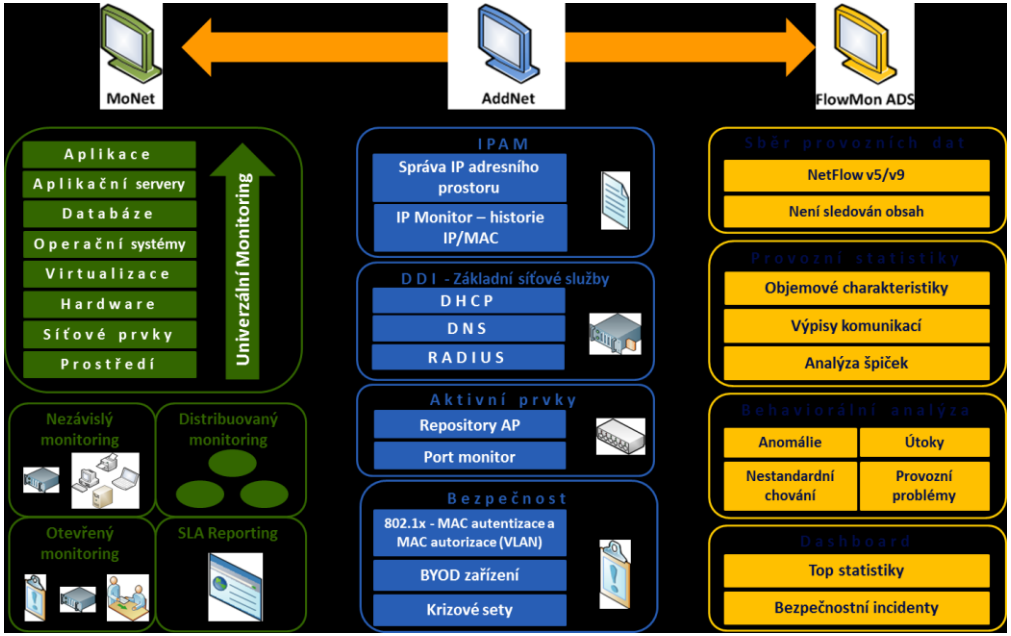
Behaviorální analýza
- Útoky, Malware, APTs
- Síťové anomálie, porušení politik
- Konfiguratční a provozní problémy

Dashboard
- Top and traffic statistics
- Bezpečnostní incidenty

Řešení pro zajištění ZoKB

- **Ověření připravenosti k ZoKB**
- **Distribuovaný monitoring infrastruktury**
- **IPAM/DDI/L2 monitoring - distribuovaná správa IP adresního prostoru a základních síťových služeb (DNS, DHCP, RADIUS)**
- **NAC – distribuovaná 802.1x/MAC autentizace a autorizace**
- **Zálohování a podpora obnovy konfigurací aktivních prvků**
- **Ve spolupráci s INVEA-TECH**
  - Flow monitoring
  - NBA
    - Behaviorální analýza
  - APM

Bezpečnost na 4 kliknutí



- **Zajímavá služba pro stanovení dopadů ZoKB na organizaci**

Služby ověření úrovně kybernetické bezpečnosti

a porovnání s požadavky zákona 181/2014 Sb. - Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.

V pátek 29. 8. 2014 byl ve Sbírce zákonů pod č. 181/2014 Sb. publikován zákon o kybernetické bezpečnosti. Přijetím této normy Česká republika reaguje na rizika zneužití informačních a komunikačních technologií s potenciálně značnými škodami.
Zákon odráží vzrůstající závislost společnosti na informačních technologiích, kdy riziko zneužití těchto technologií může mít rozsáhlé dopady a může vést ke značným škodám. Všechny vyspělé země, mezi něž Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů. Zákon bude účinný od 1. ledna 2015.

Protože problematika kybernetické bezpečnosti je s ohledem na okruh dotčených odborností značně rozsáhlá, připravili jsme pro vás službu, která vám usnadní orientaci v tom, jakým způsobem se tato věc dotýká právě vaší organizace a nakolik je vaše organizace připravena vypořádat se s povinnostmi, které jí touto normou budou uloženy.

Zkušení odborní konzultanti vám pomohou ve spolupráci s vámi provést

Ověření organizačních opatření (§ 5, odst. 1 zákona)

- **Identifikace existujícího systému řízení bezpečnosti informací organizace**
- **Identifikace způsobu řízení rizik organizace**
- **Identifikace bezpečnostní politiky organizace a její aplikace**
- **Identifikace úrovně organizační bezpečnosti organizace a její aplikace**

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

- **VUMS Datacom**
  - Šárka Business Park
  - Lužná 591
  - 160 00 Praha 6
  - www.datacom.cz
  -

Novicom Channel Partner