
SECURITY & PERFORMANCE
FROM THE INSIDE OUT
7-8 maja 2026
Hotel Mazurski Raj
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ARROW
ectacom
EXCLUSIVE NETWORKS
CLICO
ExtraHop

ExtraHop

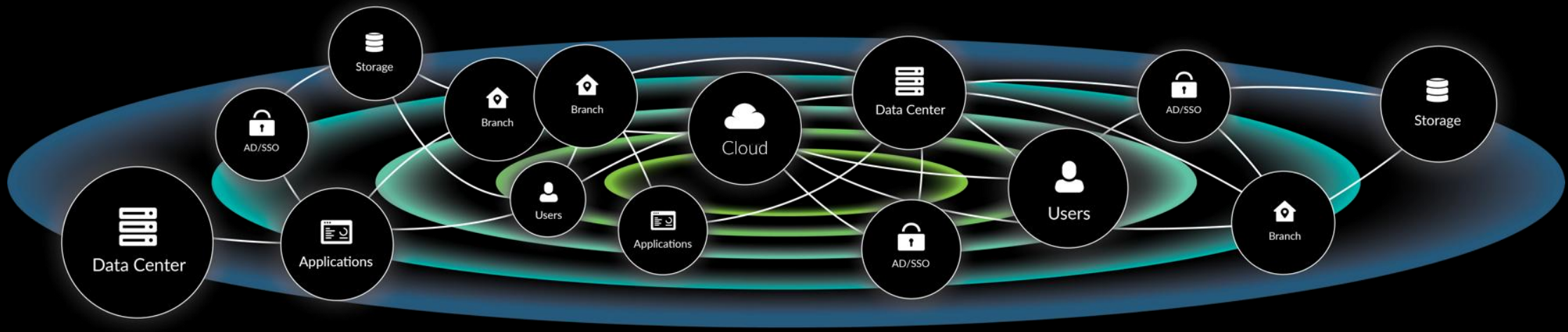
SECURITY & PERFORMANCE FROM THE INSIDE OUT

Network Detection & Response in Practice

Jak wykrywać zagrożenia ukryte w ruchu sieciowym dzięki NDR. Widoczność lateral movement, anomalie i szybsza reakcja SOCi

Tomasz Szymański
CISA, CISM, AMBCI,
ISO27000 Lead Auditor

NOWOCZESNE HYBRYDOWE ORGANIZACJE SĄ ROZLEGŁE I SKOMPLIKOWANE



BEZPIECZNICY ORAZ IT PODCHODZĄ DO ZAGADNIEŃ ZŁOŻONOŚCI ŚRODOWISKA Z RÓŻNYCH PERSPEKTYW

DLACZEGO POTRZEBUJEMY ANALIZĘ RUCHU W SIECI?

ATAKUJĄCY ZNAJĄ SŁABOŚCI OBECNYCH ZABEZPIECZEŃ:

70% inwestycji w Security to **BRZEG SIECI**

SIEM – Jest tak dobry jak **ŹRÓDŁA** danych, sam nie ma wiedzy

EDR – Coraz więcej urządzeń **IoT / BYOD**, drukarki, CCTV, SmartTV, systemy dostępowe, zarządzania budynkiem…
EDR Można wyłączyć!!!

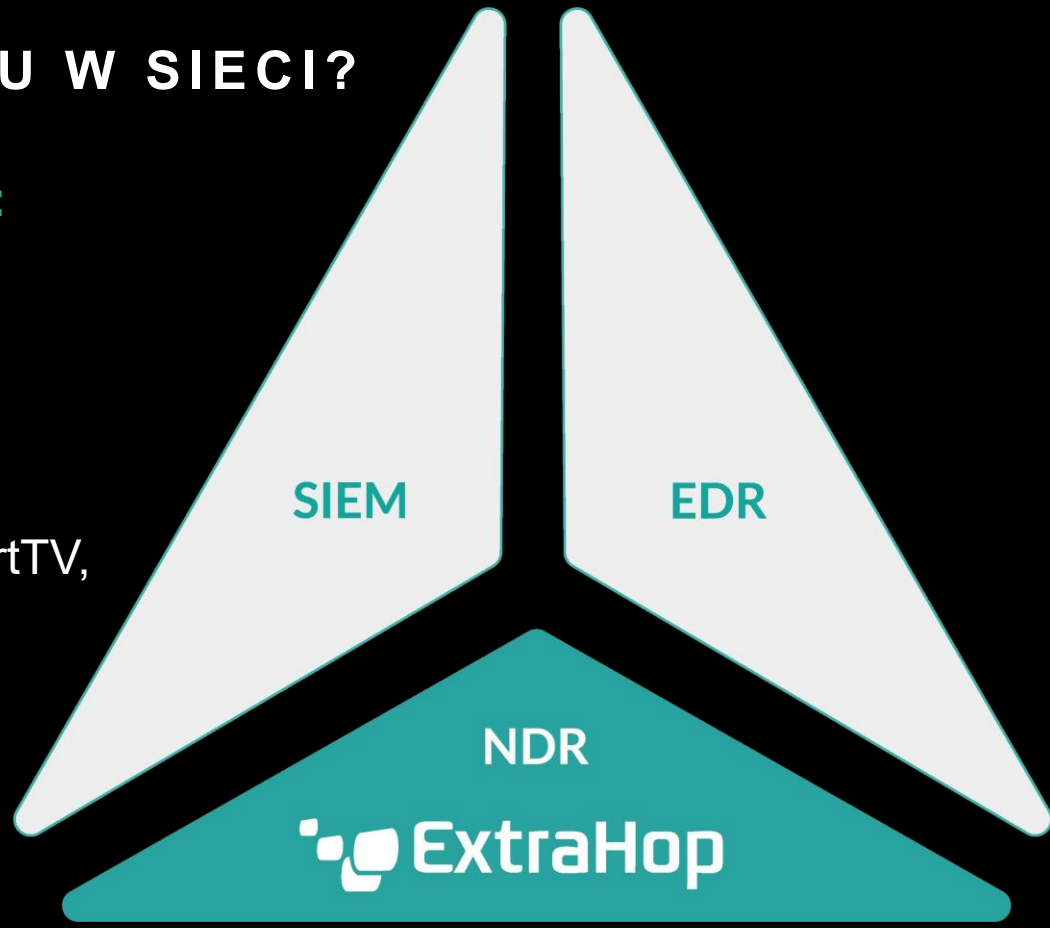
IPS /IDS – Wykrywają **ZNANE** ataki, szyfrowanie!

SANDBOXING – odłożone w **CZASIE** wolno działające ataki

NetFlow – dane **STATYSTYCZNE** nie zaprojektowane pod cybersec

POPRAWKI – Gdy podatności są **ZNANE** a systemy **WSPIERANE**

SOCJOTCHNIKA – Wielki powrót **SOCJOTECHNIKI** obchodzących wszelkie zabezpieczenia brzegowe! Atakujący po dostaniu się do środka czują się swobodnie i **BEZKARNIE**



DLACZEGO POTRZEBUJEMY ANALIZĘ RUCHU W SIECI?

NARZĘDZIA DO MONITOROWANIA WYDAJNOŚCI NIE ZNAJĄ KONTEKSTU:

Widzą obciążenie serwera, ale nie **POLECENIE** które je spowodowało

Nie mają wiedzy o parametrach **SIECIOWYCH** takich jak RTT

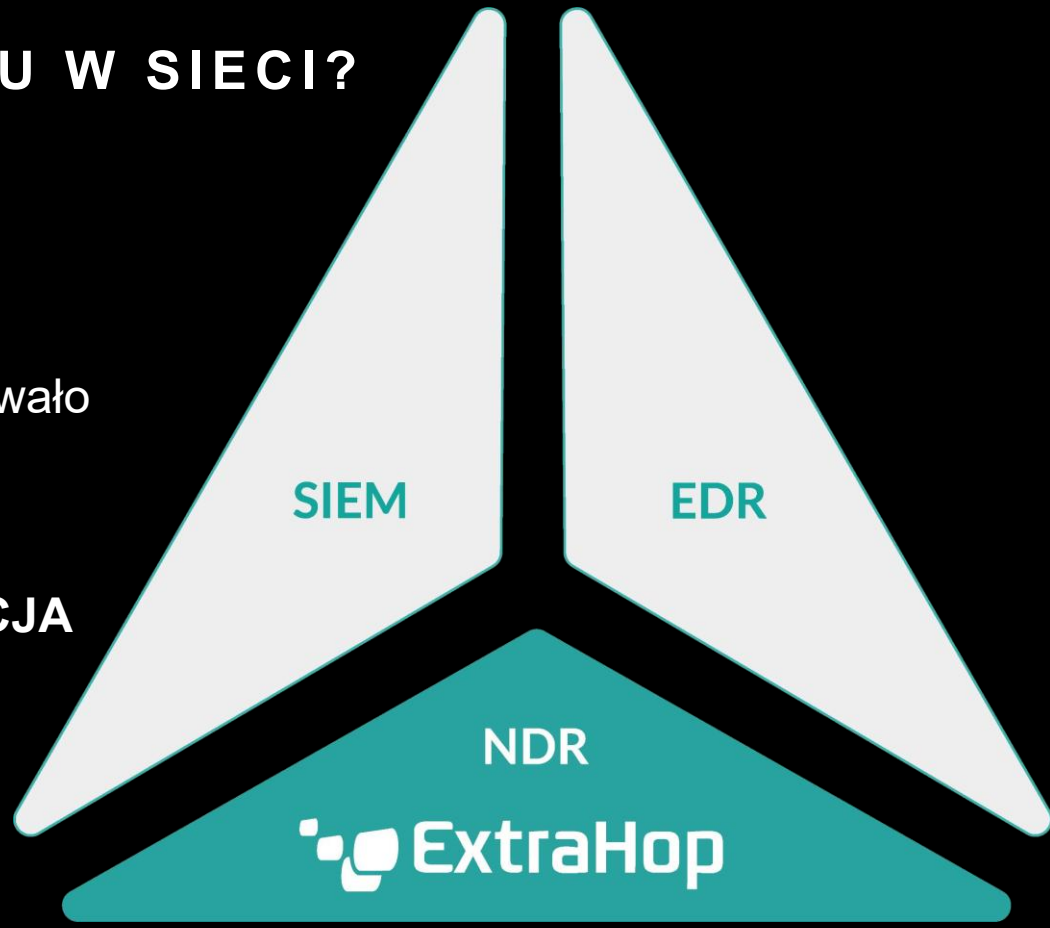
Nie odpowiadają na pytanie: winna **SIEĆ**, **SERWER** czy **APLIKACJA**

Nie widzą wzajemnych **ZALEŻNOŚCI** różnych komponentów wymieniających dane w sieci

Widzą efekty, ale nie **PRZYCZYNY** problemów w komunikacji komponentów

Brakuje im widoczności w środowiskach **HYBRYDOWYCH**

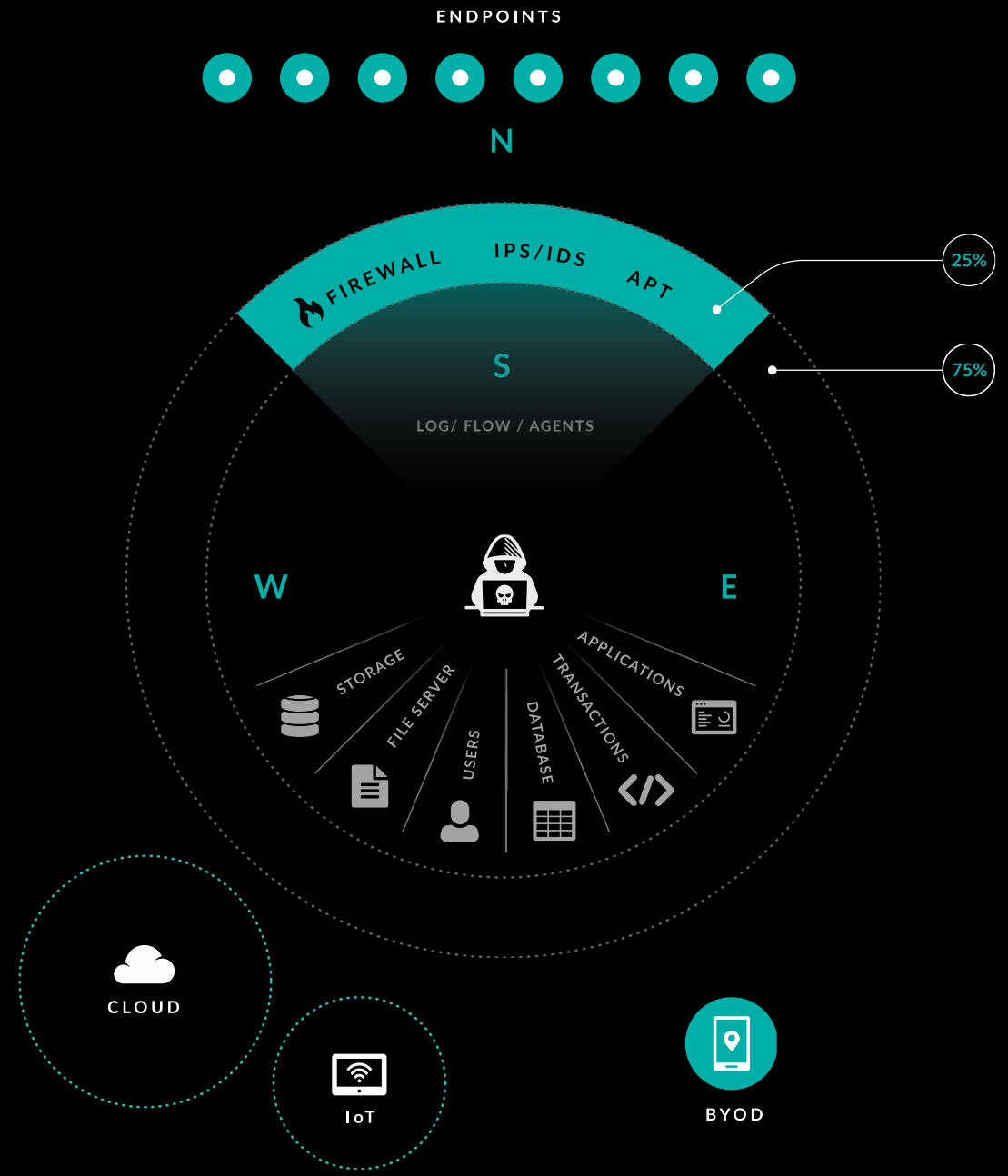
Wymagają **WIELU** elementów: agentów, logów, odpytywania SNMP etc...



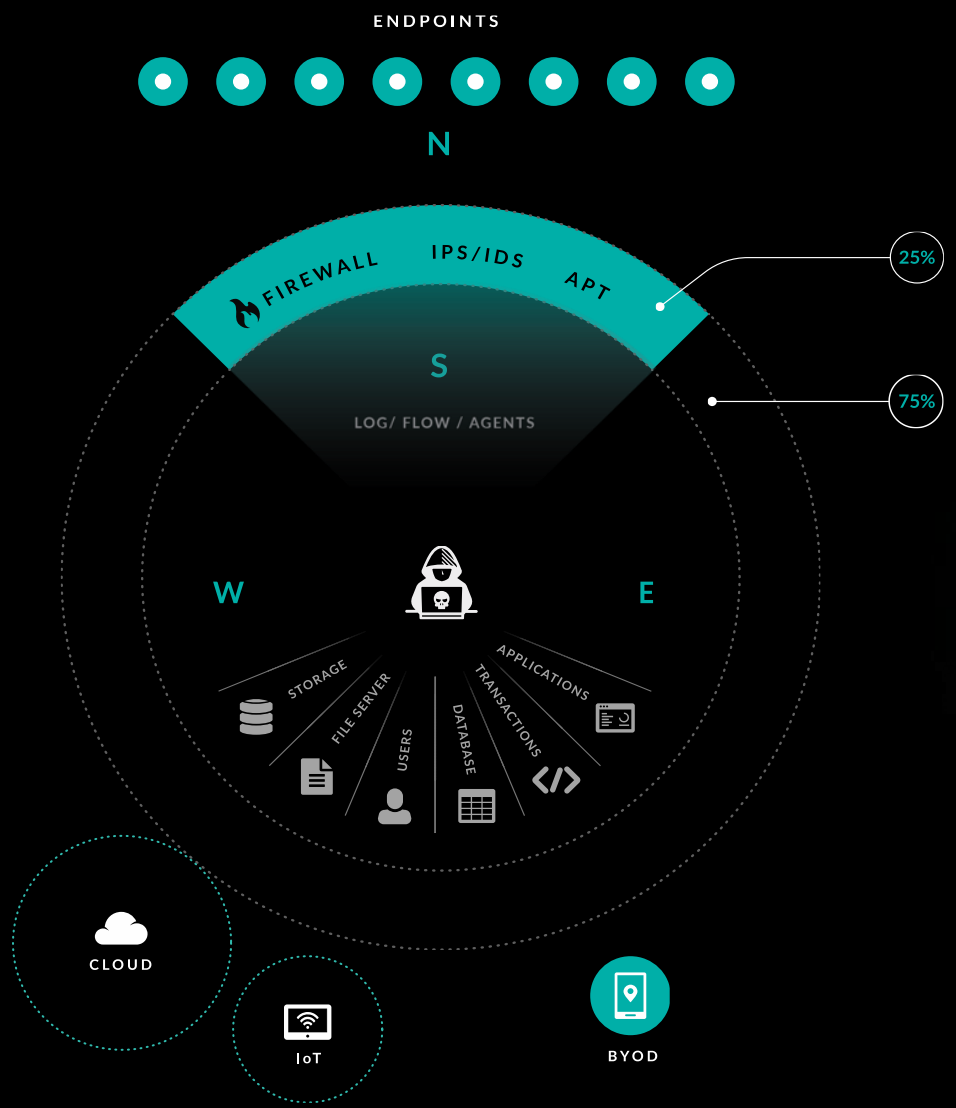
BRAK WIDZIALNOŚCI DZIAŁAŃ WSCHÓD-ZACHÓD

Gdzie mamy ciemne zakątki sieci?

- Brak możliwości instalacji agenta / EDR
- Ruch wschód-zachód którego nie analizujemy ze względu na skalę
- Serwisy od których nie otrzymamy logów
- Zaszyfrowana zawartość której nie zobaczymy
- Ograniczony monitoring bez kontekstu end-to-end
- Chmury, kontenery, mikroserwisy



DZIAŁANIA PO PRZEŁAMANIU ZABEZPIECZEŃ UKRYWAJĄ SIĘ W RUCHU WSCHÓD-ZACHÓD

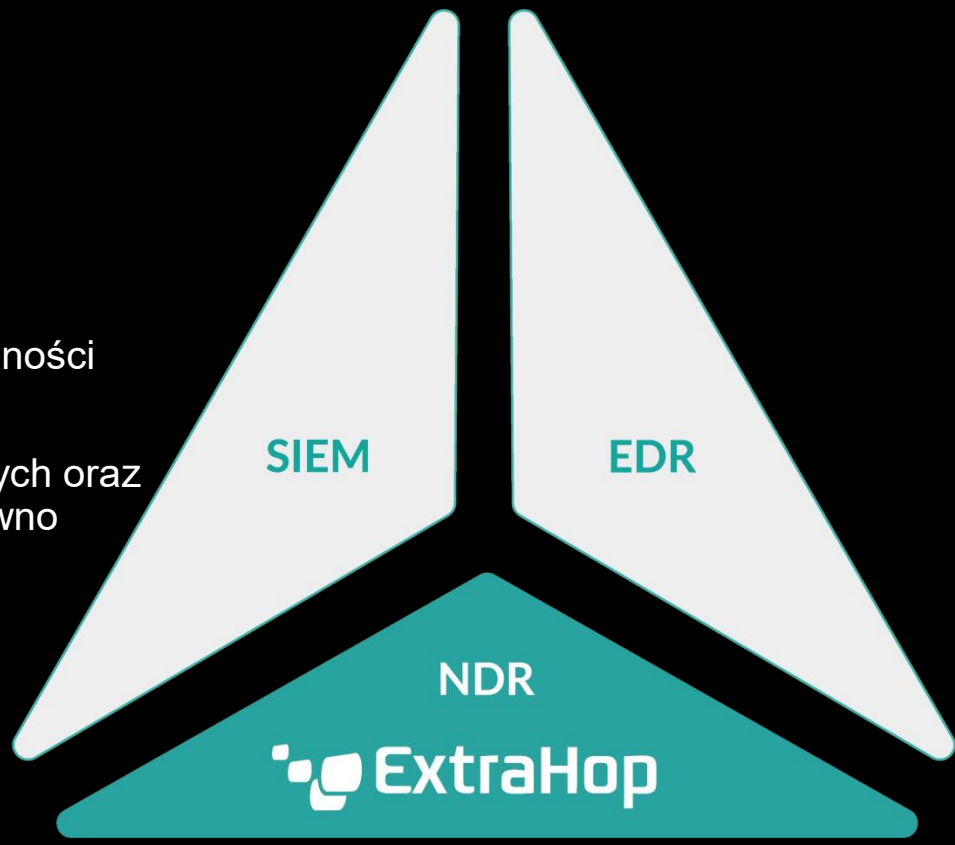


Recon	Network Privilege Escalation	Command and Control	Malicious Encryption
Unauthorized Access	Exploitation	Lateral Movement	Data Exfiltration

CO ROBIĆ? JAK ŻYĆ?

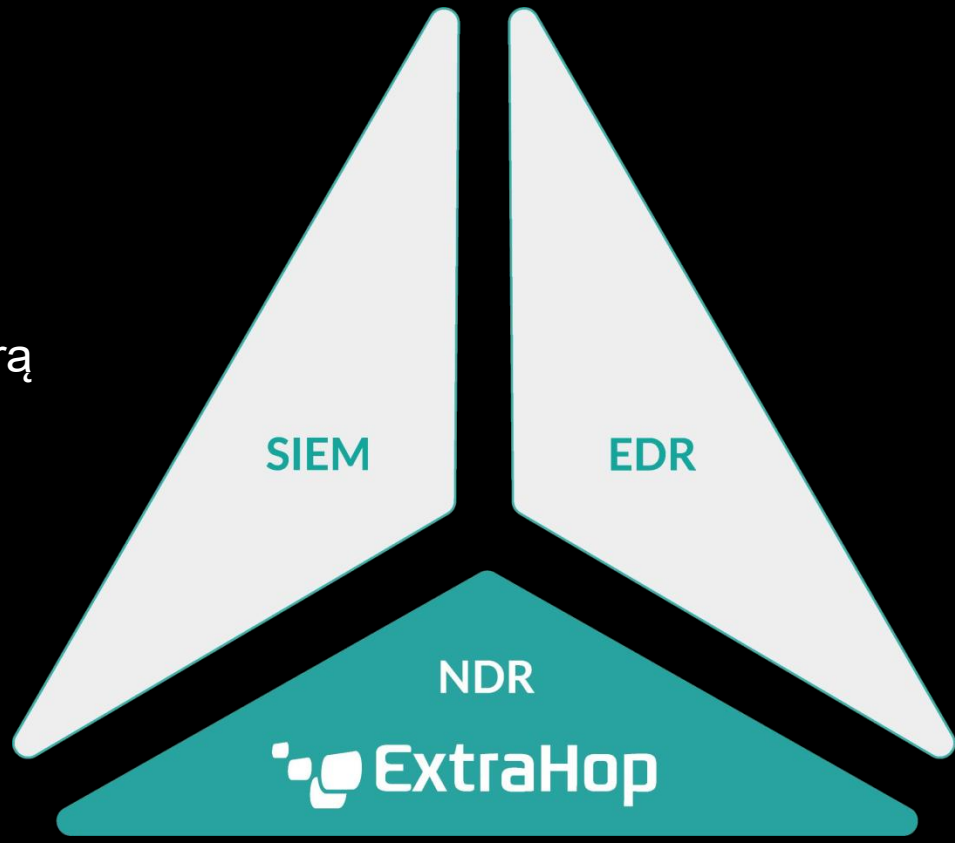
CZEGO POTRZEBUJEMY ABY ROZPOZNAWAĆ NOWOCZESNE ATAKI:

- Model matematyczny opisujący bieżący oraz historyczny stan sieci
- Deszyfracja aby wykrywać zagrożenia ukryte w zaszyfrowanym ruchu
- Liczne i szczegółowe metadane wydobyte również z zawartości pakietów w tym zaszyfrowanych i opisujących parametry: połączeń, bezpieczeństwa i wydajności
- Algorytmy Uczenia Maszynowego mające do dyspozycji olbrzymie ilości metadanych oraz historyczne dane przewidujące przyszły stan sieci i wykrywające anomalie – zarówno bezpieczeństwa jak i wydajnościowe
- Wysokiej jakości Threat Intelligence na bieżąco aktualizowany
- Identyfikacja użytkowników i śledzenie ich działań
- Możliwość zgrywania całego ruchu i szybkiego odnalezienia pakietów powiązanych z zagrożeniami do celów forensicowych (nice to have)



JAKICH EFEKTÓW SPODZIEWAMY SIĘ PO ANALIZIE SIECIOWEJ?

- Wykrywanie znanego i nieznanego złośliwego oprogramowania
- Wykrywanie zagrożeń od własnych użytkowników lub atakujących podszywających się pod nich
- Wystarczająco szczegółowe dane śledcze aby odnaleźć ścieżkę którą dostają się zagrożenia, a nie tylko obserwacja objawów
- Przejrzystość wszelkich działań w sieci zarówno z perspektywy bezpiecznika jak i administratora IT



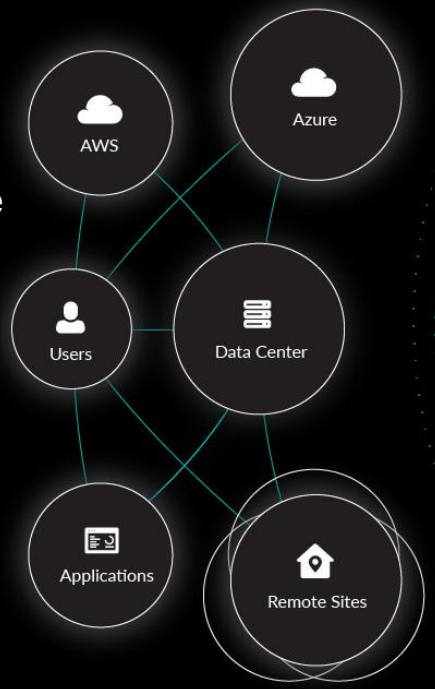
Czy jest to podejście efektywne?

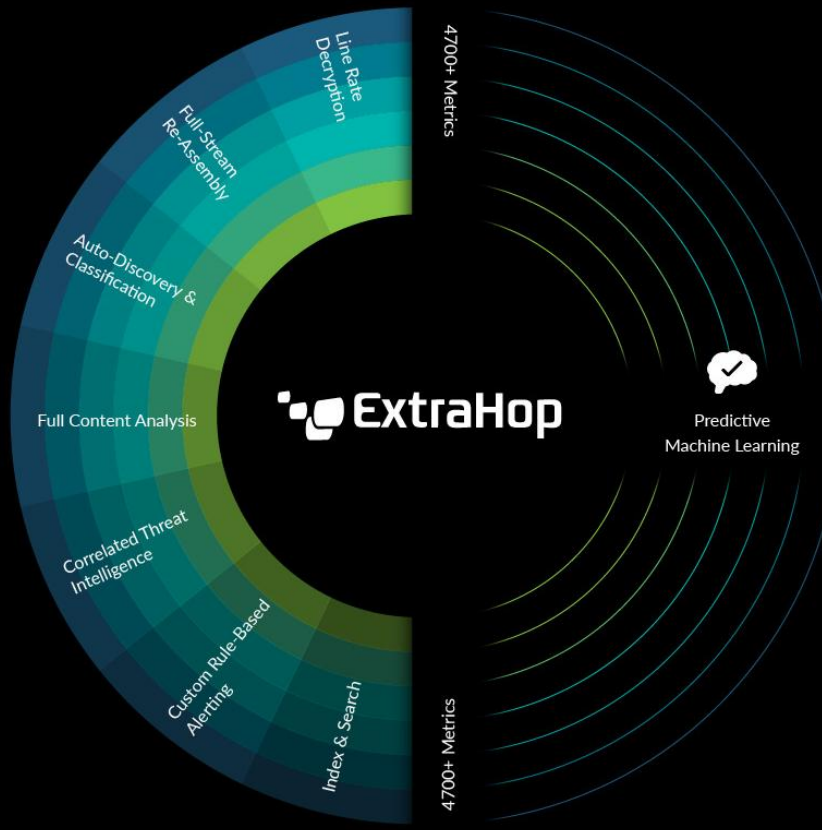
OCZYWIŚCIE!!!

Wszystkie nowoczesne ataki zostawiają ślady sieciowe, musimy mieć narzędzia aby je odnaleźć.

EXTRAHOP: ANALITYKA SIECI DLA ZŁOŻONYCH ORGANIZACJI

- Deszyfracja z prędkością łącza
- Sensory do 400Gbps
- 50+ protokołów L2-L7
- Rekonstrukcja sesji: Składanie pełnego strumienia danych
- Automatyczne wykrywanie i klasyfikacja zasobów
- Pełna analiza zawartości pakietów
- Skorelowane TI
- Alertowanie oparte na indywidualnych regułach
- Indeksowanie i wyszukiwanie
- 4700+ metryk!
- Uczenie maszynowe





Bezpieczeństwo

Precyzyjna detekcja

Hardening i compliance

Wykrywanie krytycznych zasobów

Śledzenie przebiegu ataku w linii czasu

Automatyczne akcje dzięki SOAR

Detekcja ataków w szyfrowanych protokołach MS: Kerberos, MSRPC, WinRM,SMBv3, LDAPs

Wydajność

Analityka aplikacji w czasie rzeczywistym

Wykrywanie anomalii dzięki ML

Wizualizacja zależności aplikacji

Widoczność i weryfikacja działania

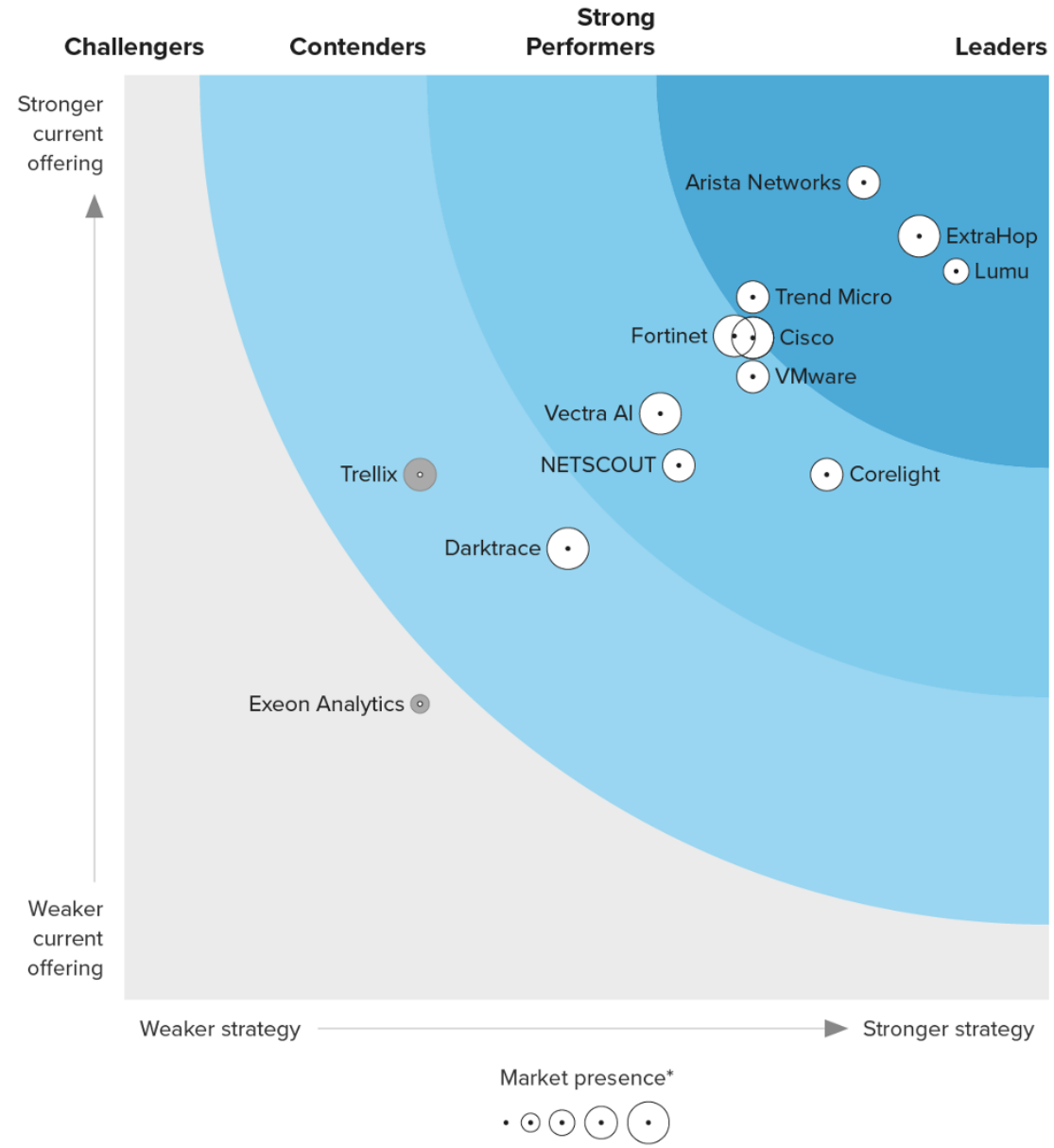
Wspomagane śledztwa

RAW NETWORK TRAFFIC → REAL-TIME ANALYTICS → BUSINESS RESULTS

THE FORRESTER WAVE™

Network Analysis And Visibility

Q2 2023

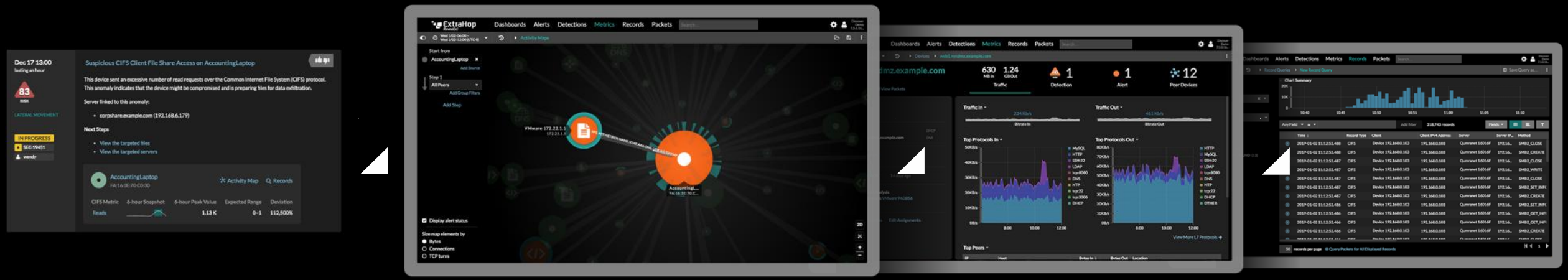



CHALLENGERS
LEADERS
Darktrace
Vectra AI
ExtraHop
Corelight
Stellar Cyber
NetWitness
Trend Micro
ThreatBook
Gatewatcher
Arista Networks
Trellix
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of April 2025
© Gartner, Inc

Gartner

EXTRAHOP-LOGICZNY CIĄG DZIAŁAŃ

Wykrycie i dochodzenie w ciągu sekund, automatyczna reakcja



DETEKCJA DOCHODZENIE TRANSAKCJE AKCJA!

Lista wszystkich integracji:
www.extrahop.com/partners/integrations

EXTRAHOP-Integracje Automatyczna Odpowiedź

Jira

Atlassian | Jira

Automates Jira ticket creation based on RevealX detections.

CHECK POINT

Check Point | Smart-1

Integrates RevealX network telemetry and detection data for automated response on gateways.

cisco Cisco ISE

Cisco | ISE

Automates containment, isolation, or communication abilities of devices in your network.

cisco Meraki

Cisco | Meraki

Send ExtraHop detections and metrics to Meraki. Enable detections to automatically quarantine devices.

CROWDSTRIKE

Crowdstrike | Falcon

Correlate network insights with endpoint details and threat intelligence.
Automatically quarantine devices.
Discover endpoints that do not yet have a CrowdStrike agent.

CROWDSTRIKE

Crowdstrike | Threat Intelligence

RevealX detections are enriched by CrowdStrike Falcon® Adversary Intelligence Premium threat intelligence.

FORTINET

Fortinet | FortiGate

Enables FortiGate to automatically quarantine, block, or unblock devices in a network.

Microsoft

Microsoft | Defender for Endpoint

Enables automated virus scanning or containment via Microsoft Defender for Endpoint.

CORTEX XSOAR BY PALO ALTO NETWORKS

Palo Alto Networks | Cortex XSOAR

Creates investigations, orchestrated responses, and more in Cortex XSOAR based on RevealX detections.

paloalto NETWORKS

Palo Alto Networks | Panorama

Quarantine compromised devices based on RevealX detection data.

SentinelOne

SentinelOne | Singularity Endpoint

Quarantine compromised devices based on RevealX detection data.

SOPHOS

Sophos | Firewall

Quarantine compromised devices based on RevealX detection data.

splunk> a cisco company

Splunk | SOAR

Intitate, automate, and orchestrate workflows with RevealX detection data and metrics.

vmware Carbon Black

VMware | Carbon Black EDR

Quarantine endpoints based on RevealX detections.

tines

Tines.io | SOAR

Allows Tines SOAR users to automate workflows using RevealX detection data.

Trellix

Trellix | Endpoint Security

Quarantine endpoints based on RevealX detections.

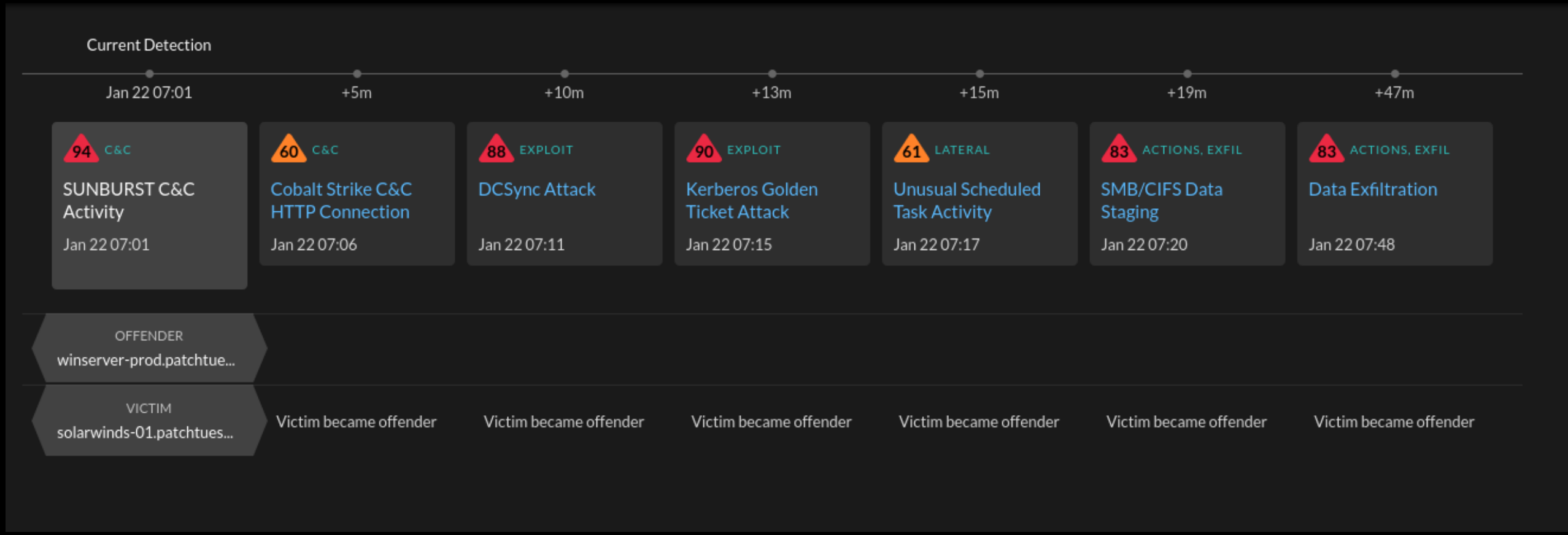
Symantec

Symantec | EDR

Enables Symantec to contain endpoints based on RevealX detection data.

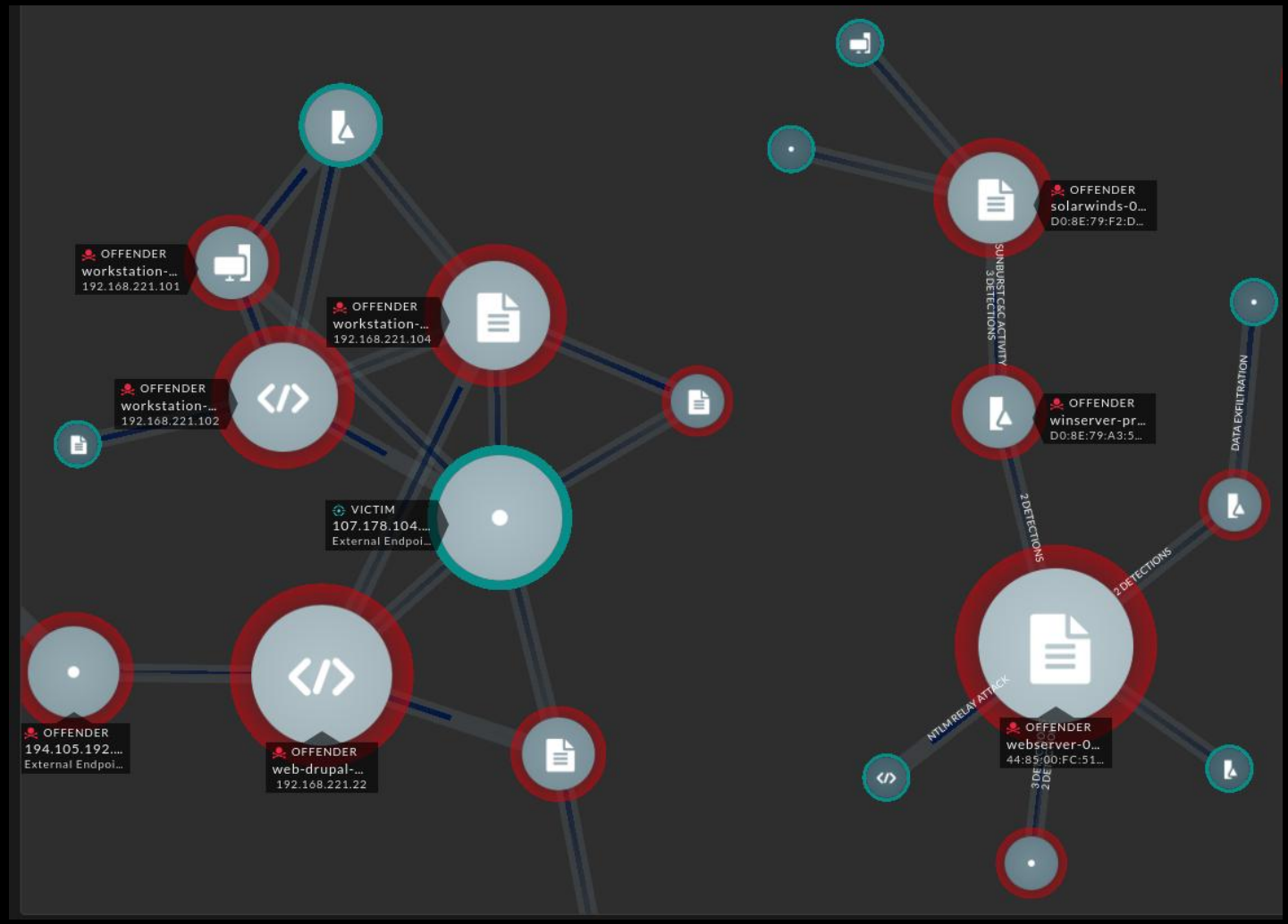
EXTRAHOP-LOGICZNY CIĄG DZIAŁAŃ

Wizualizacja rozwoju ataku i użytych technik w linii czasu



EXTRAHOP-LOGICZNY CIĄG DZIAŁAŃ

Wizualizacja rozwoju ataku i użytych technik w postaci mapy

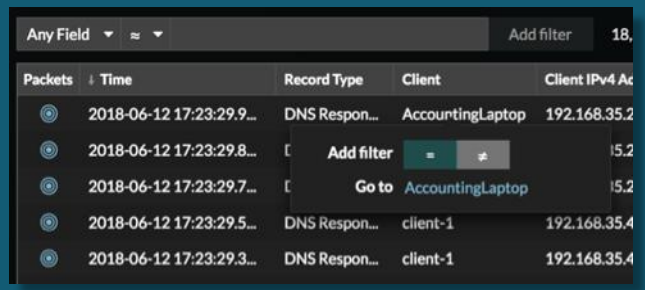


REACTIVE + PROACTIVE = “CIRCLE OF LIFE”

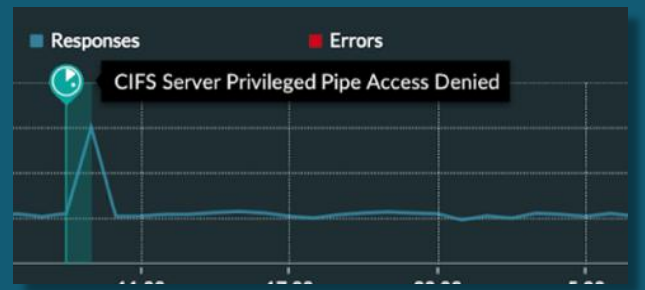
DETEKCJA ZAGROŻEŃ

Detekcja włamań i Odpowiedź
Wykrycie late-stage oraz wrogiej aktywności wschód-zachód

Detekcja zagrożeń typu Insider
Detekcja, powstrzymanie i dokumentacja złego czy złośliwego zachowania



Obrona przed Ransomware
Powstrzymanie i minimalizacja aktywnych ataków, odzyskanie danych

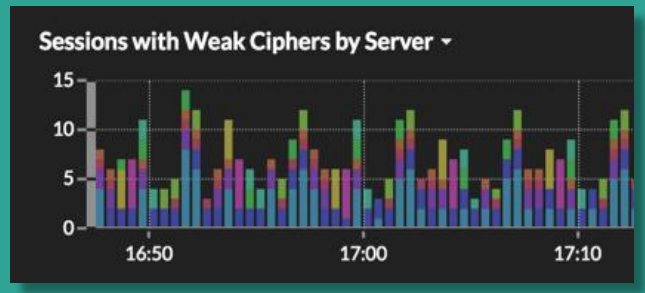


POPRAWA ODPORNOŚCI

Produktywność SOC
Prioretyzowanie detekcji, redukcja False Positives

Red Team/Ustalenia Audytowe
Odnalezienie lub potwierdzenie zastrzeżeń i podatności

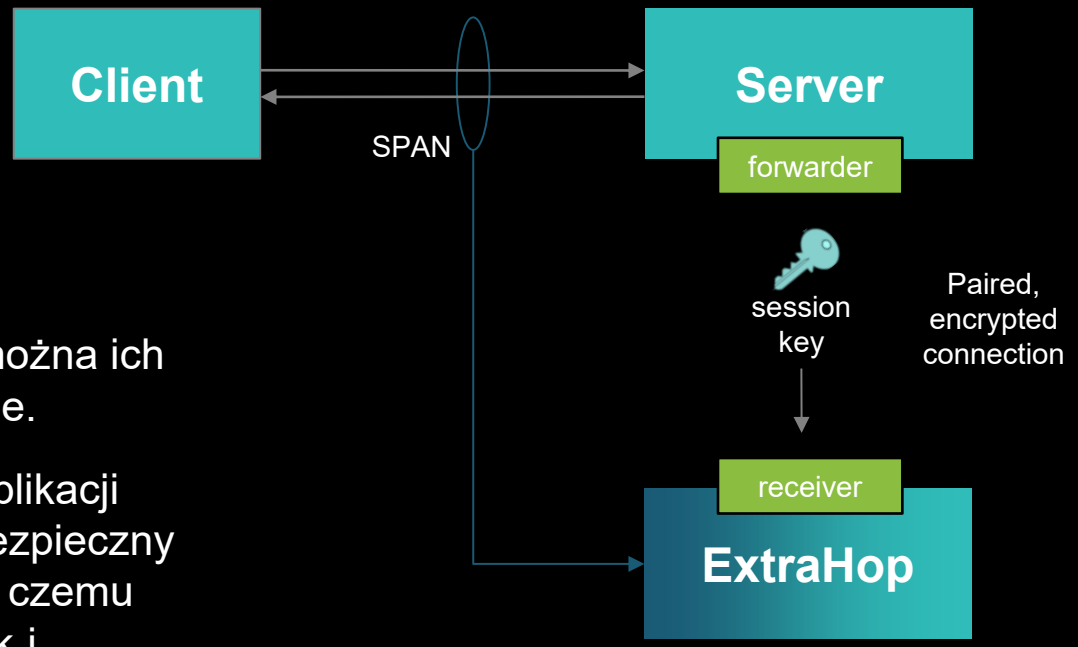
Zmniejszenie Powierzchni Ataku
Poprawienie higieny poprzez usuwanie zbędnych asetów I serwisów



EXTRAHOP: A CO Z RUCHEM SZYFROWANYM?

WSPÓŁDZIELENIE POUFNOŚCI

- Utrzymuje integralność kompleksowego szyfrowania
- Rozwiązanie Out-of-band wykorzystujące port mirroring, SPAN lub tap sieciowy
- Analiza rzeczywistych pakietów
- Dostęp do pakietów na zasadzie need-to-know



Dzięki Perfect Forward Secrecy klucze sesyjne są ulotne i nie można ich uzyskać z klucza prywatnego, więc dane sieciowe są bezpieczne.

Unikalną funkcją Extrahop jest deszyfracja w locie PFS dzięki aplikacji forwardera zainstalowanej na chronionych serwerach który w bezpieczny sposób przesyła do Extrahop kopię każdego klucza sesji, dzięki czemu możliwa jest deszyfracja ruchu i zdobycie szczegółowych metryk i metadanych tego ruchu.

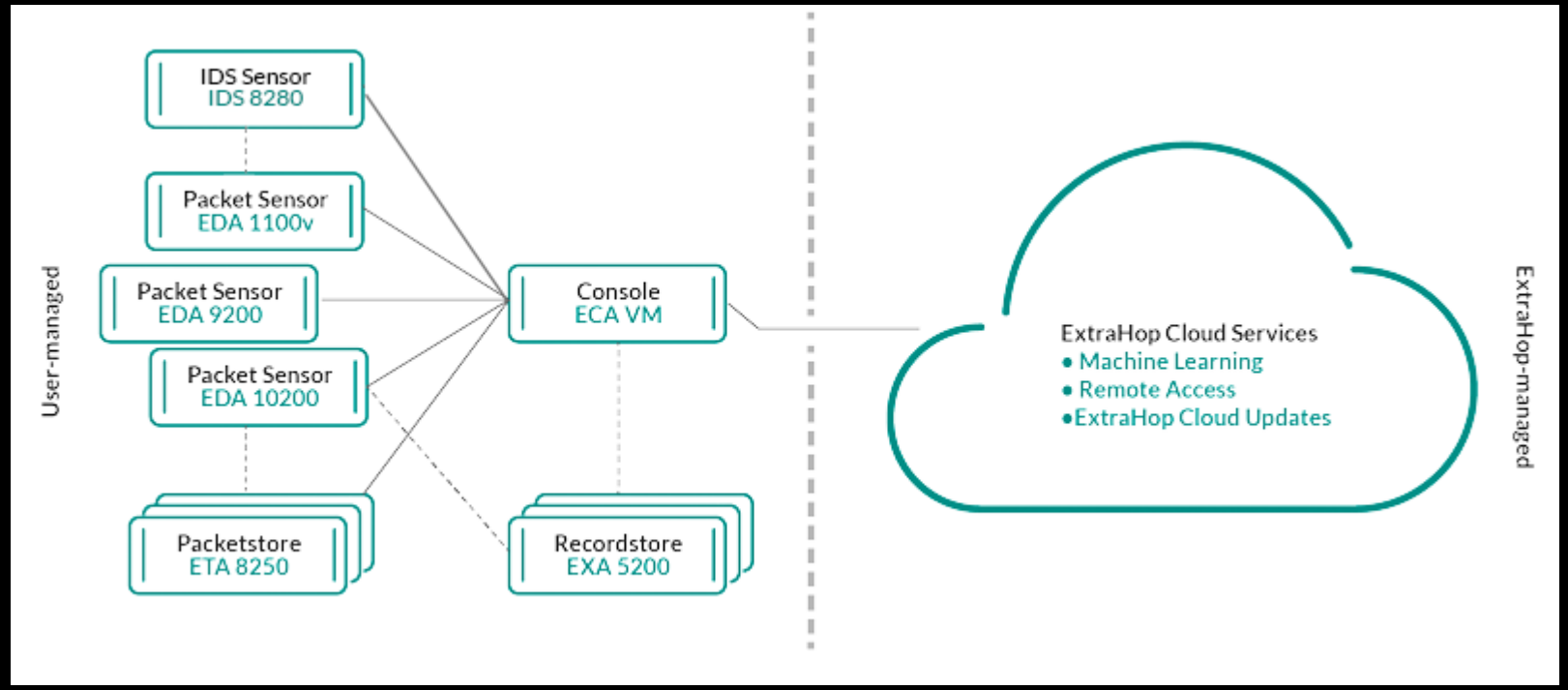
Extrahop działa Out-of-band więc nie musi z powrotem szyfrować danych. Możliwe jest zgranie kopii pakietów wraz z kluczami aby możliwa była późniejsza analiza.

JAK WYGLĄDA ARCHITEKTURA

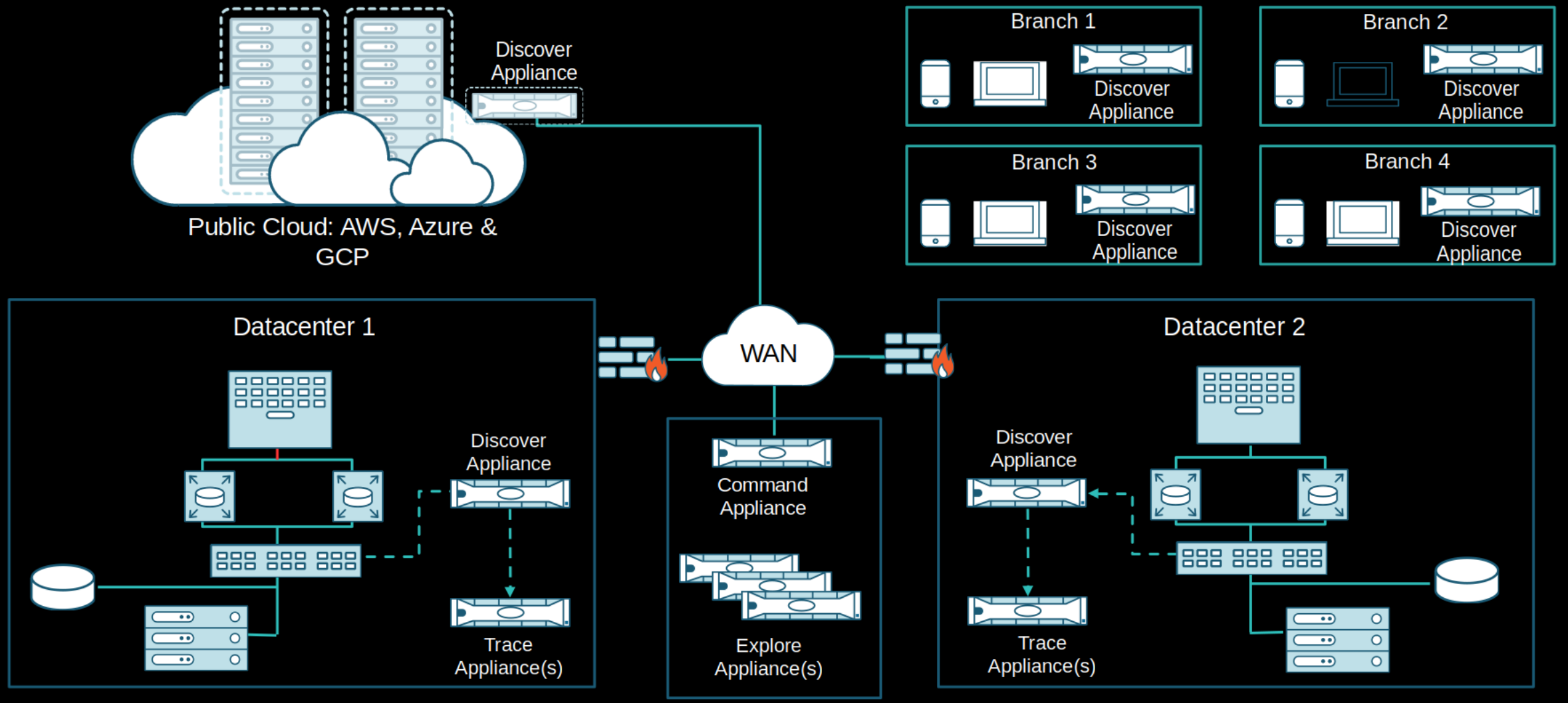
- Moduły:
  - NPM - Network Performance Monitoring
  - NDR - Network Detection and Response
  - Packet Forensics – full packet capture (w połączeniu z NDR&NPM)
  - Intrusion Detection Systems (dla NDR)

PLATFORMY I ARCHITEKTURA

- Rozwiązania:
  - **Reveal(x) Enterprise**
  - Reveal(x) Enterprise rozwiązanie typu self-managed i zawiera:
    - Sensory,
    - Konsolę,
    - Packetstores,
    - Recordstores, oraz
    - Dostęp do ExtraHop Cloud Services.



Reveal(x) Enterprise High-Level Architecture

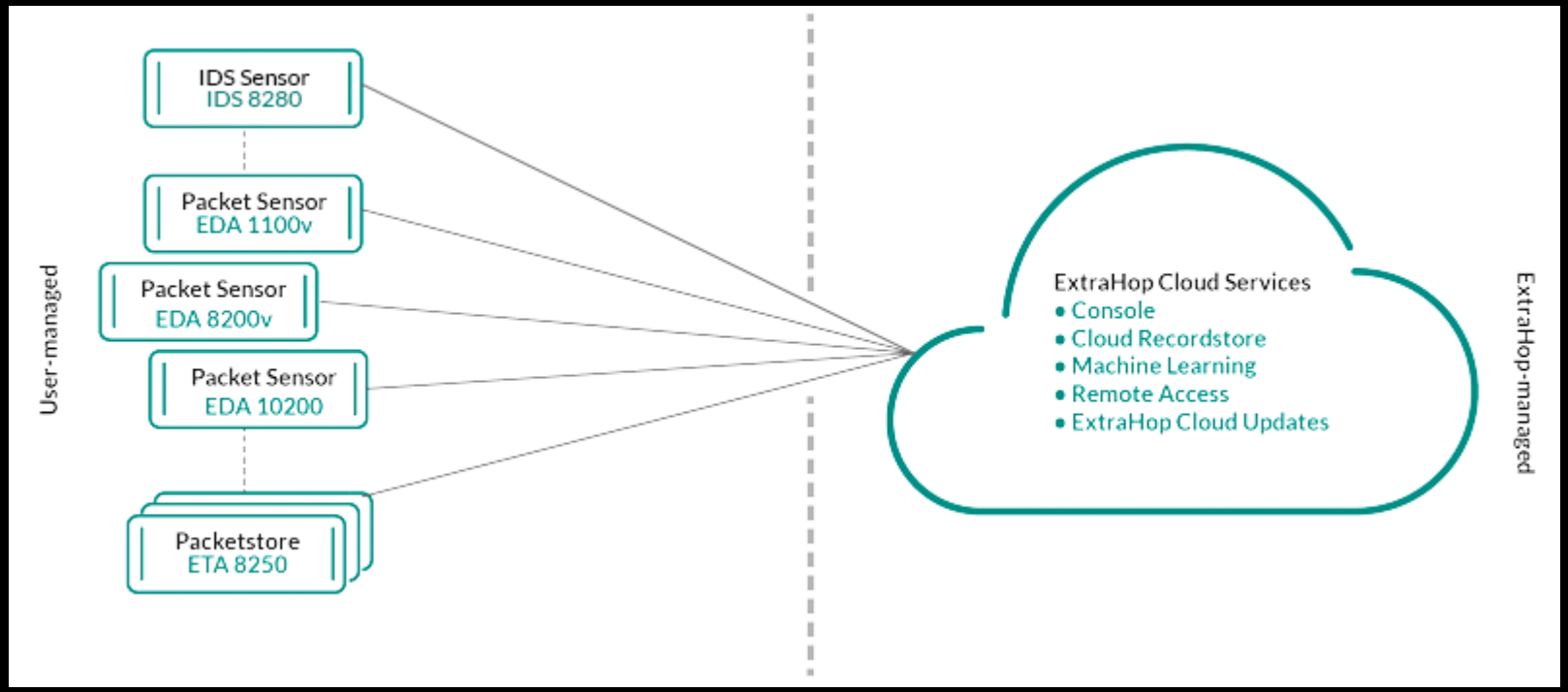


ExtraHop

PLATFORMY I ARCHITEKTURA

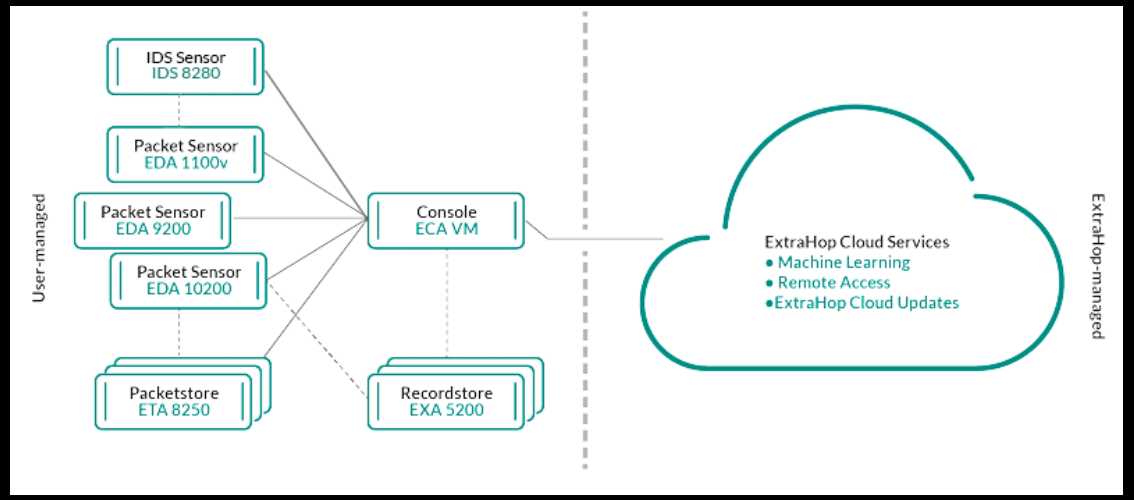
- Rozwiązania:
  - **Reveal(x) 360**
  - Reveal(x) 360 jest rozwiązaniem software-as-a-service (SaaS) I zawiera:
    - Sensory
    - Packetstores

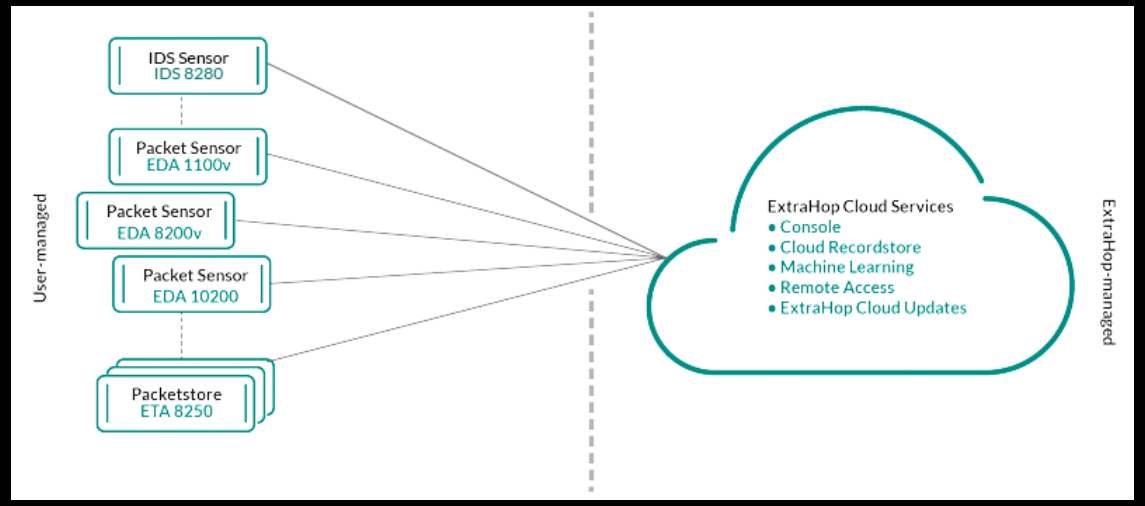
    a także chmurowe:
    - Cloud-based recordstore,
    - Konsola,
    - Dostęp do ExtraHop Cloud Services.



PLATFORMY I ARCHITEKTURA

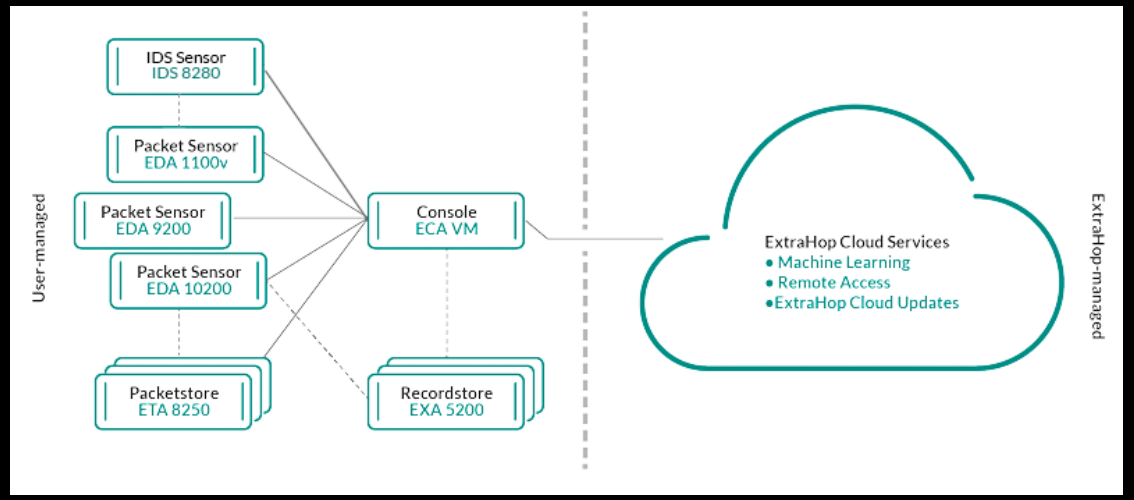
- Szczegóły komponentów
  - Packet sensors
    Odbiera ruch i analizuje do metryk
  - IDS sensors
    integruje się z packet sensors by wykrywać za pomocą sygnatur IDS
  - Flow sensors
    dostępne tylko dla Reveal(x) 360 I zbierają VPC flow logs aby widzieć ruch zarządzany przez AWS SaaS services
  - Recordstores
    integruje się z sensorami i konsolą by przechowywać transakcje oraz połączenia które mogą być wyszukiwane przez system Extrahop
  - Packetstores
    integrują się z sensorami i konsolą by dostarczać zapisywanie pakietów w trybie ciągłym do celów śledczych
  - Consoles
    Centrum sterowania I analizy poprzez przeglądarkę

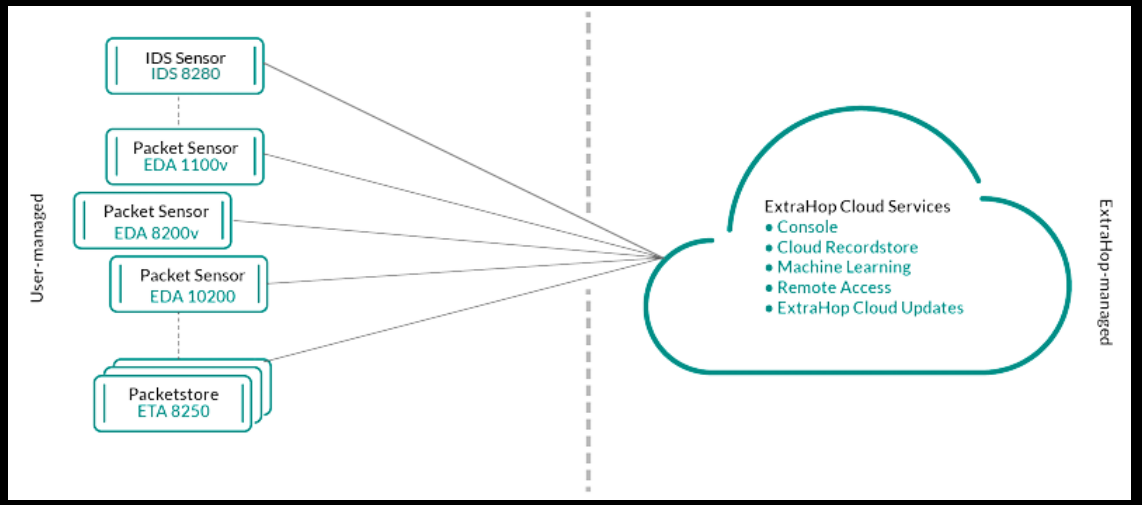




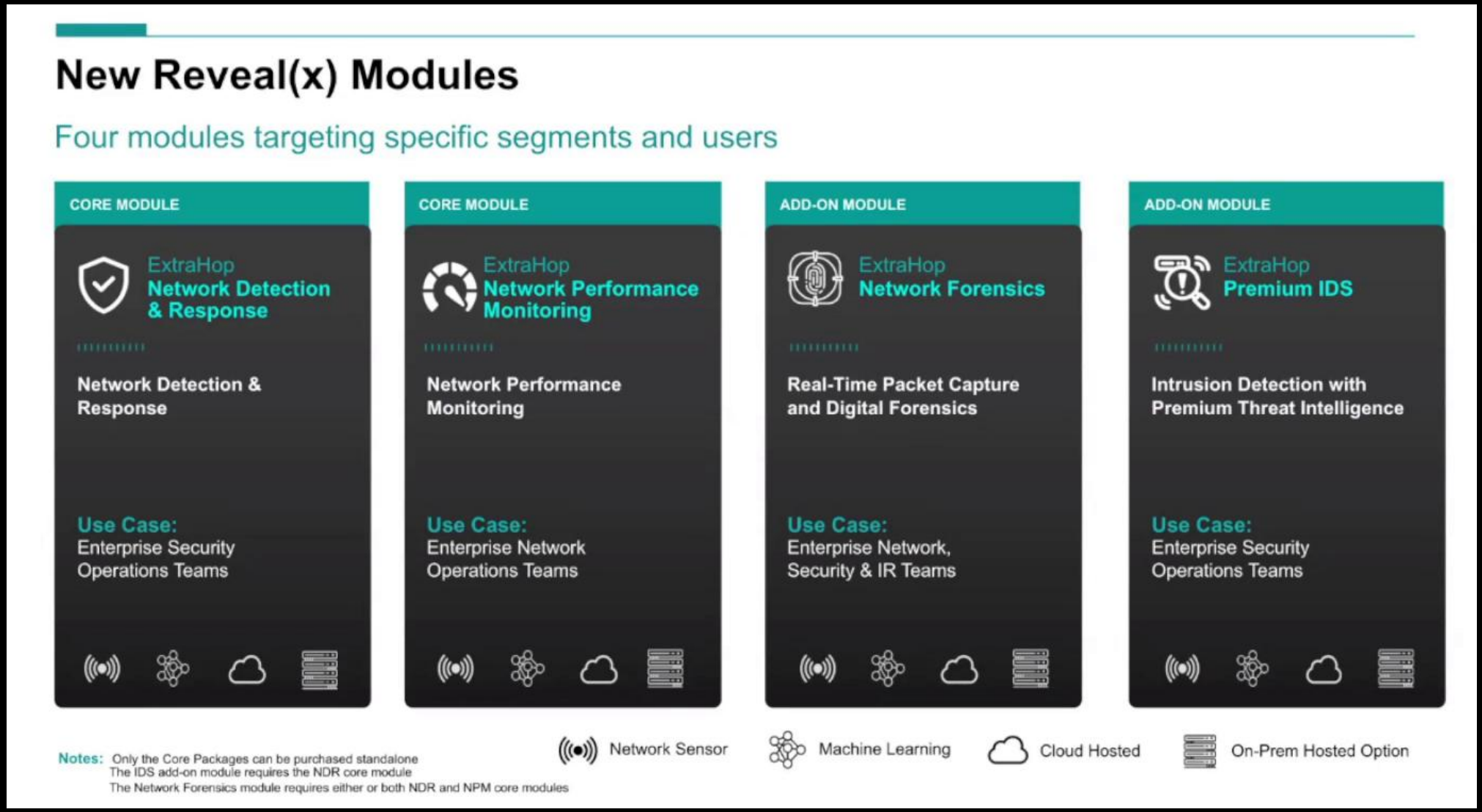
PLATFORMY I ARCHITEKTURA

- ExtraHop Cloud Services
  - ExtraHop Cloud Services automatycznie uaktualniają sensory o nowe detekcje i o krytycznych zagrożeniach
- Typy Sensorów:
- Kopia ruchu
  pasywnie obserwuje nieustrukturyzowane pakiety przez mirror port, SPAM port lub TAP sieciowy i przechowuje dane na lokalnym dysku. Pakiety poddawane są przetwarzaniu strumieniowemu w czasie rzeczywistym, które przekształca je w ustrukturyzowane dane sieciowe
- Dane o przepływach
  Flow sensors są dostępne dla Reveal(x) 360 i zapewniają ciągłą widoczność sieci w oparciu o Flow logi VPC, aby zabezpieczyć środowiska AWS. Flow logiVPC umożliwiają przechwytywanie informacji o ruchu IP przychodzącym i wychodzącym z interfejsów sieciowych VPC i są rejestrowane jako dzienniki Flow log, czyli log zdarzeń składające się z pól opisujących przepływy sieciowe





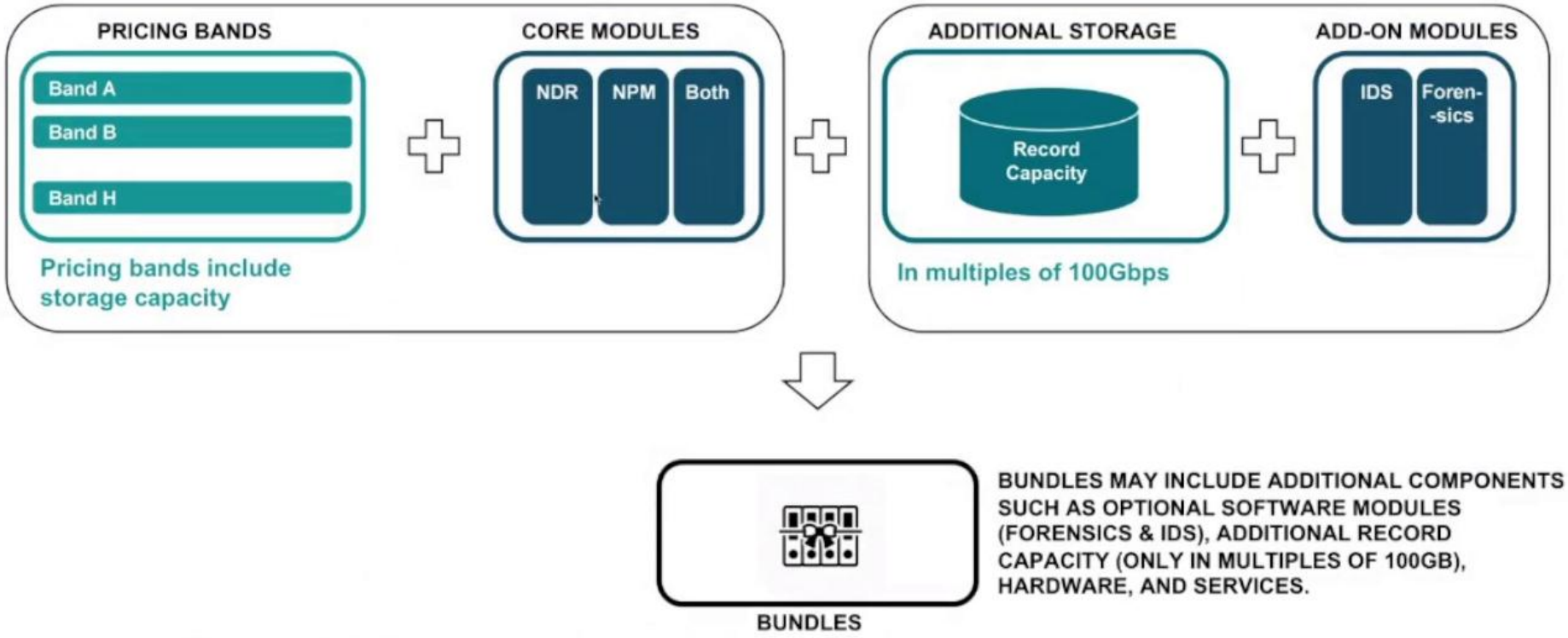
LICENCJONOWANIE



LICENCJONOWANIE

Pricebook Implementation: SKU Framework

The initial SKU creation framework will rely on the foundational elements of bands, core modules, and capacity to form bundles



ExtraHop

DZIĘKUJEMY

ZAPRASZAMY DO KONTAKTU