AhnLab XTD

OT 可视性和威胁检测监控解决方案

AhnLab XTD 是一款专为 OT 环境设计的安全解决方案，
提供 OT 网络可视化并实时检测异常行为和安全威胁。

产品介绍

AhnLab XTD 是一款面向工业控制网络（OT 环境）打造的专业级安全解决方案，旨在帮助用户全面实现 OT 资产的可视化管理与安全威胁的实时监控。该产品采用非侵入式的被动扫描模式运行，保障工业系统的稳定性和连续性；通过自主研发的协议识别与深度数据包检测（DPI）技术，能够精准识别多种工业资产及其通信行为，实现对关键设备的持续监控。同时，可有效检测来自 IT 网络的恶意代码、漏洞攻击等威胁，以及 OT 网络内部系统之间传播的安全风险，为工业环境构建多层次、全方位的防护体系。

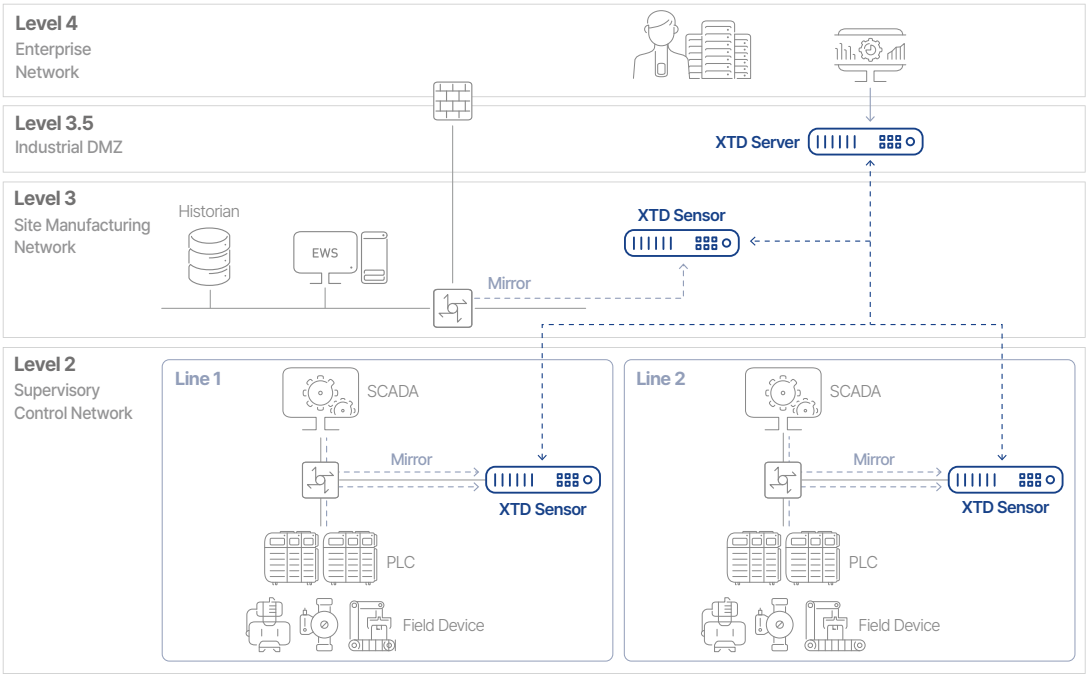
基于资产信息与 DPI 的协议分析
网络会话与拓扑结构

恶意代码、漏洞等威胁检测
异常协议与控制逻辑行为检测

为保障可用性的镜像模式部署
无需更改现有网络架构

系统架构

AhnLab XTD 的基本架构由中央管理服务器与部署在各个网络区域的传感器（Sensor）组成。部署在不同网络区域的传感器负责采集镜像流量，进行协议解析与威胁检测，并将分析结果实时传送至中央服务器。中央管理服务器对收集的数据进行统一分析与处理，实现资产可视化、安全威胁监测及安全策略配置等功能。对于设备较少的小型场景，AhnLab XTD 也支持探针与服务器一体化的 All-in-One 部署模式，为用户提供简洁高效的安全解决方案。



主要功能

资产可视化

在涵盖 OT 与 IT 的 CPS（信息物理融合系统）环境中，若要实现高效的安全管理，必须实时采集与监控各类资产相关信息。AhnLab XTD 采用被动流量监控方式，在保障 OT 系统可用性的同时，实现对网络资产的全面可视化。

AhnLab XTD 可收集并展示 OT 资产的详细信息，包括资产网络连接状态、通信流量、网络拓扑结构，同时支持多种 IT、OT 及工业控制协议的深度解析。

此外，为了提升可视化效率与安全管理水平，AhnLab XTD 提供学习模式与运行模式两种操作方式。在学习模式下，系统会在部署初期自动识别并注册受控资产；而在运行模式中，则可对未注册（Unknown）资产进行单独管理，从而兼顾安全性与管理效率。

- 资产类型、制造商
- IP/MAC、区域、组
- 操作系统信息、风险级别等

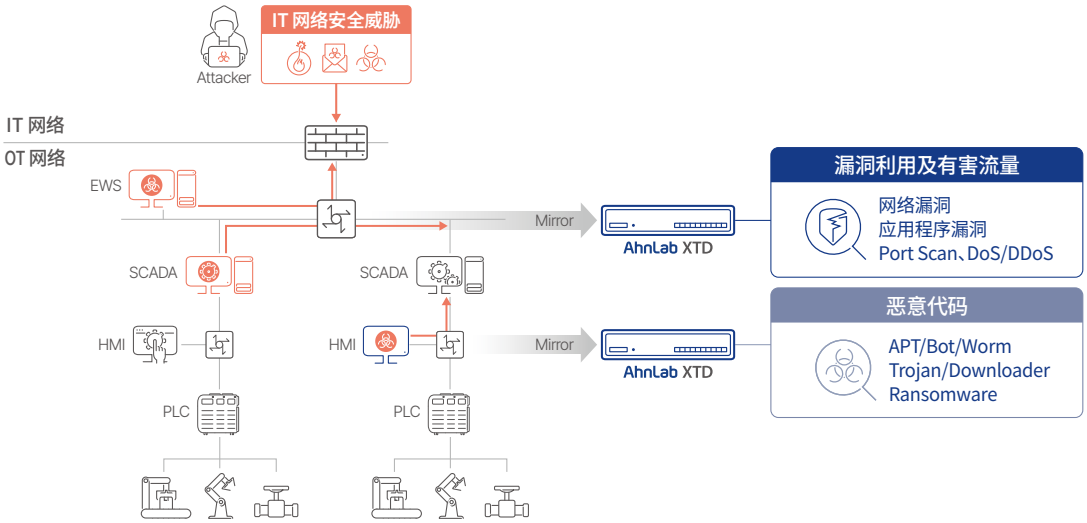
- 服务、会话
- 流量
- 拓扑结构

- ICS 协议
- Function code, value 等

威胁检测与管理

尽管 OT 网络多为独立运行，但由于使用老旧操作系统、缺乏安全补丁、移动设备管理不完善等问题，仍面临多种潜在威胁。而传统 OT 环境中对内网威胁的检测与响应能力普遍不足。

AhnLab XTD 可对 OT 内部网络中的通信流量进行分析，实时检测并管理多种安全威胁，包括勒索软件在内的各类恶意代码、漏洞利用行为、扫描（Scan）攻击、DoS 攻击等异常流量，并第一时间告警通知。特别值得一提的是，AhnLab XTD 集成了 AhnLab 自主研发的高性能杀毒引擎，具备对已知与未知恶意软件的精准、高效检测能力。



基线异常检测

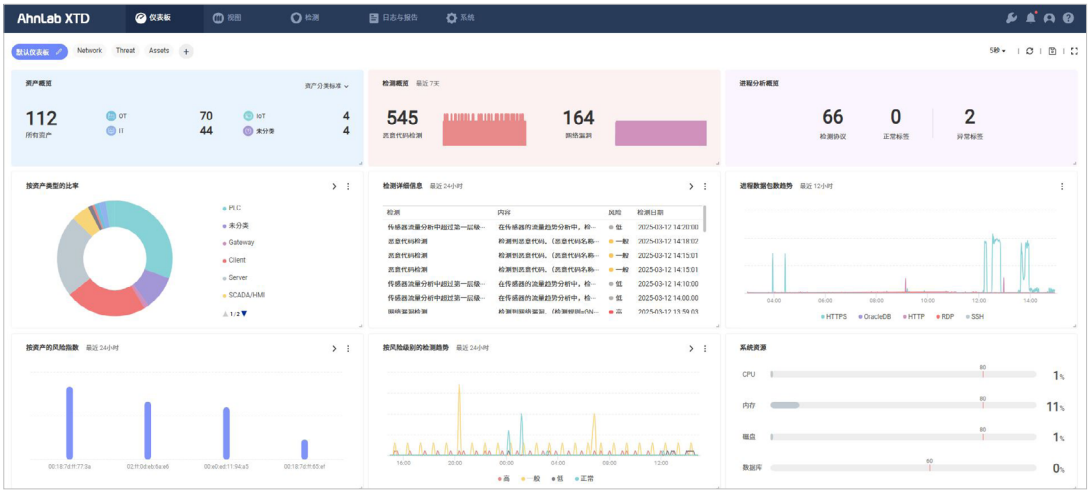
AhnLab XTD 基于对多种工业控制协议的 DPI（深度数据包检测）技术，提供通信行为基线异常检测功能。系统可根据管理员设置的特定进程参数进行学习与建模，形成统计学意义上的行为基准线（Baseline），并对超出或低于该基准的异常行为进行识别与预警。该功能有助于实时发现因恶意攻击或误操作引起的设备运行异常，及时通知安全管理人员，预防控制系统故障或停机事故的发生。

威胁源跟踪

AhnLab XTD 具备威胁传播路径追踪能力，能够追溯 OT 网络中已发生攻击的源头，即使在可视化能力不足的环境下也能有效识别威胁起点。系统可还原攻击的传播链路，帮助管理者精准定位威胁源与传播路径。此外，配合便携式防病毒解决方案 AhnLab Xcanner，可对受感染系统执行恶意代码扫描与清除，有效阻断攻击蔓延。

可视化监控仪表板

AhnLab XTD 配备基于 Web 的管理控制台，界面简洁直观，支持多种管理操作。系统提供动态图形化仪表板，可实时展示资产状态、安全事件、网络流量等关键指标信息。管理员还可根据业务需求创建自定义仪表板与监控小组件（Widget），灵活配置所需信息视图，提升整体运维效率。

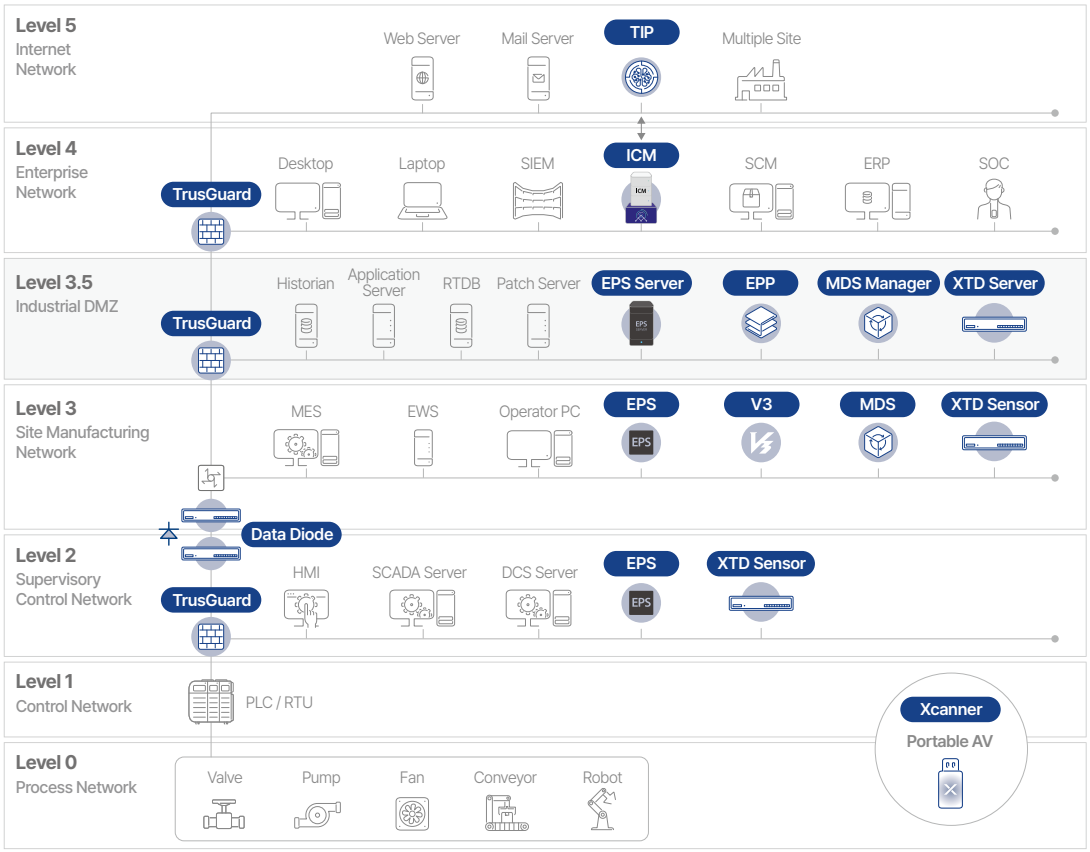


为什么要选择 AhnLab XTD?

基于平台的 CPS 综合安全防护

AhnLab 致力于构建统一的 CPS（信息物理融合系统）安全体系，推出覆盖 OT 端点、网络层及其连接的 IT 环境的综合性 CPS 安全平台——AhnLab CPS PLUS。融合了 AhnLab 在威胁检测与响应（TDR）方面的专业能力与 OT 安全技术实力，AhnLab CPS PLUS 以端点与网络的联动安全技术为基础，在 IT 与 OT 融合环境中实现从资产识别（可视化）、威胁检测到快速响应的一体化闭环防御。AhnLab CPS 平台下的各类安全模块均可灵活集成，并通过 CPS 安全统一管理平台 AhnLab ICM 实现集中化管理与可视化监控。

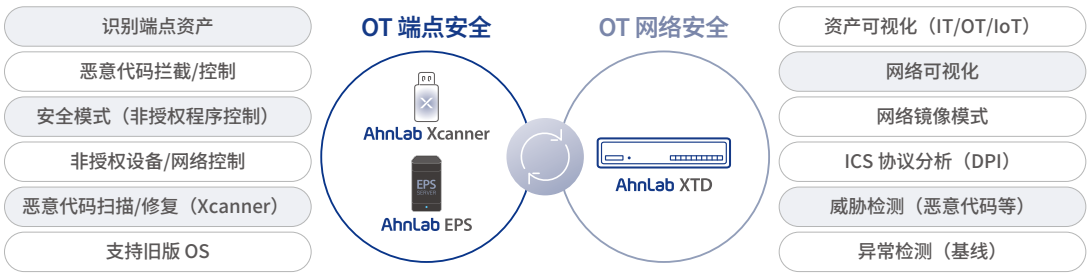
AhnLab CPS PLUS 可覆盖现有 CPS 安全平台中最广泛的场景需求，凭借领先的技术与平台协同优势，为客户带来真正差异化的安全体验。



端点与网络联动的安全防护

AhnLab XTD 通过与 OT 端点安全解决方案 AhnLab EPS 的深度联动，构建出区别于传统方案的 OT 端点 - 网络一体化安全能力，为用户带来独有的安全防护体验。

具体而言，AhnLab XTD 可采集和识别网络中资产的可视化信息，并结合 AhnLab EPS Agent 收集的端点资产信息，实现 CPS 环境下更全面、更精准的可视性扩展与验证。对于检测到的威胁事件，AhnLab XTD 还可通过 AhnLab EPS 进行可疑端点的远程恶意代码检测与即时响应处理，大幅提升响应效率与安全覆盖范围。



北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区新镇路1699弄E栋303室
https://www.ahnlab.com/cn | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）

AhnLab