

**DOOSAN**

(주)두산  
디지털이노베이션



AI 기반 엔드포인트(EDR) 보안



CPS 환경 보안 \*CPS(Cyber-Physical Systems): 사이버 물리 시스템

# 지능형 사이버 위협에 제대로 대응하는 방법



## SaaS(Cloud)와 On-Prem 모두 최고 수준으로 보호하는 엔드포인트 보안 솔루션, 사이버리즌



### NGAV / EDR



- ✓ AI 기반 MalOp™ 엔진으로 방대한 데이터를 상관 분석하여 오탐 제거 및 정확한 탐지
- ✓ 공격의 전과정을 하나의 스토리로 제공

### MDR

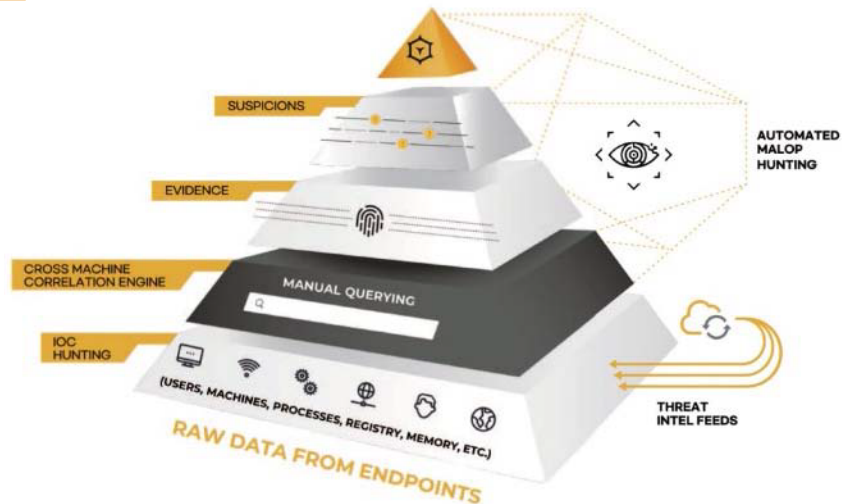


- ✓ 지능형 정오탐 분류와 선제적 위협 차단
- ✓ 4개의 글로벌 SOC 운영
- ✓ EDR과 통합된 탐지 및 대응 서비스

\*NGAV: Next-Generation Antivirus

\*EDR: Endpoint Detection and Response

\*MDR: Managed Detection and Response



## 최신 버전 서버부터 레거시 서버까지

## 모든 서버 환경을 강력하게 보호하는 사이버리즌 서버 EDR

| Windows                                                                                                                                                                                                                                                                                                                                                                                                                                   | Mac                                                                                                                                                                                                                                                       | Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Windows 7 SP1 (*)</li> <li>• Windows 8</li> <li>• Windows 8.1</li> <li>• Windows 10 IoT</li> <li>• Windows 10, up to Windows 10 22H2</li> <li>• Windows 11, up to Windows 11 23H2</li> <li>• Windows Server 2008 R2 SP1</li> <li>• Windows Server 2012</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> <li>• Windows Server 2022</li> </ul> | <ul style="list-style-type: none"> <li>• macOS Sequoia (15.0.0)</li> <li>• macOS Sonoma (14.0.0)</li> <li>• macOS Ventura (13.0.0)</li> <li>• macOS Monterey (12.1.x – 12.6.x)</li> <li>• macOS Big Sur (11)</li> <li>• macOS Catalina (10.15)</li> </ul> | <ul style="list-style-type: none"> <li>• RHEL /CnetOS/Oracle Linux 6(*)</li> <li>• CentOS 7, 8, 9 (9.5 미지원)</li> <li>• Red Hat Enterprise Linux 7, 8, 9</li> <li>• Oracle Linux 7, 8, 9</li> <li>• Ubuntu 14 LTS, 16 LTS, 18.04 LTS, 20.04 LTS, 20.10, 22.04 LTS, 22.10, 23.04</li> <li>• SLES 12 (limited support), 15<br/>– SLSE : SUSE Linux Enterprise Server</li> <li>• Debian 8, 9, 10, 11, 12</li> <li>• Amazon Linux AMI 2017.03</li> <li>• Amazon Linux 2</li> <li>• Amazon Linux 2023</li> <li>• Rocky Linux 8.5 to 9.2</li> <li>• CloudLinux 7</li> <li>• AlmaLinux 8.6, 8.8, 9.2, 9.4</li> </ul> |



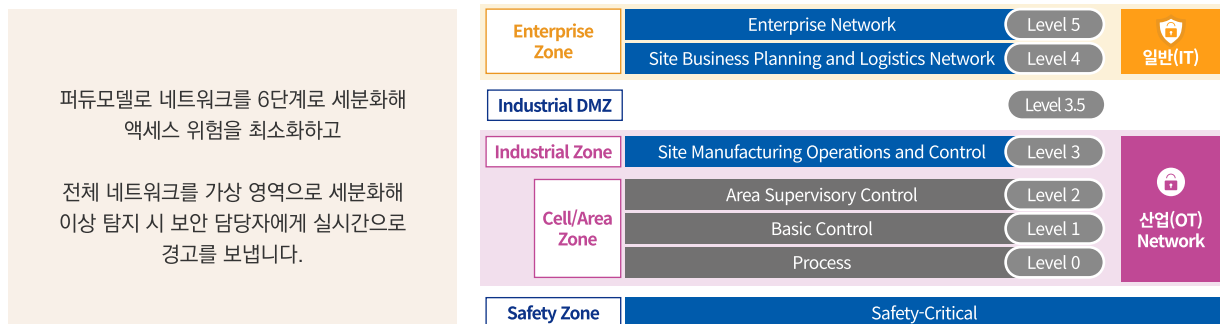
## 제조 기반 시설을 겨냥한 사이버 공격의 급증!

## 클래로티(Claroty)는 모든 사이버물리시스템(CPS)를 보호합니다



### 실시간 모니터링과 신속한 경고 알림

클래로티는 퍼듀모델(Purdue Model) 및 가상 영역(Virtual Zone) 기반으로 공격 확산을 막고 위협을 실시간 모니터링합니다.



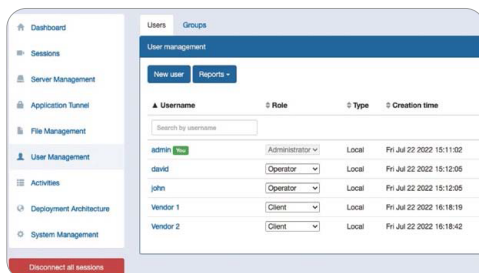
### 알려진 위협부터 비정상적 기능, 악의적인 행동 징후까지

고객의 OT/XIoT 자산에 최적화된 가시성을 제공해 보안 취약점(CVE)을 정확하게 식별합니다.



### 운영 환경에 영향 주지 않는 안정적인 OT 원격 관리

OT 보안 표준 지침을 모두 충족하는 원격 관리 및 원격 제어로 잠재적 위협을 최소화합니다.



승인된 사용자만 원격 접속을 허용하며 역할 기반 액세스 제어로 제로트러스트 아키텍처를 구현합니다.



위험 경고 알림 발생 시 원격으로 직접 연결 해제가 가능하며 세션을 자동 녹화해 사후 대응 조치 및 조사에 활용합니다.



## MITRE ATT&amp;CK™

## 3년 연속 최고 평가를 받은 엔드포인트 보안 솔루션

사이버리즌은 MITRE ATT&CK 2024테스트에서 SOC 효율성과 운영 우수성 부문에서 리더로 인정 받았습니다.

- 100% 설정 변경 없음: 별도의 설정 변경 없이 즉시 탐지 및 대응
- 100% 탐지: 79개의 공격 단계 모두 완벽하게 탐지
- 100% 가시성: 완전한 가시성 커버리지 제공
- 100% 정확성: 20건의 공격에 대해 100% 정탐 결과 확인
- 100% SOC효율성: 악성 이벤트 전체 실시간 탐지 및 즉각 대응

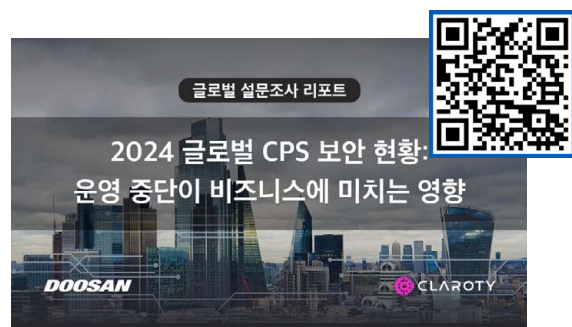
[평가 결과 자세히 보기](#)클래로티 2025 Gartner® Magic Quadrant™  
CPS 보안 리더 선정

Magic Quadrant™ 의 첫 CPS PP (Cyber-Physical Systems Protection Platforms) 평가에서 실행 역량과 비전 완성도 부문 가장 높은 평가를 받았습니다.

- CPS 자산 발견 및 맵핑
- CPS 보안 문제 우선 순위 결정 및 조치
- CPS 보안 모니터링 및 조직 보안 전략 목표와의 일치성

[평가 결과 자세히 보기](#)

## 보안 담당자라면 알아야할 사이버보안 인사이트 리포트



## 사이버보안, 이제 전문가에게 물어보세요!

(주)두산 디지털이노베이션BU는 IT보안부터 OT, xIoT보안까지 모든 영역을 아우르며 컨설팅, PoC 및 구축, 기술 제공 뿐만 아니라 전문가 연동 및 고객사 대응 프로세스 수립까지 종합적인 지원을 제공합니다.