25th International Scientific Conference UNITECH

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025
GABROVO

ПРОУЧВАНЕ НА СЪЩЕСТВУВАЩИ РЕШЕНИЯ ЗА ИЗСЛЕДВАНЕ НА МРЕЖОВ ТРАФИК

Виктория Ивова Иванова

Технически университет – Габрово, България
Кореспондиращ автор: viki_ivova@abv.bg

STUDY OF EXISTING SOLUTIONS FOR NETWORK TRAFFIC ANALYSIS

Viktoria Ivova Ivanova

Technical University of Gabrovo, Gabrovo, Bulgaria
Corresponding author: viki_ivova@abv.bg

Abstract
Network traffic analysis (NTA) is a foundational process critical for ensuring cybersecurity, optimizing performance and enabling efficient troubleshooting across modern hybrid and cloud infrastructures. The shift towards distributed architecture makes comprehensive network visibility a paramount concern, as traffic remains the sole undeniable source of truth regarding network operations. This report conducts an in-depth study of the three primary NTA solutions based on their network analysis methodologies: deep packet inspection (DPI) tools, flow-based analyzers and modern AI-driven network detection and response (NDR) systems. The evaluation of the NTA solutions is uniquely structured around four industry-recognized criteria: forensic depth, scalability, Zero-Day detection efficiency and total cost of ownership (TCO). The study indicates that there isn't a single solution that is universally effective, as each excels in a specific situation. The report concludes that an optimal strategy for contemporary security operations requires a synergistic, complex approach combining all three existing solutions. The originality of the study lies in bridging technical evaluation with strategic integration, guiding adoption of hybrid NTA solutions.
Keywords: Network Traffic Analysis (NTA), Network Visibility, Network Analysis Methodologies, Artificial Intelligence (AI), Cybersecurity.

ВЪВЕДЕНИЕ

Изследването и анализът на мрежовия трафик са фундаментални процеси за осигуряване на киберсигурност, оптимизация на производителност и отстраняване на проблеми в съвременните компютърни системи и мрежи.

С преминаването към хибридни и облачни архитектури, мрежовата видимост (Network Visibility) е критичен компонент на всяка мрежова разработка. Мрежовият трафик се превръща в единствения неоспорим източник на информация за това какво се случва в една мрежова инфраструктура.

Липсата на качествен анализ на трафика може да доведе до забавянето на критични софтуерни приложения, отказ на мрежови услуги, неефективно използване на мрежови ресурси, както и до неоткрити пробиви и аномалии в една мрежа.

В настоящия доклад е реализиран задълбочено проучване на основните съществуващи решения за изследване на мрежов трафик и пазарното им развитие в глобален мащаб. Той се фокусира върху техните ключови методи за събиране на данни и за анализ на трафик, технически възможности, предимства,

Print ISSN: 1313-230X, Online ISSN: 3033-1404

недостатъци и приложимост. Също така, е извършена сравнителна оценка на решенията въз основа на ясно дефинирани критерии.

ИЗЛОЖЕНИЕ

Решенията за анализ на мрежовия трафик (Network Traffic Analysis, NTA) използват машинно обучение, индикатори за компрометиране (Indicators of Compromise, IoC), поведенчески анализ и предварително дефинирани правила за откриване на заплахи и аномалии в мрежовия трафик. NTA решенията подобряват мрежовата сигурност, осигурявайки пълна видимост на всички устройства, свързани към една мрежа. Като например управляеми и неуправляеми устройства, IoT (Internet of Things) реализации, както и системи, осъществили неоторизиран достъп до мрежата.

Методологията на настоящето проучване е вдъхновена от добри практики на Cisco Systems и представлява комбинация от три основни метода:

- *Аналитичен метод:* за описание и анализ на функционалността, предимствата, недостатъците и приложението на NTA решенията;
- *Сравнителен метод:* за систематична оценка на решенията по предварително дефинирани критерии;
- *Синтетичен метод:* за обобщаване на резултати, с цел формулиране на препоръка за избор на най-подходящо решение;

1. Съществуващи видове NTA решения.

Решенията главно се категоризират според използвания метод за прихващане и анализиране на мрежовия трафик. Трите основни типа NTA решения са:

а) Анализатори на мрежови пакети (Packet Analyzers) – инструменти, като Wireshark и tcpdump, предоставящи висока степен на детайлност на прихванатите от тях мрежови пакети. Методът на анализ на мрежовия трафик, който прилагат е дълбока инспекция на мрежови пакети (Deep Packet Inspection, DPI). Те работят между каналното и мрежовото ниво от модела на взаимодействието между отворените системи (Open System Interconnect, OSI), прихващайки целия трафик (Full Packet Capture) [1]. За гарантиране на пълно прихващане на трафика при високи скорости на предаване се използват хардуерни решения като мрежови TAP (Test Access Point) устройства.

- **Метод на събиране на данни:** Копиране на пълното съдържание на пакета. За висикоскоростни мрежи (над 10 Gbps) се използват системи с циклични буфери (ring buffers) и хардуерно ускорение за ефективно записване на данни на диск.
- **Приложимост:** Използват се за задълбочено отстраняване на мрежови проблеми (troubleshooting), проверка и отстраняване на грешки и несъответствия на протоколите, както и анализ след настъпил инцидент в мрежата. Чрез DPI инструментите се измерват ключови показатели като времето за реакция на приложенията (Application Response Time) и времето за двупосочно предаване на пакет между източник и получател (Round Trip Time, RTT) [2].
- **Предимства:**

  – *Дълбочина на анализа:* Предоставят пълното, необработено състояние на комуникацията в една мрежа.

  – *Гъвкавост:* Позволяват прилагане на сложни филтри за прецизен анализ и възстановяване на пълното съдържание на комуникационни сесии между устройства по различни протоколи (TCP, TLS, HTTP, DNS и др.).
- **Недостатъци:**

  – *Не са мащабируеми:* Генерират огромен обем данни (терабайти), което ги прави непрактични за постоянен мониторинг на висикоскоростни мрежи. Съхранението и управлението на тези данни е изключително скъпо.

  – *Изследването на прихванатите пакети изисква експертни познания в областта на компютърните мрежи и мрежовата сигурност.*

б) Анализатори на потоци от данни (Flow-based Analyzers) – инструменти, като NetFlow Analyzer, които са оптимизирани за мащабен мониторинг на мрежовата производителност и потребление. Вместо да прихващат всеки пакет, те събират метаданни за потоците от данни (кой, кога, колко и с кого комуникира).

- **Използвани мрежови протоколи:**

  – *Протоколи NetFlow и IPFIX (Internet Protocol Flow Information Export):* Про-

токоли за събиране на информация за мрежов трафик. Те записват метаданни за потоците от данни, без да съхраняват реалното съдържание на мрежовите пакети. IPFIX е стандартизираният наследник на NetFlow версия 9 [3], [4].

– *Протокол sFlow:* Протокол, който анализира само части от трафика. Тоест е по-подходящ за висикоскоростни мрежи (над 40 Gbps), но има по-ниска статистическа точност.

- **Метод на събиране на данни:** Експортиране на метаданни от мрежови устройства (маршрутизатори, комутатори и други) и от облачни платформи като Microsoft Azure и Amazon Web Services.
- **Приложимост:** Използват се за генериране на отчети за потреблението на ресурсите, наблюдение на тенденциите на трафика, откриване на претоварвания и анализ на ефективността на политиките за качеството на обслужване (Quality of Service, QoS) [5]. Тези NTA решения позволяват съвместна работа с протоколи като NetFlow, IPFIX и технологията Cisco NBAR2 (Network Based Application Recognition 2) за мониторинг на приложения от приложното ниво на OSI модела [6].
- **Предимства:**

– *Изключителна мащабируемост:* Драстично намаляват обема на съхраняваните данни и могат да обработват трафик от международни (WAN) мрежи.

– *Минимално натоварване:* Работят с вградените ресурси на мрежовата инфраструктура, без да изискват допълнителен хардуер или значителна изчислителна мощност.

- **Недостатъци:**

– *Липса на съдържание (Payload):* Предават се само метаданни, без реалното съдържание за осъществената комуникация. Тоест не могат да се извлекат ключови данни като потребителски имена, пароли или съдържание на HTTP заявки. Следователно тези NTA решения не са подходящи за задълбочен анализ на мрежовия трафик.

– *Зависимост между качеството на потока от данни и устройството:* Качеството на потока е пряко зависимо от неговата поддържка и конфигурация от дадено мрежово устройство. Ако то няма необходимата версия на даден протокол, събирането на данни е невъзможно или непълно. Протоколът sFlow анализира само част от трафика. Това създава риск от пропускане на редки, но критични събития, като атаки, извършени за кратък период от време.

в) Системи за откриване и реагиране на мрежови заплахи (Network Detection and Response, NDR) – NDR системите са еволюцията на традиционните системи за откриване на проникванията (Intrusion Detection System, IDS) и NTA решенията. Използват машинно обучение за създаване на основа за „нормално“ поведение (behavioral baselining) на потребителите и устройствата в дадена мрежа [7]. Следователно те са интелигентни системи, които откриват аномалии в мрежи чрез поведенчески анализ - метод за анализ на трафика. Голяма част от NDR системите прилагат, както DPI, така и анализ на потоци от данни, за по-добра мрежова видимост и допълнителна информация за мрежовата активност. Представители на тези модерни NTA решения са ExtraHop, Darktrace и други.

- **Метод на събиране на данни:** Комбинация от прихващане на мрежови пакети (за интелигентно извличане на метаданни), анализ, базиран на потоците от данни и алгоритми за машинно обучение.
- **Приложимост:** Използват се за автоматизирано откриване на аномалии и заплахи в реално време, внедряване в SOAR (Security Orchestration, Automation and Response) системи и SIEM (Security Information and Event Management) софтуерни решения [8], [9].
- **Предимства:**

– *Адаптивност към нови и непознати заплахи:* Благодарение на обучаемите модели, получени като резултат от процеса на машинното обучение.

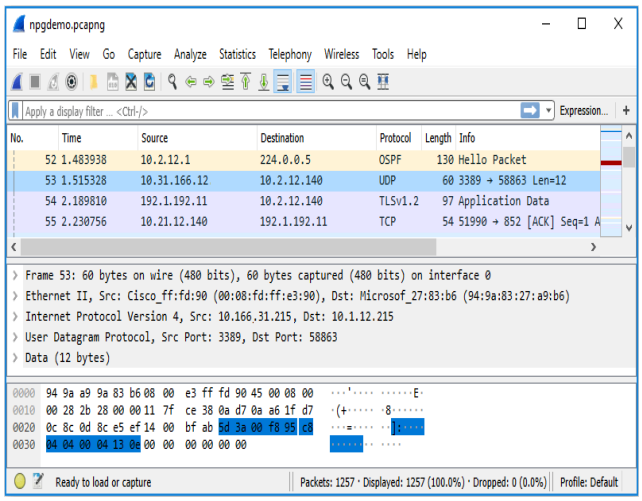
– *Откриване на заплахи в криптиран мрежов трафик:* Чрез поведенческия анализ и анализа на потоците от данни, NDR системите идентифицират аномалии без нужда от декриптиране на съдържанието.

- **Недостатъци:**

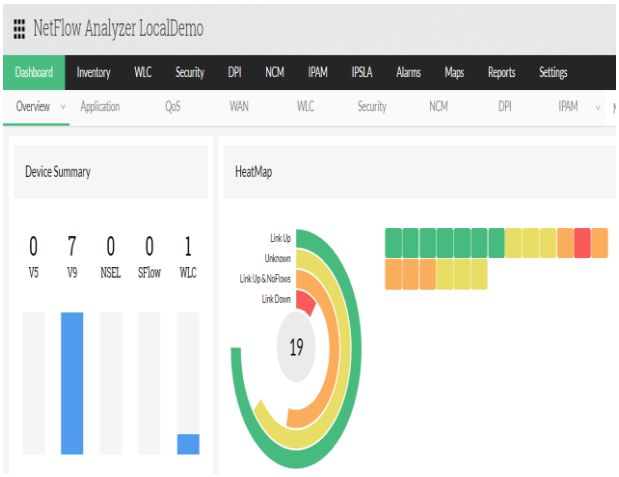
– *Висока цена:* Значителни разходи за една организация. Тези системи могат да изискват разполагане на сензори в мрежите, инвестиране в носители на данни с голям капацитет за съхранение на мрежовия трафик и т.н.

– *Изисква големи изчислителни ресурси: NDR* системите използват сложни модели, в резултат от машинното обучение, които изискват процесорна мощност и голям обем оперативна памет.

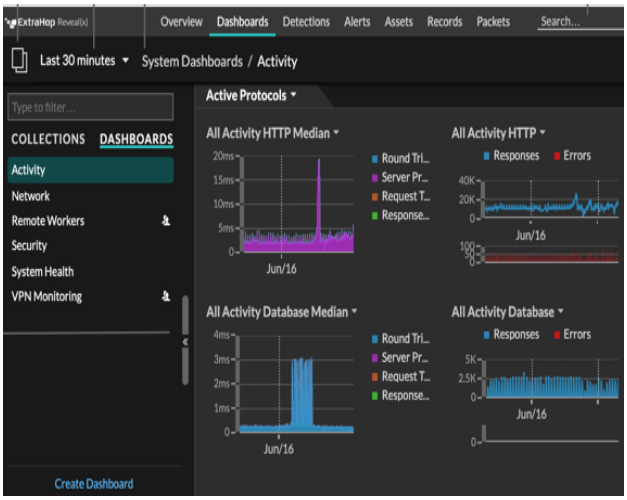
На фигури 1, 2 и 3 са показани графични интерфейси (Graphical User Interface, GUI) на различни NTA решения.



***Фиг. 1**. GUI на анализатора на мрежови пакети Wireshark.*



***Фиг. 2**. GUI на анализатора на потоци от данни NetFlow Analyzer.*



***Фиг. 3**. GUI на NDR системата ExtraHop.*

2. Оценка на NTA решенията въз основа на предварително дефинирани критерии.

Значимостта на настоящата публикация се изразява в предлагането на систематизирана и оригинална рамка за оценка на решенията за анализ на мрежовия трафик, съчетавайки технически характеристики с оперативна приложимост. Докладът е насочен към специалисти по киберсигурност, архитекти и мениджъри в сферата на информационните технологии и други, които търсят ефективни стратегии за интеграция на NTA решения в сложни хибридни инфраструктури.

Критериите за оценка представляват стандарти, показатели или характеристики, които се използват за обективно измерване, сравнение и избор на решение според неговото качество, ефективност и приложимост. NTA решенията са оценени на базата на следните критерии:

а) Дълбочина на анализа на мрежовия трафик - определя степента на детайлност на събраната информация и поддържката на декодиране на приложни протоколи, използвани на седмото ниво от OSI модела. Този критерии е от ключово значение за разследване на инциденти, както и за откриване и отстраняване на проблеми в мрежата.

б) Мащабируемост и хибридна работа с облачни технологии - оценява доколко решението е приложимо в големи мрежи с висококоростно предаване на трафик (над 10 Gbps), както и способността му за работа в облака.

в) Ефективност при откриване на заплахи - способността на решението да иден-

тифицира неизвестни (Zero-Day) и сложни атаки, като странично придвижване в мрежата, без да се базира на предварително дефинирани сигнатури. Това е показател, който е пряко свързан с нивото на развитие и ефективност на NTA решението.

г) Обща цена на притежание (Total Cost of Ownership, TCO) - сумата от всички преки и косвени разходи, свързани с внедряването и поддръжката на NTA решението през целия му очакван експлоатационен период. Включва инвестиции в специализиран хардуер, лицензи, абонаменти, квалифициран персонал, разходи за поддръжка на мрежовата инфраструктура и т.н.

Таблица 1 представя оценката на NTA решенията спрямо описаните критерии.

Таблица 1 „Оценка на NTA решенията“

Критерии за оценка	Тип NTA решение	Оценка
Дълбочина на анализа на мрежовия трафик	Анализатори на мрежови пакети	Висока
	Анализатори на потоци от данни	Ниска
	NDR Системи	Средна
Мащабируемост и хибридна работа с облака	Анализатори на мрежови пакети	Ниска
	Анализатори на потоци от данни	Висока
	NDR Системи	Средна до висока
Ефективност при откриване на заплахи	Анализатори на мрежови пакети	Ниска
	Анализатори на потоци от данни	–
	NDR Системи	Висока
Обща цена на притежание	Анализатори на мрежови пакети	Висока
	Анализатори на потоци от данни	Ниска
	NDR Системи	Висока

3. Резултати от проведеното проучване.

Обективните аналитични резултати, получени след сравнение на оценките са:

- Правопропорционална зависимост между ефективността при откриване на заплахи и общата цена на притежание. NDR системите демонстрират висока ефективност, което е свързано с високата им цена, поради необходимата поддръжка на сложни модели за машинно обучение и тяхното съхранение.
- Правопропорционална зависимост между дълбочината на анализ и общата цена на притежание. Анализът изисква значителни инвестиции в специализиран хардуер за прихващане и съхранение на мрежов трафик, както и висококвалифициран персонал за ръчна експертна оценка.
- Обратнопропорционална зависимост между дълбочината на анализ и мащабируемостта на NTA решенията. Пълното прихващане и инспекция на пакети генерира огромен обем данни, което изисква значителни ресурси за съхранение и обработка. Това води до затруднена хибридна работа и мащабируемост.
- NDR системите, въпреки своята висока обща цена, постигат оптимизация на оперативните си разходи. Този резултат е пряко следствие от автоматизацията на процеса по откриване и реагиране на заплахи, което намалява зависимостта от ръчен експертен анализ.
- Липса на ефективност за откриване на заплахи при анализаторите на потоци от данни. Работата им само с метаданни ограничава техните функции до мониторинг на мрежовото потребление и производителност.

Проучвания на световния пазар показват, че има тенденция към нарастваща нужда от NTA решенията. Тя е задвижвана от необходимостта от висока мащабируемост, ефективност при откриване на заплахи и хибридна работа с облачни технологии. В резултат от това, пазарът на NTA решенията, който към 2025 година е оценен на стойност близо 5 милиарда щатски долара (USD), е предвиден да се удвои за период от 10 години. Водещи държави на пазара са: Съединените американски щати (САЩ), Великобритания, Китай и Япония. Прогнозира се, че до 2035 г. те ще достигнат следните приходи [10]:

- САЩ (11.7 милиарда USD);
- Китай (1.6 милиарда USD);
- Великобритания (681.2 милиона USD);

- Япония (479.6 милиона USD);

Следователно, САЩ категорично доминира пазара на NTA решенията. Това е резултат от значително по-високите им инвестиции в киберсигурността и бързото внедряване на високоскоростни мрежи.

ЗАКЛЮЧЕНИЕ

Направените оценки в това проучване отразяват техническите възможности, ограниченията и ефективността на трите типа NTA решения. Установените аналитични зависимости показват, че дълбочината на анализа е правопропорционална на общата цена на притежание и обратно-пропорционална на мащабируемостта и хибридната работа с облачни технологии.

Основният извод е, че нито едно от решенията не е универсално. Изборът на оптимален вариант е стратегически и зависи от приоритетите на организацията, като производителност и сигурност.

Всяко NTA решение изпълнява конкретна роля. За отстраняване на проблеми и анализ при настъпили инциденти в една мрежа инструментите за инспекция на мрежовите пакети са незаменими. От друга страна, анализаторите на потоци от данни са по-подходящи за мониторинг на капацитета, тенденциите и потреблението на ресурси в големи мрежи. А за изграждане на многослойна мрежова сигурност, модерните NDR системи предлагат най-добрата защита, като автоматизират откриването на сложни и вътрешни заплахи чрез поведенчески анализ.

Пазарът на NTA решенията се характеризира с прогнозна експоненциална експанзия. Въпреки потенциала за растеж в Азия, стратегическото лидерство и пазарната тежест на САЩ ще останат определящи за глобалната доминация през следващото десетилетие.

Заключителната препоръка от направеното проучване в този доклад е, че за реализирането на една ефективна мрежова стратегия се изисква хибриден подход, използващ комбинация от няколко NTA решения. По този начин, хибридният модел реализира многопластова защита с добра видимост върху мрежовия трафик и дава възможност за адаптация към разнообразни инфраструктури. Критично за ефективността е централизирането на управлението на данните и гарантирането на съвместимост между компонентите.

Настоящият доклад, може да бъде използван като фундаментална основа за планирането и реализацията на ефективни NTA решения и многослойна защита в различни организационни инфраструктури.

Източник на финансиране: Настоящият документ е изготвен с финансовата помощ на договор № НИП2025-9 за провеждане на научни изследвания по проект на тема: „Изследване и изграждане на софтуерно дефинирани мрежи” към Технически университет – Габрово.

ЛИТЕРАТУРА

[1] Kurose, J. F., & Ross, K. W, Computer Networking: A Top-Down approach, Eighth Edition, Pearson, 2020.

[2] SpeedVitals, “What is Round Trip Time - RTT vs TTFB vs latency available at: https://speedvitals.com/blog/round-trip-time, 2025 (09.10).

[3] Cisco Systems, Cisco NetFlow version 9 flow-record format available at: https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper.html, 2025 (09.10).

[4] IETF, RFC 5101: Specification of the IP flow information export (IPFIX). Protocol for the exchange of IP traffic flow information available at: https://datatracker.ietf.org/doc/rfc5101/, 2025 (07.10).

[5] Cisco Systems, Quality of Service (QoS) implementation guide available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campbest/qoscamp _2.html, 2025 (07.10).

[6] Adrem Software, Traffic flow analyzer available at:https://www.adremsoft.com/netcrunch/modules/flow-analyzer, 2025 (07.10).

[7] Gartner, Magic quadrant for network detection and response (NDR). Gartner Inc., 2025.

[8] Fortinet, What is SOAR available at: https://www.fortinet.com/resources/cyberglossary/what-is-soar’, 2025 (05.10).

[9] Microsoft, Introduction to SIEM available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem, 2025 (05.10).

[10] Future Market Insights, Inc., Network Traffic Analysis Solutions Market available at: https://www.futuremarketinsights.com/reports/network-traffic-analysis-solutions-market, 2025 (06.10).