AhnLab

White Paper

Unified Approach to CPS Protection

Understanding IT, OT and CPS

Organizations are now well aware of IT (Information Technology), about to understand OT (Operational Technology), and are starting to learn about the concept of CPS (Cyber-Physical System). How should we define them? How are they related to each other? What is the best way to secure today's consolidated environment? Let's find out.

First, OT stands for operational technology, monitoring and managing devices and infrastructures across industrial environments. In addition, OT security refers to actions or systemsthat protect OT environments.

Then, we should understand the difference between IT security and OT security. A fundamental difference lies within the terms themselves. While IT security highlights "information", OT security focuses on "operations." Although the two may seem similar at first, organizations will eventually realize that they require entirely different security approaches.

Let's examine IT and OT security in terms of the three pillars of cyber security: confidentiality, integrity, and availability. All of them are essential aspects of security, but IT and OT have different priorities.

Typically, in IT security, the highest priority is given to confidentiality, followed by integrity and availability, thus being abbreviated as "C.I.A." On the other hand, OT security prioritizes availability followed by integrity and confidentiality, abbreviated as "A.I.C". One might ask why the two domains differ in their priorities, and the reason is actually quite simple: computers can be rebooted, but industrial facilities should always stay safe and up and running.

IT and OT environments are composed of different machines. The IT domain comprises devices like desktops, laptops, mobile phones, and servers, while industrial control systems (ICS) are dominant in the OT environment. The exemplary OT machine is a programmable logic controller (PLC) that issues commands to pumps, valves, and robot arms in facilities. Equipment in IT and OT domains also have different life spans – 3-4 years for IT machines, whereas 20-25 years for those in OT.

There is an essential difference between IT and OT, and it is why two domains are usually separated using a DMZ. Until now, 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.

Thus, 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 represents both cyber and physical aspects of broad systems encompassing OT, IT, IoT, and even the cloud. It goes beyond typical manufacturing facilities and covers smart factories, medical systems, autonomous vehicles, etc. 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.

Breach Cases

Traditional OT machines tend to possess various vulnerabilities. They often run outdated systems over ten years old and have insufficient patches, so damage from cyberattacks can easily be spread. Such traits of OT equipment put the entire cyber-physical systems and businesses at stake.

The manufacturing and water supply industries have reported recent major CPS security incidents. Some cases have also targeted social infrastructures such as power plants and energy facilities. The attack types can be classified into two categories. The first involves applying IT attack techniques to the OT environment. There has been an increasing trend of infecting OT machines with ransomware, like in IT devices, and malware that exploits residual vulnerabilities. The second involves modifying control commands to disrupt the operation processes.

First, the WannaCry ransomware infection at the Taiwanese semiconductor company TSMC in 2019 forced the organization to shut down its factories for approximately 48 hours, resulting in significant financial losses. The ransomware infection at TSMC initially began due to using a compromised USB device within the internal OT network, which quickly spread through the "Eternal Blue" vulnerability. There was also collateral damage as ransomware propagated to other overseas factories connected to the affected facility.

The second case is the incident at the water treatment facility in Oldsmar, Florida. The attacker infiltrated the OT network and extorted account credentials to access systems by planting malware on a website that was likely to be visited by the facility administrator. They then attempted to manipulate the concentration of sodium hydroxide by using the remote access program "TeamViewer." Fortunately, the administrator, who had been monitoring at the time, prevented further attacks by detecting the unusual mouse movements. Nevertheless, the incident could have become a disaster, changing the drinking water supply for thousands of citizens into lye water.

Understanding CPS Threats

A cyber-attack against cyber-physical systems is complicated as OT systems are more exposed to external environments than ever before. However, if we must keep the concept simple, then it can be described as striking OT systems by leveraging IT (or external) networks, assets, and practices, thereby compromising the entire cyber-physical systems.

In that sense, cyber threats around cyber-physical systems usually occur through IT networks, remote control programs, storage devices, third-party access, or supply chains.

1. IT Network

As explained, OT systems are normally separated from external access, but recent digitalization has been expanding IT-to-OT access. Insufficient network segmentation is a great entry point for OT-targeting attacks, including malware.

2. Remote Control Program

Many OT machines are managed via remote control programs. Once threat actors gain control of these programs, they can easily manipulate or damage OT systems. Thus, organizations must prevent the leakage of any account credentials of remote-control programs.

3. Storage Device

OT systems can be directly connected to storage devices such as USB drives. Theoretically, the maintenance personnel should scan all storage devices using anti-malware programs before connecting devices to the production line system. However, if a storage device is used without proper scanning, it can be infected by malware such as worms or ransomware. There may also be a case where the vulnerable internal system infects the storage device and spreads malware to other systems. In extreme cases like the TSMC incident in Taiwan, malware that is able to self-propagate can halt the entire production line.

4. Third-Party Access

Partner companies that perform machine maintenance often have direct access to OT systems. If the attacker can place malware into storage devices and other utilities used by partner companies, they can directly compromise the internal systems.

5. Supply Chain

OT machines are usually created and delivered by dedicated manufacturers. The attacker can target these manufacturers by planting malware in their programs and amplify the damage. The "Havex" malware discovered in 2013 is a notable case that malware was injected into the installation file on a software manufacturer's website. It becomes difficult to trace the origin of malware if it comes from compromised supply chains.

Understanding the Architecture

It is crucial to understand the structure of cyber-physical systems to establish an effective security strategy. The "purdue model" that segments OT layers from Level 0 to Level 5 has been widely received as a standard for building the OT security architecture. Although the next-gen cyber-physical systems will go beyond the purdue model, the model is still very effective in protecting CPS environments and meeting IT-OT converged security requirements of today and the near future.

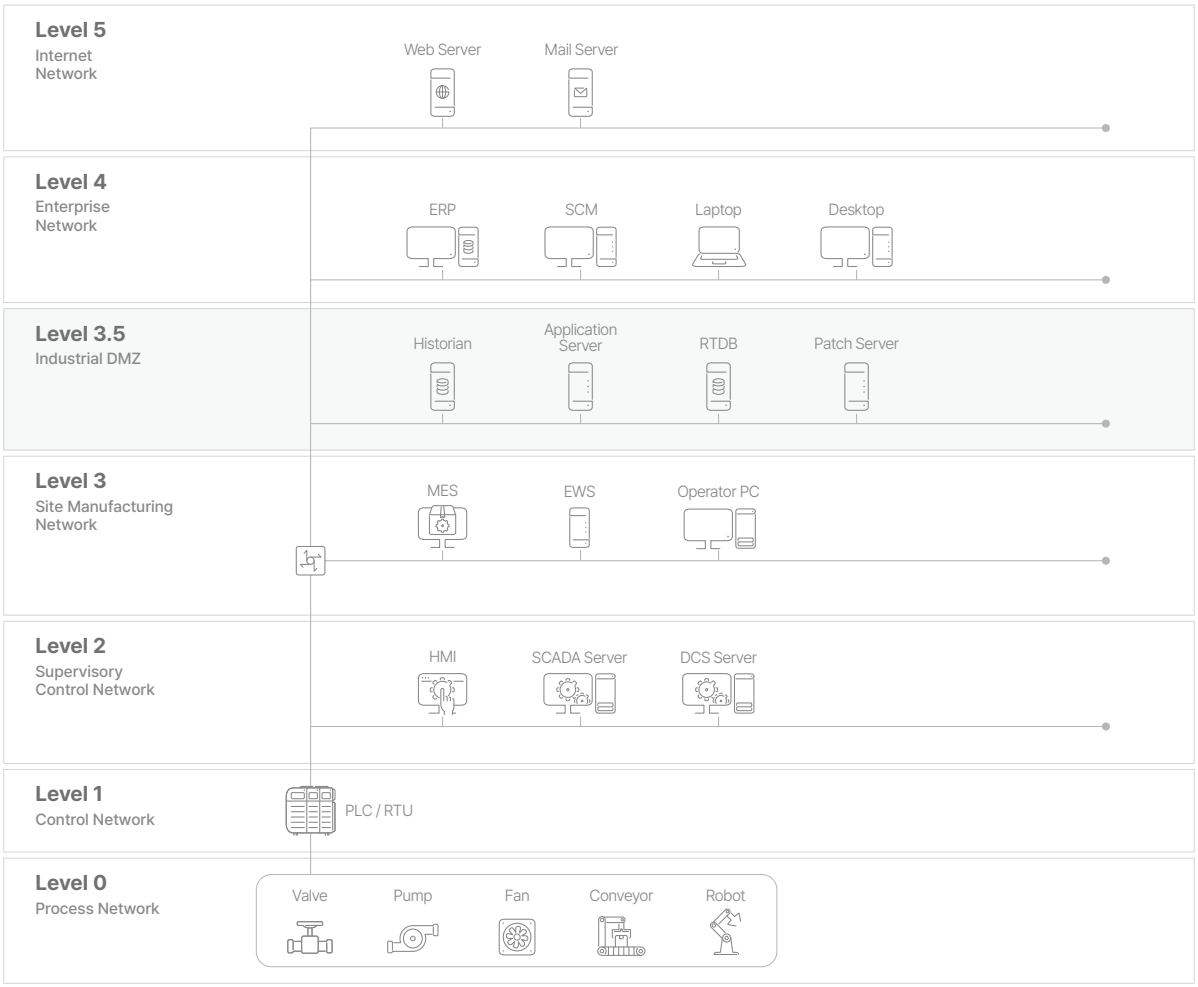

Figure 1. Purdue Model

Level 0: Process Network - This is the level for physical devices operating in the facility. It consists of sensors such as valves, pumps, conveyors, and robots that collect data from production devices. Actuators receive commands from level 1 machines such as switches.

Level 1: Control Network - Level 1 processes commands from Level 2 and delivers them to Level 0. It also sends information and data collected from Level 0 to Level 2. Major devices are programmable logic controllers (PLC) and remote terminal units (RTU), which are responsible for issuing commands and controlling devices at Level 0.

Level 2: Supervisory Control Network - Level 2 has systems that manage and operate lower-level devices. Systems include supervisory control and data acquisition (SCADA) and human-machine interface (HMI). SCADA collects field data through PLC and RTU in level 1 and controls multiple devices simultaneously. The HMI allows operators to control the devices in a specific area of the manufacturing process.

Level 3: Site Manufacturing Network - Level 3 manages the entire production system and enhances operational efficiency. It consists of systems such as the manufacturing execution system (MES) for optimizing production activities, engineering workstations (EWS) for controlling devices, and product lifecycle management (PLM) for managing product lifecycles. It also hosts the main HMI to control the entire facility.

Level 3.5: Industrial DMZ - Also known as the industrial demilitarized zone, this level is where the OT network is connected to the external IT environment. It includes real-time databases (RTDB), historians, application servers, and patch servers. With the increase in OT breaches and the focus on the importance of IT-OT unified security, more attention has been drawn to this level.

Level 4: Enterprise Network - Level 4 consists of resources generally used by companies in IT environments, such as enterprise resource planning (ERP), supply chain management (SCM), and customer relationship management (CRM). This is where administrators manage company-wide IT systems related to production.

Level 5: Internet Network - Level 5 is the layer that directly faces external networks. This layer has public-facing assets such as mail servers and web servers.

How CPS Attacks Play Out

From the CPS protection perspective, we can segment the purdue model based on the network perimeter. The levels can essentially be divided into the IT network (levels 4 - 5) and OT network (levels 0 - 3.5), and the OT network can be further divided into the control network (levels 0 - 2) and operational network (levels 3 - 3.5). The table below summarizes the components of each layer.

Level	Type	Key Components	Description
0	Control network (OT)	· Sensors · Actuators · Production devices	Devices performing field tasks
1		· PLC · RTU	Machines issuing commands and controls field devices
2		· SCADA · HMI · DCS	Systems for remotely managing and operating field devices
3	Operational Network (OT)	· MES · PLM	Machines for overall production system management and operation
3.5	Industrial DMZ	· RTBD · Historian · Application servers	Interfaces or buffer areas between OT and IT domains
4	Enterprise Network (IT)	· ERP · SCM · CRM	Managing IT systems related to production
5	Internet Network (IT)	· Web servers · Mail Servers	Assets directly facing external networks

Table 1. Summary of components per network level

Now, let's examine the flow of cyber-attacks targeting CPS environments.

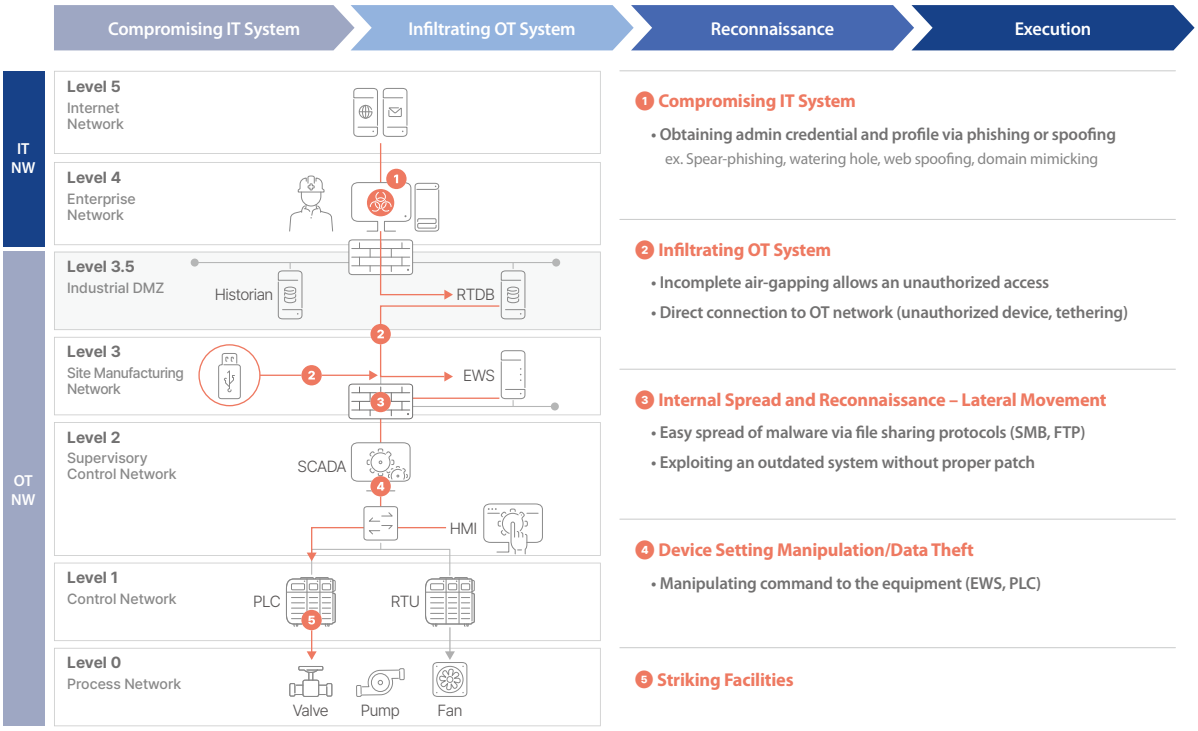

Figure 2. CPS attack process

Keep in mind. CPS attacks usually start from the IT domain. There are incidents due to unauthorized devices directly connected to the OT systems, but most occur as threat actors infiltrate the IT network and move to the OT network. OT networks are usually air-gapped and have narrow attack surfaces, but their connection to IT management systems makes them exposed to credential theft via a compromised IT network. Again, this is why the importance of the "Industrial DMZ (Level 3.5)" where networks are segmented is growing.

Attackers use various techniques, such as phishing and advanced persistent threats (APT), to breach the IT network that manages the OT network. Then, they can steal various profile information such as administrator account details, IP addresses, and URLs required for accessing the OT systems. Afterward, they spot and exploit a weak network air-gapping policy or poorly managed domain to infiltrate the OT network. Also, malware can spread to the OT network through unsafe USB drives. Connecting unauthorized laptops to the field device via mobile tethering can let malware bypass the OT network perimeter security.

Subsequent operations are relatively easy for attackers. They identify the target system and drop malware. The OT environment is filled with SMB ports, remote file transfers, and remote accesses, along with outdated and unpatched systems, perfect conditions for malware to spread at a rapid pace. Also, attackers can strike systems directly by connecting to SCADA or HMI to run abnormal control commands through EWS and PLC or manipulate the device settings.

This is an overview of how CPS attacks usually play out. Again, if you are considering proper CPS protection, you should go beyond OT security and (at least) seek IT-OT unified security strategies.

CPS Protection Requirements and Unified Approach

In terms of the approach, OT security is no different from IT security since it requires the same process of "identification > detection > response". However, to effectively respond to the latest OT security threats, it is important to design the IT & OT converged security system that can cover all aspects: the OT domain, IT and OT connection, and IT domain. IT & OT converged security should be capable of securing endpoint, network, and ICS based on the previously mentioned process. The figure below is a summary of the entire process and the requirements for each security domain.

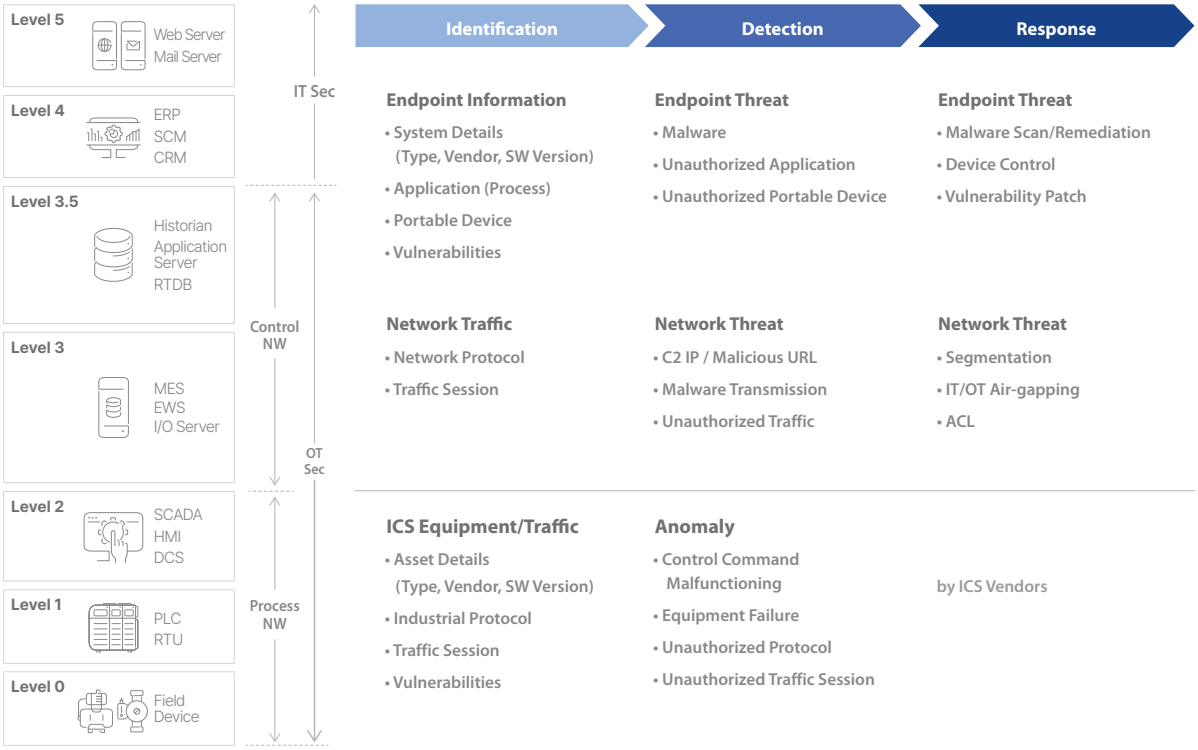

Figure 3. CPS protection process and requirements for each domain

A. Identification

The "identification" refers to obtaining transparent visibility on assets and relevant information; visibility is crucial as it establishes the foundation of adequate CPS protection.

There are various assets with long lifecycles in OT networks, making it challenging to centrally manage their location, status, and network communication. If assets are not precisely identified, it becomes very difficult to detect and respond to cyber threats or device malfunctions that may compromise system availability.

In CPS environments, there are two visibility criteria: assets and networks. Asset visibility means gaining a view of entire devices in the control network as well as servers and workstations in the operational network. Network visibility represents the view of network sessions between assets and multiple IT/OT protocols.

Due to the characteristics of OT environments where asset or network changes seldom occur, identified elements can be used as a standard to detect unidentified cyber threats and abnormal activities.

For the control network, organizations should monitor asset details such as asset type, vendor, software version, OT protocol, and traffic session. It is particularly important to be able to analyze and standardize different OT protocols.

Moving on to the operational network, there are security requirements for both endpoint and network domains. In the endpoint domain, visibility into system details - system type, vendor, software version, etc. - must be obtained. In addition, organizations should identify the application, process, and removable device in use across the entire environment. As for the network domain, network protocols, and traffic sessions should be monitored at all times.

B. Detection

After obtaining visibility through identification, all present threats and abnormalities in the CPS environment must be detected.

First, abnormalities around OT machines within the control network should be checked. Administrators need to carry out comprehensive monitoring to detect control command malfunctions, device failures, and the presence of unauthorized protocols and traffic sessions to secure the facility's stability.

The operational network requires continuous monitoring of malware, lateral movement, unauthorized applications, and removable devices around OT endpoints. Also, ongoing detection of cyber threats such as malware transmission and unauthorized traffic is needed.

C. Response

Response refers to finding the most optimal measure against breaches and anomalies that were identified or detected to minimize the damage to operations. Considering its unique nature, a cyber-physical system demands collaborative support from security professionals and OT personnel regarding incident response; the utmost priority of CPS protection is always to ensure operational continuity.

Although response options are limited in the CPS environment compared to the IT domain, there is room for proactive incident response in the operational network. Administrators who detect malware against OT endpoint machines can perform scanning and remediation to address the issue. Also, there is a way to enhance the security postures of the CPS environment by leveraging device control and patch management features. On the network side, proper network segmentation is one of the most basic but useful practices to ensure the security of the CPS environment. Then, implementing solid access control will be the ice on the cake.

Suppose you are looking for security controls to build a systematic architecture. The baseline will be a dedicated IDS for gaining visibility across assets and cyber threats, along with a firewall for network segmentation. Harnessing unidirectional data transfer will further enhance communication safety between OT and external networks.

To safeguard the endpoint of cyber-physical systems, allowlist-based application and device control is required to prevent any unauthorized execution. Patch management and portable anti-malware can help organizations reduce attack surfaces and remove malware from OT machines. In addition, organizations must keep their IT devices safe to make entire cyber-physical systems secure. Implementing a robust endpoint protection platform (EPP) will be a great start.

Above all, security controls must be centrally managed as requirements for protecting current sophisticated cyber-physical systems are beyond a point-product-based approach. Organizations should pursue a platform-centric approach that supercharges them with unified monitoring and management capabilities.

AhnLab CPS PLUS: Unified CPS Protection Platform

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.

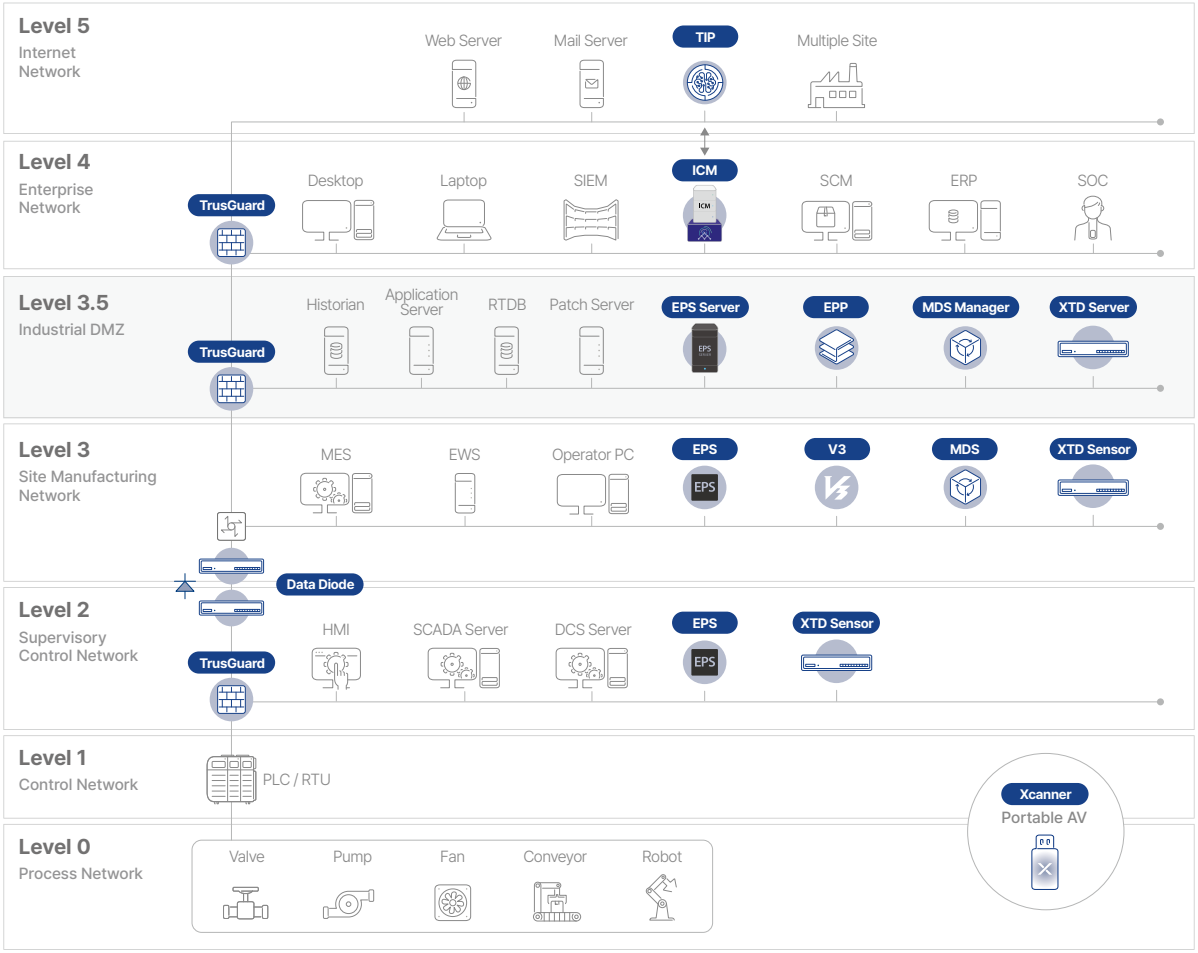

Figure 4. AhnLab CPS PLUS

AhnLab ICM
Central monitoring and management of CPS protection modules

AhnLab EPS
Portable AV scanning and cleaning malware 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
Anti-malware and patch management for IT systems in CPS environments

AhnLab TIP
CPS threat intelligence across IT and OT environments

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.

Domain	Module	Phase 1 Monitoring & Identification	Phase 2 Threat Detection	Phase 3 Response	Phase 4 Follow-up Actions
IT & OT	ICM	• IT & OT Asset List	• Log Analysis • In-depth Analysis Report	• Managing Lockdown Exceptions • Checking Agent Policy Status	• Checking Remediation Status • Applying Rest API Policy
Endpoint (OT)	EPS	• Equipment Identification	• Known Malware	• Malware Scan • Blocking Unauthorized Process • Blocking Device Execution	• Lock Mode Activation • AhnReport Analysis Request
Network (OT)	XTD	• OT Asset Identification • Traffic Identification by Asset	• Malware Propagation • Network Threat (Vulnerability) • Abnormal PLC Logic	• Threat Detection/Response Alert	
Endpoint (OT)	Xcanner			• Malware Scan/Clean on Devices	
IT & OT	TrusGuard		• Network Threat • Unauthorized Traffic	• Blocking Unauthorized Sessions • Blocking Malicious Traffic	• Firewall Policy Settings • Network Segmentation
Network (OT)	Data Diode			• Unidirectional Data Transfer	
IT & OT	MDS		• Unknown/Known Malware • Network Anomaly • Behavior Analysis Evasion	• Detection Validation • Pinpoint Analysis	
Endpoint (IT)	EPP/V3	• Patch Management	• IT Malware	• IT Malware Remediation	• EPP/AV Policy Settings
IT & OT	TIP				• Threat Intelligence Lookup

Figure 5. AhnLab CPS PLUS modules and their roles

Role of CPS Protection Modules

Our nine CPS protection modules serve different roles but have the same objective: protecting cyber-physical systems. Let's examine their functions and how they interoperate with each other.

ICM (+TIP)

The first and foremost requirement for a security platform is central monitoring and management backed by seamless integration; this is what AhnLab ICM does. Administrators can gain holistic visibility across cyber-physical systems on the intuitive dashboard, which centrally monitors and manages core CPS protection modules.

Integrated with security modules, including 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.

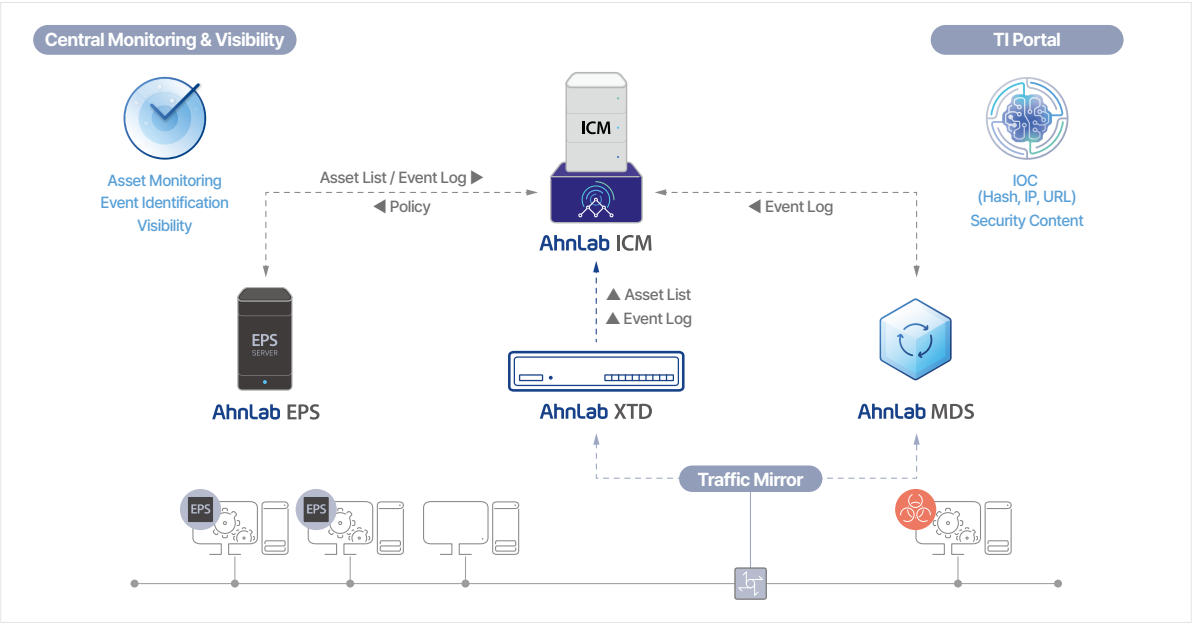

Figure 6. Central management architecture of AhnLab ICM

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.

EPS (+Xcanner)

A cutting-edge OT endpoint security module, AhnLab EPS has been protecting diverse manufacturers and power plants for a decade. Its intuitive web-based console enables precise identification and unified management of OT machines scattered across facilities. Also, it does all the heavy work, such as in-depth analysis on its server, and always keeps its agent light to guarantee operational stability. It supports Windows and Linux operating systems, even outdated ones lacking security updates and patches.

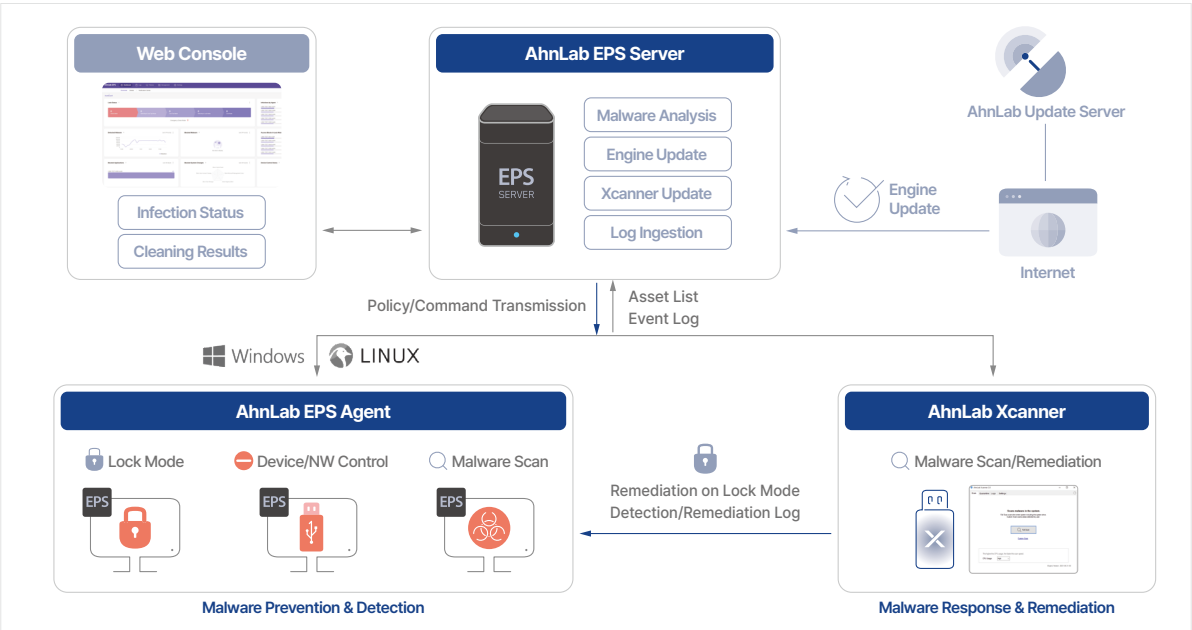

Figure 7. Structure of AhnLab EPS and Xcanner

The module's core strength is its allowlisting technology, which allows only authorized devices and networks to run in the system, minimizing the possibility of potential security incidents. This technology also relieves administrators from the burden of drudgery policy configuration tasks, as allowlists are automatically updated on the EPS server and applied to the EPS agent.

EPS empowers customers with convenient management and robust security settings by harnessing the three-stage operation modes: "Unlock Mode" for unlocking systems for system updates, "Lock Test Mode" for testing, and "Lock Mode" for actual operation. The "Lock Mode" prevents any system change besides exceptions to ensure operational stability and continuity.

EPS can also detect and prevent known malware targeting OT equipment. It detects malware at the agent level and performs a robust analysis on its server, delivering real-time detection, analysis, and prevention of malware without compromising system performance.

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.

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 while gaining holistic visibility and precisely detecting cyber threats.

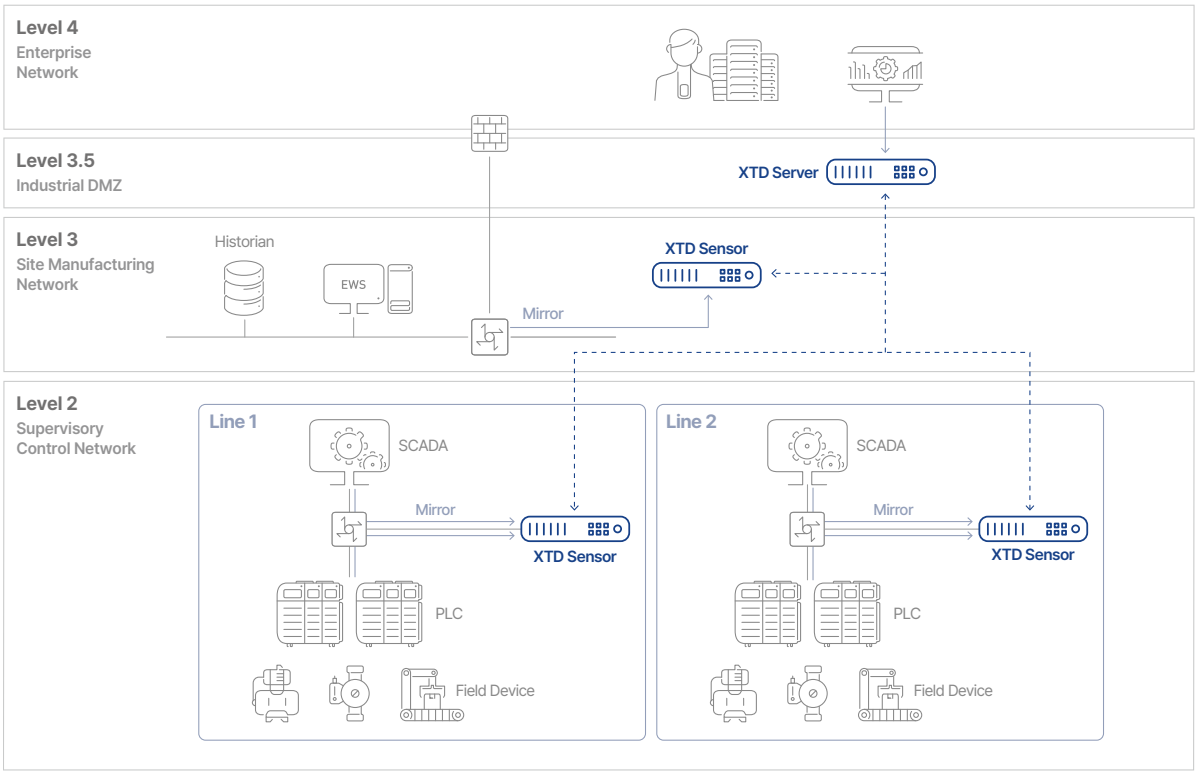

Figure 8. Architecture of AhnLab XTD

Powered by deep packet inspection (DPI) technology, XTD analyzes 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.

Its synergy with endpoint protection extends to malware detection and remediation by leveraging Xcanner. 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.

In addition, XTD also helps customers track the source of cyber threats. Administrators can trace back the path of cyber threats and identify where malware or malicious behavior has begun and how threat actors performed lateral movement. It allows them to address not just imminent attacks but also the root cause of cyber threats by understanding the full picture.

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.

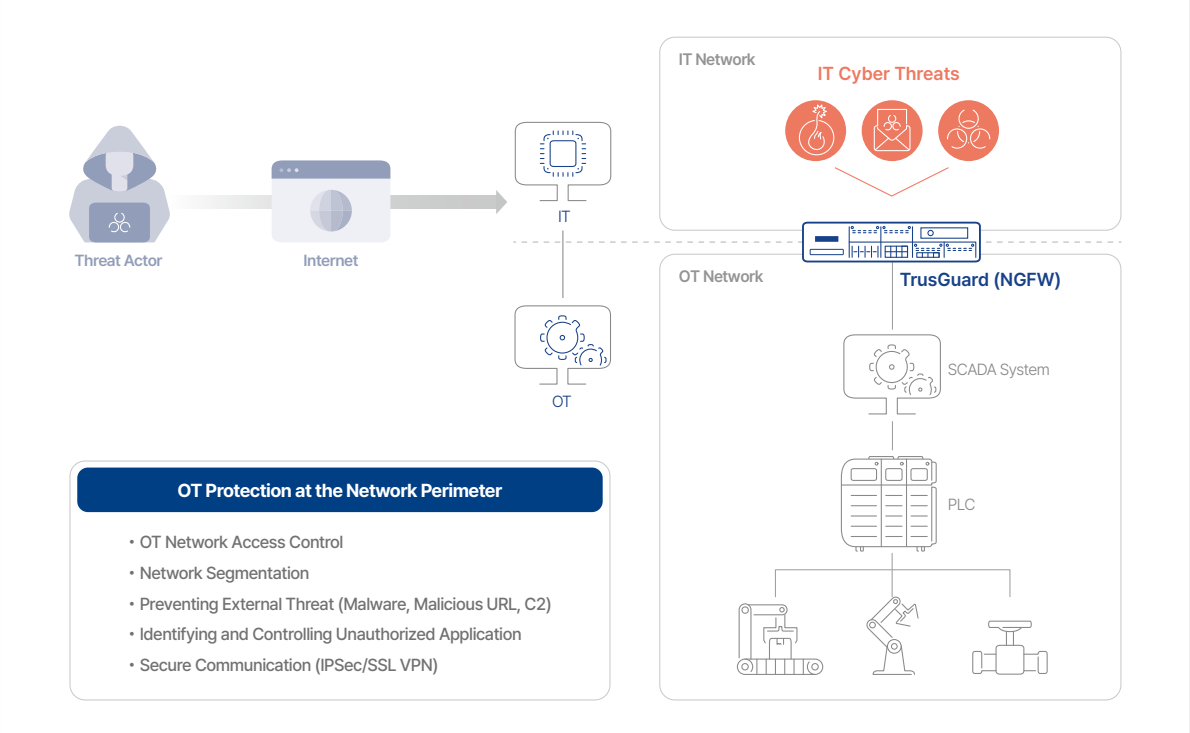

Figure 9. AhnLab TrusGuard performing a perimeter security

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.

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.

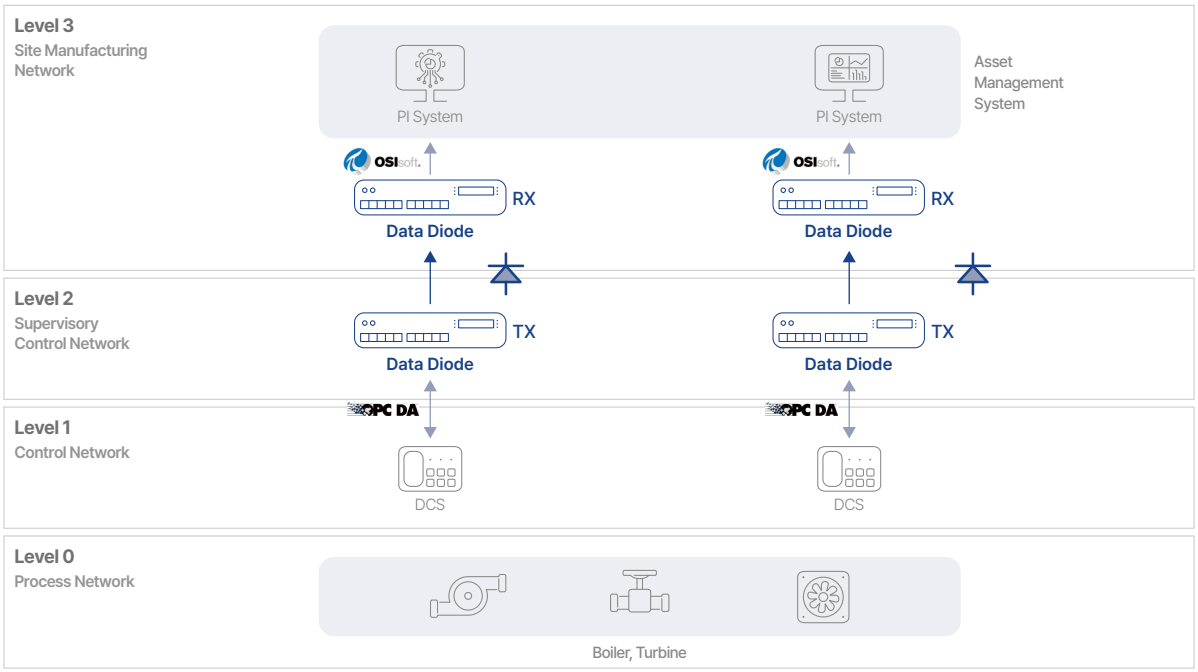

Figure 10. Architecture of AhnLab Data Diode

Thanks to our extensive protocol support across IT and OT domains, customers can flexibly deploy the module in their OT environment. Its flexibility can satisfy various use cases encompassing IT/OT protocols, CCTV streaming, and databases.

MDS

As cyber threats continue to evolve, there has been a rise in APTs and new malware variants. Therefore, it has become paramount to be able to analyze and respond to unknown malware in addition to those already known.

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.

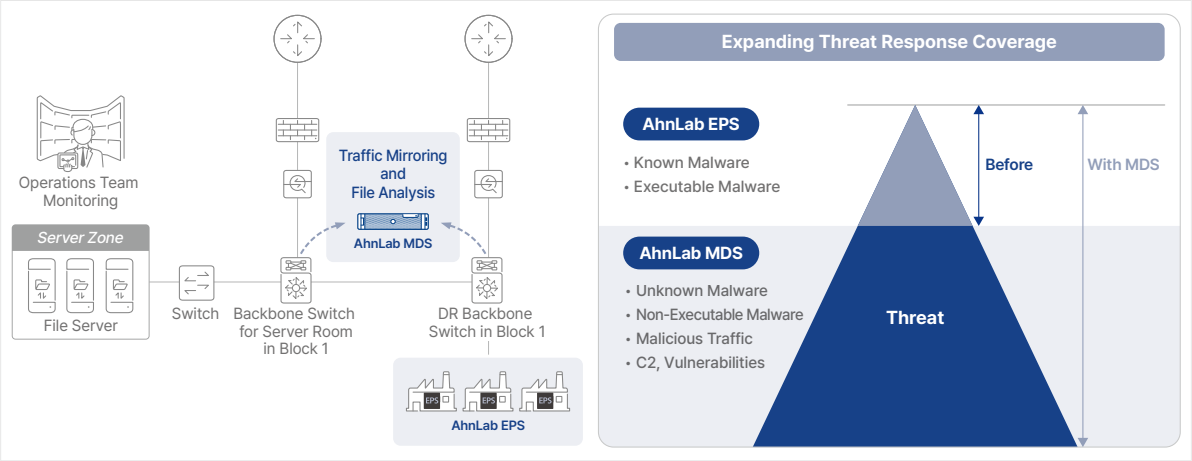

Figure 11. Architecture of AhnLab MDS and EPS

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.

AhnLab EPP/V3

As mentioned earlier, customers should think beyond OT security and consider the IT domain that manages or makes connections 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.

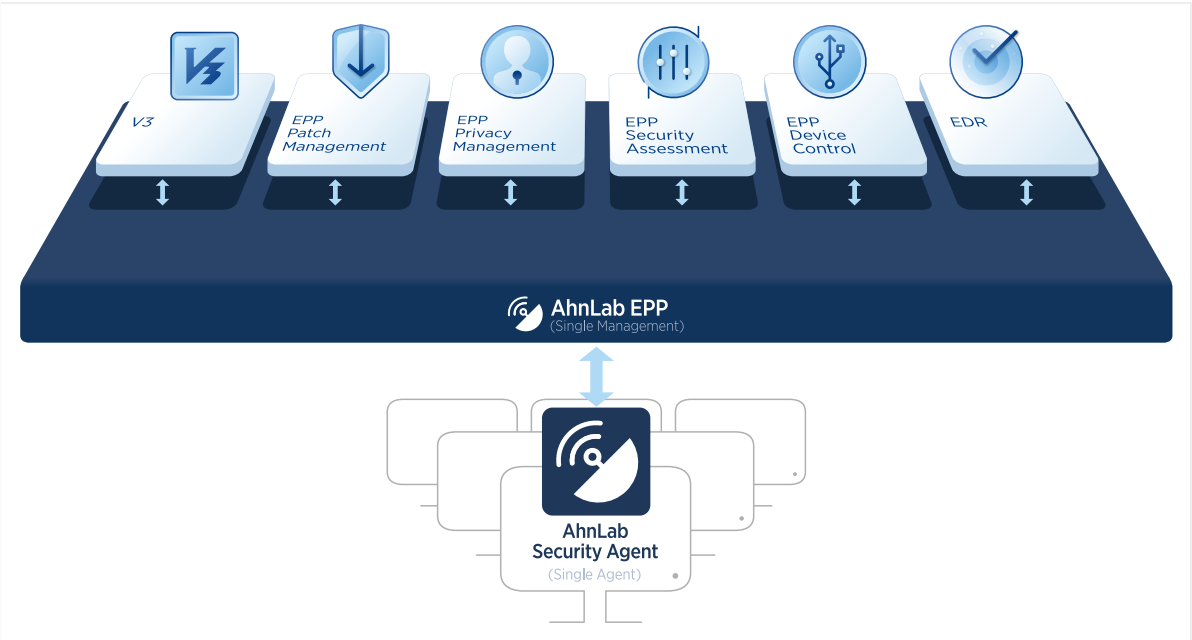

Figure 12. AhnLab EPP

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

AhnLab CPS PLUS unifies IT and OT security to help customers successfully address CPS protection requirements. By doing so, organizations can truly accelerate their journey to digital innovation.

Benefit #1: Ensuring Business Continuity

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.

Benefit #2: Systematic Threat Management

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

Benefit #3: Central Management and Monitoring

AhnLab ICM, the central management console, truly makes AhnLab CPS PLUS a "platform." ICM enhances visibility and operational efficiency by consolidating management and monitoring of CPS endpoint and network security modules, the threat intelligence platform (TIP), and even security information and event management (SIEM).

Conclusion

Cyber-attacks against cyber-physical systems are constantly escalating, and the scale of damage is expected to be greater than in the past. Organizations have just begun understanding OT security, but now we must start thinking of IT and OT, two completely different environments, together. It may sound too much for organizations, but at the same time, it is not an impossible mission if we have a proper understanding, approach, and architecture regarding CPS protection.

In that sense, here are three principles that you should keep in mind as you drive the CPS protection initiative.

#1. IT security must be taken into consideration along with OT security.

Cyber threats against OT environments often originate from IT domains connected to OT networks. Future cyber-physical systems are expected to go beyond IT and OT, but for now, organizations should take an IT and OT converged approach to achieve sufficient CPS protection.

#2. Pursue the process of "identification > detection > response" by default.

Asset identification, threat detection, and response are fundamentals of CPS protection. Also, changes are rarely made to assets or networks in OT environments. Establishing the baseline of the process that enables proper threat response based on deep asset visibility and precise threat detection will be helpful.

#3. Go beyond point-product. Pursue a platform-centric approach.

Today's CPS attacks are already beyond the level that a single product can solve, and they will get worse in the future. This situation demands a CPS protection platform comprised of multiple modules seamlessly integrated with each other. The platform delivering optimal features, unified visibility, and central management is the only way to tackle ever-evolving CPS attacks.

Amid the sophistication of CPS attacks, AhnLab is the perfect partner for addressing the evolving needs of CPS protection. AhnLab CPS PLUS sets itself apart with the most extensive protection coverage powered by central monitoring and management of security modules interoperating with each other. Consequently, the platform's excellence has been proven by numerous references across multiple industries. In the future, we will further enhance each security control while deepening integration between modules to support the use cases of tomorrow.

AhnLab

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