## AUNES for Service

# 실시간 서비스 인시던트 관리

실시간으로 네트워크 및 애플리케이션 성능을 모니터링하여
감시·진단·분석 단계로 서비스 장애 및 성능 저하 문제를 예측합니다.

Trust & Communications
eNsecure
엔시큐어㈜

# 제품개요 01

AUNES for Service는 실시간 인시던트 관리 시스템으로 네트워크 전 구간의 트래픽을 수집·분석하여 웹 및 애플리케이션 서비스의 품질 상태를 직관적으로 파악하고 장애 및 이상징후를 탐지하며 서비스 성능 저하 및 장애를 사전에 예측·진단합니다. 사용자가 직접적으로 체감하는 품질을 중심으로 인시던트를 조기에 감지하고 선제 대응을 지원함으로써 효율적인 IT 인프라 운영을 가능하게 합니다.

# 개발배경 02

### 인시던트 관리 패러다임의 진화

기존의 임계치 기반 모니터링은 예상치 못한 장애에 즉각적으로 대응하기 어려웠습니다. 이제는 실시간으로 인시던트를 탐지하고 그 이상징후를 조기에 식별하여 선제적으로 대응하는 관리 체계로 전환되고 있습니다.

사용자가 체감하는 서비스 품질을 중점으로 장애 가능성을 사전에 예측해 민첩하게 대응할 수 있는 지능형 인시던트 관리 시스템이 요구됩니다.

### 복잡한 인시던트의 신속한 해결

해킹, 비인가자의 접근, 데이터 손상 및 변조 등 다양한 형태의 인시던트가 증가하면서 네트워크 기반 서비스의 안정성 확보가 더욱 중요해졌습니다.

서비스 지연 구간 분석과 업무 간 연관성 파악, 장애 시점 재현 기능 등을 통해 정확한 원인 진단이 가능해야 하며 실시간 대응 체계를 갖춘 인시던트 관리 솔루션이 필요합니다.

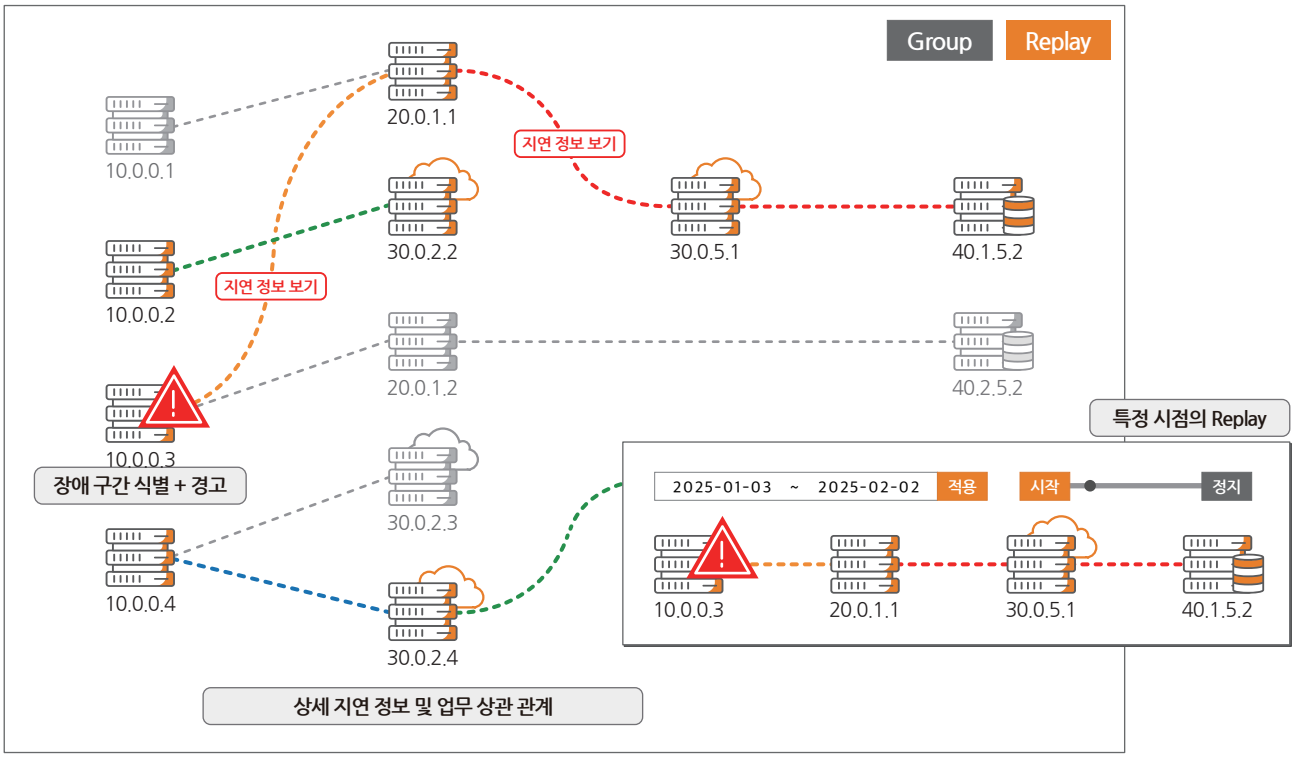
### 운영 효율성과 IT 투자 최적화

IT 인프라가 고도화됨에 따라 운영 관리의 효율성과 ROI(투자 대비 수익)를 고려한 접근이 중요해졌습니다.

실시간 분석과 자동화된 진단을 통해 비효율적인 리소스의 낭비를 줄이고 보다 전략적인 IT 인프라 서비스의 운영과 생산성 향상을 실현하는 인시던트 관리 방안이 필요합니다.

# 장애구간 03

AUNES for Service는 Topology Map을 통해 시스템 운영 상황과 사용자 별 서비스 인시던트 현황을 시각화합니다.




Client 구간 ↔ WEB 구간 ↔ WAS 구간 ↔ DBMS 구간

**상세 지연 정보**

| Server | Client | Risk | Syn Wait | Rsp Wait | Session | App | Trans | RTT | SRT | FPS | CPS | TPS | UPS | PPS | BPS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.0.0.3 | 463/715 | 86% | 0% | 0% | 544/913 | 544/913 | 1,669/2,569 | 10,000 | 8,897 | 5/17 | 2/14 | 16/41 | 3/11 | 46/399 | 388.69K/3.32M |

# 제품특징

04

## 실시간 가시성 확보

- 시스템 성능 문제를 1초 단위로 감시하여 신속하게 인시던트 해결
- 특허받은 eNgenRISK 알고리즘을 적용하여 인시던트 위험 수준의 직관화 실현
- 엔트로피 기반 이상징후를 탐지하여 인시던트 발생 가능성의 조기 감지

## 안정적인 대용량 패킷 분석

- 10Gpbs 이상 대용량 네트워크 패킷을 중단 없이 최대 200만 PPS 성능으로 실시간 분석
- 패킷 미러링 방식(Agentless)을 사용하여 서비스 사용의 지연 및 부하가 발생하지 않음
- 서비스 성능 문제를 트랜잭션 단위로 정밀 검색 및 분석

## 통합 인시던트 운영체계

- 사용자-네트워크-서버 등 전 시스템의 흐름을 중앙에서 연계 모니터링하여 인시던트 파악
- 인시던트 발생 시점을 정확하게 분석하기 위해 리플레이 재현 가능
- 온프레미스 또는 클라우드 망 내 네트워크 트래픽 모니터링 지원

## 상관관계 분석

- 사용자가 체감하는 성능 저하의 원인을 다각적으로 분석
- 상관관계 비교 분석을 통해 인시던트 유발 요소와의 연관성 식별
- 인시던트 발생 원인을 파악하여 자원의 남용 및 투자 낭비를 줄이고 경쟁력 강화

## 인시던트 대응 시간 단축

- 사전에 인시던트 임계치를 설정하여 위험을 미리 인지하고 선제 조치 가능
- 고위험군에 대해 정확하게 인시던트 발생 가능성 예측
- 인시던트 처리 프로세스의 수립과 전체 대응 시간 단축

## 사용자 중심 성능 측정

- 사용자의 체감 응답 속도를 웹 페이지 단위로 측정해 인시던트 영향도 분석
- 서비스 지연의 근본적인 원인을 분석하여 사용자에게 미치는 영향 파악 (Service Delay Root Cause Analysis)

# 적용대상

05

시스템 각각 개별적으로 모니터링 솔루션을 구축했으나, 실시간 인시던트 발생 원인과 담당 조직을 특정하기 어려운 곳

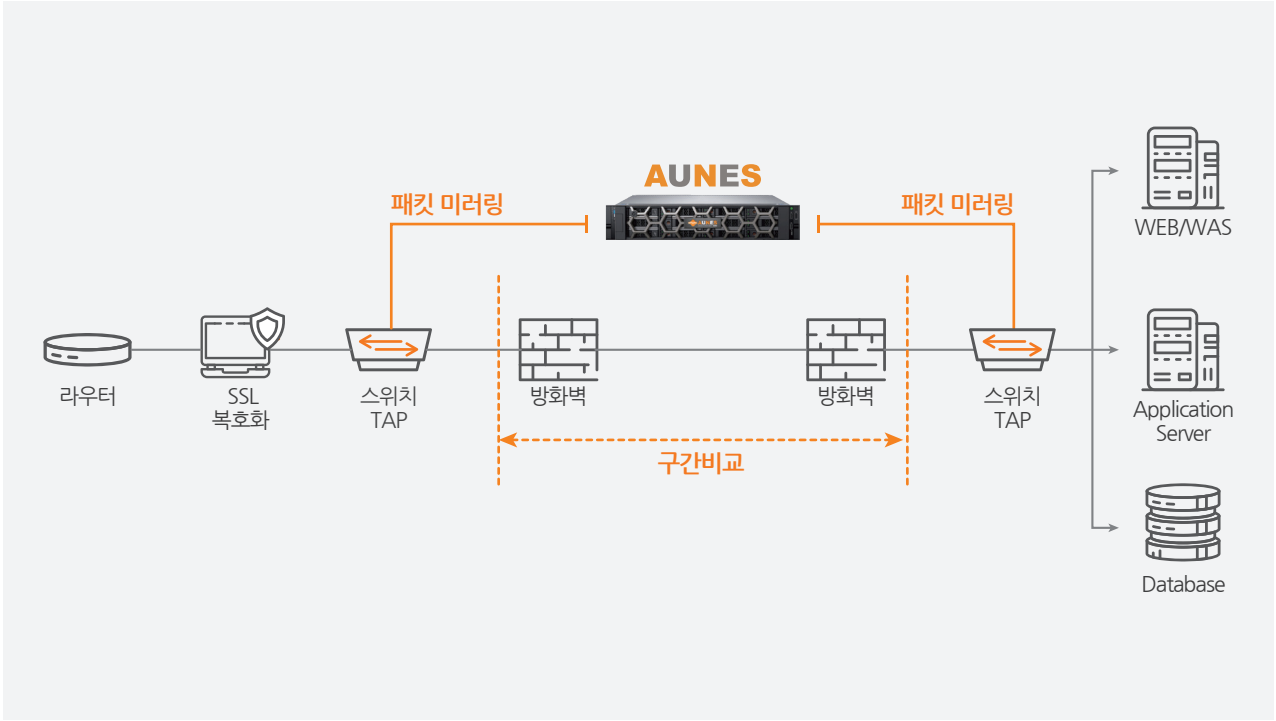
전체 인프라의 서비스 지연에 대한 직관적인 원인 규명을 하지 못하며, 사후 인시던트 분석에만 그치는 곳

네트워크나 장비 성능에는 이상이 없으나, 서비스 및 시스템 이용 지연 또는 문제가 발생하는 곳

대민/대외 서비스를 제공하기 때문에, 서비스의 안정성 확보 및 서비스 실시간성이 중요한 곳

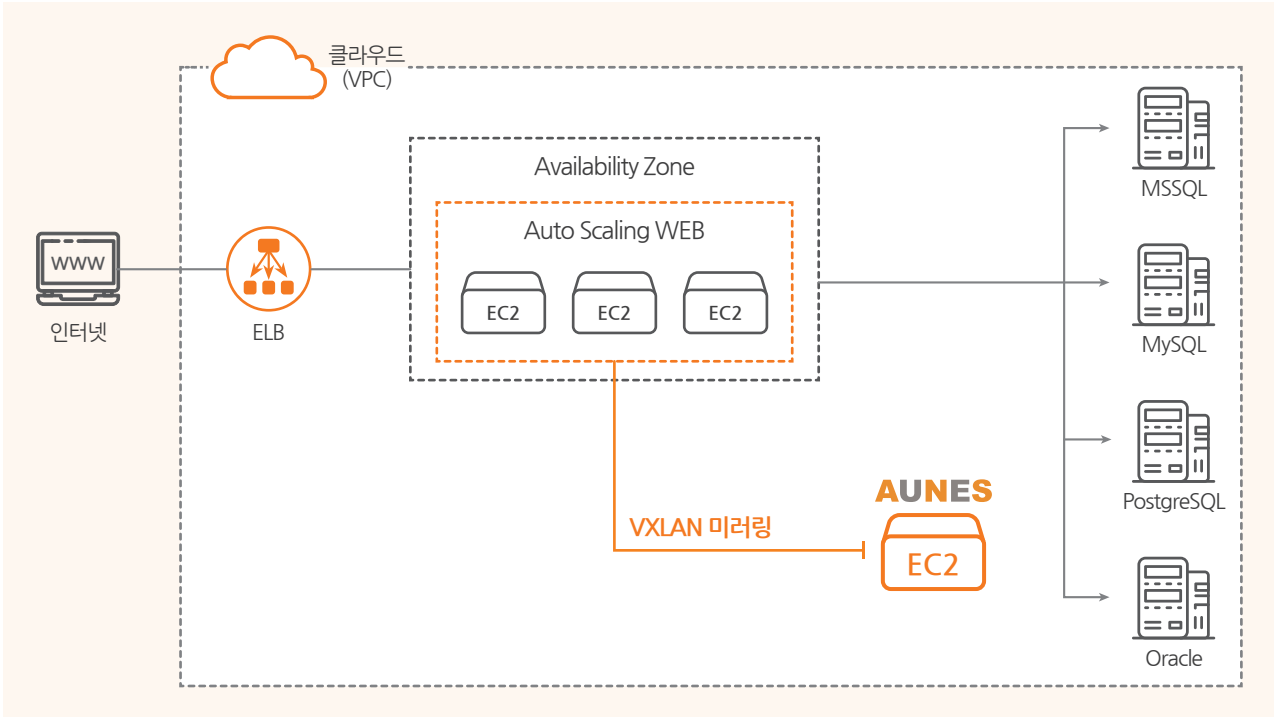
## On-premise

인시던트 발생 위험이 있는 구간 또는 시스템에 대한 서비스 트래픽을 미러링합니다.




## Cloud

VXLAN 터널을 이용하여 클라우드 환경의 패킷을 모니터링합니다.



# 주요기능

07

대용량 고속 패킷 처리 기술 등 다양한 자체 특허 기술을 바탕으로 안정성과 사용자 만족을 동시에 충족시킬 수 있습니다.

| | | |
|---|---|---|
| 메인 | 대시보드 | ▪ 다양한 트래픽 정보의 최대, 축척, 통계, 집계값을 일괄적으로 모니터링<br>▪ 실시간으로 네트워크 패킷 흐름, 세션, 트랜잭션, 가용성, 장애, 지연 상황 확인<br>▪ 위험도가 높은 순으로 서버, 클라이언트, 애플리케이션, 지역별 Top 10 정보 표시<br>▪ 실시간으로 위험 경고 알림 및 상황 확인 |
| 서버관리 | 서버맵 | ▪ 토폴로지 맵을 통해 서버를 매핑하여 네트워크 흐름의 가시성 제공<br>▪ 손쉽게 서버 그룹 및 노드 추가 가능<br>▪ 리플레이 기능으로 동 시간대 인시던트 상황 및 패턴을 비교 분석 |
| | 관심서버 | ▪ 성능 저하 또는 주의가 요구되는 장비를 특정하여 관리<br>▪ 인시던트 임계치를 초과한 서버의 목록을 실시간으로 확인 |
| 실시간정보 | 추이 그래프 | ▪ 네트워크 트래픽 양을 다양한 그래프로 가시화<br>▪ 모니터링 중인 모든 트래픽(BPS, PPS, APS)에 대한 추이 확인 |
| | 모니터링 | ▪ 인프라 장비의 성능 및 트래픽의 변화를 1초 단위로 감시<br>▪ 서버, 클라이언트, 애플리케이션, 에이전트, 네트워크, 지역별 실시간 위험도 측정<br>▪ 위험이 높은 순으로 정렬된 트래픽 정보 목록 확인<br>▪ 모든 이상 동작, 지연, 장애를 자동으로 감지하여 실시간 경고 알림 생성 |
| 로그분석 | 로그추이 | ▪ 특정 시점의 서버 운영 및 리스크 로그를 비교 분석<br>▪ 장애 및 성능 저하에 대한 혼합/상관관계 분석 자료 제공 |
| | 로그상세 | ▪ 모든 로그 이벤트를 수집 및 저장<br>▪ 특정 시점의 서버, 클라이언트, 애플리케이션, 지역별 경고 로그 확인 |
| 보고서 | 보고서 | ▪ 기간별 다양한 보고서 및 통계 결과 제공<br>▪ 특정 장비 또는 리스크의 범위를 지정 및 검색하여 결과 확인 |
| 설정 및 백업 | 경고 | ▪ 경고 알림의 기준이 되는 세부적인 인시던트 임계값 설정 (위험도에 따라 색상으로 표시) |
| | 사용자 | ▪ 사용자 계정 목록 및 로그인 이력 관리<br>▪ 접속 가능한 허용 IP의 수정 및 추가, 삭제 |
| | 백업 | ▪ 스케줄을 지정하여 자동 백업 설정 |

# 기대효과

08

## 효율성 향상

- IT 서비스 전 구간의 가시성을 확보하여 시스템 운영의 효율성 향상
- 무분별한 인프라 장비의 투자를 방지하여 경쟁력 강화
- 체계적인 성능 분석을 통해 전체 시스템의 운영 자원 최적화

## 생산성 증가

- 인시던트 조기 감지 및 해결로 대응 시간이 단축되어 비즈니스 생산성 향상
- 서비스 성능 저하로 인해 발생할 수 있는 대내외 악영향을 최소화
- 인시던트 발생 상황에 대한 담당자의 대처 능력 향상 및 선제 대응 가능

## 안정성 증대

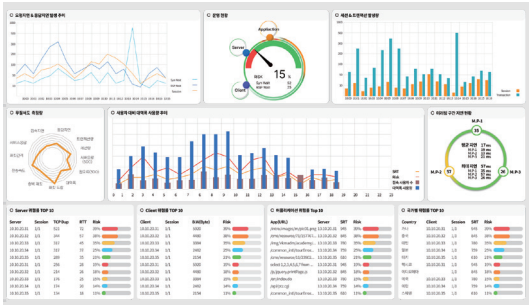
- 실시간 상황을 모니터링하여 문제 발생 시 신속한 대처 가능
- 인프라 운영 자원을 간소화하고 대응 프로세스의 확립 지원
- 특허 받은 대용량 트래픽 처리 기술로 안정적인 운영 가능

## 사용자 만족

- 인시던트 원인을 규명하여 각 시스템 담당자에게 위험 관리 가이드 제공
- 성능 저하 및 서비스 지연으로 발생할 수 있는 부정적인 경험 최소화
- 사용자가 체감하는 서비스 품질을 향상시켜 긍정적인 기업 평판 구축

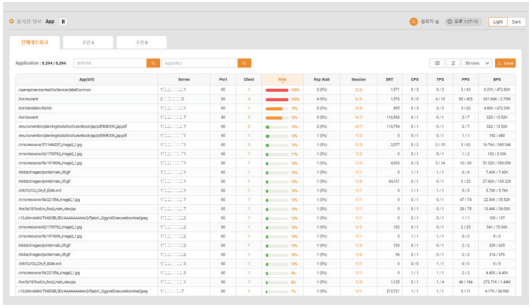
# 대시보드





**AUNES for Service 통합 대시보드**

서비스 운영 상태 실시간 모니터링



**트랜잭션 추적 분석**

애플리케이션별 사용자-서버 사이의 상태값 비교 분석


제 작 엔시큐어(주)
홈페이지 www.ensecure.biz
대표번호 02-2191-5010
유선문의 070-7826-6807
이메일 문의 mktg@ensecure.co.kr
팩 스 02-540-7425
주 소 서울특별시 용산구 한강대로 71길 4, 7층 엔시큐어


특 허 **제 10-2025483호 멀티 IP 클래스 처리 장치 및 방법**
**제 10-2213368호 멀티 키워드 고속 검색 시스템 및 방법**
**제 10-2563247호 네트워크 시스템 성능 저하 실시간 모니터링 장치**

특허청 1등급 GOOD Software 한국저작권위원회 ISMS INNOBIZ 기술혁신형중소기업