AhnLab

AhnLab CPS PLUS

통합 CPS 보안으로 이루는 디지털 혁신

IT-OT를 융합한
CPS 통합 보안 플랫폼

배경

그 동안, OT 환경은 외부에서의 접근이 엄격히 통제되는 폐쇄성으로 인해 IT 환경과 비교해 상대적으로 안전하다고 여겨져 왔습니다. 하지만, 디지털화가 빠르게 진행되고 IT 영역과의 접점이 늘어나면서 OT 환경에 대한 사이버 공격도 증가하는 추세입니다. 이제, OT에 대한 보안의 중요성이 높아진 것은 물론 OT와 IT를 연계한 새로운 통합 보안 접근이 필요한 상황입니다.

CPS(Cyber-Physical System)는 기존 OT 영역의 외부 연결이 확대됨에 따라 OT, IT를 포함한 포괄적인 영역들을 아우르는 개념입니다. 여러 환경을 아우르는 CPS를 효과적으로 보호하기 위해서는 기본적으로 OT 환경에서 우선시되는 '가용성(availability)'을 보장하고 자산 가시성을 제공하는 가운데, 여러 보안 모듈 간 연동 및 중앙 관리를 통해 보안 효율성을 확보할 수 있어야 합니다.

가용성 확보

IT와 OT를 아우르는 CPS 환경에서는 우선 사용 연한이 길고 보안 패치가 어려운 OT 환경의 여러 설비들을 보안 위협으로부터 보호하고, 안전하게 동작할 수 있도록 해야 합니다.

가시성 확보 및 위협 탐지/대응

가시성 확보가 어려운 OT 환경에서 자산 정보, 네트워크 상태, 보안 위협 및 취약점 현황에 대한 가시성을 확보해야 합니다. 또한, 각종 설비의 가용성을 보장하는 범위에서 보안 위협을 탐지하고 대응해야 합니다.

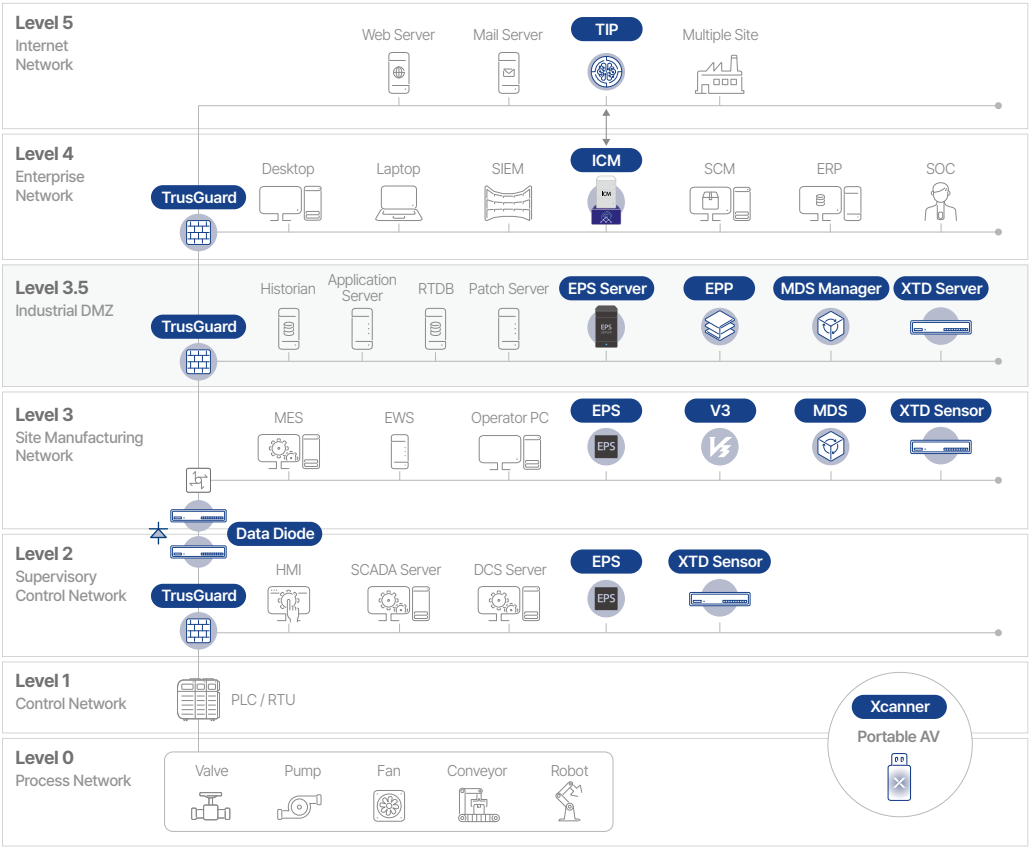
IT 및 OT 연계 보안

OT망은 폐쇄망이지만 IT망 시스템과의 접점이 확대되면서 다양한 공격들이 빈번하게 발생하고 있습니다. 이에, IT와 OT 보안을 연계한 CPS 보안 관점의 접근이 필요합니다. 또한, 개별 솔루션이 아닌 보안 모듈 간 연동과 중앙 관리를 지원하는 통합 보안 플랫폼이 요구됩니다.

Why AhnLab CPS PLUS

AhnLab CPS PLUS는 제조, 정유, 운송 등 다양한 산업의 OT 엔드포인트와 네트워크, 그리고 OT와 연결된 IT 환경까지 폭 넓게 보호하는 통합 CPS 보안 플랫폼입니다. 안랩의 위협 탐지 & 대응 전문성과 OT 기술력을 결합한 AhnLab CPS PLUS는 엔드포인트와 네트워크 보안 기술을 바탕으로 IT와 OT를 아우르는 CPS 환경에서 ▲식별(가시성) ▲위협 탐지 ▲대응으로 이어지는 빈틈없는 보안을 제공합니다. 플랫폼 내에서 유연하게 연동되는 보안 모듈들은 CPS 보안 통합 관리 솔루션 'AhnLab ICM'을 통해 효율적으로 모니터링 및 운영할 수 있습니다.

AhnLab CPS PLUS는 현존하는 CPS 보안 플랫폼 중 가장 폭 넓은 커버리지를 자랑합니다. 여기에, 탁월한 기술력과 통합의 시너지가 더해져 고객들에게 차별화된 CPS 보안 경험을 제공합니다.



AhnLab ICM
CPS 통합 모니터링 기반 가시성 제공 및 보안 모듈 관리

AhnLab EPS
OT 엔드포인트 프로세스 및 매체 제어, 악성코드 진단

AhnLab XTD
OT 네트워크 가시성 확보 및 이상 행위 등 위협 탐지

AhnLab Xcanner
OT 엔드포인트 악성코드 진단 및 치료용 휴대용 안티멀웨어

AhnLab TrusGuard
OT 네트워크 보안 및 세그멘테이션

AhnLab Data Diode
물리적 일방향 데이터 전송을 통한 OT 환경 접근 제어

AhnLab MDS
네트워크 샌드박스 분석으로 알려지지 않은 악성코드 탐지

AhnLab EPP/V3
CPS 환경 내 IT 기기에 대한 안티멀웨어 및 통합 패치 관리

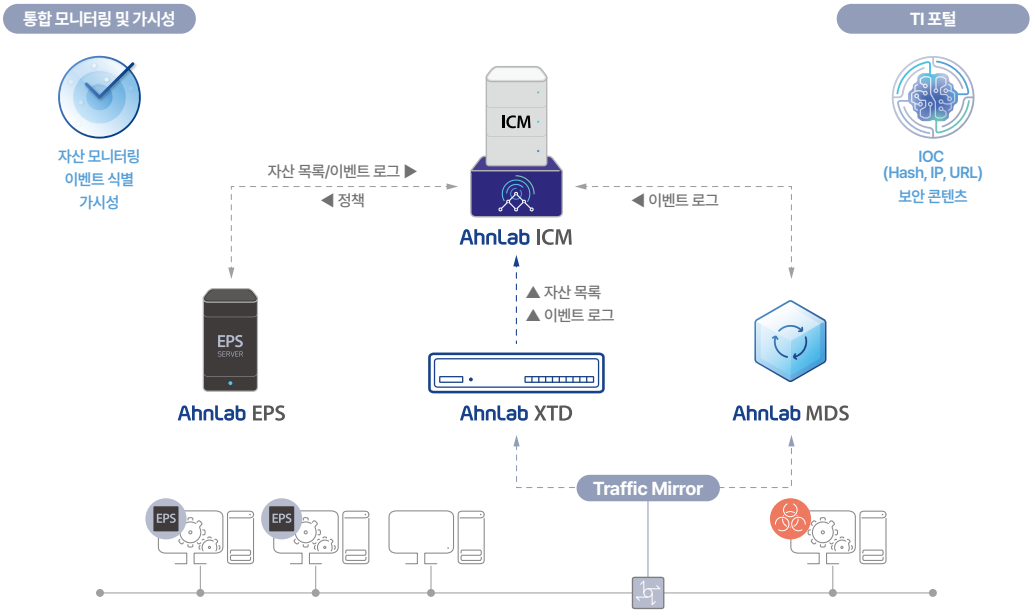
AhnLab TIP
IT와 OT 환경에 걸친 CPS 위협 인텔리전스

구성 모듈

1. AhnLab ICM (+TIP)

CPS 보안 통합 관리를 담당하는 AhnLab ICM은 한 눈에 연동 모듈의 현황 파악이 가능한 대시보드를 통해 CPS 환경에 대한 통합 가시성을 확보할 수 있습니다. AhnLab EPS, XTD, MDS 등 CPS 환경 전반에 걸친 모듈 현황과 자산 정보 수집 및 이벤트 모니터링을 통해 조치가 필요한 이슈를 실시간으로 확인할 수 있습니다. 이러한 플랫폼 기반 중앙 관리 역량을 기반으로 통합 가시성과 종합적인 위협 모니터링을 제공해 이슈 조치 시간을 단축시키고, 업무 연속성과 생산성을 향상시킵니다.

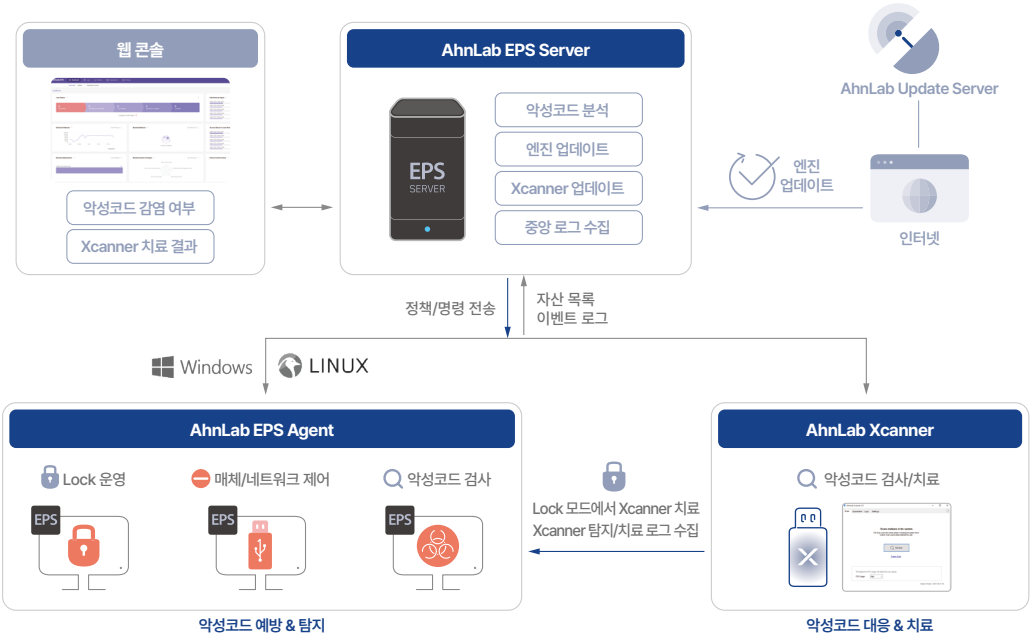
AhnLab TIP는 AhnLab ICM 연동을 통해 CPS 보안 플랫폼에 위협 인텔리전스를 공급합니다. AhnLab ICM에서 IT와 OT를 아우르는 CPS 환경의 보안 위협에 대한 침해지표(IoC)를 통해 보다 자세한 정보를 실시간으로 확인할 수 있습니다.



2. AhnLab EPS & Xcanner

OT망 설비 보안에 최적화된 AhnLab EPS는 비즈니스 연속성 확보를 위해 불필요한 프로그램, 이동식 매체, 네트워크 접속 등을 차단합니다. 또한, 설비의 사용 연한이 환경의 특성에 맞게 윈도우, 리눅스, 임베디드 버전 등 다양한 OS에 대해 구형부터 최신 버전까지 운영을 지원합니다. 설비 가용성 보장을 위한 초경량 에이전트로 시스템 리소스 소모를 최소화하며, 허용 리스트 기반 통제 적용 시 3단계 Lock 운영 모드를 지원하여 정책을 유연하게 적용할 수 있도록 합니다.

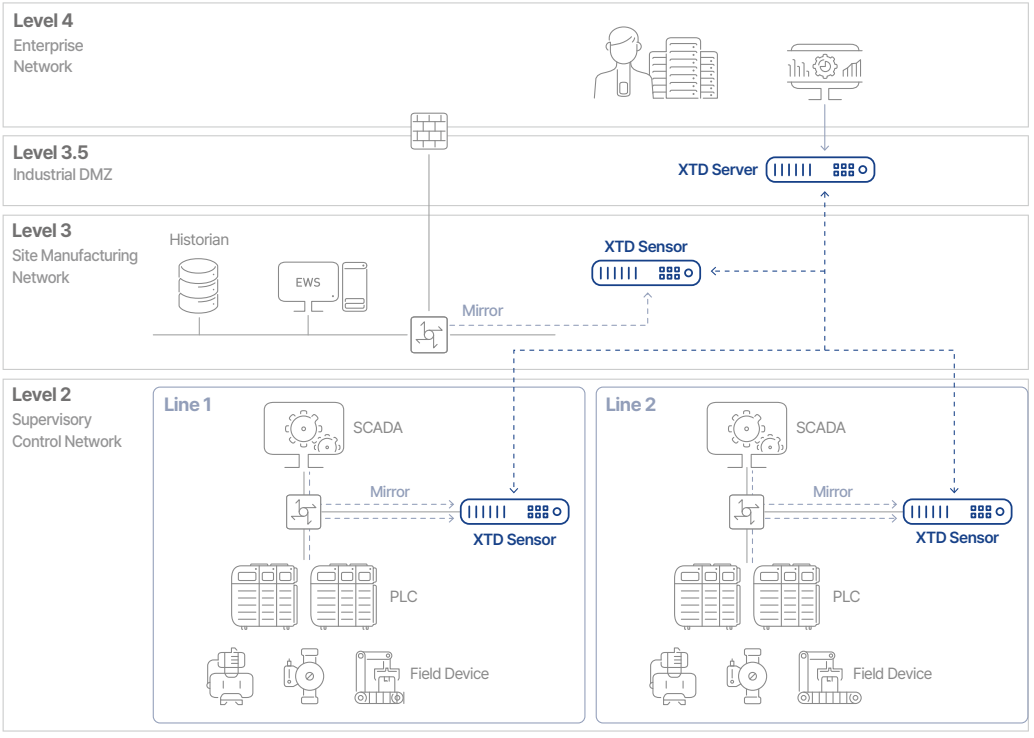
더불어, 악성코드에 감염된 것으로 의심되는 시스템에 대해서는 OT 휴대용 안티멀웨어 AhnLab Xcanner를 활용하여 별도 솔루션 설치 없이 악성코드 진단 및 치료가 가능합니다. AhnLab Xcanner는 인가된 이동식 디스크에 탑재하거나, EPS Server에서 EPS Agent로 전송해 원격 실행하는 형태로 사용 가능하며 검사 및 치료 현황은 EPS Server에서 모니터링 및 관리할 수 있습니다.



3. AhnLab XTD

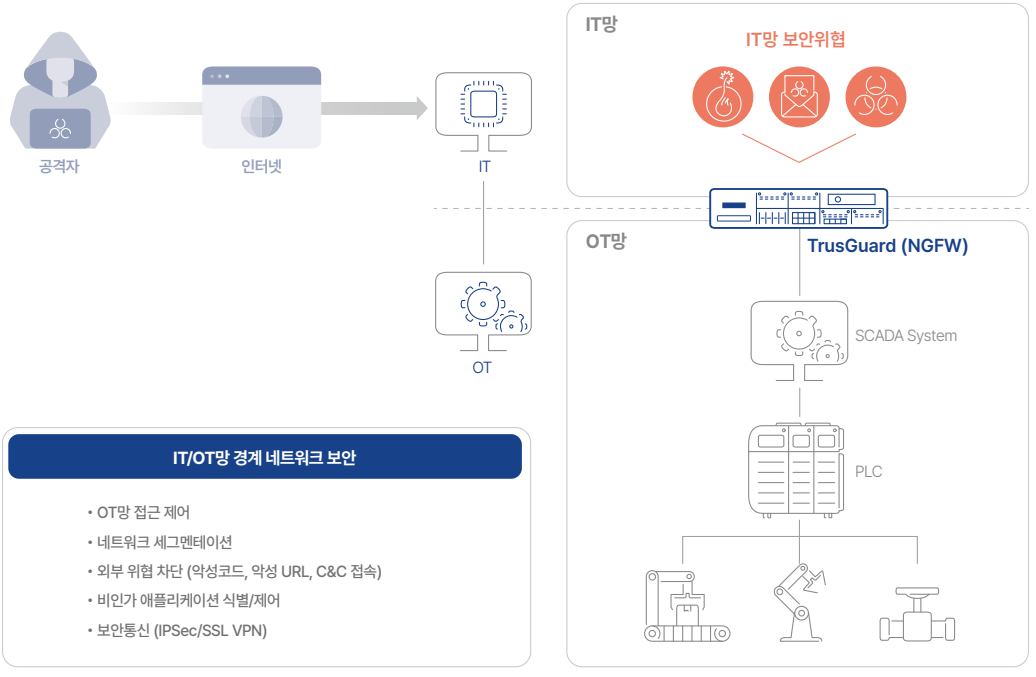
AhnLab XTD는 OT망 네트워크 기반 가시성 및 위협 탐지 모듈로 다양한 OT 망 자산에 대한 가시성을 제공합니다. 또한, IT망으로부터 유입되거나 OT망 내부 시스템 간 전파되는 악성코드 혹은 취약점 등 보안 위협을 탐지합니다. OT 설비 가용성을 보장하는 패시브 스캔(passive scan) 방식을 사용하며, 자체 개발한 프로토콜 프로파일링 기술과 심층 패킷 분석(DPI) 기능을 바탕으로 다양한 종류의 설비 식별과 비정상 제어 로직에 대한 탐지 및 분석을 제공합니다.

아울러, OT 엔드포인트 보안 모듈 AhnLab EPS 연동을 통해 에이전트 기반으로 수집된 디바이스 상세 정보들을 결합하여, 폭 넓고 상세한 자산 가시성을 제공합니다. 두 모듈의 연동은 OT망 네트워크로 전파되는 보안 위협을 탐지하고 대응하는 측면에서도 독보적인 능력을 발휘합니다. AhnLab EPS 서버의 Restful API 연동을 통해 Xcanner 원격 검사를 지원하여 일차적으로 네트워크에서 악성코드 전파 또는 취약점 악용 유해 트래픽이 탐지되면, 엔드포인트 영역에 위치한 의심 시스템에 대해서도 다시 한번 악성코드 검사를 실시할 수 있습니다.



4. AhnLab TrusGuard

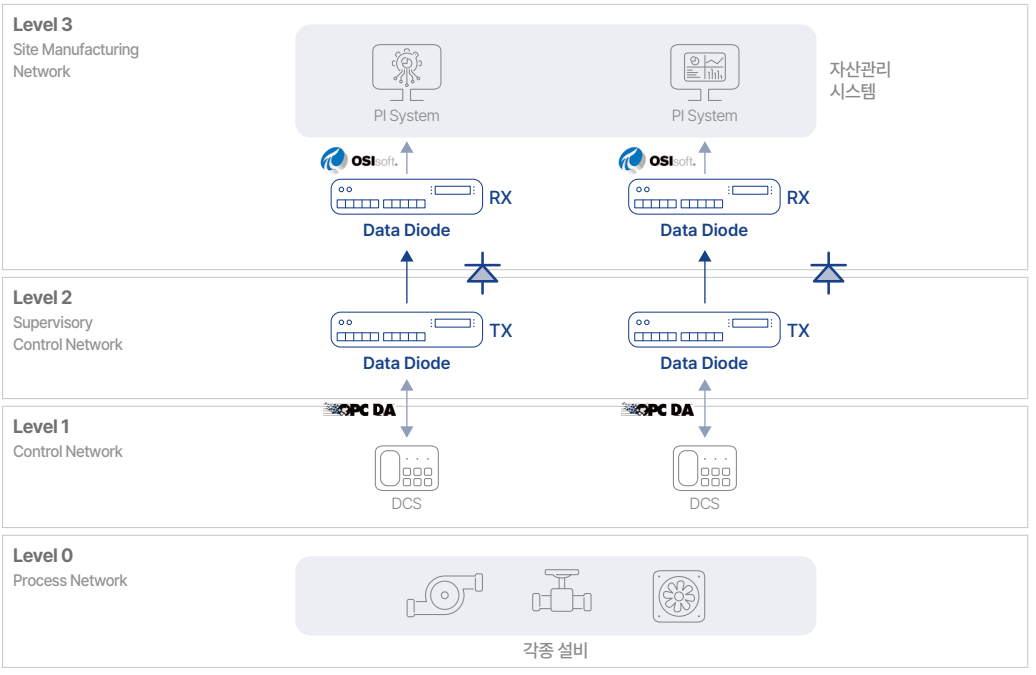
차세대 방화벽 AhnLab TrusGuard는 OT망 경계(perimeter)에서 네트워크 접근 제어와 세그멘테이션을 제공합니다. 악성 URL과 C&C 접속을 차단하고 IPSec/SSL VPN 등 보안 통신을 지원합니다. 또한, OT 프로토콜 분석 기술이 적용되어OT망 내부에서 산업용 프로토콜을 상세하게 제어할 수 있습니다. 구체적으로는 Modbus, DNP3 등 프로토콜 별 제어 뿐만 아니라 function code까지 식별하여 제어 가능합니다.



5. AhnLab Data Diode

AhnLab Data Diode는 보안 수준이 서로 다른 네트워크 간 연결에서 보안 수준이 높은 곳으로의 접근을 강화하기 위해 물리적 일방향 전송을 바탕으로 필요한 데이터만 안전하게 외부로 전송하도록 합니다. 전송하는 데이터에 대해 암호화, 전진 오류 수정(Forward Error Correction, FEC), 데이터 송신 오류 제어, 악성코드 검사 등 다양한 기술들을 적용해 신뢰도와 안정성을 극대화했습니다.

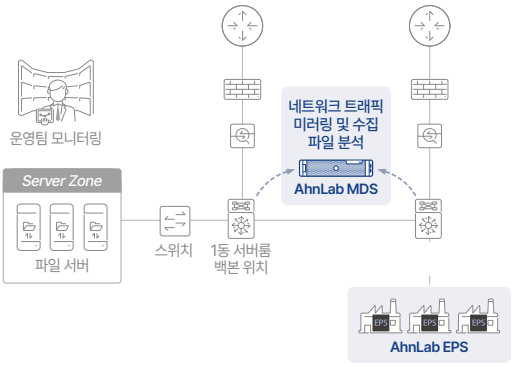
또한, IT와 OT 환경을 아우르는 광범위한 프로토콜 지원 기술을 기반으로 다양한 환경에 최적화된 형태로 적용 가능합니다. 각종 IT/OT 프로토콜, CCTV 스트리밍 데이터, 데이터베이스 등 여러 활용 사례(use case)들을 맞춤형으로 지원하는 유연성도 갖추고 있습니다.

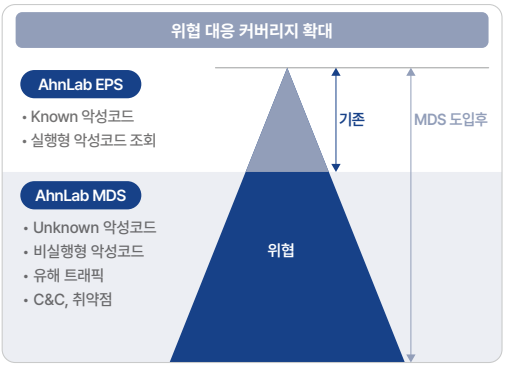


6. AhnLab MDS

네트워크 샌드박스 모듈 AhnLab MDS는 고도화되는 알려지지 않은 신종 및 변종 악성코드에 대응하기 위해 생산망 트래픽으로 전송되는 파일을 수집하여 악성코드 동적 분석을 수행합니다. 또한, 공격자의 C&C IP 연결, 악성코드 확산, 취약점 등 다양한 보안 위협에 대한 탐지와 모니터링을 기반으로 탁월한 대응 역량을 제공합니다.

또한, OT 엔드포인트 보안 모듈 EPS와 연동 시, MDS의 동적 분석 기능을 바탕으로 신종, 변종 및 알려지지 않은 악성코드까지 모두 방어가 가능해 종합적인 위협 대응 커버리지를 확대할 수 있습니다.





7. AhnLab EPP/V3

CPS 환경에서는 OT 보안 뿐만 아니라, OT 환경과 연결된 혹은 OT 환경을 관리하는 IT 영역의 보안까지 고려해야 하며, 필수적으로 요구되는 역량은 패치 관리를 통한 취약점 최소화와 안티멀웨어를 통한 강력한 위협 차단입니다.

AhnLab EPP는 안티멀웨어부터 패치 관리까지 다양한 모듈을 유기적으로 연동하여, IT 환경에서의 위협이 OT 환경을 침해하는 것을 방지합니다. 우선, 다수 엔드포인트 시스템에 대해 안정적이고 폭 넓은 패치 관리 기능을 제공하여, 엔드포인트에 대한 하드닝(Hardening)을 제공합니다. 또한, 안티멀웨어 모듈(V3)은 AV-TEST 등 글로벌 인증 평가에서 오랜 기간 최상위 수준 진단율을 기록하고 있으며, 검증된 기술력을 바탕으로 세계 최고 수준의 위협 차단 역량을 제공합니다.

도입 효과

AhnLab CPS PLUS는 IT-OT 융합 보안을 통해 CPS 보안 요구사항을 효과적으로 해결하여, 고객 여러분이 진정으로 디지털 혁신을 가속화할 수 있도록 지원합니다.

가용성 보장

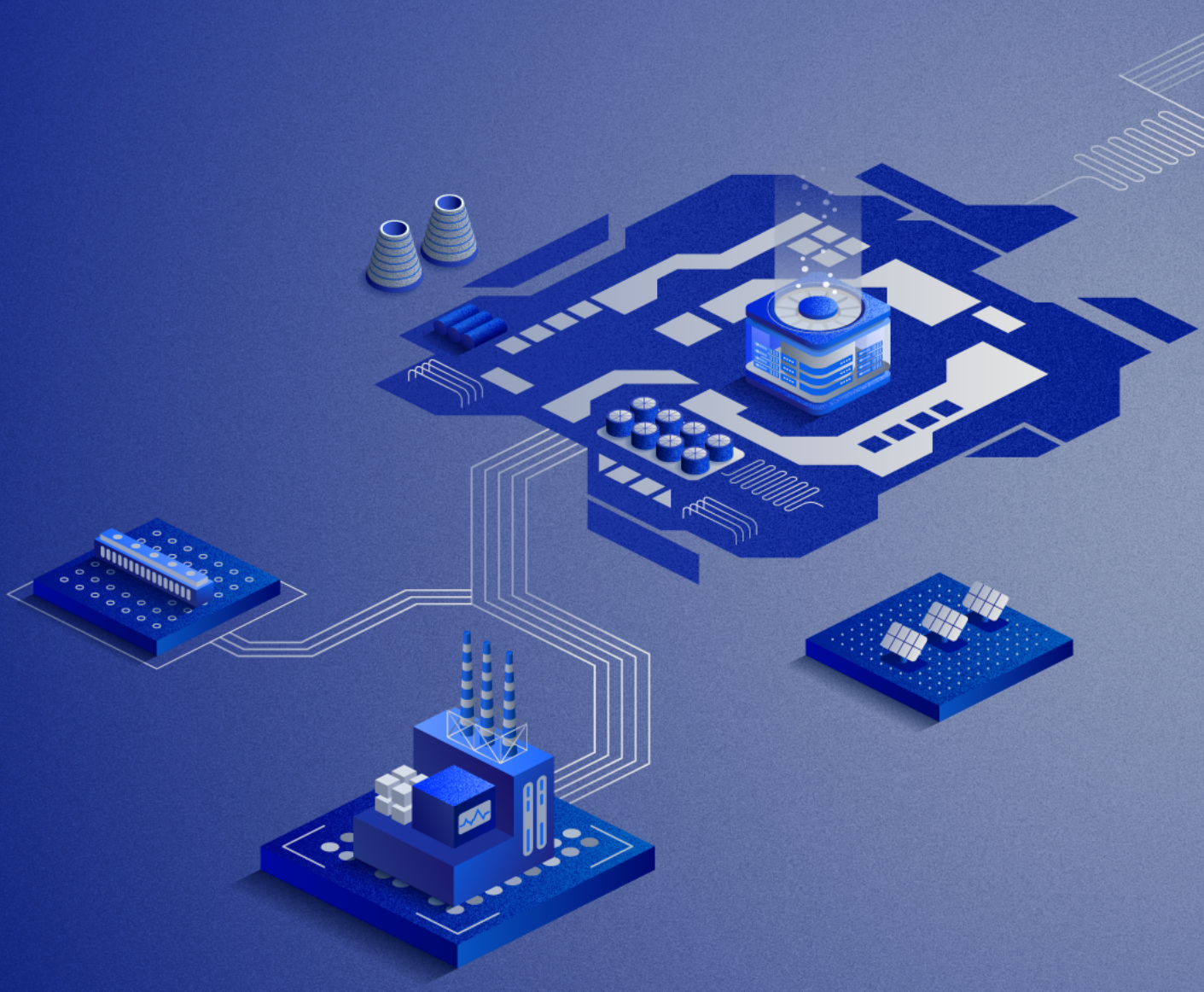
AhnLab CPS PLUS는 CPS 환경의 특수성을 반영한 여러 보안 모듈들을 통합하여 시스템 부하 없이 강력한 보안을 구현합니다.

체계적인 위협 관리

AhnLab CPS PLUS 각 모듈 간 통합으로 '식별 > 탐지 > 대응'으로 이어지는 프로세스를 구현하여 체계적인 위협 모니터링과 대응을 제공합니다.

통합 가시성 및 운영

통합 관리 콘솔 AhnLab ICM으로 CPS 환경의 다양한 자산과 네트워크 현황에 대한 통합 가시성을 제공하며, SIEM, TIP 연동을 통해 향상된 운영 편의성을 제공합니다.



경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2024 AhnLab, Inc. All rights reserved.

AhnLab