

M.I.T.
Consulting



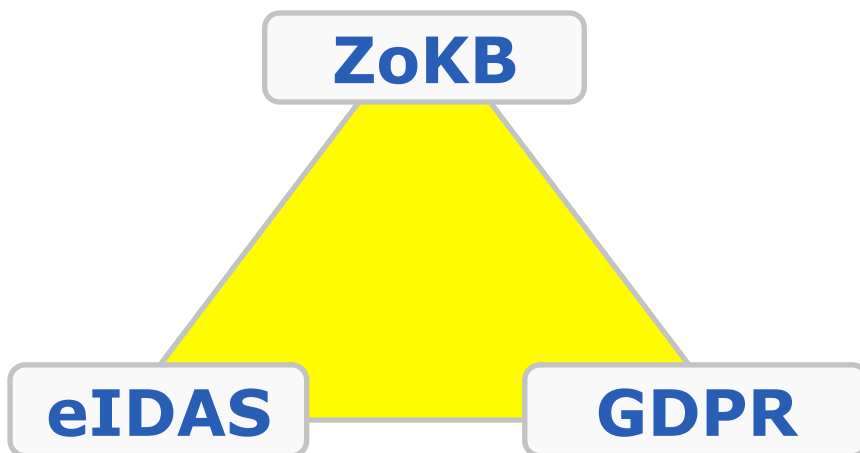
ORACLE®

GDPR, eIDAS, ZOKB

**Nové legislativní povinnosti
organizací – a co s tím?**

24.5.2017

Nové/pozměněné legislativní povinnosti, dotýkající se ochrany osobních dat, identity a kybernetické bezpečnosti.



Postup pro vypořádání se s legislativními povinnostmi:

- **Akceptování rizik vyplývajících z nekonání**
- **Nevnímat jednotlivé oblasti izolovaně**
- **Zpracovat GAP analýzy**
- **Navrhnout opatření**
- **Implementovat opatření**

Internet

Aktivní bezpečnost sítě a zajištění požadavků eIDAS a GDPR

Řízení bezpečnostních incidentů
SOC (Security Operation Center)

Ochrana perimetru

Firewall

IDS/IPS

Network DLP

Nástroje pokročilé detekce

LogManagement/SIEM

Řízení a zabezpečení interní sítě

NBA, DDI/NAC



Monitoring interní sítě

Infrastruktura, L2, datové toky, aplikace

Ochrana klientů

EndPoint
Security / DLP

Antivirus
Antimalware

Klienti
Desktopy
Mobilní klienti

Síť
Síťové prvky
Wifi

ORACLE®

Důvěryhodné
úložiště
eIDAS

M.I.T.
Consulting

Infrastruktura
Servery
Aplikace

Platforma a technologie
pro bezpečné ukládání
osobních dat - GDPR

GDPR, kybernetická bezpečnost a zabezpečení interní sítě



AddNet

integrovaný DDI/NAC nástroj

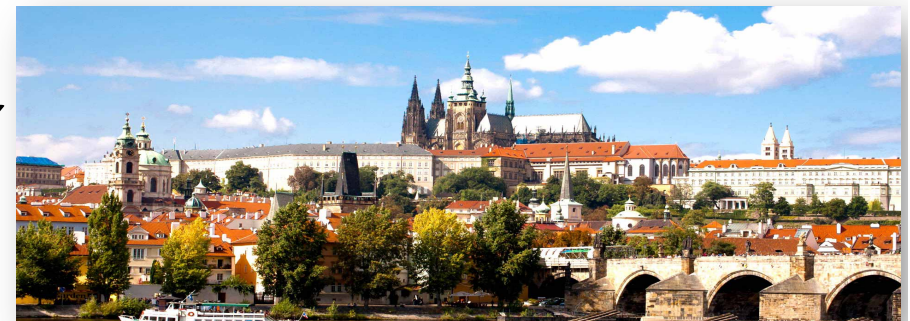
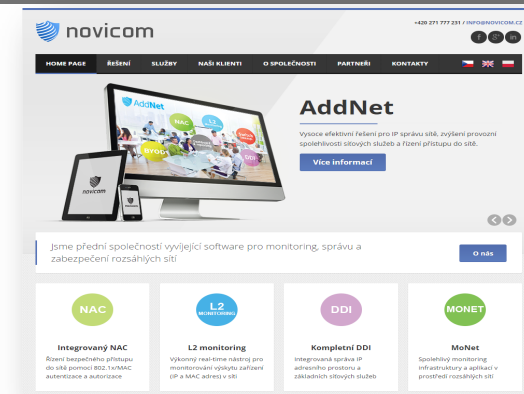
Jindřich Šavel

24.5.2017

Představení společnosti Novicom





















- **Český výrobce řešení pro síťovou**
 - **Správu, monitoring, bezpečnost**
- **Orientace na**
 - střední a velké zákazníky
 - zákazníky vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých sítí
- **Společnost s historií – více než 22 let IT trhu**
- **Společnost s ambicemi**
 - úspěšně se prosazuje v zahraničí
 - v roce 2017 aktivní v 8 zemích



Významní zákazníci



 MINISTERSTVO VNITRA ČR	 MINISTERSTVO OBRANY ČR	 MINISTERSTVO FINANCÍ ČR	 MINISTERSTVO KULTURY	 ICOM TRANSPORT A.S.	 TOPTRANS EU, A.S.
 ČESKÁ POŠTA	 OBOROVÁ ZDRAVOTNÍ POJIŠTOVNA	 ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD	 HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY	 THOMAYEROVA NEMOCNICE	 UNIVERZITA TOMÁŠE BATA VE ZLÍNĚ
 ČESKÝ ROZHLAS	 KOFOLA ČESKOSLOVENSKO A.S.	 WÜSTENROT - STAVEBNÍ SPORITELNA A.S.	 OFFICE DEPOT S.R.O.	 MĚSTSKÁ ČÁST PRAHA 8	 MAGISTRÁT MĚSTA OSTRAVY

Aktivní bezpečnost sítě



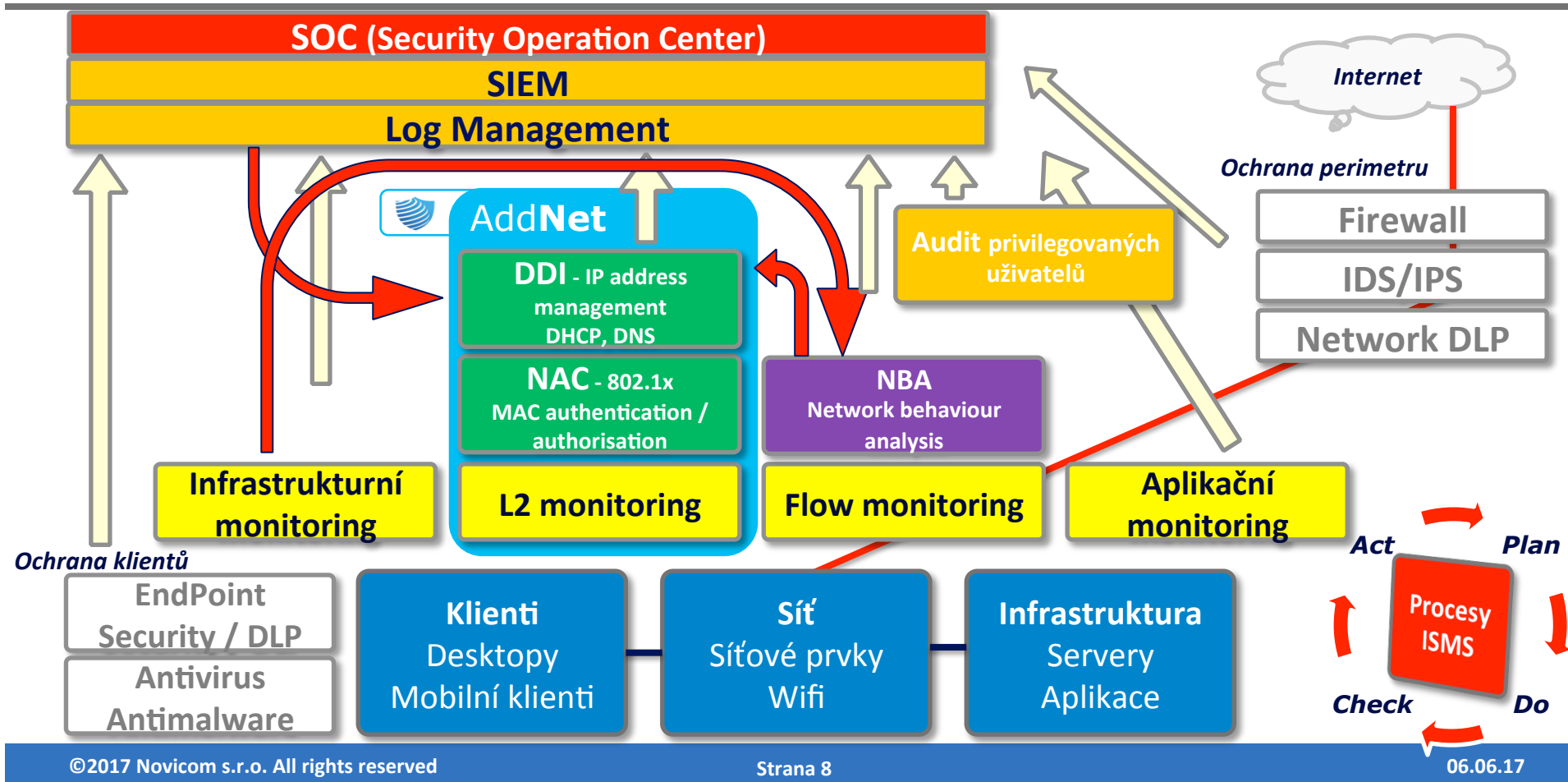
- **Koncept připravený na půdě NSMC**
- **Network Security Monitoring Cluster**
 - *kooperační odvětvové uskupení zaměřené na oblast bezpečnosti počítačových sítí a bezpečnosti v ICT*
- **Aktivity klastru**
 - společné projekty v oblasti technické infrastruktury inovačního charakteru, aplikovaného výzkumu, vývoje a inovací
 - návrh a integrace komplexních řešení v oblasti monitorování bezpečnosti sítí
 - osvěta týkající se bezpečnosti počítačových sítí a informací, školení a vzdělávání
 - návrhy úprav 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,...)
 - tvorba a akreditace výukových programů kybernetické bezpečnosti pro střední a vysoké školy



Our Vision Your Security



Koncept Aktivní bezpečnosti sítě



- **Stávající legislativa**

- **Dílčí normy národní normy – příklad z ČR nejvýznamnější:**

- ZoKB (181/2014 Sb.) + prováděcí vyhlášky (316 a 317/2014 Sb.) + nařízení vlády (315/2014 Sb.)
 - Zákon o ochraně osobních údajů (101/2000 Sb.)
 - Občanský zákoník (*Péče řádného hospodáře apod.*)

- **Dopad pouze na omezenou množinu subjektů**

- Správci kritické a významné infrastruktury
 - Pro ostatní subjekty – významný PR aspekt
 - Pouze nevýznamné sankce při neplnění povinností
 - Pozvolná akceptace nutnosti komplexního řešení kybernetické ochrany

Přicházející legislativa

- **Změny vycházející z EU směrnice NIS – úpravy/rozšíření ZoKB**
 - rozšíření dotčených subjektů dle ZoKB
 - ostatní změny jsou minoritní
- **Nové EU nařízení GDPR – *General Data Protection Regulation***
 - významné zpřísnění v oblasti ochrany osobních dat
 - dopad na všechny subjekty – instituce i firmy
 - přináší **zásadní pokuty za porušování nových pravidel**
 - až **20.000.000 Euro** nebo **4% z obrátu** a
 - a dále **náhradu škody**
 - zavádí novou nezávislou kontrolní funkci **DPO – Data Protection Officer**
(Pověřenec pro ochranu osobních údajů)



Jak se s GDPR vypořádat?

Cesta ke splnění GDPR požadavků

- Srovnávací analýza stavu ochrany OÚ
- Plán implementace
- Analýza rizik zpracování OÚ
- Posouzení vlivu na ochranu OÚ
- Implementace a zdokumentování procesů
- Zahájení technické úpravy IS (+ možné zavedení podpůrných nástrojů)
- Technická úprava IS
- Školení uživatelů
- Testy a přezkoumání systému ochrany



25.5.2018

GDPR – akceptování závažnosti

- Platí pro všechny firmy a organizace
- Rozšiřuje definici významu osobních dat
- Zpřísňuje pravidla pro získání platného souhlasu s použitím osobních údajů
- Požaduje jmenování inspektora ochrany údajů (DPO – Data Protection Officer)
- Zavádí povinné PIA – Privacy Impact Assessment
- Zavádí podmínku oznámení úniků dat pro všechny
- Zavádí právo být zapomenut
- Rozšiřuje odpovědnost správce údajů osobních dat
- Vyžaduje ochranu soukromí již v návrhu systému
- Zavádí koncept jednotného přístupu

A jak to souvisí s Novicom a jeho řešeními?

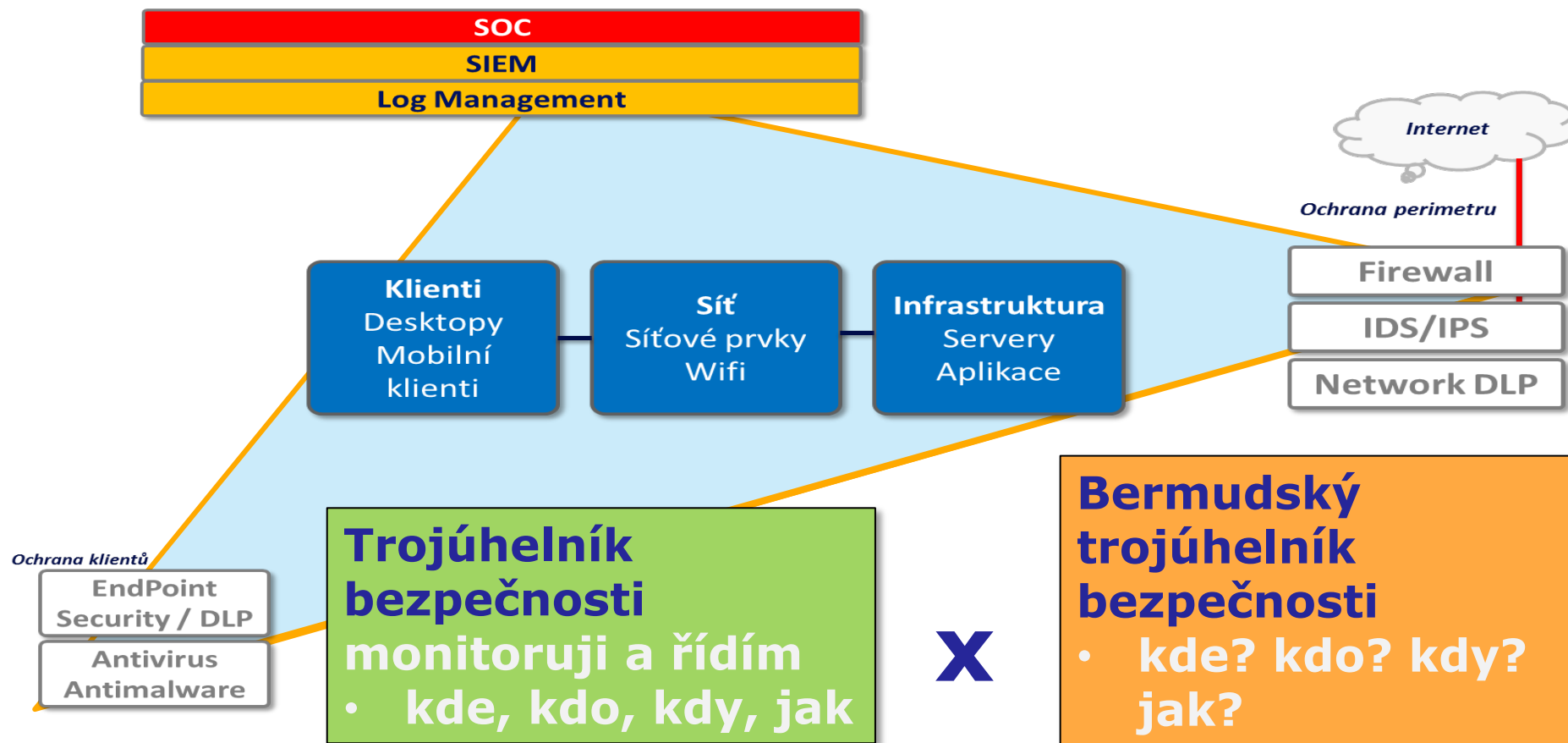


- GDPR se zaměřuje především na zajištění ochrany osobních údajů



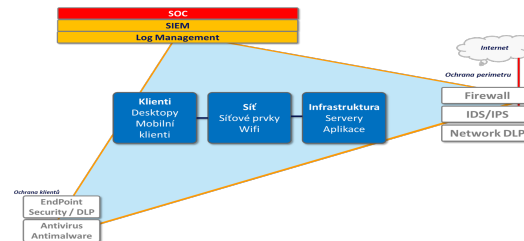
- **Se svými partnery vám pomůže provést systematickým zaváděním GDPR**
- **Řešení Novicomu se pak přímo zaměřuje na**
 - zajištění interní sítě proti provozu neoprávněných zařízení v síti
 - L2 monitoring
 - NAC – autentizace a autorizace
 - zvýšení dostupnosti a zajištění bezpečnosti i pro distribuované sítě (DDI/NAC)
 - ve spojení s nástroji pokročilé detekce (NBA, SIEM) - minimalizace doby nezbytné pro eliminaci škodlivých zařízení v síti

Bezpečnost vnitřní sítě



Bermudský trojúhelník bezpečnosti

- kde? kdo? kdy? jak?



Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ❖ **Žádné řízení přístupu do sítě (NAC)**
- ❖ **Evidence IP adres v excelu**
- ❖ **Dynamicky přidělované IP adresy DHCP**
- ❖ **Samostatné DNS**
- ❖ **Pouze základní monitoring**
 - ❖ **Infrastruktura**
- ❖ **Žádný pokročilý monitoring síťového provozu**

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
 - ✓ **IPAM, DHCP a DNS**
- ✓ **Pevné IP přidělované DHCP**
- ✓ **Multispektrální monitoring**
 - ✓ **L2 Monitoring, Infrastruktura,**
 - ✓ **Flow Monitoring, Aplikace**
- ✓ **Pokročilá ochrana vnitřní sítě - NBA**

Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
 - SIEM vyhodnotí bezpečnostní incident
 - SOC operátor kontaktuje síťového správce
 - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
 - Převezme z fronty požadavků
 - Začne **lokalizovat zařízení**
 - dynamická adresa?/ hledání v logách...
 - Přihlásí se na switch a **odpojí port**
 - Informuje admina PC
- **Provedení nápravných opatření - Administrátor PC**
 - Vyžádá si fyzické zařízení
 - Provede odvirování
 - Požádá síťáře o znovuzapojení do sítě

minuty

minuty/
hodiny/
???

minuty/
hodiny

Pokročilé řešení kybernetických incidentů

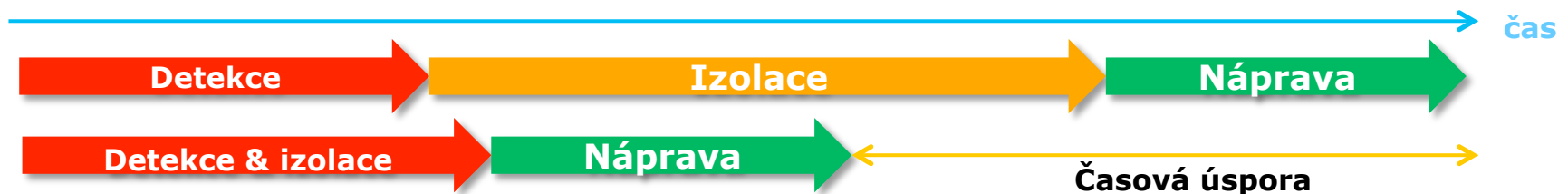


- **Identifikace a eliminace hrozby – operátor SOC**
 - SIEM **vyhodnotí** bezpečnostní incident
 - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
 - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
 - případně **změní IP adresu** v integrovaném DDI nástroji
 - kontaktuje administrátora PC
- **Provedení nápravných opatření - Administrátor PC**
 - Vyžádá si fyzické zařízení
 - Provede odvirování
 - Požádá správce sítě o znovupřipojení zařízení do sítě



Shrnutí

- Je v pořádku, že se věnujete ochraně
 - **Perimetru a Klientů**
- Počítejte ale s tím, že tato ochrana bude překonána
 - **Signature based protection**
- Zajistěte si nástroje pokročilé detekce a monitoringu v síti
 - **NBA**
 - **SIEM**
- Investujte do integrovaných nástrojů, které vám pomohou výrazně zkrátit reakční dobu při řešení zjištěných bezpečnostních incidentů a navíc řádově usnadní správu sítí
 - **L2 monitoring DDI NAC**

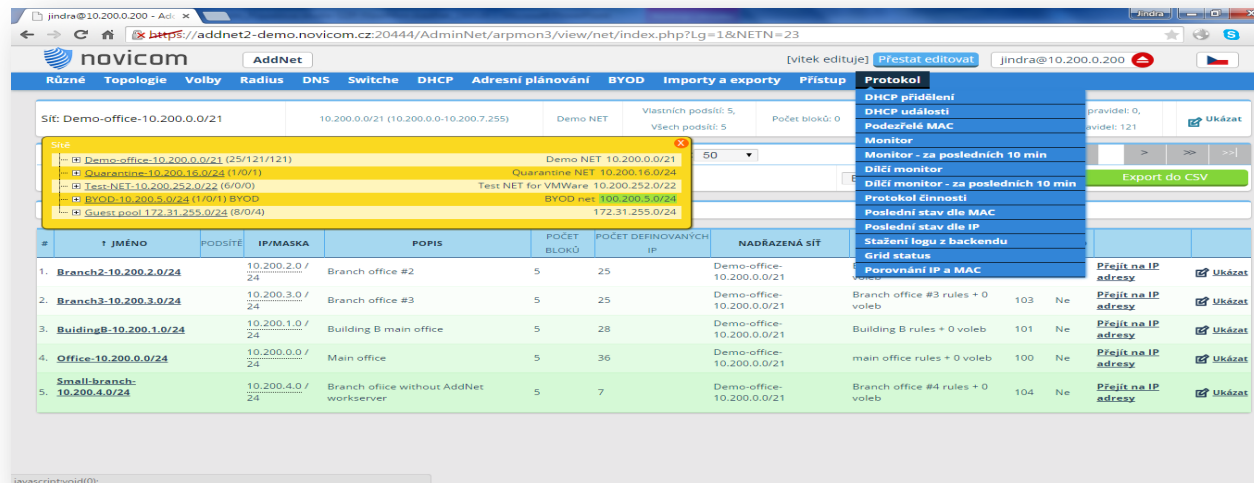


Integrovaný
DDI/NAC nástroj
pro pokročilou
správu IP adresního
prostoru
a řízení bezpečnosti
přístupů v síti



Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích.**

Toho je dosaženo **integrací systémů** L2 monitoringu, správy IP adresního prostoru, základních síťových služeb (DHCP, DNS), řízení přístupu do sítě (NAC) a pokročilé komunikace s aktivními prvky sítě.



The screenshot shows the AddNet web interface. The main content area displays a tree view of network sites and a table of network segments. A dropdown menu is open, showing various monitoring and management options.

#	JMÉNO	PODSÍŤ	IP/MASKA	POPIS	POČET BLOKŮ	POČET DEFINOVANÝCH IP	NADŘAZENÁ SÍŤ	POČET PRAVIDEL	POČET MAC	POČET IP	POČET MAC	POČET IP	POČET MAC
1.	Branch2-10.200.2.0/24	10.200.2.0/24	10.200.2.0/24	Branch office #2	5	25	Demo-office-10.200.0.0/21	Branch office #3 rules + 0 voleb	103	Ne	Přejít na IP adresy	Ukázat	
2.	Branch3-10.200.3.0/24	10.200.3.0/24	10.200.3.0/24	Branch office #3	5	25	Demo-office-10.200.0.0/21	Building B rules + 0 voleb	101	Ne	Přejít na IP adresy	Ukázat	
3.	BuidingB-10.200.1.0/24	10.200.1.0/24	10.200.1.0/24	Building B main office	5	28	Demo-office-10.200.0.0/21	main office rules + 0 voleb	100	Ne	Přejít na IP adresy	Ukázat	
4.	Office-10.200.0.0/24	10.200.0.0/24	10.200.0.0/24	Main office	5	36	Demo-office-10.200.0.0/21	Branch office #4 rules + 0 voleb	104	Ne	Přejít na IP adresy	Ukázat	
5.	Small-branch-10.200.4.0/24	10.200.4.0/24	10.200.4.0/24	Branch office without AddNet workserver	5	7	Demo-office-10.200.0.0/21						

Původní Novicom technologie



▪ Novicom SGP (Secure Grid Platform)

- technologická platforma pro nadstandardní provozní spolehlivost Novicom systémů a jejich integrovaných klíčových služeb (L2monitoring a základní síťové služby DHCP/ DNS/ NAC)
- **vícenásobná redundance typu Active-Active, podpora hierarchického a distribuovaného modelu** v prostředí rozsáhlých sítí

SGP
Secure
Grid
Platform

▪ Novicom SDP (Secure Delivery Protocol)

- vlastní komunikační protokol navržený pro zajištění spolehlivé komunikace v prostředí potenciálně nekvalitní sítě
- **pracuje na linkách s chybovostí až 95%**
- garance maximálního zabezpečení přenášených dat (military grade security)

SDP
Secure
Delivery
Protocol

▪ Novicom FireBox platforma

- systém HW a virtuálních apliančí, zvyšující bezpečnost, spolehlivost a servisní flexibilitu pro klíčové komunikační a bezpečnostní funkce
- je založené na OS Linux s bezpečnostními úpravami, s nezávislými prvky centrální správy a zálohování/obnovy
- Flexibilní správa s Grid Managerem

FireBox
appliances

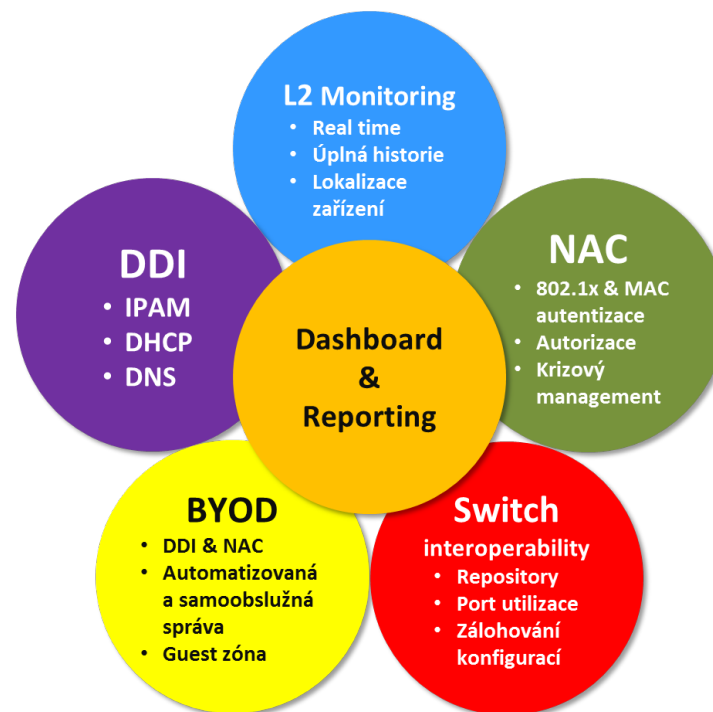
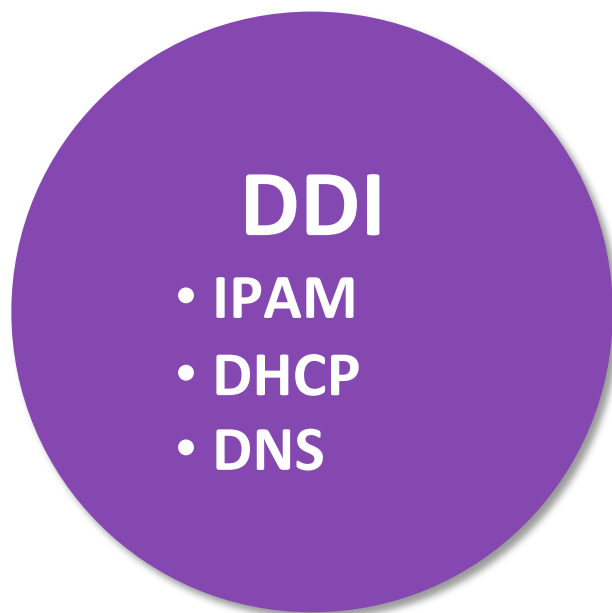


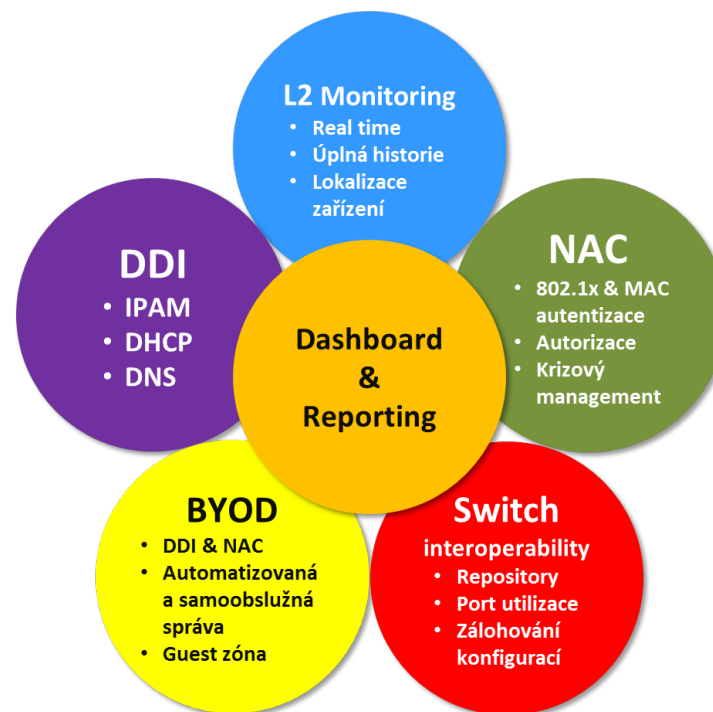


L2 Monitoring

- Real time
- Úplná historie
- Lokalizace zařízení

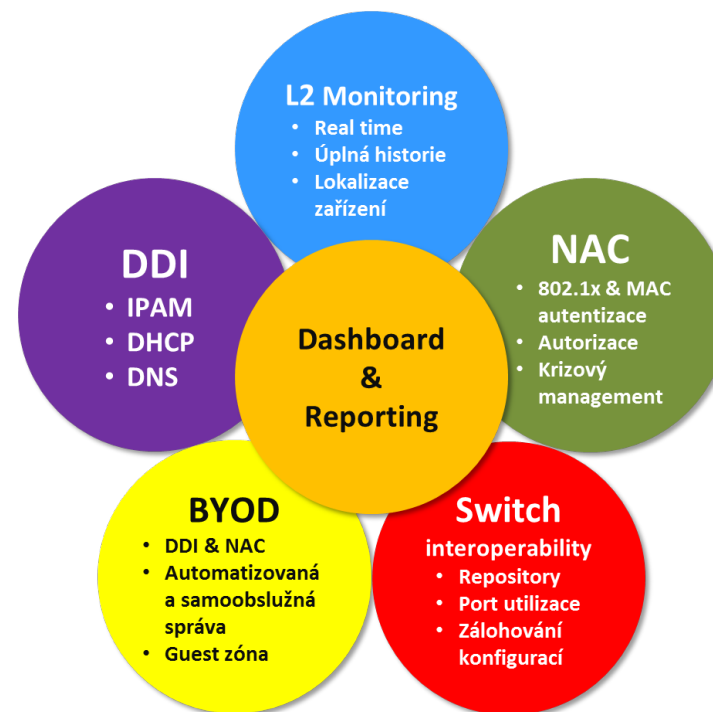


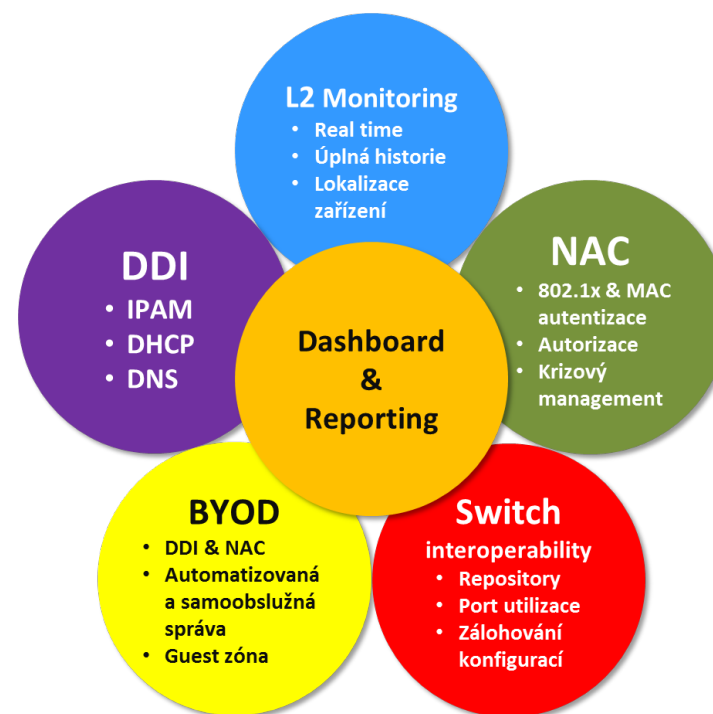




BYOD

- DDI & NAC
- Automatizovaná a samoobslužná správa
- Guest zóna

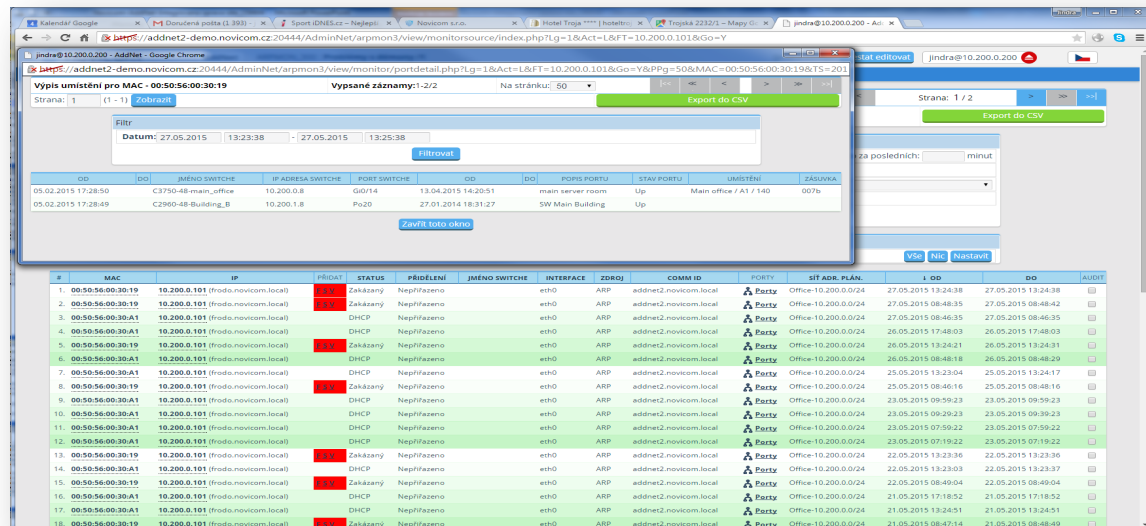






L2 monitoring

- Základní stavební kámen AddNetu
- Poskytuje informace o výskytu zařízení v síti
 - **KTERÁ**
 - **IP/MAC**
 - **KDE**
 - **se nachází v síti**
- Real-time monitoring
- Úplná historie výskytu zařízení v síti
- Podpora kabelové knihy
 - Možnost importu



Výpis umístění pro MAC - 00:50:56:00:30:19

DD	DD	JMÉNO SWITCHE	IP ADRESA SWITCHE	PORT SWITCHE	DD	DD	POPIS PORTU	STAV PORTU	UMÍSTĚNÍ	ZÁSUJKA
05.02.2015 17:28:50		C3750-48-main_office	10.200.0.8	Gi0/14	13.04.2015 14:20:51		main server room	Up	Main office / A1 / 140	007b
05.02.2015 17:28:49		C2960-48-Building_B	10.200.1.8	Po20	27.01.2014 18:31:27		SW Main Building	Up		

#	MAC	IP	PRŮJED	STATUS	PŘÍDELNÍ	JMÉNO SWITCHE	INTERFACE	ZDROJ	COMM ID	PORTY	SIF	ADR. PLÁN	I DD	DD	AUDIT
1.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	27.05.2015 13:24:38	27.05.2015 13:24:38		
2.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	27.05.2015 08:48:35	27.05.2015 08:48:35		
3.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	27.05.2015 08:46:35	27.05.2015 08:46:35		
4.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	26.05.2015 17:48:03	26.05.2015 17:48:03		
5.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	26.05.2015 13:24:21	26.05.2015 13:24:21		
6.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	26.05.2015 08:46:18	26.05.2015 08:46:18		
7.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	25.05.2015 13:23:04	25.05.2015 13:23:04		
8.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	25.05.2015 08:46:16	25.05.2015 08:46:16		
9.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	23.05.2015 09:59:23	23.05.2015 09:59:23		
10.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	23.05.2015 09:29:23	23.05.2015 09:29:23		
11.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	23.05.2015 07:59:22	23.05.2015 07:59:22		
12.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	23.05.2015 07:19:22	23.05.2015 07:19:22		
13.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	22.05.2015 13:23:36	22.05.2015 13:23:36		
14.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	22.05.2015 13:23:03	22.05.2015 13:23:03		
15.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	22.05.2015 08:49:04	22.05.2015 08:49:04		
16.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	21.05.2015 17:18:52	21.05.2015 17:18:52		
17.	00:50:56:00:30:A1	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:A1	DHCP	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	21.05.2015 13:24:51	21.05.2015 13:24:51		
18.	00:50:56:00:30:19	10.200.0.101 (frodo.novicom.local)	00:50:56:00:30:19	Zakazany	Nepřifazeno		eth0	ARP	addnet2.novicom.local	Party	Office-10.200.0.0/24	21.05.2015 08:47:14	21.05.2015 08:47:14		

AddNet L2 monitoring je schopný v reálném čase upozornit na rozpor mezi adresním plánem a realitou v síti!

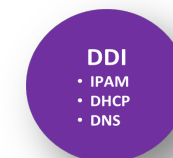
L2 Monitoring

- Real time
- Full history
- Physical locality

IPAM – Repository síťových zařízení

Umožňuje řízení DNS, IP adresních dat a přístupové politiky (pro NAC) na úrovni rozsáhlých organizací s jednotnou správou, monitoringem a auditem.

- **Repository zařízení**
 - Filozofie umožnění komunikace pouze známých (povolených zařízení) v síti
 - Možná správa doplňkových informací
 - Vazba na L2 monitoring
 - Vazba na aktivní prvky
- **IP Adresní plánování**
 - **IPAM** – vytváření a správa IP adresního plánu
 - Správa **DHCP a DNS**
- **Správa NAC**
 - **Autentizace**
 - řízení přístupů zařízení do sítě (802.1x / MAC autentizace)
 - **Autorizace**
 - řízení přiřazování zařízení do VLAN
 - **Podpora krizového řízení**



IPAM - Adresní plánování

- **Přidávání a konfigurace síťových zařízení**
 - Možnost rychlého přidělení IP přímo z prostředí monitoringu
 - Automatická provázanost na DHCP/DNS/Radius
 - Maximální uživatelské přívětivost a proaktivnost
 - ***Dramatické snížení pracnosti síťové správy***
 - Snadné přidání zařízení do sítě bez konfigurace – změna z „dynamic“ na „fixed“
 - Přiřazení další volné IP adresy
- **Podpora krizového řízení**
 - Možnost vytvoření tzv. Krizových setů
 - V případě incidentů umožňuje okamžité odpojení všech zařízení, mimo krizový set
 - Po odstranění příčin a/nebo důsledků incidentu je možné postupně obnovit síťový provoz na vybraných zařízeních
- **Historie přiřazení adres IP/MAC**



▪ Flexibilní model nasazení DDI

- **Centralizovaný** x
- **Distribuovaný**
- *Možnost zajištění plné redundance služeb i v lokalitě, která je dočasně nedostupná*

▪ DHCP

- Výhody integrace s L2 monitoringem
- Rozšířený set funkcionality
- Vysoký výkon díky multithreadové architektuře
 - (High Performance DHCP services)

▪ DNS

- Distribuovaný model
- Podpora více interface
- Bezproblémová spolupráce se stávající infrastrukturou



NAC – Řízení přístupů do sítě

Integrovaná komunikace s aktivními prvky a podpora standardu 802.1x (RADIUS) a jeho subsetů – MAC autentizace a autorizace (dynamické řízení VLAN)

- **Podpora full 802.1x a/nebo MAC autentizace s ochranou** – bez nákladů na administraci
- **Při požadavku zařízení na síťovou komunikaci** příslušný switch provede dotaz do integrovaného Radius serveru AddNetu, který dá informaci
 - zda má zařízení povolenou komunikaci – **Autentizace**
 - případně zařadí zařízení do nastavené VLAN – **Autorizace**
- **Při požadavku na odpojení zařízení** je tato informace distribuována do integrovaného Radiusu. Při opětovném dotazu aktivního prvku (Reautentikace) je přístup odepřen a zařízení nemůže komunikovat na síti. Alternativou je pouze změna Autorizace – např. zařazení zařízení do karanténní sítě
- **Výhodná dvoufázová implementace**
 - **Fáze 1.** – součást DDI – **zavedení MAC autentizace s ochranou**
 - **Fáze 2.** – následné zvyšování ochrany formou **postupného zavádění full 802.1x**

Řeší problémy nedokončených NAC implementací s 802.1x

- *Suplikanty nejsou pro 100% zařízení*
- *Nezvládnutá správa výjimek – portů vyjmutých z ochrany*



Network Visibility & Security

Advanced Network Monitoring
Distributed IP Network Management



AddNet

DDI/NAC

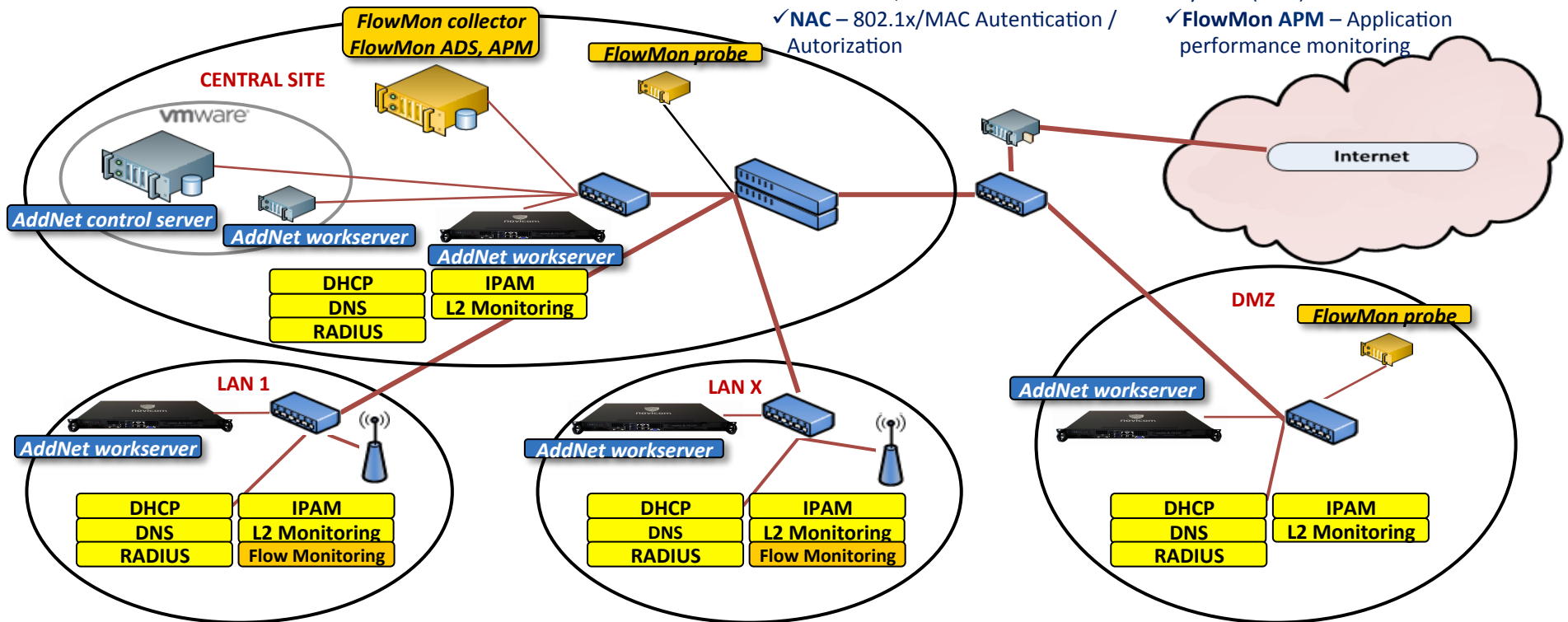
- ✓ L2 monitoring
- ✓ IPAM – address space management
- ✓ DDI - DHCP, DNS
- ✓ NAC – 802.1x/MAC Authentication / Authorization



Flowmon (ADS)

Flow monitoring

- ✓ IP-flows monitoring
- ✓ FlowMon ADS – Anomaly detection system (NBA)
- ✓ FlowMon APM – Application performance monitoring



Snadné nasazení AddNetu

- **Využití původní Novicom implementační metodiky NIM**
 - Definované postupy a výstupy
 - Kontrola kvality
- **Hlavní fáze**
 - **Vstupní analýza**
 - **Příprava SGP infrastruktury**
 - **Aplikační nastavení AddNetu**
 - **Iniciační sniffing**
 - **Nastavení finální IP strategie**
 - **Spuštění DDI**
 - **Spuštění NAC**
 - **Zahájení provozní podpory**



Klíčové přínosy AddNetu



- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC – snadné zavedení a správa**
 - full 802.1x a/nebo MAC autentizace s ochranou
 - následná autorizace (řízení přidělování síťových zařízení do VLAN)
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení
- **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** díky sledování utilizace aktivních prvků
- **Plná heterogenost** - bezproblémová spolupráce běžnými síťovými technologiemi
- **Schopnost okamžité reakce** na kybernetické bezpečnostní incidenty
- **Snadná implementace** a ověřené projektové postupy

Drive přínosů AddNetu



V čem je AddNet jiný?

▪ Využití vlastních technologií

- **Novicom SGP** – Secure Grid Platform
- **Novicom SDP** – Secure Delivery Protocol
- **Novicom FireBox appliance**

▪ Flexibilní podpora topologie nasazení

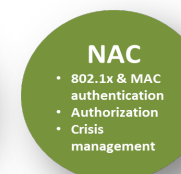
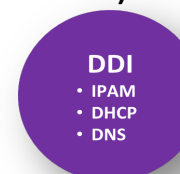
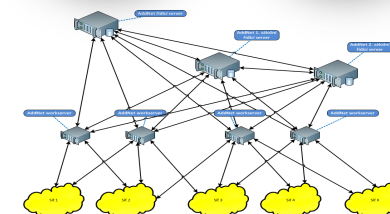
- Centralizované nasazení
- Plně distribuovaného nasazení
- Kombinované nasazení

▪ Nadstandardní provozní spolehlivost a škálovatelnost

- Provoz v distribuovaných lokalitách i při nedostupnosti řídicí lokality
- Podpora aktivního clusteringu na všech úrovních
- Nadstandardní bezpečnost dat (appliance, datový přenos, architektura)

▪ Unikátní spojení DDI a NAC

- DDI nástroj je doplněný o NAC
- Optimalizované pro rozsáhlé distribuované sítě



- **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