EXTRAHOP

Company & Product Overview

AGENDA

ExtraHop은 무엇인가

시장 동향 및 TAM (Total Addressable Market)

업계에서의 인정

왜 NDR은 중요한가

왜 ExtraHop 인가

기술 파트너 – Crowdstrike

EXTRAHOP

사이버 보안을 위한 네트워크 Intelligence 선두주자 보안 팀이 첨단 사이버 위협을 신속하게 감지하고 대응하여 기업을 방어할 수 있도록 합니다.

높은 성장
47%의 ARR 성장, 650명 이상의 직원, 그리고 글로벌 진출.

신뢰성
28,000대의 장비를 관리하는 1,000명 이상의 글로벌 고객

혁신
47개의 AI 및 ML 특허

네트워크 분석 전문가: 확장성, 복호화, Protocol fluency

LEADING
매달 1,500개 이상의 고위험 위협 식별

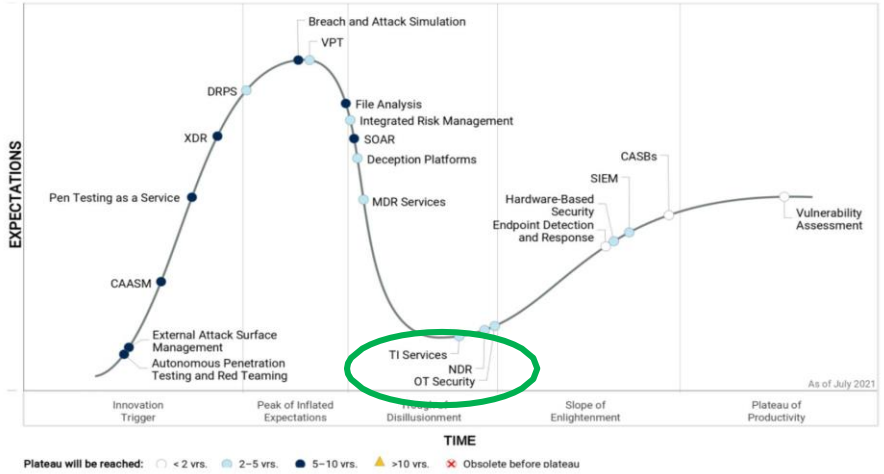
네트워크 가시성 분야의 Gatner 리더

사이버 보안 전문 지식을 갖춘 업계 최고의 금융 회사들의 지원을 받고 있습니다.

CROSSPOINT CAPITAL BainCapital

트렌드

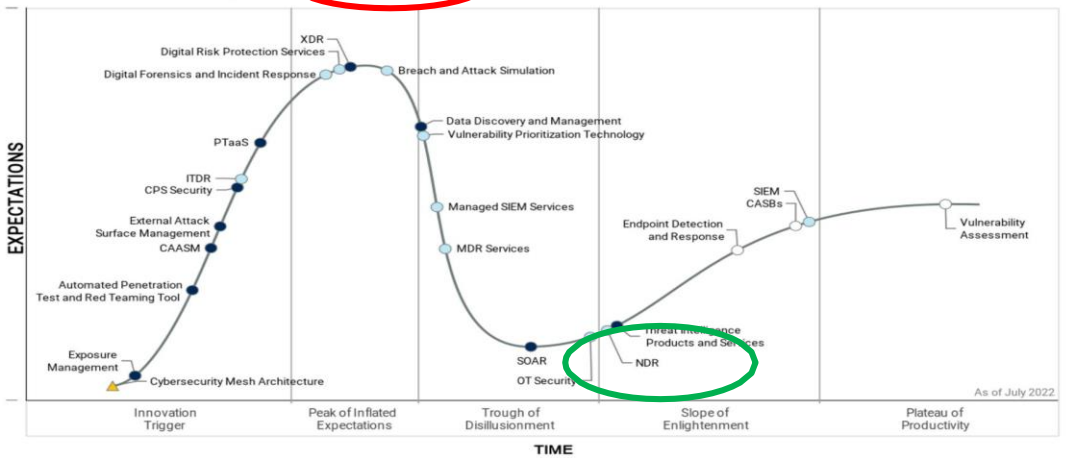
Hype Cycle for Security Operations, 2021



Source: Gartner (July 2021)

7475

Hype Cycle for Security Operations, 2022

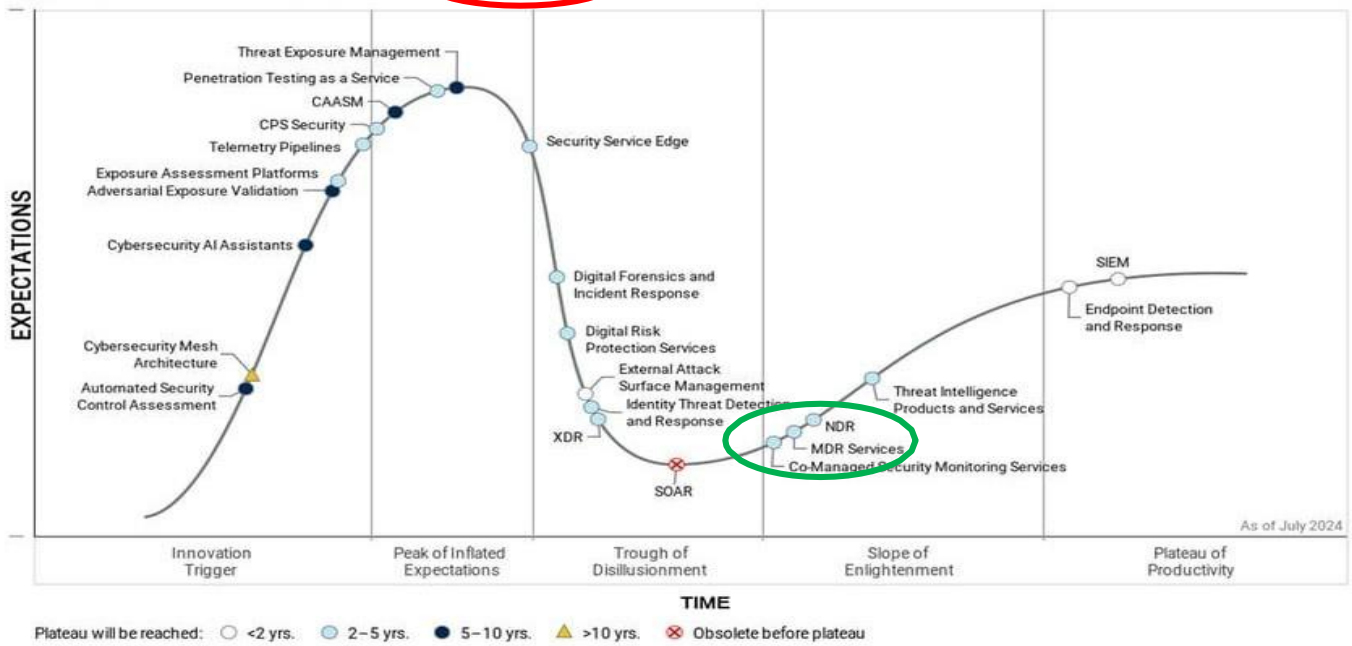


Gartner

Hype Cycle for Security Operations, 2023

Gartner

Hype Cycle for Security Operations, 2024



Gartner

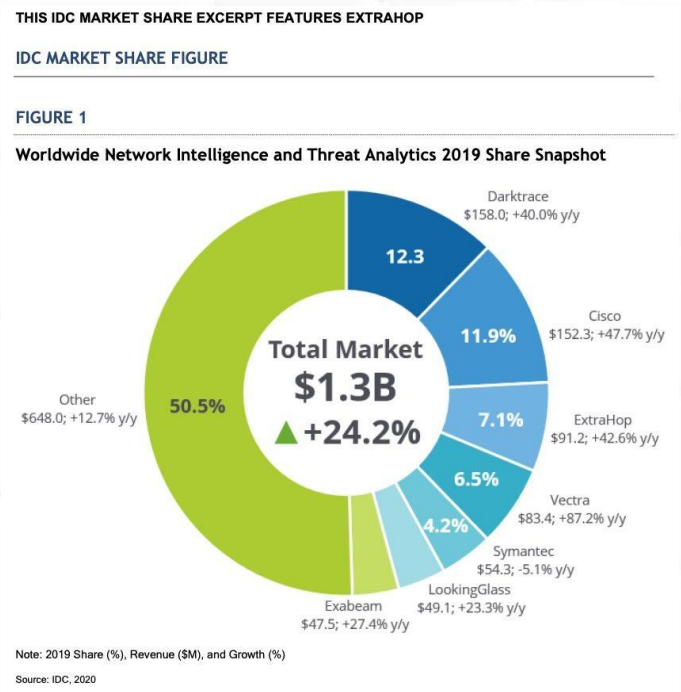
APJ TAM

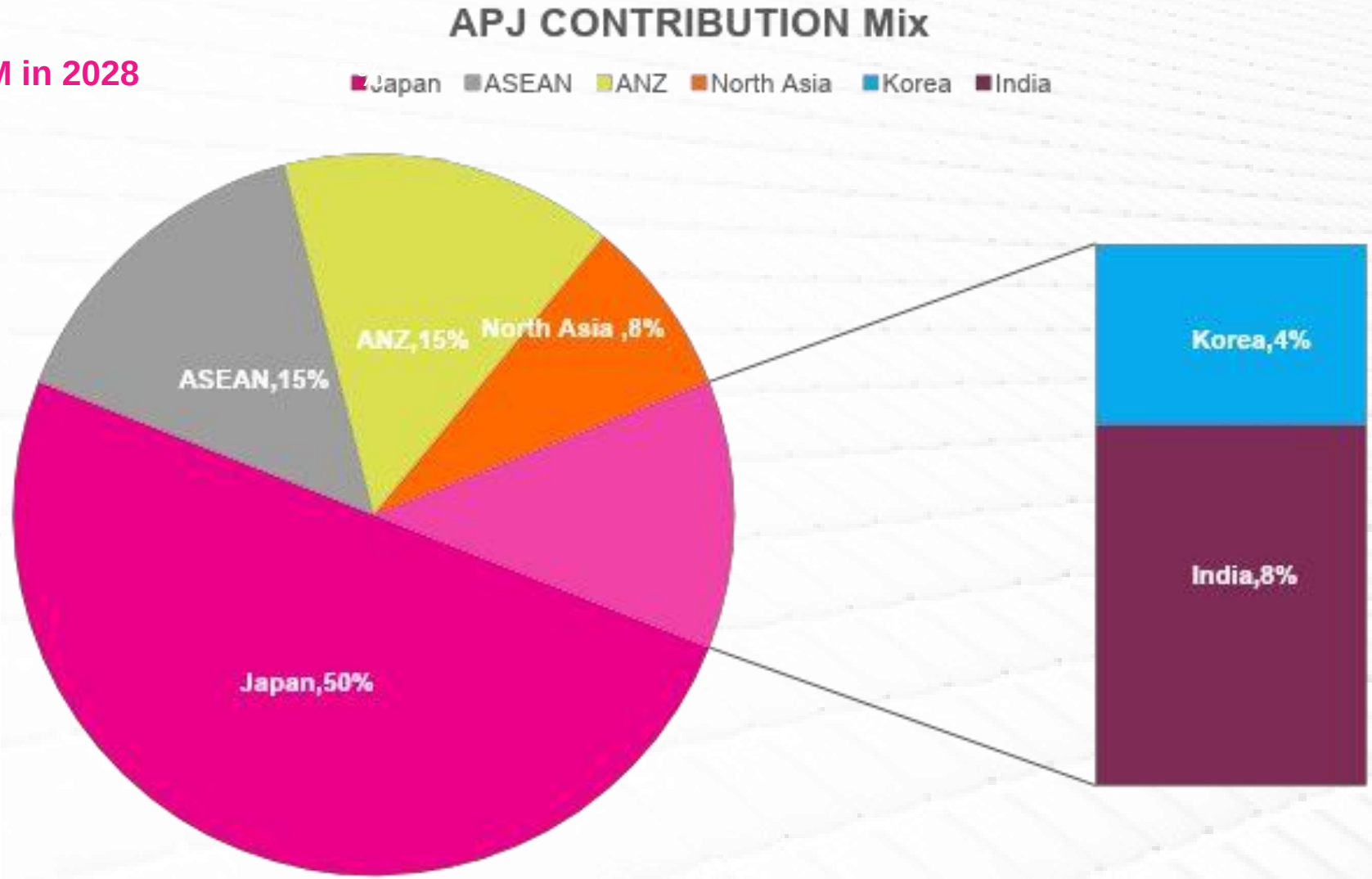
전망:

2025 APJ NDR 매출 = 512M >> 863M in 2028

CAGR = 13.7%

- 동남아 = 77M
- ANZ = 77M
- 북아시아 = 41M
- 한국 = 20M
- 일본 = 256M
- Others = 61M





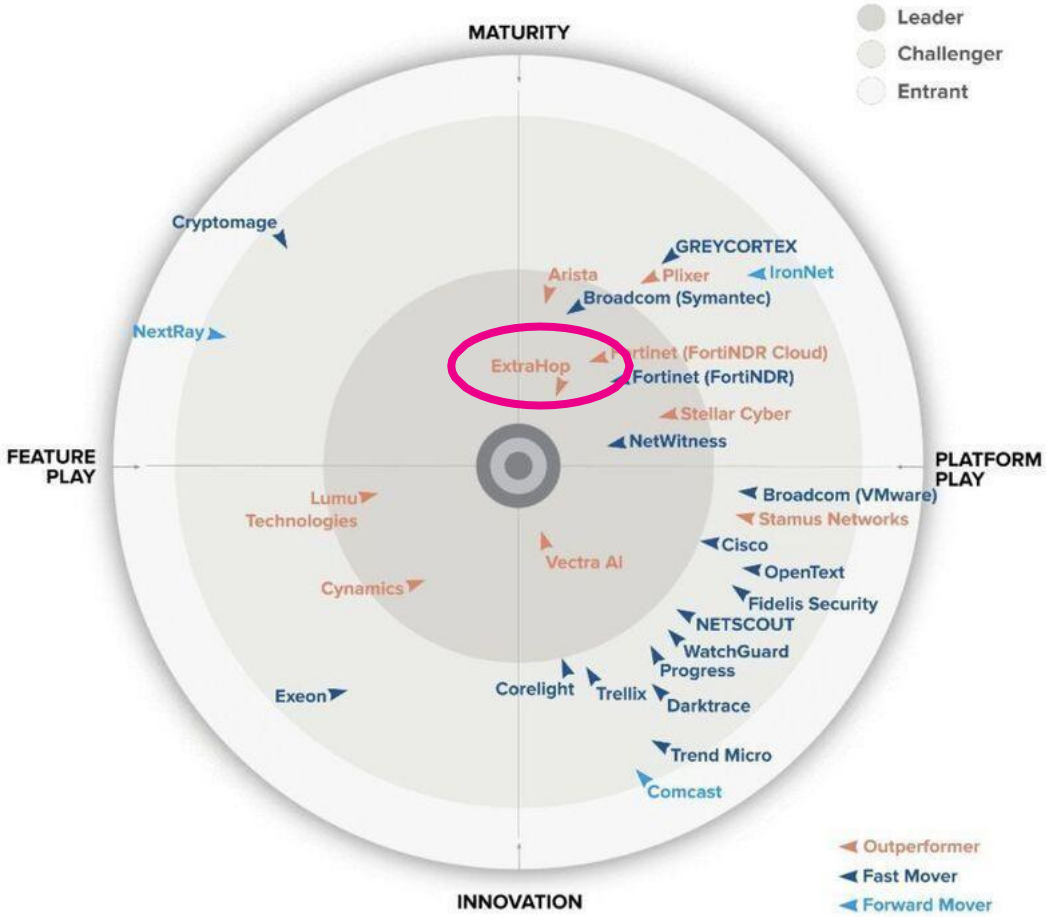
EXTRAHOP

30개 이상의 보안 업계에서 인정!!!

FORRESTER® Network Analysis & Visibility

Source: Forrester WAVE - Network Analysis and Visibility - June, 2023

GIGAOM RADAR — NETWORK DETECTION & RESPONSE (NDR)

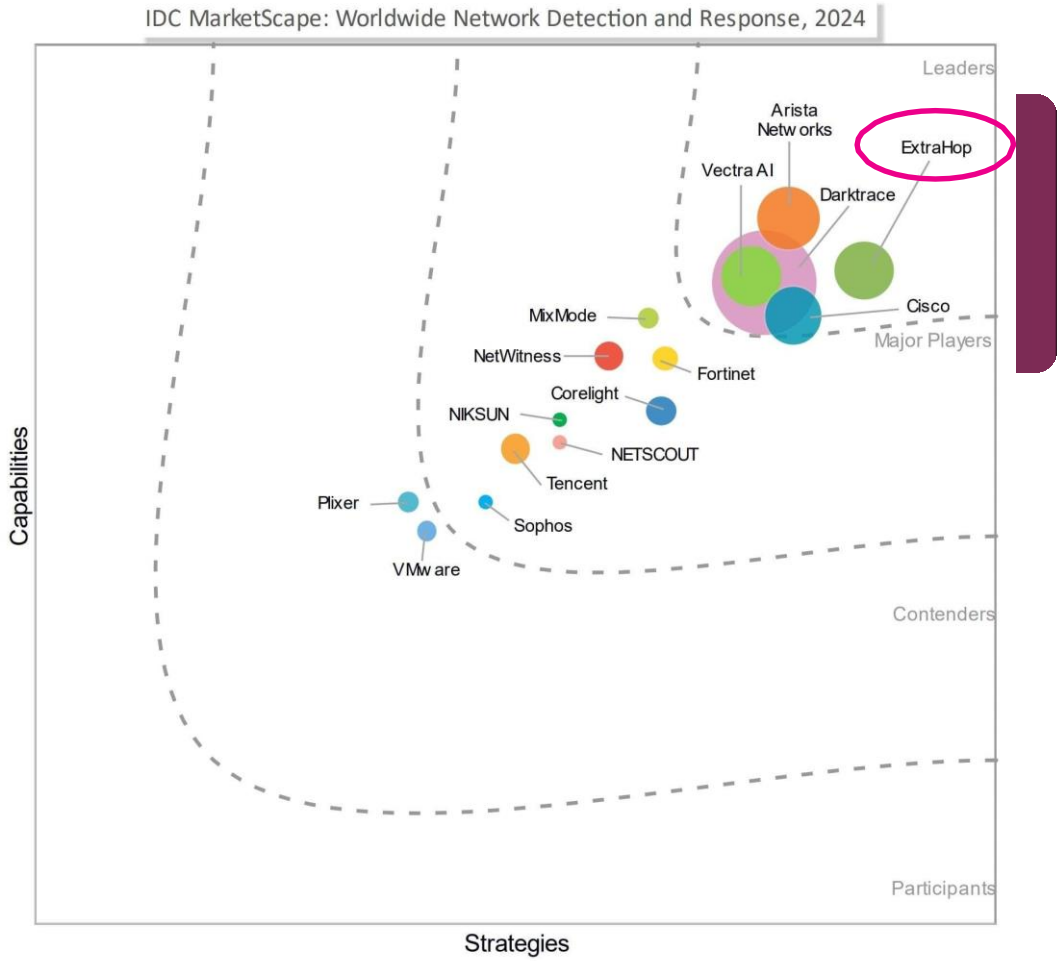


EXTRAHOP

ExtraHop IDC Market에서 리더로 선정

전 세계 네트워크 탐지 및 대응, 2024

"ExtraHop을 NDR에서 독특하게 만드는 점은 애플리케이션, 네트워크, 그리고 애플리케이션 성능(보안 문제나 병목 현상이 될 수 있음)과 같은 여러 관점에서 네트워크를 모니터링하며, 향상된 위험 프로파일을 제공합니다."



LEADER

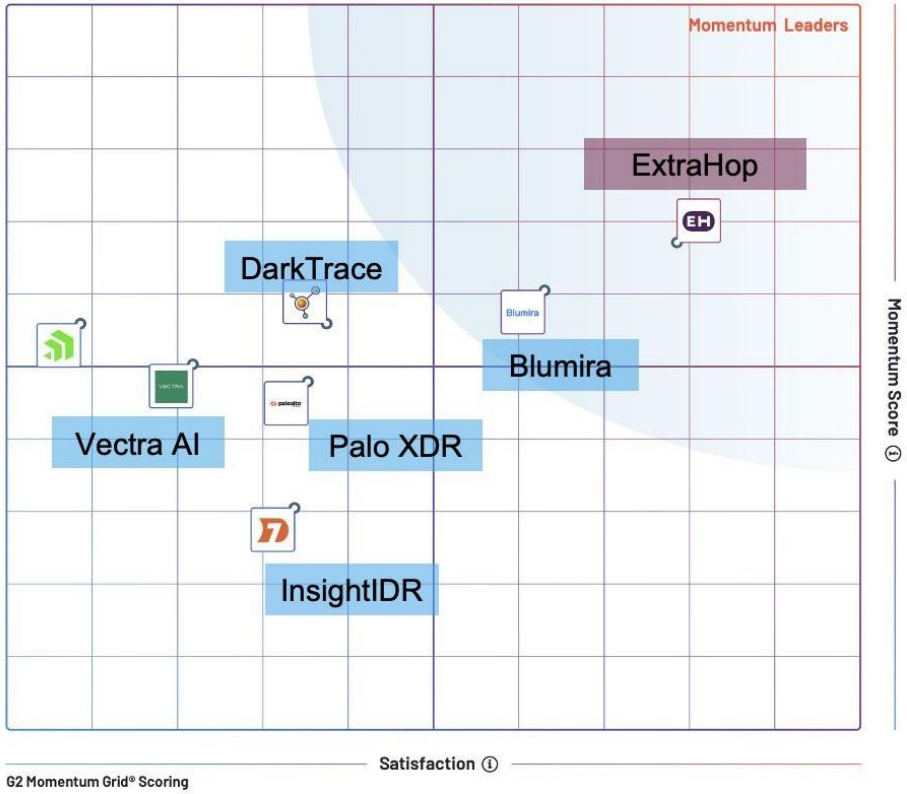
- 업계에서 가장 강력한 전략을 가진 것으로 인정 받았습니다.
- 트래픽 추적, 비정상적인 포트 활동, 네트워크 프로토콜을 기반으로 하는 이상 징후와 같은 NDR 사용 사례에 강점.
- 네트워크 가시성, 사용자 행동 분석, 작은 단위의 이벤트 분석 등 보안을 넘어서는 네트워크의 전체적인 관점의 가시성을 사용자가 경험할 수 있습니다.
- 침해 지표를 찾을 수 있는 능력 : 플랫폼에서 실시간 분석을 실시하고 온프레미스, 하이브리드, 멀티클라우드, IoT 환경을 위한 통합 제어가 가능합니다.

ExtraHop

30개 이상의 보안 업계 상과 표창!!!

트렌드 네트워크 탐지 및 응답(NDR) 소프트웨어

네트워크 탐지 및 응답(NDR)의 모멘텀 점수는 아래에 나와 있습니다. 모멘텀 그리드는 각 제품의 모멘텀 점수를 세로축으로, 제품의 만족도 점수를 가로축으로 강조 표시합니다. 이 점수는 G2의 만족도와 모멘텀 알고리즘을 기반으로 합니다. 모멘텀 그리드 점수가 상위 25%인 제품은 아래 음영 처리된 영역에 표시됩니다.



PRODUCTS

See everything. Risk nothing.

Performance

Network Performance Monitoring (NPM)

RevealX NPM™

네트워크 데이터와 머신 러닝을 활용하여 네트워크 및 애플리케이션 성능 문제를 식별하고 대응 시간을 단축합니다.

Security

Network Detection and Response (NDR)

RevealX NDR™

네트워크 가시성 및 AI를 통해 실시간 탐지, 신속한 조사, 그리고 모든 위협에 대한 지능적인 대응을 합니다.

NDR이 중요한 이유

Cyber Risk is Business Risk

보안 침해 사고에 대한 실질적 비용

$250M - $1B

SEC 서류에 보고된 실제 침해 비용을 기준으로 한

Long-term, end-to-end 비용

10% - 35%

주가 하락

73% 감소

분기별 수익 (순이익)

개인 위협

CISO의 생계, 경력, 청렴성이 위태.

(형사 고발)

고객이 **$1B** 달러의 위약금을 감당할 수 있나요?

EXTRAHOP

네트워크 가시성은 필수

사이버 리스크 관리 및 비즈니스 회복

공격자는 **취약점을 악용하여 탐지를 회피하고** 영향력을 확대하기 위해 지속적으로 공격 수법을 변경 합니다.

70%

네트워크 트래픽은 **암호화** 되어 있습니다.

37%

조직의 중요한 **장치가 관리되지 않습니다.**

47%

중요한 장치들이 **공공 인터넷에 노출 됩니다.**

98%

조직에서 하나 이상의 **보안 되지 않는 네트워크 프로토콜을 실행**

기존 툴로는 부족 합니다!!

EDR

모든 엔드포인트를 포함하지 않으며 공격자가 회피할 수 있습니다.

SIEM

공격을 감지하는데 신뢰할 수 있는 데이터 소스가 아니며 로그를 비활성화할 수 있습니다.

IDS

알려진 위협만 탐지 합니다.

NGFW

가시성이 부족하며, 데이터를 조사하는 워크플로우 생성이 불가 합니다.

SOC Triad 가시성 패더라임

NDR - Network

EDR - Files, processes, registries

SIEM - logs

전체적인 감지 View

Host 내부 View

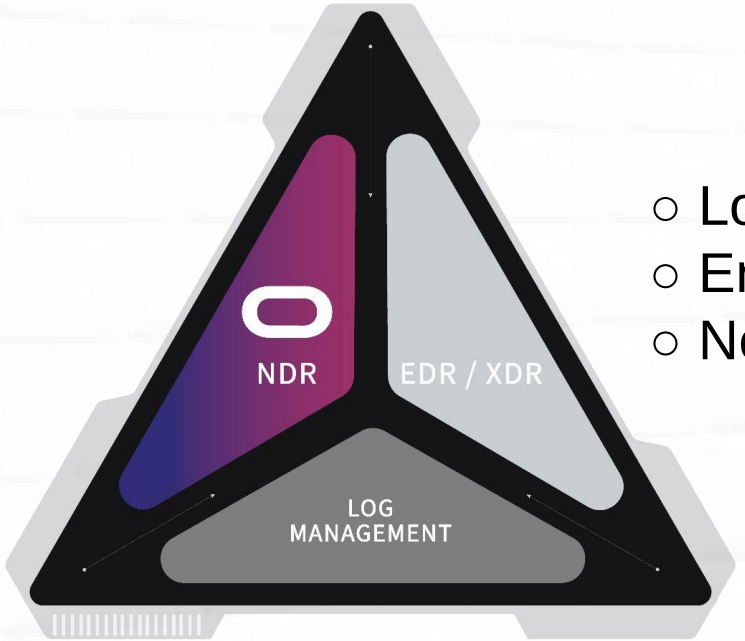
Gaps: Legacy 서버, IoT, 관리되지 않는 장치

제한적인 View

EXTRAHOP

NDR은 왜 중요할까요?

보안 가시성을 위한 세 가지 필수 요소



- Logs (SIEM)
- Endpoint Data (EDR)
- Network Data (NDR)

SEE MORE | 비즈니스 사각지대를 없애고 놓치지 마세요.

KNOW MORE | 실시간 Insight를 얻고, 모든 변화를 앞서 가세요.

STOP MORE | 공격 우위를 강화하고, 전략적 우위를 확보하세요.

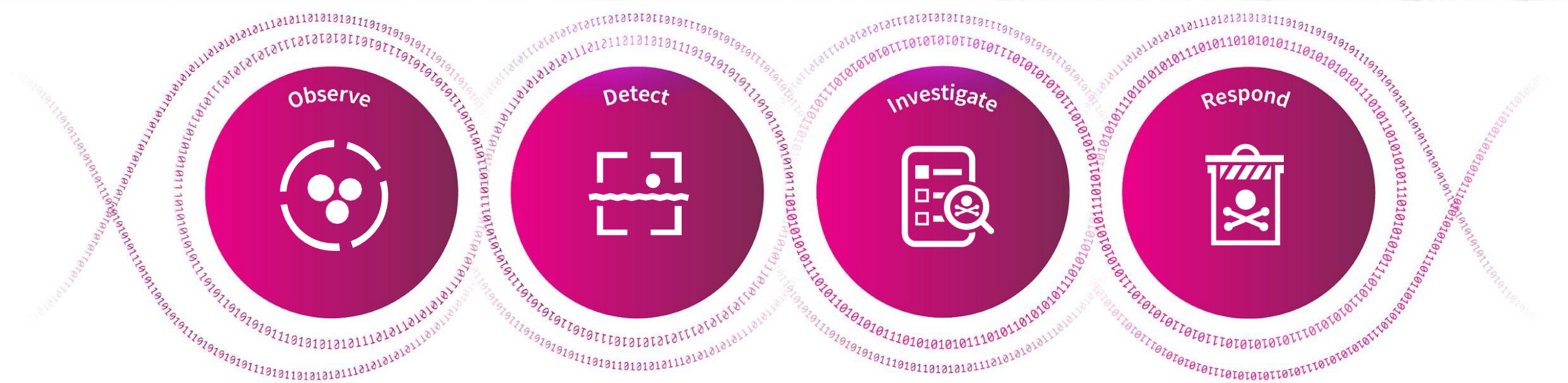
> [해커]의 최악의 악몽은 모든 데이터를 캡쳐하고 비정상적인 행동을 이해하는 네트워크 [툴] 입니다.
>
> ***Rob Joyce,*** *National Security Agency*

공격자가 다른 도구들을 회피할 수 있는 이유는 무엇일까요?

	공격에 대한 완벽한 가시성	행동 기반 설정	사후 탐지 포렌식	IT자산의 지속 관리	알려진 CVE 및 IOC의 지속적인 탐지	알려지지 않은 위협 탐지
EXTRAHOP	✓	✓	✓	✓	✓	✓
EDR	50-60%의 Endpoint	관리되는 장치만	관리되는 장치만	✗	✓	관리되는 장치만
SIEM	✗	✗	수작업	구성 완료된 장치만	✓	✗
취약성 관리	간헐적 스캔	✗	✗	간헐적 스캔	✓	✗

NDR 핵심 가치

ExtraHop NDR |Cybersecurity



완벽한 공격 표면 가시성

사전 및 사후 이벤트의 실시간 감지

가속화된 탐지 분류 및 조사

통합 보안 생태계

EXTRAHOP

사이버 리스크를 줄이는 네트워크 가시성

다른 보안 도구가 볼 수 없는 것들을 RevealX가 확인했습니다

기술 차별화 요소

FULL PCAP

PROTOCOL FLUENCY

전략적 복호화

CLOUD 규모

OUT OF BAND

ExtraHop은 조직이 전체 공격 표면에 걸쳐 광범위한 위험 가시성을 제공하여 고객이 다음을 수행할 수 있도록 합니다:

BUSINESS & CYBER 성과

스마트한 탐지

위협을 더 빠르게 방지

위험의 속도로 대응

EXTRAHOP

기술 파트너 협업 :

ExtraHop and Crowdstrike Overview

고급 위협은 일반적인 취약점을 노립니다

공격자들은 당신이 모든 것을 지켜볼 수 없다는 것을 알고 있습니다.

위협 행위자들은 **취약점을 악용**하고 탐지를 피하고 영향을 확대하기 위해 TTP(전술, 기술, 절차)를 **지속적으로 변화**시킵니다.

68%

엔드포인트가 보호되지 않아 공격에 취약합니다.

37%

중요한 장치가 관리되지 않고 있습니다.

98%

하나 이상의 취약한 네트워크 프로토콜을 실행하고 있습니다.

MITRE TTPs	EDR	NDR
Command & Control	✓	✓
Data Staging	✓	✓
Domain Escalation	✓	✓
Network Lateral Movement	X	✓
Target Enumeration	X	✓
Malware Execution	✓	✓
On-Host Data Encryption	✓	X
On-Host IOC Detection	✓	X
Process Spawning	✓	✓

EXTRAHOP

차세대 보안 운영 제공

ExtraHop RvealX + CrowdStrike Falcon.

SOC 진화

- **NDR, EDR, SIEM의 삼위일체**는 보안 분석가들이 초기 탐지나 경고를 넘어 더 넓은 범위의 영향력으로 나아갈 수 있도록 지원합니다.
- **AI 기반 분석**은 이 개념을 더욱 발전시키는 데 도움을 줍니다. 이를 통해 더 빠른 조사, 더욱 효율적인 **클라우드 규모의 로그 처리**, 그리고 더 **광범위한 데이터 소스**를 추가하여 위협을 상관분석하고 식별하며 대응할 수 있습니다.
- **결과적으로**, 더 **신뢰**할 수 있고 관련성 높은 보안 경고를 더욱 **빠르게** 제공하며, 보다 깊이 있는 **상황 정보**를 제공합니다.

가치 제공

- **확장된 공격 표면 커버리지:**관리 및 비 관리 자산에 대한 완전한 가시성을 확보하고, MITRE ATT&CK 프레임워크에 대한 커버리지를 확장합니다.
- **빠르고 포괄적인 조사:** 엔드포인트 및 네트워크 기반 탐지를 상관분석하여 더 스마트하게 조사하고, 사건 조사 및 대응 시간을 단축합니다.
- **효율적인 워크플로우:** 양방향 자동화 워크플로우와 지능적인 대응 조치를 제공하는 통합된 SOAR 플레이북을 통해 모든 위협에 신속하고 일관된 대응을 보장합니다.

CrowdStrike + ExtraHop 통합의 주요 요소

광범위한 제품 통합이 뛰어난 탐지 및 대응(D&R) 결과를 이끌어냅니다.

CROWDSTRIKE + EXTRAHOP

엔드포인트 커버러지 가시성

RevealX는 네트워크에서 Falcon 에이전트를 실행 중인 장치를 수동으로 식별할 수 있어, 커버리지 확장에 용이 합니다.

위협 인텔리전스

RevealX는 Falcon Intelligence에서 IOC와 위협 메타데이터를 실시간으로 가져와, 추가 비용 없이 탐지 및 데이터를 풍부하게 만듭니다.

향상된 탐지

네트워크 원격 데이터 수집 및 기존 Falcon 워크플로우를 통합하고, Falcon IOC를 사용하여 **RevealX** 탐지를 유도합니다. MTTR을 줄이며, 신뢰할 수 있고 반복 가능한 대응을 가능하게 합니다.

차세대 SIEM

기존의 LogScale 및 XDR 통합을 기반으로 Falcon NG-SIEM과 통합되어, 네트워크와 엔드포인트 전반에 걸쳐 통합된 탐지 및 대응을 지원합니다.

COMING SOON

Thank You