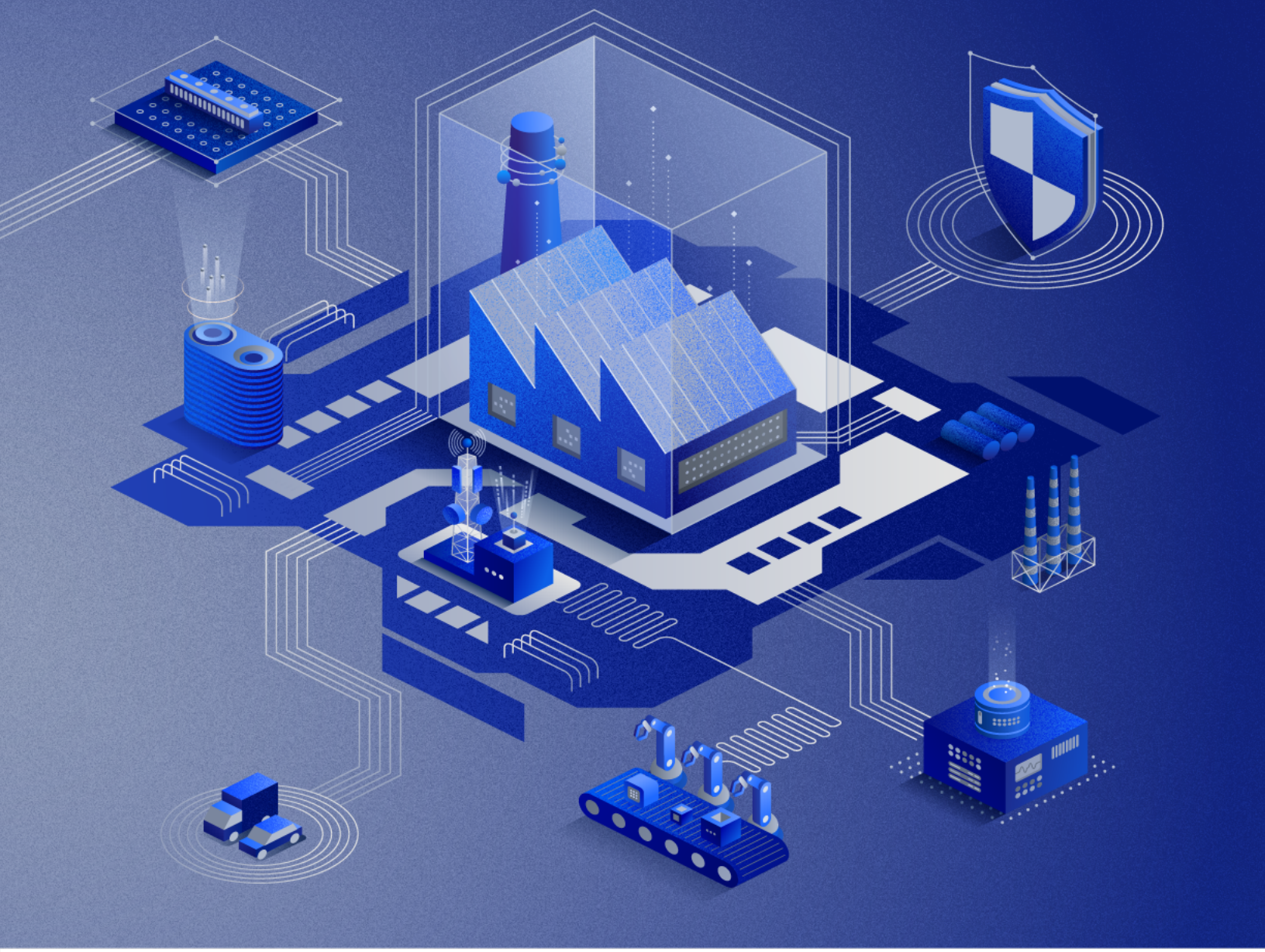
AhnLab



AhnLab CPS PLUS

Unified CPS Protection for Digital Innovation

The CPS protection platform with the most extensive coverage

Challenge

The importance of OT security has been relatively understated due to the closed nature of the environment with strict control over external access. Yet, as digitalization rapidly advanced for OT, more areas became intertwined with the IT network, leading to increased attacks against OT environments with the scale of damage growing as well. Now, organizations should consider a unified security strategy (at least) across IT and OT security to protect their businesses. This is why the concept of “CPS protection” has emerged.

CPS (Cyber-Physical System) represents both cyber and physical aspects of broad systems encompassing OT, IT, IoT, and even the cloud. To protect cross-domain cyber-physical systems, organizations should obtain extensive asset visibility and secure efficiency by leveraging unified management of diverse security modules while ensuring system availability.

Stability Required

Many OT systems that comprise cyber-physical systems are outdated and hard to patch but should stay stable. Organizations must ensure the robust security and continuous availability of these systems while protecting them from sophisticated cyber threats.

Avoiding Fragmented Visibility

Organizations are required to secure comprehensive visibility into assets, networks, vulnerabilities, and cyber threats across a complex OT environment. Also, threat detection and response measures should be taken without compromising system performance.

IT-OT Convergence

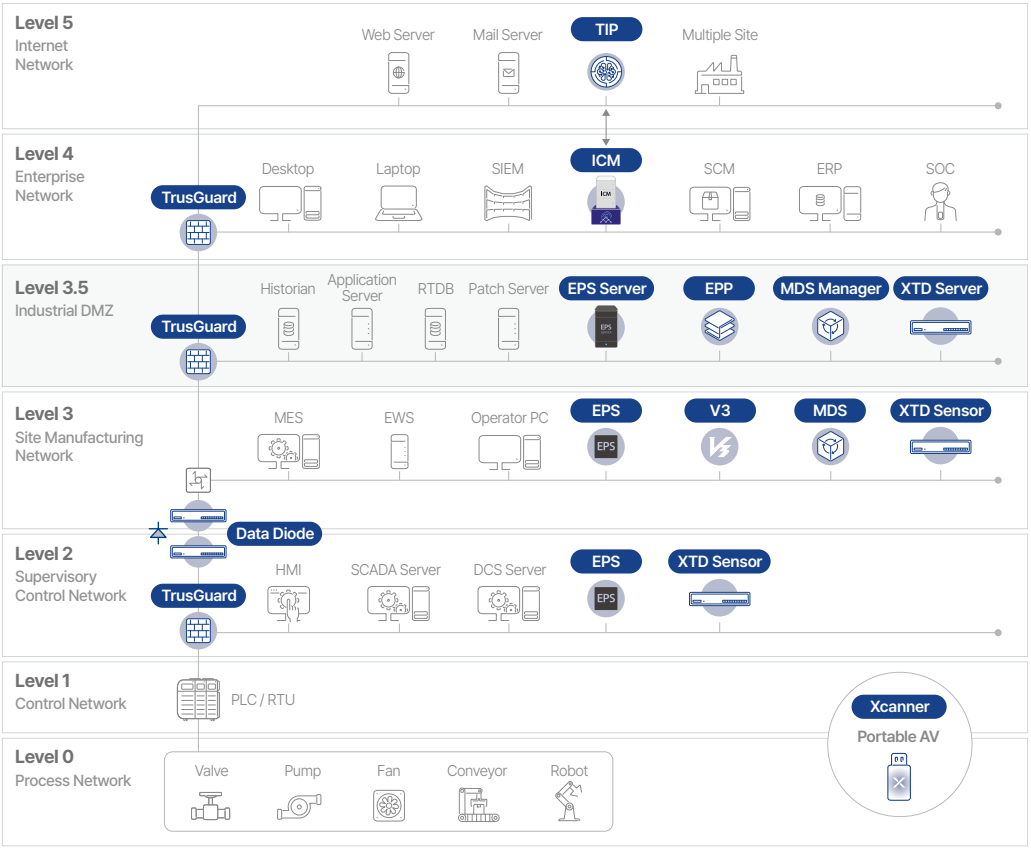
Current OT systems with more attack surfaces demand an IT-OT converged security approach from a CPS perspective. It is time for organizations to accelerate a platform-centric approach powered by seamless integration of security modules and central management.

Why AhnLab CPS PLUS

AhnLab CPS PLUS is our unified CPS protection platform that secures cyber-physical systems across OT endpoints, networks, and IT domains connected to OT networks. The platform has been protecting the CPS environments of customers from various industry verticals, encompassing manufacturing, gas, energy, transportation, etc.

The platform sets itself apart from competitors by providing one of the most extensive CPS protection coverages. Rooted in the platform-centric approach that enables the interoperation of security modules, AhnLab CPS PLUS delivers the next-level customer experience with enhanced efficiency and productivity.

Powered by our threat detection and response capabilities and OT-specialized technologies, AhnLab CPS PLUS delivers seamless protection for cyber-physical systems based on the process of “identification > detection > response". The platform is comprised of nine security modules, and core modules are centrally managed by AhnLab ICM, the platform's management console.



AhnLab ICM
Central monitoring and management of CPS protection modules

AhnLab EPS
Application/device control and malware detection for OT endpoint

AhnLab XTD
OT network visibility & threat and anomaly detection

AhnLab Xcanner
Portable AV scanning and cleaning malware for OT endpoint

AhnLab TrusGuard
OT network segmentation and perimeter security

AhnLab Data Diode
OT network access control via unidirectional data transfer

AhnLab MDS
Network sandboxing for addressing unknown malware

AhnLab EPP/V3
Endpoint protection for IT systems in CPS environments

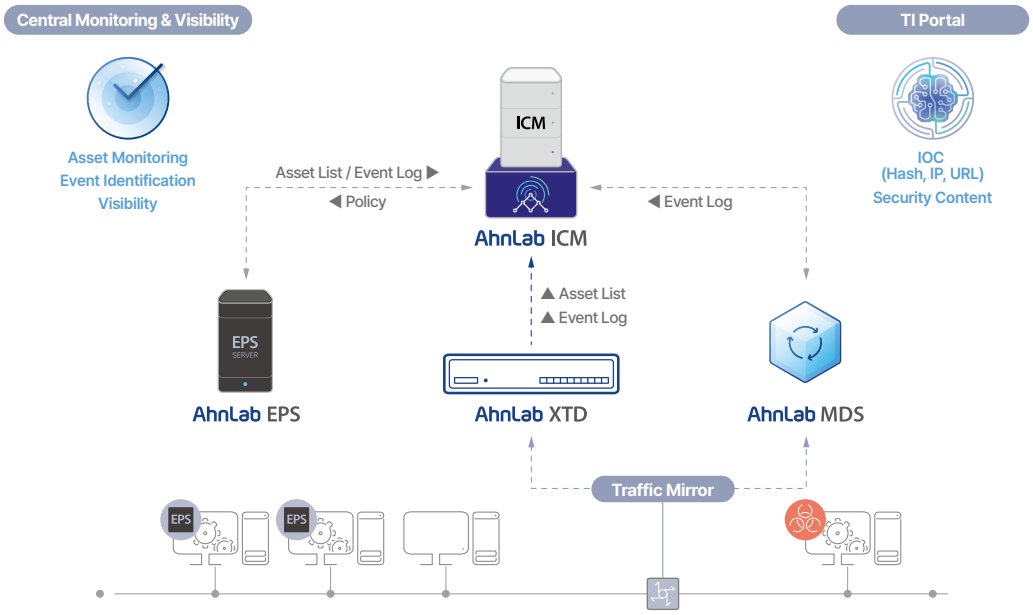
AhnLab TIP
CPS threat intelligence across IT and OT environments

Module of AhnLab CPS PLUS

1. AhnLab ICM (+TIP)

AhnLab ICM delivers holistic visibility across cyber-physical systems on the intuitive dashboard, which centrally monitors and manages core CPS protection modules. Integrated with AhnLab EPS, XTD, and MDS, ICM displays each module's real-time status and log so that administrators can understand and identify issues that need to be addressed immediately. ICM's central monitoring and management capability truly fuels customers' acceleration of business continuity, efficiency, and productivity while enjoying the benefits of the CPS protection platform.

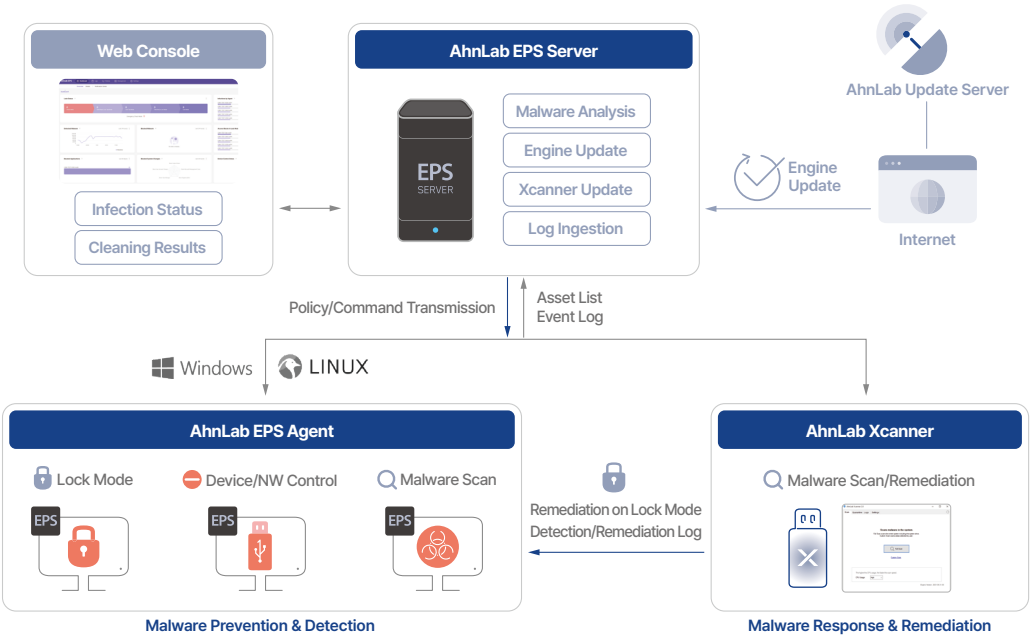
In addition, its integration with AhnLab TIP, our threat intelligence platform, realizes intelligence-driven CPS protection. Customers can check indicators of compromise (IoCs) across cyber-physical systems in real-time and understand the underlying details of cyber threats targeting IT and OT environments.



2. AhnLab EPS & Xcanner

AhnLab EPS, a cutting-edge OT endpoint security module, essentially blocks unauthorized programs, storage, devices, and network connections. Supporting a wide range of operating systems across Windows, Linux, and embedded OS, including outdated ones lacking security updates, EPS minimizes resource usage with its lightweight agent. Its three-stage operation modes – Unlock Mode, Lock Test Mode, and Lock Mode – grant flexibility, stability, and robust control over OT systems.

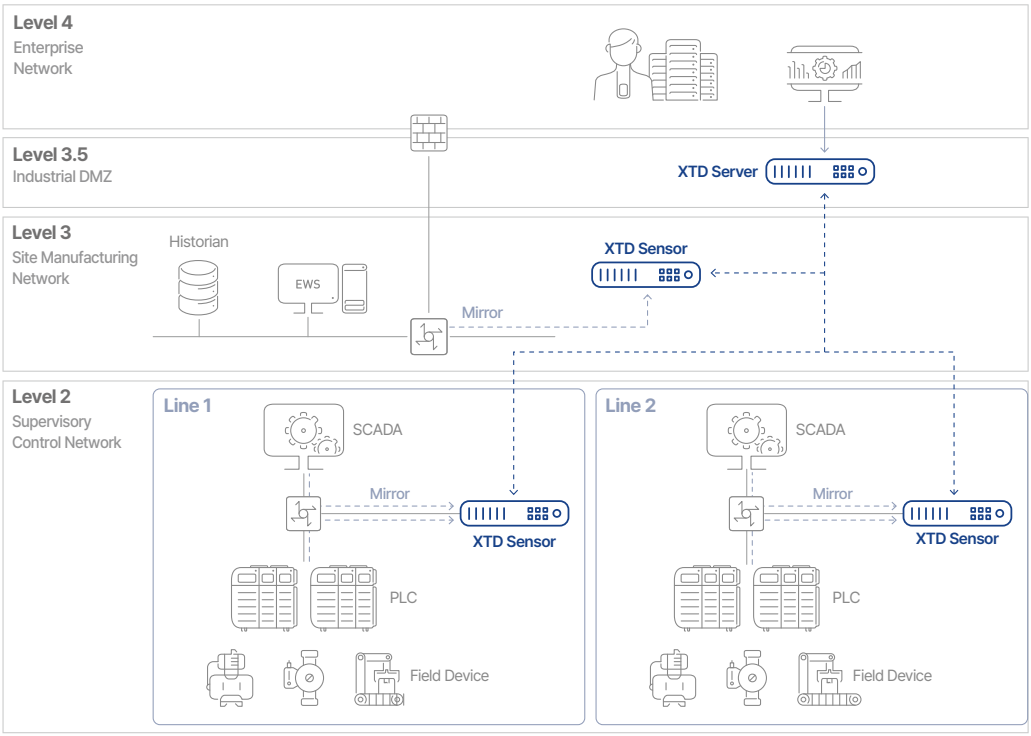
EPS can also detect and prevent known malware targeting OT systems. Once OT machines are infected, AhnLab Xcanner, a portable AV, removes malware from the equipment. The module can be either installed on an authorized USB flash drive or downloaded by the EPS agent. Its inspection, remediation, and related logs can be centrally monitored and managed from the EPS server. We kept the malware remediation process using Xcanner very simple so that even untrained staff can effectively cope with breach incidents.



3. AhnLab XTD

AhnLab XTD is an OT visibility and threat detection module developed to provide comprehensive visibility across OT networks and detect malicious traffic and abnormal behavior in real-time. Prioritizing system availability, XTD leverages the passive monitoring method that mirrors network traffic to minimize the performance impact. Its deep packet inspection (DPI) technology fuels XTD to analyze various OT protocols and enables administrators to identify assets accurately and detect abnormal changes in the settings or commands of OT assets.

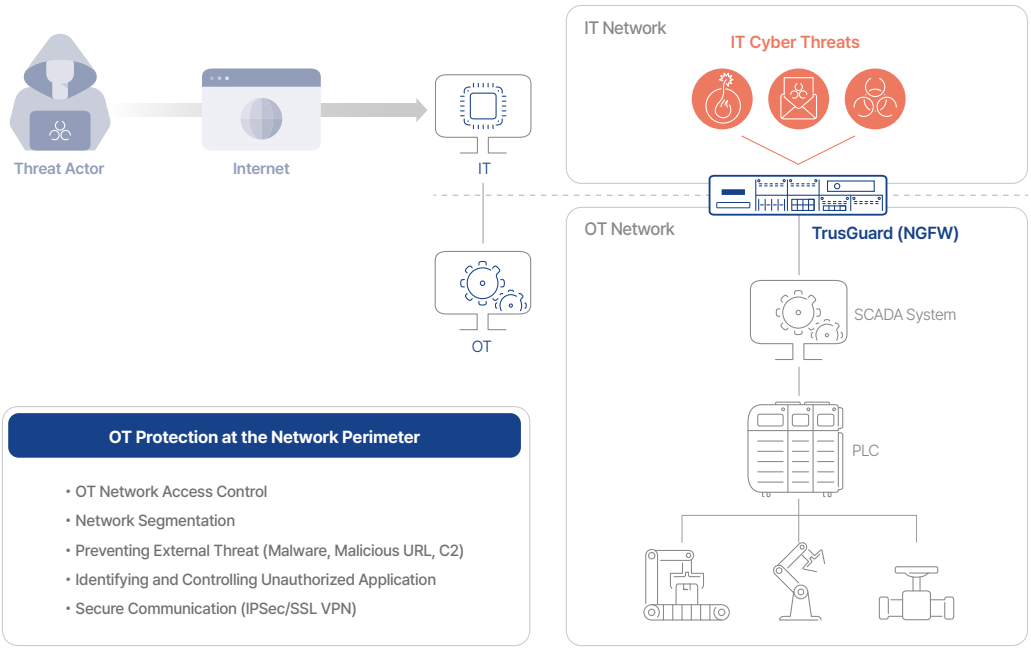
The key strength of XTD is its deep visibility into OT assets and networks powered by integration with EPS, the OT endpoint protection module. Unlike our competitors, who only identify assets at the network level, XTD delivers deeper visibility into OT assets, not just network data but also endpoint information such as CPU, OS version, and patch status of EPS-agent-installed devices. It can also extend its endpoint module integration to AhnLab Xcanner, a portable AV. Once XTD detects malware infiltration or malicious traffic from the network, it can implement malware inspection on suspicious endpoint devices by remotely executing Xcanner to determine whether the system is affected.



4. AhnLab TrusGuard

AhnLab TrusGuard, the firewall module, controls inbound and outbound traffic at the OT perimeter and detects and blocks malicious traffic, including malware, harmful traffic, and C2 connection. It carries out network segmentation to ensure sufficient air-gapping of the OT network and supports secure communications via IPSec and SSL VPN.

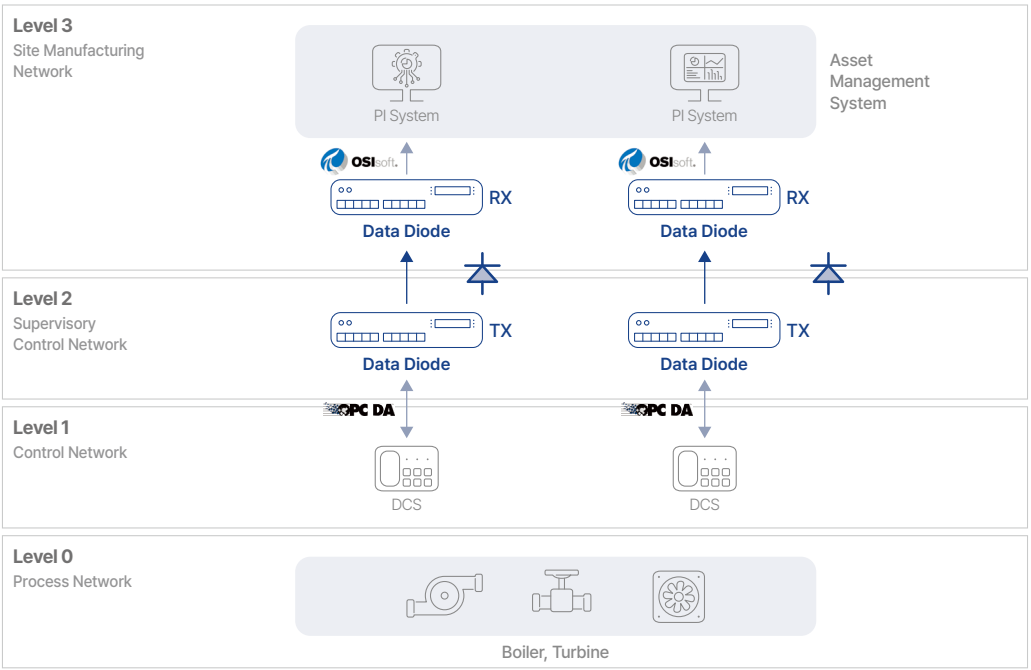
Backed by OT protocol analysis technology, TrusGuard provides delicate control over OT protocols within the network. The module can identify and control protocols, including Modbus and DNP3, as well as function codes.



5. AhnLab Data Diode

AhnLab Data Diode is a simple but powerful security module that strengthens network air-gapping by delivering unidirectional data transfer capabilities. It ensures the separation of the OT network, which tends to be more secure with less exposure, by forcing one-way communication from the OT to the IT network. As a result, customers can safely send data to external networks while restricting data transmission from outside. We applied technologies such as data encryption, forward error correction (FEC), error control, and malware inspection to further reinforce the security and integrity of data.

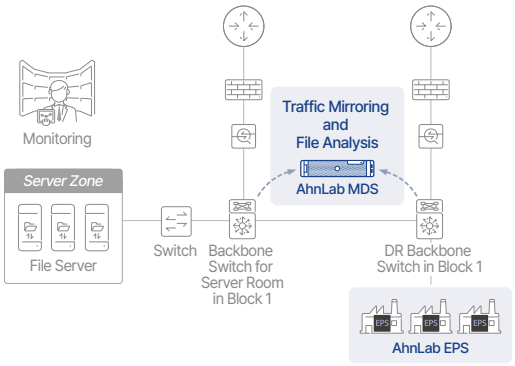
Thanks to our extensive protocol support across IT and OT domains, the module deployment can be optimized for the customer environment. Its flexibility can satisfy various use cases encompassing IT/OT protocols, CCTV streaming, and databases.

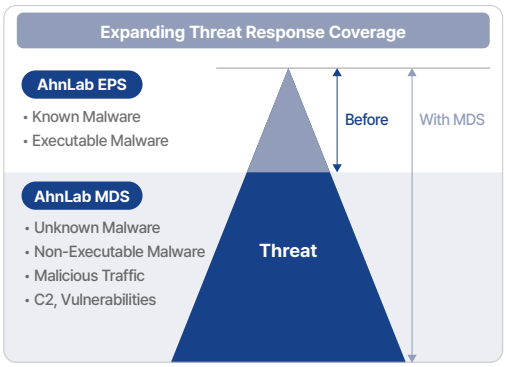


6. AhnLab MDS

AhnLab MDS, the network sandboxing module, collects and analyzes files within the network traffic and performs dynamic analysis on unknown malware. The module can monitor and analyze malware distribution path, C2 connection, and vulnerability while responding to device infection.

Its integration with EPS, which detects and prevents known malware, is particularly meaningful as the platform can extend its threat detection, prevention, and response coverage against known and unknown malware.





7. AhnLab EPP/V3

Organizations should think beyond OT security and consider the IT domain that manages or connects to the OT domain to achieve comprehensive CPS protection. From an IT security standpoint, customers can start by reducing attack surfaces via patch management and preventing malware by leveraging anti-malware.

AhnLab EPP integrates IT endpoint security controls from anti-malware to patch management to prevent IT threats from spreading to OT environments. Its holistic and optimal patch management keeps systems up-to-date and minimizes threat exposure. In particular, V3, the anti-malware module, offers the best-in-industry malware prevention capabilities proven in many anti-malware evaluations, including AV-TEST.

Benefits

Successful CPS protection requires seamless collaboration of multiple security modules. AhnLab CPS PLUS addresses modern CPS protection requirements that can only be solved with a platform-centric approach.

Ensuring Operational Availability

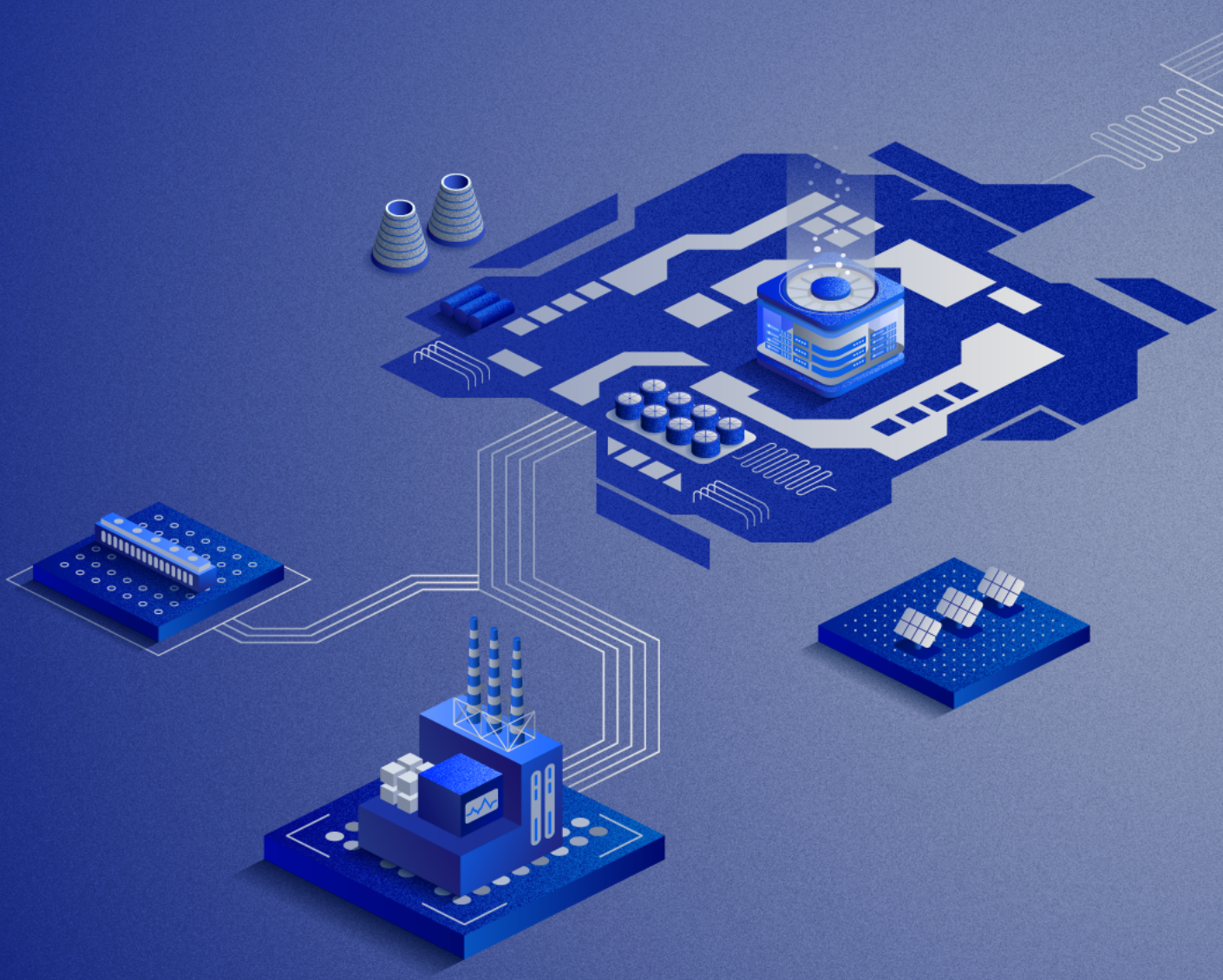
The first and foremost priority of cyber-physical systems is business continuity. AhnLab CPS PLUS's seamlessly integrated security modules deliver powerful and extensive CPS protection capabilities without compromising system performance.

Systematic Threat Management

AhnLab CPS PLUS supercharges customers with a systematic threat management process: identification > detection > response. It provides deep visibility into CPS assets, precisely detects threats and anomalies, and implements optimal responses.

Central Management and Monitoring

AhnLab ICM, the central management console, truly makes AhnLab CPS PLUS a “platform.” ICM enhances visibility and efficiency by consolidating management and monitoring of CPS endpoint and network security modules, TIP, and SIEM.



AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com
© 2024 AhnLab, Inc. All rights reserved.

AhnLab