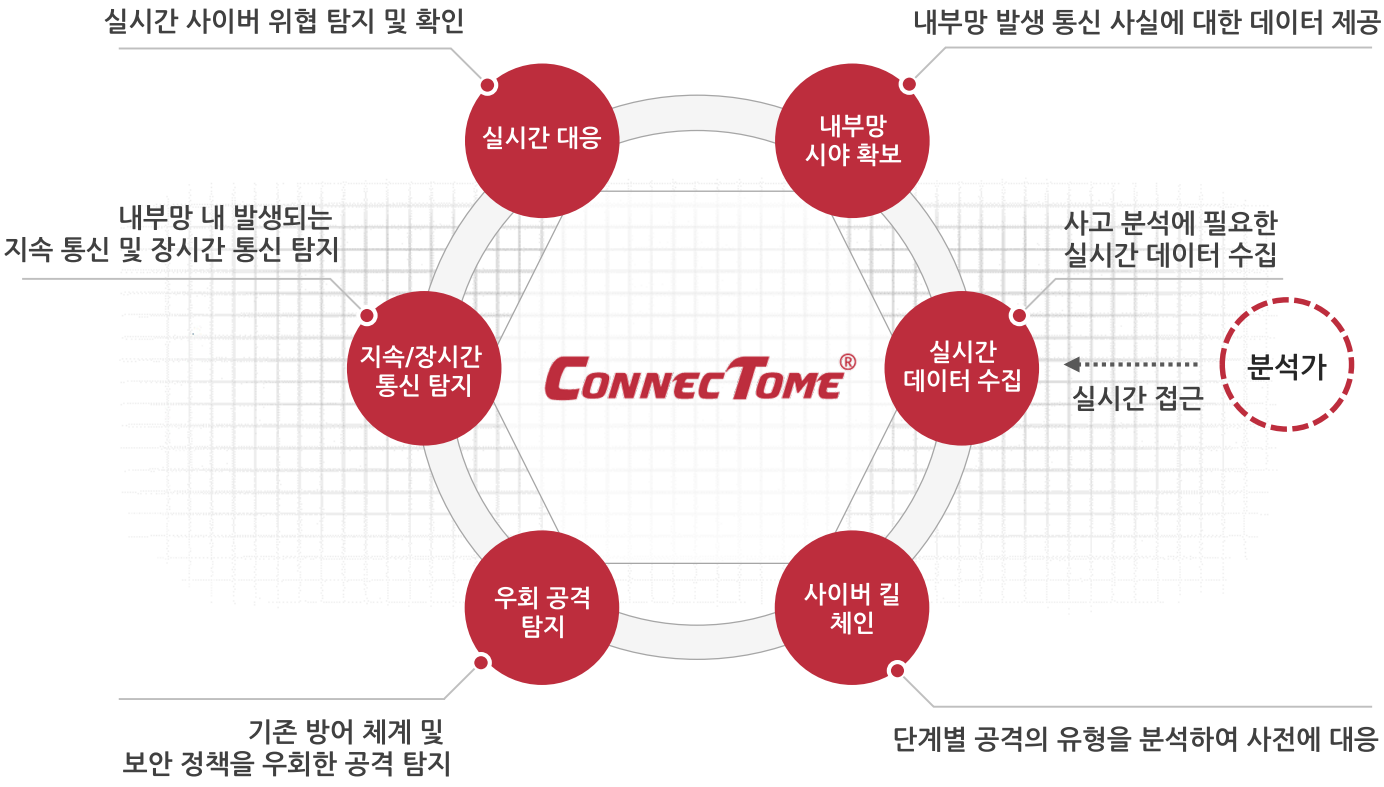
ConnecTome®

내부망 시야확보를 통한 빠른 대응

㈜나루씨큐리티 ConnecTome은 데이터기반의 데이터분석을 통하여 내부망 주요변화에 대한 탐지 지표를 수립하며, 기업 및 기관의 중요 자산이 존재하는 **내부망에 예방체계를 우회하여 침투하는 공격 탐지에 최적화된 솔루션**입니다.



내부망 보안 관련 특허

ConnecTome의 내부망 보안 기술은 국내/외 특허를 보유하고 있습니다.

- 내부망공격 탐지장치 및 방법
- DNS 강제우회 기반 악성트래픽 통제 및 정보유출탐지 서비스를 제공하는 방법, 서버 및 기록매체
- 명령제어채널 탐지장치 및 방법 [미국 특허]

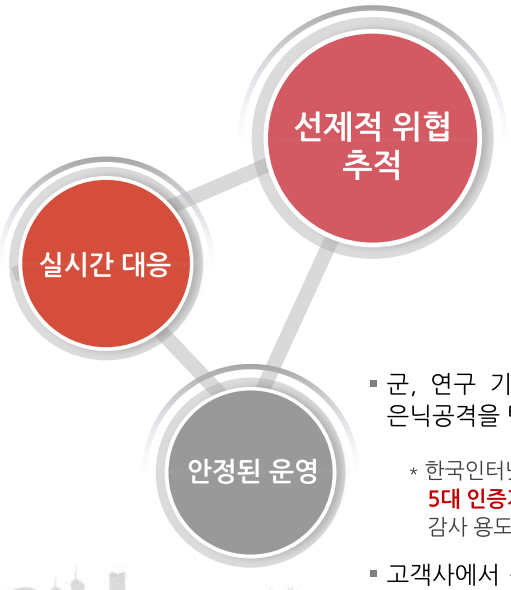
Making Sense of the Unknown
NARUSECURITY

완전한 내부망 시야확보를 통해
사고가 일어나기 전 빠른 대응을 가능하게 합니다.

중앙 집중 방식의 로그 저장방식으로 완벽한 시야 확보

내부망 현황을 실시간으로 제공하여, 보안 사고 발생 전 대응이 가능하게 합니다.

- ☑ 모든 통신 사실을 확보하여 공격자의 움직임을 파악
- ☑ 관리 편의성을 위한 중앙 집중 저장방식으로 원하는 데이터에 접근 가능
- ☑ 사이버 킬 체인 기반의 침해사고 단계별 이벤트, 지속통신 리스트, 내부망 이동 및 데이터 유출의 시각화 기능
- ☑ 로그 저장 기간 확대를 위한 확장 가능 스토리지 기능



- 보안 사고를 미연에 방지함으로써 사후 분석에 소모되는 시간 및 노력 비용 감소
- 감염된 시스템에서 발생된 트래픽을 추적하고, 초기 단계에서 탐지 가능
- 사이버 킬 체인 기반의 분석 결과를 대시보드를 통하여 제공

- 내부망에서 발생하는 모든 네트워크 트래픽의 통신 사실 확인
- 네트워크 행위 분석을 통한 보안 지표 제공
- 내부망에 상존하는 악성 행위를 탐지하여, 공격자의 의도 파악 가능

- 군, 연구 기관, 공공 기관 등 다수의 고객사에서 은닉공격을 탐지하는데 ConnecTome 활용

  * 한국인터넷진흥원은 ConnecTome을 활용하여 **5대 인증기관**(금융결제원, 코스콤, 한국정보인증 등) 감사 용도로 활용

- 고객사에서 운영중인 서비스 성능에 영향을 미치지 않도록 트래픽 미러링 방식 사용

제품 문의 및 데모

(주) 나루씨큐리티
www.narusec.com

(06087) 서울시 강남구 영동대로 621,
621 빌딩 8~9 층

P. 02-522-7912 F. 02-522-5765
E. sales@narusec.com

CONTACT US

Naru Security, Inc.
www.narusec.com

(06087) 8~9F, 621 Building, 621 Youngdong-daero, Gangnam-gu, Seoul

P. +82-2-522-7912 F. +82-2-522-5765
E. sales@narusec.com

NARUSECURITY
Making Sense of the Unknown

ConnecTome

내부망 시야확보를 통한 빠른 대응

공격자는 이미 정보를 탈취 할 준비를 완료했습니다.

모든 정보가 디지털화 되고 기업이 보유하고 있는 다양한 형태의 자산은 공격자들에게 매우 매력적인 금전적 가치를 갖게 되었습니다. 끊임없는 공격자의 노력은 방어자가 상상할 수 없는 금전적 대가로 돌아오기 때문에 각 기업이나 기관에서는 내 조직에서 어떠한 상황이 일어나는지 바로 알 수 있는 전반적인 시야를 확보하고 있는 것이 중요합니다. 보안에 있어 어떠한 투자도 100% 미만의 가시성 확보는 빈 공간을 노리고 공격하는 공격자를 고려한다면 실패한 투자입니다.

나루씨큐리티의 커넥텀은 이러한 100% 가시성을 확보하기 위해 설계된 최적화된 시스템이며 최근 망분리, 다양한 보안 기자재 도입을 통한 보안 강화에 이어 내부망, 즉 기업 및 기관의 중요 자산이 존재하는 곳을 실시간으로 지키는 내부망 CCTV 역할을 하는 유일한 솔루션입니다. 커넥텀은 고객에게 공격자가 갖지 못하는 100% 가시성을 제공하여 내부망의 주인이 누구인지 확인시켜 줍니다.

CONNECTOME®

커넥텀은 내부망 현황을 실시간으로 제공하여, 사고가 일어나기 전에 대응 가능하게 합니다.

커넥텀은 보안전문가 뿐만 아니라 의사결정권자가 보안전문가가 아니어도 현재 각 기업이나 기관의 네트워크 전반에 대한 이해를 돕기 위해 현황 지표를 제공하며, 보안전문가는 고도화된 공격에 대응하기 위해 공격채널로 이용되는 지속통신 및 백도어, Cyber Kill Chain 이벤트를 통해 공격자의 의도와 움직임을 파악 할 수 있게 합니다.

중앙 집중방식의 로그 저장방식으로 완벽한 시야확보 :

- 미러링을 통해 모든 통신 사실을 확보하여 공격자의 움직임을 파악합니다.
- 중앙 집중식 저장방식으로 센서가 아무리 많아도 원하는 데이터 접근이 용이하며 관리 편의성이 떨어지지 않습니다.
- 사이버킬체인 기반의 침해사고 단계별 이벤트 및 지속통신 리스트, 내부망 이동, 데이터 유출을 시각화하여 공격 징후를 파악하고 적절한 대응에 대한 결정을 내릴 수 있게 합니다..
- 확장가능 스토리지 – 원하는 기간동안 과거기록을 열람 및 보관 하실 수 있습니다.

---

*"한국인터넷진흥원은 **커넥텀을 활용**하여 대한민국에서 최고의 보안성이 유지되고, 공인인증업무를 관장하는 **5대인증기관**(금융결제원, 코스콤, 한국정보인증 등)을 감사하는 용도로 사용합니다."*

BENEFITS

- **실시간 대응**

실시간으로 위협을 탐지하고, 확인할 수 있습니다.

- **100% 완벽한 내부망 시야**

선제적 침해사고 대응을 위한 내부망 발생 통신 사실에 대한 완전한 데이터를 제공합니다.

- **확장가능성**

어느 기업사이즈에도 적용가능하며, 원하는 만큼 과거기록을 스토리지 증설로 보관 가능합니다.

- **강력한 분석기능**

사고분석에 필요한 데이터는 실시간으로 수집되며 분석가가 언제든지 접근 가능합니다.

- **공격자 의도 파악**

공격을 탐지 할 뿐만 아니라, 공격자의 의도를 파악 할 수 있는 정보를 제공합니다.

- **기존의 방어체계를 우회하는 공격 탐지**

기존 방어체계 및 정책체계를 우회한 진행중인 공격을 탐지하는 유일한 장비입니다.

- **사이버 킬체인**

근본 원인을 파악하여, 향후 공격이 이루어지기 전에 사전에 차단합니다.

- **지속통신/백도어 통신**

공격자를 찾기 위해 상존하는 모든 지속통신/백도어를 특허기술로 탐지합니다.

- **안전한 미러링 구성**

네트워크 미러링을 통해 안정적인 조사를 지원하며, 서비스에 영향을 끼치지 않습니다.

USE CASES

- 사고 조치 상태 확인
- 공격 탐지
- 침해사고 대응
- 징후 분석
- 선제적 위협 추적
- 대응 우선순위 제공
- 지속통신/백도어 탐지 (C2)

실시간 대응 :

- 사고를 미연에 방지 함으로서 사후분석에 소모되는 시간, 노력과 비용을 현저히 줄여드립니다.
- 감염 시스템에서 발생된 트래픽을 확인하여, 공격이 기업 전반에 퍼지기 전에 감염된 시스템을 초기단계에서 탐지하여 알려드립니다.
- Cyber Kill Chain 기반의 명령제어채널, 내부망 이동, 데이터 유출비율을 한 화면에서 제공하여 침해사고대응팀이 새로운 공격 및 신종 악성코드에 대응 할 수 있게 합니다.
- 완전한 내부망 시야확보를 통해서만이 보안센터와 요원들의 보안역량을 향상 시킵니다.

선제적 위협 추적:

- 내부망에서 발생하는 모든 네트워크 트래픽 통신 사실을 확인하고, 네트워크 행위 분석을 통한 보안 지표들을 제공하여 보안 현황을 실시간으로 확인하고 공격이 이루어지기 전에 사전에 대응 할 수 있게 합니다.
- 내부망에 상존하는 악성 행위를 탐지하고 기업 및 기관 내부에 퍼지는 것을 방지하며, 궁극적으로 공격자의 의도를 파악할 수 있게 합니다.
- 기 운영 중이거나 신규 도입예정인 해외 유명 보안장비와 연동이 용이합니다.

안정된 운영:

- 어플라이어스 장비로 별도의 숨겨진 라이선스 비용이 없습니다 .
- 다수의 고객사 보유 - 군대, 연구기관, 공공기관, 금융권 등의 폐쇄망/개방망에서 보안 장비로 활용되고 있습니다. 특히, 망분리 환경에서 보안 강화를 위해 관심을 받고 있습니다.
- 안전한 시스템 운영을 위해 미러링을 통해 복사된 트래픽을모니터링하여, 혹시모를 사고에도 기업 및 기관의 서비스에 영향을 미치지 않습니다.

TECHNICAL FEATURES

- 엔터프라이즈급 기업까지 적용할 수 있는 확장성
- 모든 트래픽 통신사실 수집을 통한 완전한 내부망 시야 확보
- L3 - L7 걸쳐 프로토콜 식별 가능
- 빅데이터 분석을 통한 은닉공격자 식별
- 기타 다른 보안장비와 연계할 수 있는 유연성
- 중앙 집중식 관리 / 저장 / 제어

CONTACT US

For more information or to schedule a demo:

+82-2-522-7912
admin@narusec.com

내부망 보안 관련 특허 획득

- 내부망공격 탐지 장치 방법
- DNS 강제 우회 기반 악성트래픽 통제 및 정보유출탐지를 제공하는 방법
- 나루씨큐리티가 보유한 다수의 특허를 통해 내부망을 지켜드립니다.

커넥텀은:

완전한 내부망 시야확보를 통해 사고가 일어나기 전에 빠른 대응을 가능하게 합니다.

파트너사 웅진의 커넥텀 사용 내역

ABOUT ConnecTome

커넥텀은 가장 완벽한 차세대 은닉공격탐지 솔루션으로 기존의 보안사각지대를 밝혀 알려지지 않은 위협을 탐지하는데 그 목적이 있습니다. 커넥텀은 기존의 ESM, IDS, APT 대응 장비가 탐지 하지 못하는 부분을 탐지 할 수 있고, 사고대응팀에서 위협 관련 정보를 정확히 확인하여 공격에 대응할 수 있게 도와줍니다. 커넥텀 벤더사인 나루씨큐리티는 다수의 네트워크 보안전문가가 포진하여 인텔리전스, 분석, 보안시각화에 매진하여 솔루션 향상에 힘쓰고 있으며, 현재 커넥텀은 군부대, 공공기관, 금융권 등 엔터프라이즈 급 네트워크를 보유한 다수의 기업에서 선택 받은 솔루션입니다.

Making Sense of the Unknown
NARUSECURITY

621, Yeongdong-daero, Gangnam-gu
621 Building, 9F
Seoul, 06087 Korea, Republic of
P +82.2.522.7912 **F** +82.2.522.5765
www.narusec.com