ADDNET

novicom

Integrovaný DDI/NAC. Unikátní provozně bezpečnostní nástroj zajišťující úplnou síťovou visibilitu, vysoce efektivní správu IP adresního prostoru a pokročilé řízení bezpečnosti přístupů v síti.

ADDNET přináší zásadní zjednodušení a zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích. Toho je dosaženo integrací výkonného síťového monitoringu, systému IP adresního plánování (IPAM), základních síťových služeb (DHCP, DNS), řízení přístupu do sítě (NAC) a komunikace s aktivními prvky sítě. Integrací těchto, jinak zpravidla samostatných, služeb je dosaženo nové úrovně efektivity síťové správy a zabezpečení sítě.

ADDNET znamená robustnost, nadstandardní provozní spolehlivost, bezpečnost a flexibilitu nasazení. To všechno mu dávají originální Novicom technologie, jako je vlastní gridová platforma SGP, komunikační protokol SDP nebo systém vlastních Novicom appliancí.

Propracovaná síťová visibilita, snadná integrovatelnost ADDNETU s dalšími bezpečnostními nástroji a jeho vhodné využití s externími dohledovými centry – Security Operation Center (SOC) přináší nové schopnosti při potřebě zajistit rychlou reakci na zjištěné bezpečnostní hrozby.

KLÍČOVÉ PŘÍNOSY ADDNETU:

- **Vysoce výkonný L2 monitoring** s možností fyzické lokalizace zařízení – díky integraci s kabelovou knihou
- **Zavedení DDI – efektivní síťové správy** IP prostoru – významná úspora práce síťových administrátorů
- **Zavedení NAC** – řízení bezpečnosti přístupu do sítě s využitím full 802.1x nebo MAC autentizace a autorizace (přiřazování do VLAN)
- Plně automatizovaná **správa BYOD a mobilních zařízení** a jejich jednoznačná identifikace v síti
- **Standardizace činností síťových správců** a možnost centralizace správy rozsáhlých distribuovaných sítí
- Podstatné **zvýšení provozní spolehlivosti a výkonu DNS, DHCP, NAC,** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** – mimo jiné díky významnému snížení pracnosti a dlouhodobému sledování využití aktivních prvků
- **Plná heterogennost** a bezproblémová spolupráce s běžnými síťovými technologiemi předních výrobců
- Unikátní **podpora distribuovaného modelu sítě** – garance zajištění provozu monitoringu/DDI/NAC i ve vzdálené lokalitě v případě ztráty konektivity s centrální lokalitou
- Doplňkový **sběr dat o provozu ve vzdálených lokalitách** – syslogy, datové toky (flow)
- **Flexibilní provozování** – vhodné pro centralizované i plně distribuované organizace
- **Snadné nasazení** – díky vlastní implementační metodice postavené na best practices a výkonnému iniciačnímu sniffingu
- Připravenost na **nasazení v technologických sítích OT/SCADA**
- **Integrace ADDNET se SOC** – pro zajištění rychlého incident response (sběr událostí / vyhodnocení /reakce)
- Připravenost ADDNETU na **integrace s dalšími nástroji typu MS Active Directory, SIEM, Log management, NBA, DLP** apod.
- **Alertování** – rychlé upozornění na případné problémy na síti

ADDNET pokrývá následující oblasti:

Výkonný L2 monitoring

Real-time nástroj pro monitorování výskytu zařízení (IP a MAC adres) v síti, a to včetně návaznosti na jeho umístění (port switche / fyzická lokalita) včetně vizualizace fyzického umístění v půdorysu. Poskytuje rovněž kompletní historii provozu sítě pro následné auditní činnosti.

Kompletní DDI (DHCP/DNS/IPAM)

Přináší distribuované a spolehlivé základní síťové služby (DHCP a DNS) a jejich snadné ovládání díky integrovanému IPAM nástroji. Integrace s L2 monitoringem umožňuje v reálném čase řešit rozpory mezi realitou a IP adresním plánem a mít vždy adresní plán v souladu s realitou.

- **IPAM**

Systém správy IP adresního prostoru poskytuje přehledné a pohodlné nástroje adresního plánování s integrovaným řízením všech dalších dílčích částí (DHCP/DNS/NAC). V adresním plánování je tak možné velmi jednoduše přidat nové zařízení nebo změnit síťové parametry stávajících zařízení.

- **DHCP**

Standardní DHCP služby jsou navržené pro práci v rozsáhlých distribuovaných sítích a tam, kde je zapotřebí maximální provozní spolehlivost nebo výkon. Integrace s L2 monitoringem přináší rozšířené funkční možnosti a flexibilitu použití, včetně zavedení přidělování pevných IP adres pomocí DHCP na základě známých MAC adres.

- **DNS**

Integrované DNS služby přinášejí možnost spolehlivého provozu v distribuovaných sítích. Je možné využít flexibilní možnost ADDNETU řídit rovněž stávající DNS infrastrukturu prostřednictvím dynamických DNS updatů. Je tak zajištěna plná konzistence prostředí IPAM, DHCP a DNS.

Integrovaný NAC (řízení přístupu do sítě)

Výhodou integrovaného NAC řešení ADDNETU je nezávislost na typu výrobce infrastruktury, možnost provozovat 802.1x v kombinaci s MAC autentizací a dostupnost nasazení v prostředí rozsáhlé distribuované sítě. Je tak možné zajistit NAC funkcionalitu i ve vzdálené lokalitě, která nemá dočasně spojení s centrálou.

- **Plná 802.1x autentizace**

ADDNET je připraven zajistit bezpečné přihlášení zařízení kdekoli v síti. Autentizační údaje mohou být plně spravovány v ADDNETU, nebo mohou být zjišťovány pomocí integrace z prostředí Microsoft Active Directory a dalších zdrojů (OpenLDAP, Novell...). Jsou podporovány všechny běžné autentizační módy – možné kombinace klientský certifikát/user, id/heslo.

- **MAC autentizace s ochranou**

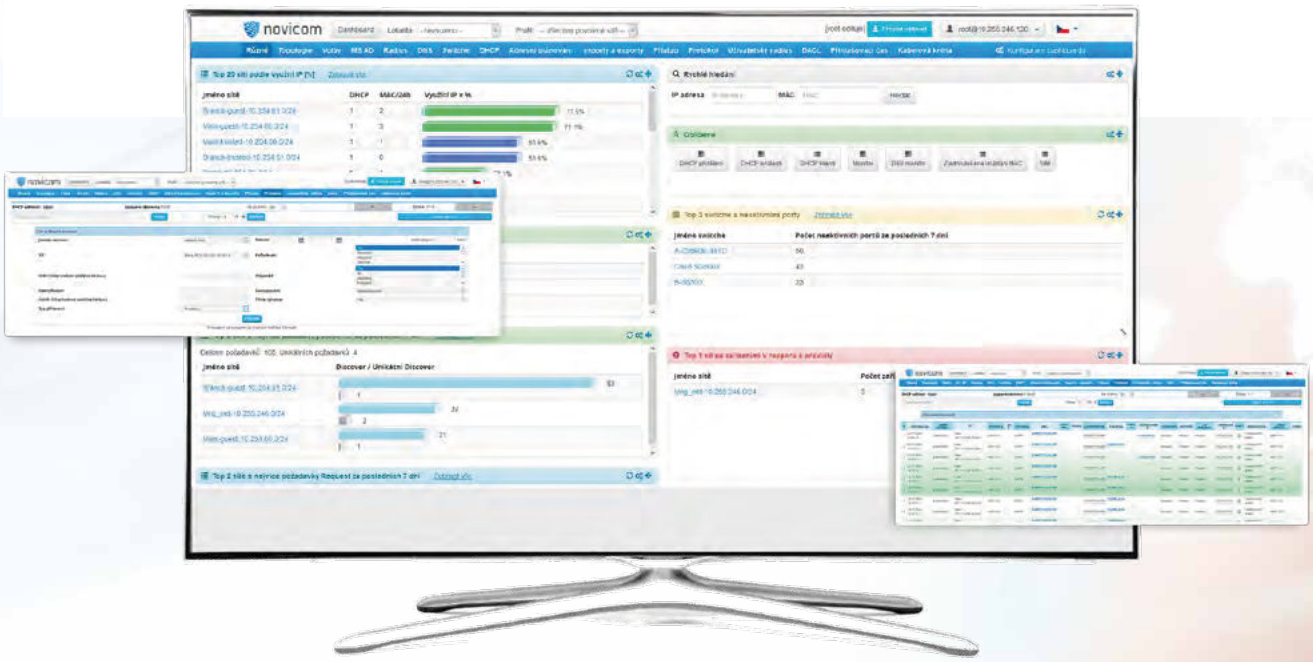
Pro zařízení, které nepodporují autentizaci pomocí supplikantů, je k dispozici alternativní MAC autentizace s ochranou. Díky integrovanému monitoringu je MAC adresa vyhodnocována ve více parametrech, například analýzou DHCP paketů a dalšími kritérii. ADDNET tak dokáže s vysokou mírou pravděpodobnosti upozornit na podvržené MAC adresy. Výhodou je odpadnutí vysoké pracnosti spojené se zavedením a správou plného 802.1x. Odpadá tak správa výjimek – všechny porty switchů jsou neustále pod kontrolou.

- **Autorizace**

Po provedení autentizace dojde v rámci procesu autorizace k přidělení zařízení do určené sítě (VLAN). V kombinaci s L2 monitoringem je ADDNET schopen zajistit dynamickou autorizaci zařízení v kterékoli lokalitě rozsáhlé sítě.

- **Real-time informace z NAC provozu**

ADDNET nabízí přehledné zobrazení informací o zařízeních, která se v rámci NAC v danou chvíli pokusila přihlásit – kdy, pod jakým jménem (v případě externí autority uživatelem), na kterém switchi a portu, s jakým výsledkem a do jaké sítě bylo zařazeno.



Podpora krizového plánování

V ADDNETU je možné definovat krizové sety, prvky kritické infrastruktury organizace. V případě bezpečnostního incidentu je možné pouhým klikem aktivovat krizový set a zajistit okamžité odpojení od sítě všech zařízení, která nejsou v krizovém setu vyjmenována.

Síťová správa a řízení přístupu pro BYOD a mobilní zařízení

ADDNET podporuje kompletní IP správu ve wi-fi sítích. Model správy DDI/NAC je doplněn o snadnou správu BYOD a mobilních zařízení. ADDNET přináší samoobslužnou zónu, kde je možné přidávat pohodlně nová zařízení do sítě. Je možné vytvářet rovněž recepční zóny. Výhodou BYOD modulu je podpora všech typů uživatelských zařízení, bez ohledu na operační systém a prostředí zařízení.

Pokročilá komunikace s aktivními prvky

ADDNET poskytuje přehledné informace o aktivních prvcích v síti v přehledovém repository. Díky kontinuálnímu sledování up/down stavu portů je ADDNET schopen monitorovat port utilizaci a určit porty aktivních prvků, které nejsou využívány. ADDNET obsahuje rovněž funkci automatického zálohování konfigurací aktivních prvků.

Přehledový Dashboard

ADDNET poskytuje na jednom místě ty nejdůležitější informace o síti a jejím využívání. Z jednotlivých zobrazovaných informací v dashboardu je možný rychlý proklik na detailní informace v dílčích částech ADDNETU. Vedle toho se nabízí možnost poskytnutí dodatečných informací o dané IP nebo MAC adrese kdekoli v aplikaci po zmáčknutí pravého tlačítka myši pro rychlé dohledání informací pomocí drilldown. Dashboard je plně přizpůsobitelný potřebám administrátora/operátora.

Detailní reporting

ADDNET nabízí široké množství pohledů na provoz zařízení v síti. Vedle informací z real-time L2 monitoringu a detailních informací z DHCP provozu poskytuje rovněž informace z aktivních prvků. Kombinace různých zdrojů vstupních informací v jednotném uživatelském prostředí přináší rozsáhlé možnosti při získávání detailních informací o zařízení, například při řešení bezpečnostních incidentů.

Pokročilé síťové politiky

- **Mikrosegmentace**

ADDNET umožňuje velmi efektivně definovat a spravovat DACL politiky na většině typů přístupových switchů. V praxi je tak možné snadno nastavit globální politiky tak, aby zařízení v rámci síťového segmentu komunikovala pouze způsobem potřebným k jejich správnému fungování. Tj. pouze v rámci povolené komunikace, ostatní komunikace nejsou povolené, a tím se násobně zvyšuje ochrana před šířením nákaz typu ransomware, a to bez nutnosti instalace agenta na stanice.

- **Důvěryhodná zařízení**

ADDNET podporuje práce s tzv. trusted zařízeními a trusted pooly, umožňujícími automatizovat nastavení síťové a přístupové politiky v rozsáhlých organizacích se vzdálenými pobočkami. Vedle své domovské sítě tak může důvěryhodné zařízení využívat odlišný způsob autentizace, autorizace a přidělení IP adresy, aniž by bylo nutné provádět jakýkoliv administrační zásah.

- **Přihlašovací čas**

V organizacích s fixní pracovní dobou lze v ADDNETu nastavit sítě tak, aby na nich bylo možné pracovat pouze v definovaných časových úsecích (např. 7:00–19:00). Toto omezení může být také nastaveno pouze pro specifická zařízení anebo některým zařízením lze naopak nastavit výjimku.

Aktivní SOC

Díky funkční flexibilitě a dostupnému distribuovanému modelu je ADDNET velmi žádaným doplňkem provozovaných Security Operation Center. Vedle informací z monitoringu přináší operátorům SOCu rovněž informace o provozu základních síťových služeb (DHCP/DNS a NAC). Ty mohou být rozšířeny o spolehlivý sběr syslogů a flow dat ze vzdálených lokalit. SOC tak dostává kompletní informace o provozu sítě a infrastruktury ve všech lokalitách sítě. Integrací nástrojů SOCu s řešením ADDNET je možné zajistit okamžitý incident response formou izolace nebo odpojení závadných zařízení operátorem SOCu, a to bez nutnosti vyžadování součinnosti od lokálního správce sítě.

Integrace

ADDNET je připraven na celou řadu integrací, které pomáhají zefektivnit síťovou správu nebo zajistit rychlý incident response.

- **Poskytování a sběr dat o provozu**

ADDNET je zdroj cenných informací pro vyhodnocení ve vrcholových nástrojích typu log management nebo SIEM. Informace o provozu nebo nestandardních stavech jsou poskytovány pomocí syslog rozhraní. ADDNET navíc dokáže, formou rozšíření svých appliancí, zajistit spolehlivý kontinuální sběr informací o síťovém provozu (flow) nebo stavu infrastruktury (syslog). Tyto informace jsou bezpečně předávány do centrální lokality k vyhodnocení specializovaným aplikacím (SIEM, NBA).

- **Aplikační integrace**

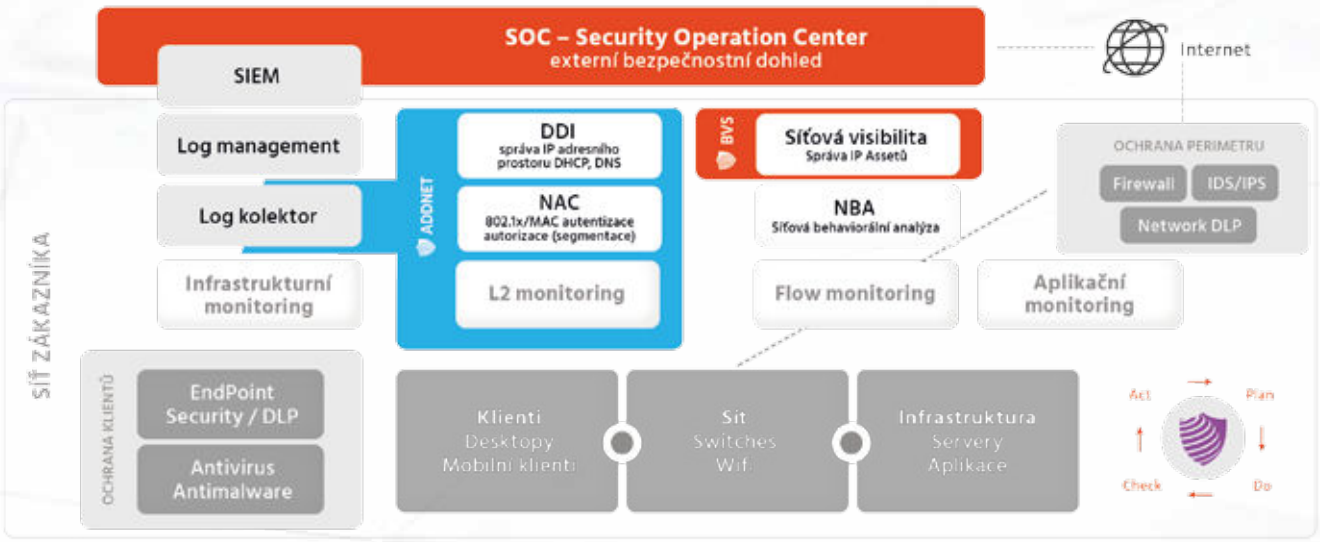
ADDNET poskytuje rozhraní pro aplikační integraci s dalšími nástroji typu behaviorální analýzy (NBA), log managementu nebo SIEM. Vedle toho je ADDNET připraven na realizaci interface pro automatizované zásahy. Důvěryhodné detekční systémy jako jsou DLP, NBA, Anti-malware nebo IDS/IPS řešení tak mají možnost předávat informace a pokyny k vykonání potřebných zásahů.

Alert Centrum

ADDNET obsahuje rozhraní, kde administrátor/operátor může spravovat své alerty o případných problémech. Účelem Alert centra je zjednodušit administrativu spojenou s vyšetřováním alertů a napomoci automatizaci celého procesu investigace. Integruje alerty z L2 monitoringu (např. duplicitní MAC), provozu NAC (např. neúspěšná autentizace 802.1x) a další.

ADDNET a Aktivní SOC

ADDNET je klíčovou součástí strategie Aktivní SOC (Security Operation Center), kterou se společnost Novicom, spolu se svými partnery, snaží prosazovat na trhu. Novicom ADDNET (pro zjednodušení a zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích) a řešení Novicom BVS (pro vizualizaci síťových zařízení včetně jejich propojení s obchodními procesy) tvoří unikátní portfolio, které připravuje zákazníky na rychlé a bezproblémové připojení ke službě SOC.



Zákazníci, využívající tuto platformu produktů, pak mohou plně **využít výhod nadstandardních služeb Aktivního SOCu**. Vybraní SOC operátoři jsou díky tomu schopni garantovat plně kvalifikovanou aktivní reakci na kybernetické útoky v režimu 24x7 bez nutné součinnosti se správci systémů u zákazníka. To plně odpovídá současnému trendu využívání vrcholového bezpečnostního dohledu (SOC) formou služby. Tím se eliminuje ekonomická nevýhodnost při pořizování kompletního spektra jednoúčelových technologií a při nutnosti mít inhouse k dispozici vysoce specializovaný tým schopný postavit se kdykoliv profesionálním hackerům.

NOVICOM – CYBER SECURITY & NETWORK MANAGEMENT HAS NEVER BEEN EASIER

novicom

Novicom, s.r.o.
Praha, Česká republika

www.novicom.cz
sales@novicom.cz

ADDNET

NVC CZ 2024-05