NOZOMI NETWORKS

OT & IoT 보안 및 이상징후탐지 솔루션

노조미 네트웍스는 OT / IoT영역에서 혁신적인 인공지능 기술을 기반으로 산업 제어 시스템 내 자산 현황 파악, 네트워크 시각화 및 모니터링을 통해 사이버 위협 및 이상징후를 탐지하는 솔루션입니다.

식별하고

OT 네트워크 내 개별 자산 정보 및 통신 현황에 대한 정확한 가시화로 네트워크 투명성 확보

분석하고

자산별 보안 취약점 및 네트워크 위협 리스크, 제어시스템 운영 현황 분석을 통해 정확한 네트워크 현황 파악

진단합니다.

네트워크를 위협할 수 있는 다양한 이상징후, 해킹징후에 대한 유형별 알람을 통해 사이버 보안 사고 방지

세계 20대 정유사 **9**개 기업 | 세계 10대 철강사 **6**개 기업 | 세계 10대 전력사 **5**개 기업 | 세계 10대 제약사 **7**개 기업 | 화학 수자원 | 제조 항공 | 자동차 물류 | 식품 교통 | 스마트 시티 스마트 빌딩

노조미 네트웍스 플랫폼 소개

Management Options

- **Vantage** — Software as a Service (SaaS) 제공
- **Central Management Console** — 분산된 사업장을 통합하는 중앙 관리 콘솔

Sensors

- **Guardian** — OT/IoT 전반의 강력한 보안과 가시성 제공
- **Remote Collector** — 소규모 단일 네트워크 내 보안 위협 감시
- **Guardian Air** — 다양한 무선 네트워크에 대한 보안 위협 감시
- **Arc** — 심층 분석 기능을 제공하는 엔드포인트 센서

Subscriptions

- **Asset Intelligence** — 자산 프로파일 제공
- **Threat Intelligence** — 최신 위협, 취약점 정보 제공
- **Smart Polling** — 자산에 대한 정밀한 정보 수집

OT 네트워크 가시화

- 제어망 네트워크의 통신 현황 그래픽 형태로 제공
- OT 프로토콜을 사용하는 제어 설비 간의 통신 가시화
- 개별 자산의 보안 취약점 및 전체 리스크 분석

하이브리드 위협 탐지

- 자산의 위협 현황, 시그니쳐 및 행위 기반의 위협 탐지
- 다양한 위협 탐지 소스 제공(CVE / TI / Assertion / 행위 기반 / Yara Rule, Packet Rule, STIX 지표 / Mitre ATT&CK)

인공지능기반 이상징후 탐지(AI&ML)

- OT 통신 학습을 통해 Baseline 기반으로 이상징후 탐지
- 설비의 잘못된 동작을 유발하는 통신 시도, 비인가된 자산의 통신 등 탐지 기능 제공

OT 네트워크의 변화 비교

- 타임머신 기능을 통해 OT 네트워크 상태를 정기적으로 스냅샷, 시점별 변화 비교 기능 제공(자산, 통신, 설정값 등 변경점 비교)

유연한 커스터마이징

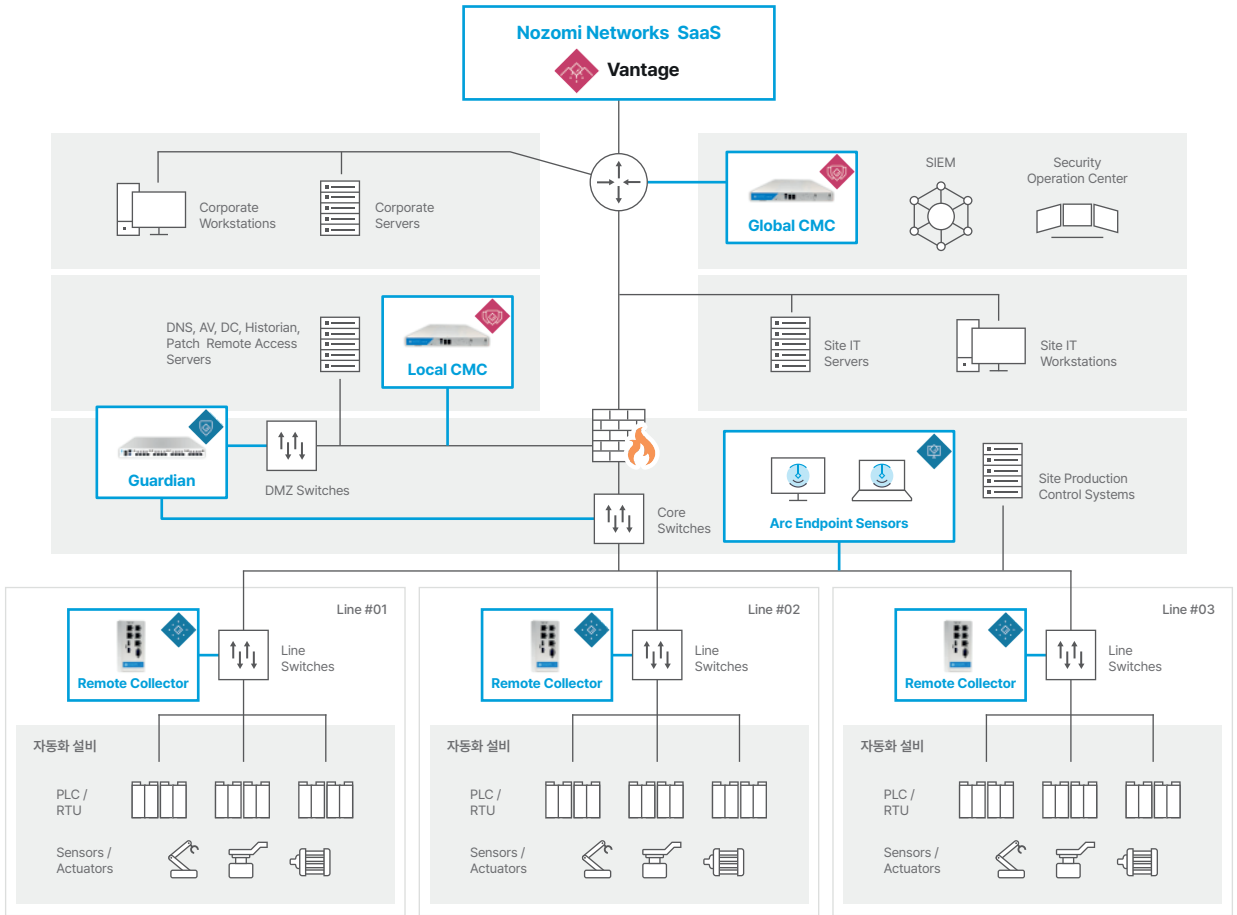
- 쿼리(Query) 기능을 사용하여 사용자가 원하는 정보를 파이차트, 막대그래프, 트렌드 차트 등 다양한 형태로 자유롭게 도식화하여 대시보드/리포트에 적용

기존 IT/SOC 환경과 통합

- 유연한 아키텍처, 광범위한 OT, IoT 및 IT 프로토콜 지원
- SIEMS, 자산, 티켓 및 ID 관리 시스템을 위한 통합 기능

Gartner peerinsights. OT 부문 고객 평가 4년 연속 1위 4.9 / 5

배포 구성



엔터프라이즈 급 규모
- 최대 500,000개 노드
- 3~6 Gbps의 최대 처리량

중소형 규모
- 최대 40,000개 노드
- 250 Mbps~1 Gbps 최대 처리량

내구성 환경
- 500~5,000개 노드
- 100~800 Mbps 최대 처리량

휴대용 기기
- 2,500개 노드
- 200 Mbps 최대 처리량

원격 데이터 수집 장비
- 50 Mbps 최대 처리량
- 가디언 기기 필요

가상 환경 및 컨테이너

VIRTUAL 타입 제품
- 1,000~40,000개 노드
- 1 Gbps 최대 처리량

컨테이너 에디션
- Gatewatcher
- Siemens RUGGEDCOM

기술 제휴 에코시스템

제어, 보안, 네트워크 및 클라우드 아키텍처와의 손쉬운 통합과 폭넓은 상호 운용성을 제공합니다.

SIEM, SOAR and Data Integrations	ArcSight, Atos, exabeam, FORTINET, IBM Security, splunk>, LogRhythm, SWIMLANE
OT, ICS Interoperability	EMERSON, ABB, Honeywell, GE Power, MITSUBISHI HEAVY INDUSTRIES, Schneider Electric, Rockwell Automation, SEL, SIEMENS, OMRON, YOKOGAWA
Other Network / IT and Security Technologies	Allied Telesis, CISCO, FORTINET, GARLAND TECHNOLOGY, Gigamon, tdi, GATEWATCHER, KEYSIGHT TECHNOLOGIES, paloalto, Tempered, WATERFALL, ZEDEDA
Cloud Service Platforms	aws, Google Cloud, Microsoft Azure, servicenow

Nozomi Networks 한국 총판 (주)투씨에스지

sales@tocsg.co.kr | 02. 320. 5050 | www.tocsg.co.kr

TOCSG 투씨에스지