AhnLab XTD

Deep Visibility into OT Assets and Cyber Threats

AhnLab XTD delivers comprehensive visibility across OT networks and detects malicious traffic and abnormal behavior in real-time.

Overview

AhnLab XTD is an OT visibility and threat detection solution developed to provide comprehensive visibility across OT networks and detect malicious traffic and abnormal behavior in real-time. Prioritizing system availability, the solution leverages passive monitoring that mirrors network traffic to minimize the performance impact. The deep packet inspection (DPI) technology fuels AhnLab 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.

Visibility

Asset visibility & protocol analysis (DPI)
Network session & topology

Detection

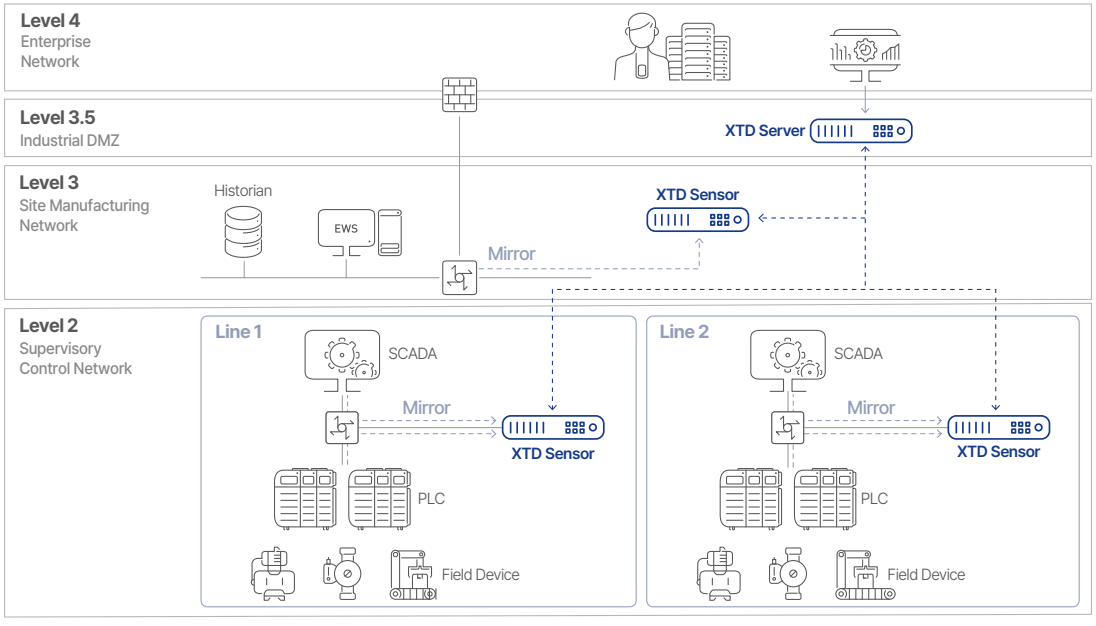
Cyber threats (malware, etc.)
Abnormal protocol & control logic

Availability

Mirror mode for availability
No changes to NW configuration

System Configuration

AhnLab XTD is composed of a central server and sensors across extensive network layers. Deployed at every corner of the OT network, the sensors analyze mirrored traffic and forward the analysis results to the central server, which then processes the ingested data to identify cyber threats and enable proper security policy configurations. AhnLab XTD also delivers an all-in-one (server consolidated to sensors) configuration for customers with small environments.



Key Features

Visibility

It is vital to secure real-time and end-to-end asset visibility to protect cyber-physical systems (CPS) across OT and IT domains. Prioritizing system availability, AhnLab XTD passively observes and analyzes network traffic to provide comprehensive OT asset visibility.

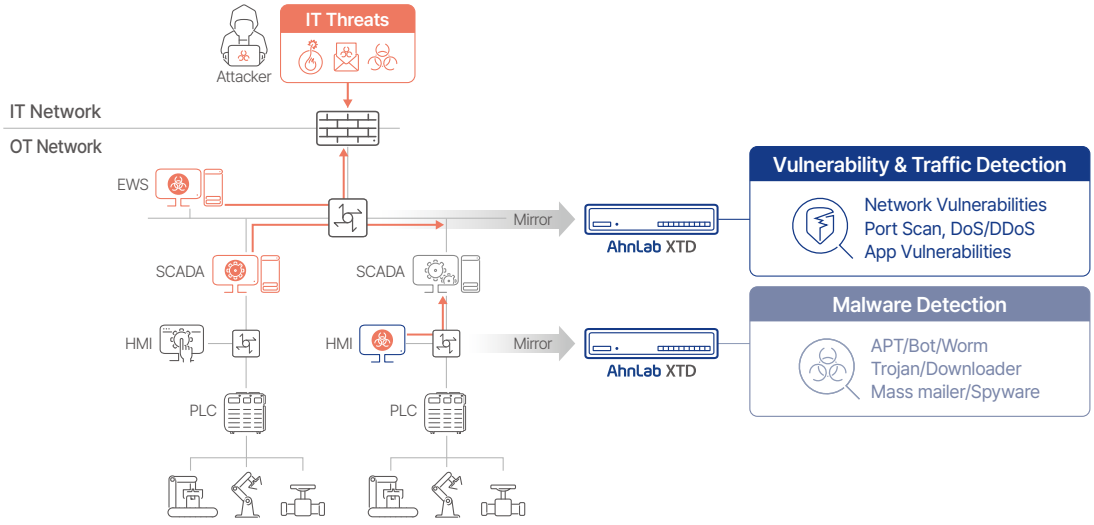
AhnLab XTD sets itself apart from its competitors by offering deep and intuitive asset details. Then, it adds extensive information, including traffic, network connection, and protocol analysis (IT, OT, and IoT) to further stretch its visibility.

The solution also provides two operational modes (learning and operating mode) for efficient asset management and anomaly detection. In learning mode, AhnLab XTD learns data from identified and registered assets. Then, it performs anomaly detection based on the data processed during the learning mode, to accelerate efficient and automated security operations.

Threat Detection

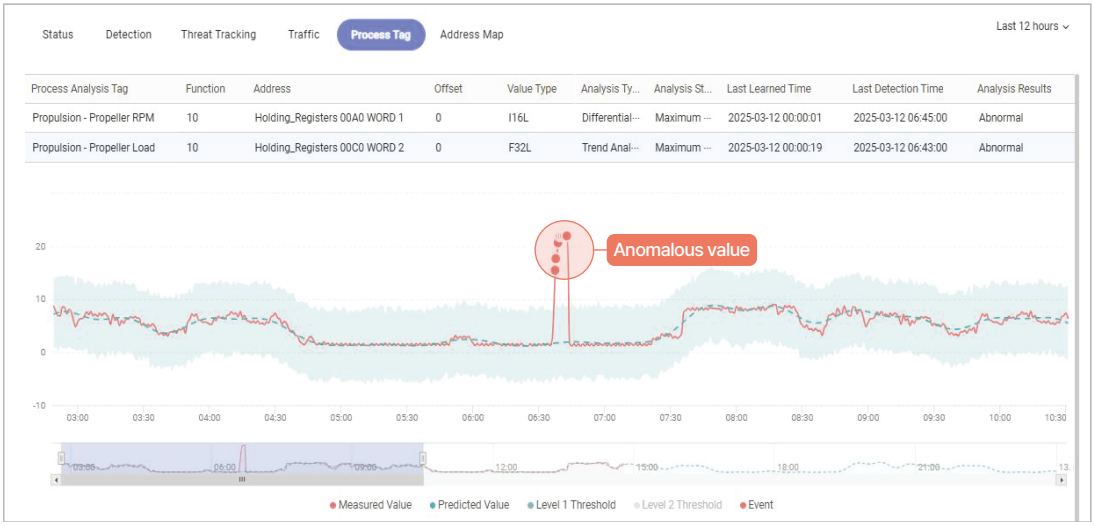
OT networks in the CPS environment are mostly isolated, but vulnerable to cyber threats due to the use of outdated and unpatched systems and unmanaged portable devices. Nevertheless, security measures for threat detection and asset monitoring still fall short.

AhnLab XTD successfully detects and manages various cyber threats spreading through network traffic. It precisely identifies malicious events associated with ransomware, vulnerability exploitation, asset discovery and denial of service (DoS), and sends alerts to the administrator. Powered by our best-in-class antivirus engine, AhnLab XTD delivers next-level detection of known and unknown malware.



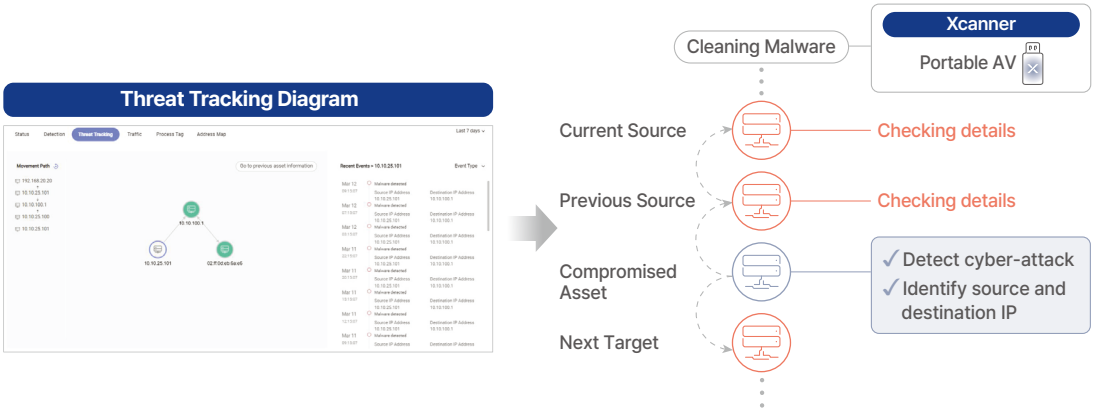
Anomaly Detection: Baseline

AhnLab XTD provides the baseline for anomaly detection powered by deep packet inspection (DPI) of various OT protocols. The product performs a statistical learning of the process value set by the administrator and defines the baseline. Then, it detects values that fall below or exceed the baseline as abnormal and sends a real-time alert to the administrator. As such, security personnel can immediately address an error due to system malfunctioning or human mistake.



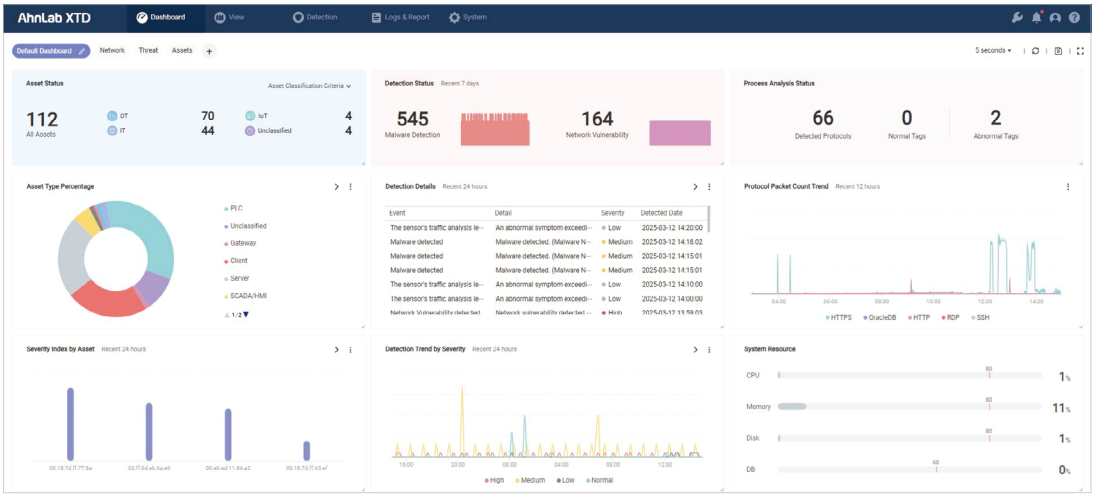
Threat Tracking

AhnLab XTD tracks the origin of cyber threats spreading within the OT network and enhances the visibility into domains that remained as a blind spot. By identifying the previous distribution path, users can understand the movement of cyber threats and take preemptive measures to prevent the next target from being compromised. Administrators can also utilize the portable AV, AhnLab Xcanner, to scan and clean malware in infected systems.



Monitoring via Dashboard

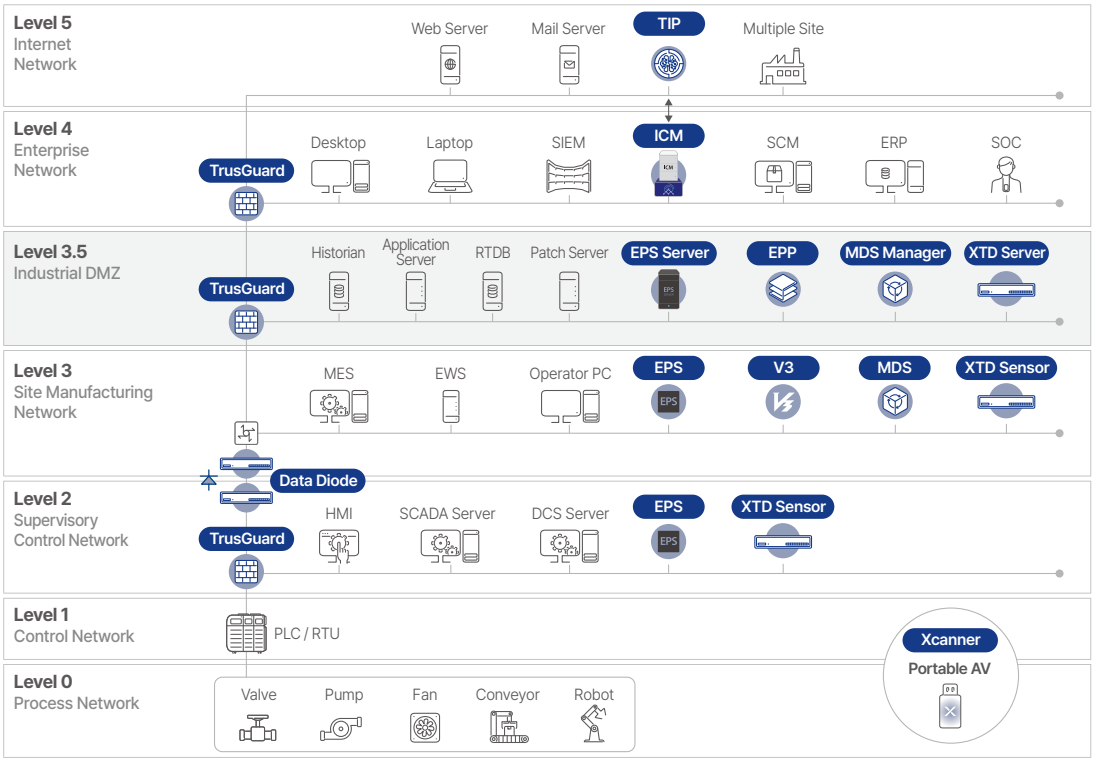
AhnLab XTD offers a web-based management console and various features for convenient operation. It supports real-time monitoring of asset and cyber threats through a dynamic and intuitive dashboard. In addition, administrators can create and configure custom dashboards with separate panels and widgets to display information as needed.



Platform-centered CPS Protection

AhnLab has been delivering the CPS protection platform called “AhnLab CPS PLUS” systematically protecting OT endpoint, OT network and IT domain connected to OT environment. Incorporating our expertise in threat detection & response with OT-dedicated technology, AhnLab CPS PLUS empowers customers with seamless CPS protection through asset identification (visibility) and threat detection and response capabilities. Integrated security modules of AhnLab CPS PLUS are centrally managed and monitored by AhnLab ICM, the central management solution.

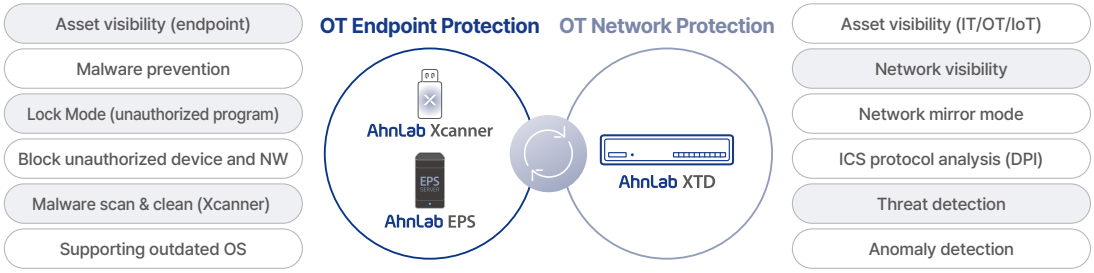
AhnLab CPS PLUS provides the most extensive CPS protection coverage in the industry. The platform offers the best CPS protection experience to customers by combining our exceptional security technology and smooth consolidation of its security modules.



Endpoint-Network Integration

AhnLab XTD provides unique OT endpoint-network security integration that customers can hardly see from our industry peers. This extraordinary offering is backed by the seamless integration of AhnLab XTD with AhnLab EPS, the OT endpoint protection solution.

In simple terms, AhnLab XTD can extend and validate network asset visibility by combining endpoint asset information identified by AhnLab EPS agents. Also, once AhnLab XTD detects cyber threats, it can leverage AhnLab EPS integration to trigger real-time malware scan on suspicious systems and address them by utilizing AhnLab Xcanner.



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

AhnLab