AhnLab

白皮书

CPS环境为什么需要“集成安全”

IT、OT和CPS的定义

如今，对于各个组织来说，IT（Information Technology）已经是一个非常熟悉的概念。此外，随着对OT（Operation Technology）的理解逐渐加深，CPS（Cyber-Physical System）概念也应运而生。那么，这些概念如何定义？它们之间有什么关联性？又如何制定有效的综合安全策略?

首先，OT是指在工业环境中管理和控制物理设备和过程的技术，涵盖广泛的领域，如工业控制系统（ICS）、可编程逻辑控制器（PLC）等。OT安全的目标是保护这些系统的稳定运行，确保它们不间断地工作。在此基础上，有必要理解IT安全和OT安全在概念上的差异。基本的差异可以在字面上找到。IT安全着重于“信息（Information）”，而OT安全则着重于“运营（Operation）”。尽管看起来并没有太大的差异，但这种本质的差异导致了方法上的根本差异。

从安全的三个要素来了解一下IT和OT安全。安全的三个要素分别为机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。这三个都是安全中必须满足的要素，但可以根据优先级进行区分。

通常，在IT安全最优先考虑的是机密性，其次是完整性和可用性。这在英文中简写为“C.I.A.”。OT安全的优先级则略有不同。最重要的是保障可用性，其次是完整性和保密性。可简写为“A.I.C”。为什么会有这样的差异？原因其实很简单：计算机重新启动即可恢复，而工厂设备则必须确保稳定性，绝对不能停机。

构成IT环境和OT环境的设备方面也所有不同。IT环境由大家所熟知的计算机、笔记本电脑、移动设备和服务器等IT设备构成。而OT环境除了传统的IT设备外，还包括工业控制系统（ICS）。工业控制设备中最具代表性的是PLC（Programmable Logic Controller）。简单来说，PLC是控制工厂中设备如水泵、阀门、机械臂的装置。IT设备与OT设备的使用年限也有所不同，IT设备的寿命约为较短的3~4年，而OT设备通常使用20~25年。

综合来看，IT和OT环境存在本质上的差异，这也是将IT网络和OT网络分开的原因。此前，由于OT领域具有严格控制外部访问的封闭性，安全的重要性相对较少受到关注。然而，随着数字化的快速发展，与IT领域的接触点不断增加，针对OT环境的攻击正在增多，且造成的损害也在不断扩大。

因此，组织需要基于至少将IT与OT融合的综合安全战略来保护其业务。这正是“CPS安全”概念诞生的背景。

CPS是一个涵盖OT、IT、IoT、云计算机等广泛领域的网络（cyber）和物理（physical）元素的概念。不仅适用于传统制造业，还包括智能工厂、医疗系统、自动驾驶汽车等各种应用场景（use case）。为了保护包括多个领域在内的CPS，必须在确保系统可用性的同时，通过对各种安全模块的综合管理确保安全效率，并且还需具备对资产的广泛可见性。

入侵案例

传统OT环境通常运行时间长达10年或更久，且使用的操作系统已过时，补丁不到位，因此存在大量漏洞。这也是网络攻击造成的损害容易扩散的原因之一，可能使CPS环境和整个业务处于风险之中。

从近期发生的重主要CPS安全事件来看，攻击主要集中在制造业，同时也针对发电、能源等社会基础设施。针对OT环境的攻击大致可分为两类。第一类是将IT环境中的攻击手法应用于OT环境。与IT环境一样，OT环境中的勒索软件感染案例正在增加，由于内部系统的安全补丁不到位，利用残留漏洞进行恶意代码感染的案例也屡见不鲜。第二类是通过篡改控制命令，直接打击生产过程，从而造成损失。下面我们分别探讨这些攻击形式的典型案例。

首先是2019年台湾半导体企业TSMC的WannaCry勒索软件感染案例。由于此次事件，TSMC的工程停产了大约48小时，造成了巨大的经济损失。此次勒索软件感染始于OT网络内部设备使用受感染的USB，随后通过“永恒之蓝（Eternal Blue）”SMB漏洞迅速传播。勒索软件甚至传播到了与该工厂连接的海外其他工厂，损失也随之扩大。

接下来是美国佛罗里达州奥兹马尔（Oldsmar）市一家水处理厂发生的攻击事件。攻击者通过漏洞在设施管理员可能访问的网站上植入恶意代码，并由此渗透到办公网络系统，窃取了账户信息和控制设备连接信息。随后，攻击者尝试通过远程访问程序TeamViewer来操纵水中氢氧化钠的浓度，幸好当时正在监控的管理员注意到鼠标的异常操作，成功阻止了这次攻击。否则，这起事件可能演变成异常把数万名市民的饮用水变成“碱水”的大规模恐怖袭击。

了解CPS威胁

随着OT系统的外部暴露扩大，针对CPS的攻击也逐渐变得更加复杂。然而，可以简单地将其理解为，通过利用IT（或者外部）网络、资产及攻击手段入侵OT系统，从而攻击整个CPS环境。

从这个角度来看，针对CPS的攻击主要通过以下五个途径进行：▲IT网络、▲远程控制程序、▲存储设备、▲第三方访问、▲供应链发生。

1.IT网络

通常情况下，OT网络与外部和互联网断开连接，因此很难进行直接攻击。然而，与IT网络相连的OT网络内的系统可能会通过IT网络感染恶意代码。攻击者不直接攻击OT网络，而是尝试通过IT网络来攻击OT网络。由于OT网络系统也常使用Windows或Linux操作系统，IT环境中的恶意代码也可以在OT环境中生效。此外，不完善的网络分段也可能为OT环境的攻击提供便利。

2.远程控制程序

诸多OT设备由远程控制程序管理。如果攻击者能控制这些程序，他们可以轻松入侵或操控OT系统。因此，组织必须特别注意保护这些程序的凭证信息，以防被窃取。

3.存储设备

很多情况下，USB等存储设备直接连接到OT系统。原则上，维护人员应在连接到生产线系统前，使用防病毒程序对存储介质进行扫描。但如果忽视这一点并直接使用存储介质，系统可能会感染蠕虫或病毒等恶意代码。此外，存储介质可能会从内部易受攻击的系统受到感染，并在连接到其他系统时传播。严重情况下，正如台湾TSMC的案例所示，勒索软件的自我传播功能可能导致生产线停工。

4.第三方访问

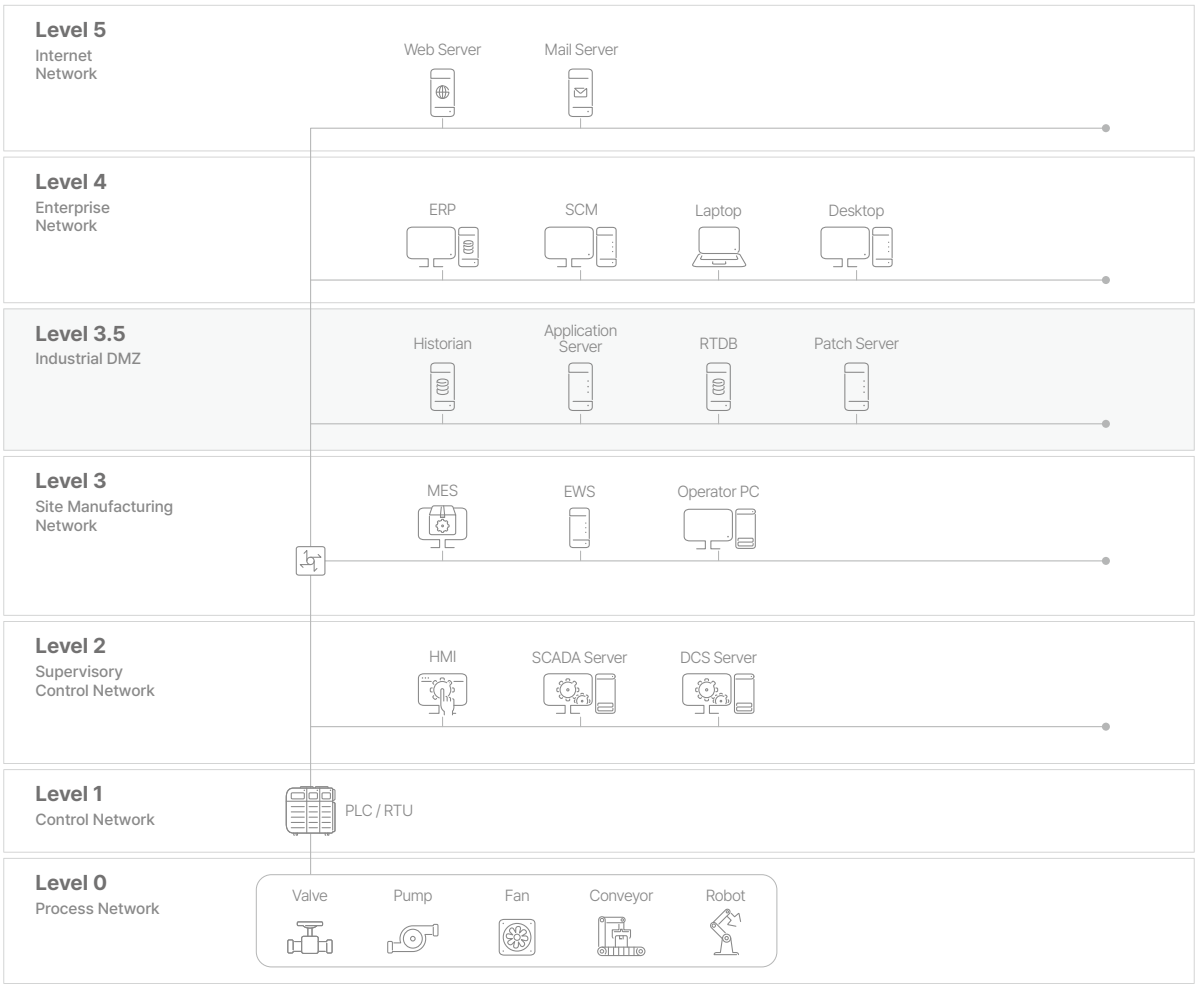
进行维护等业务的合作公司通常会直接访问OT网络内的系统。如果攻击者在合作公司使用的存储介质中插入恶意代码，便可以直接渗透到内部系统。

5.供应链

在OT网络中运行的系统是由专业制造商提供的。攻击者通过攻击这些公司，将恶意代码嵌入到开发的程序中，或者替换为包含恶意代码的安装文件。2013年发现的“Havex恶意代码”就是一个典型案例，攻击者通过入侵OT网络中运行的软件的开发者网站，在安装文件中植入恶意代码。如果在供应链提供的软件中包含恶意代码，往往很难察觉感染情况。

CPS架构

为制定有效的CPS安全战略，首先要正确理解CPS的结构。对此，将OT网络层级细分为Level 0到Leve 5的“普渡模型（purdue model）”被广泛认为是构成OT安全架构的标准。当然，在遥远的未来对于CPS的理解需要超越普渡模型，但在解决融合IT与OT的安全要求事项这一观点上，普渡模型在当前乃至不久的将来，对于CPS安全仍是有效的一个模型。



【图1】普渡模型

Level 0：进程网络（Process Network）- 该层是现场运行的设备所在的层级。包括阀门、泵、传送带和机器人等生产设备和装置。它们的数据由传感器（sensor）进行收集。此外还包括接受一级网络命令进行操作的执行器（Actuator），如开关装置等。

Level 1：控制网络（Control Network）- 一级网络处理来自二级网络（Level 2）的命令，并将其发送到零级网络（Leve 0）。同时，还将零级网络收集到的信息和数据发送到二级网络。具代表性的设备包括PLC（Programmable Logic Controller，可编程逻辑控制器）和RTU（Remote Terminal Unit，远程终端单元），它们负责向现场设备下达指令并进行控制。

Level 2：监控网络（Supervisory Control Network）- 该层由远程管理和运营现场设备的系统组成。主要系统有SCADA（Supervisory Control And Data Acquisition，数据采集与监视控制系统）和HMI（Human Machine Interface，人机界面）。SCADA通过一级网络的PLC和RTU收集现场数据，并同时控制多个现场设备。通过HMI管理员可以控制工艺过程特定领域的设备。

Level 3：现场制造网络（Site Manufacturing Network）- 该层管理整个生产系统并提高运营效率。该层由优化生产活动全程的MES（Manufacturing Execution System，制造执行系统）、用于控制设备的EWS（Engineering Workstation，工程工作站）和管理产品生命周期的PLM（Product Lifecycle Management，产品生命周期管理）组成。此外，可托管主HMI管理整个设施。

Level 3.5：Industrial DMZ – 该层称为工业DMZ，是OT环境和外部IT环境的连接点。存储传感器数据的RTDB（Real-time Database，实时数据库）、Historian、应用服务器和补丁服务器等均属于该层。随着OT安全入侵事件频发，后文中将提及的IT-OT融合安全的重要性日益凸显，这一层也逐渐引起人们的关注。

Level 4：企业网络（Enterprise Network）– 由企业一般在IT环境中使用的资源组成，如资源管理（ERP）、供应链管理（SCM）、客户关系管理（CRM）等。管理与工艺相关的全公司业务。

Level 5：互联网（Internet Network）– 该层是网络或外部环境一线相连的资产层级。设备有Web服务器、邮件服务器等。

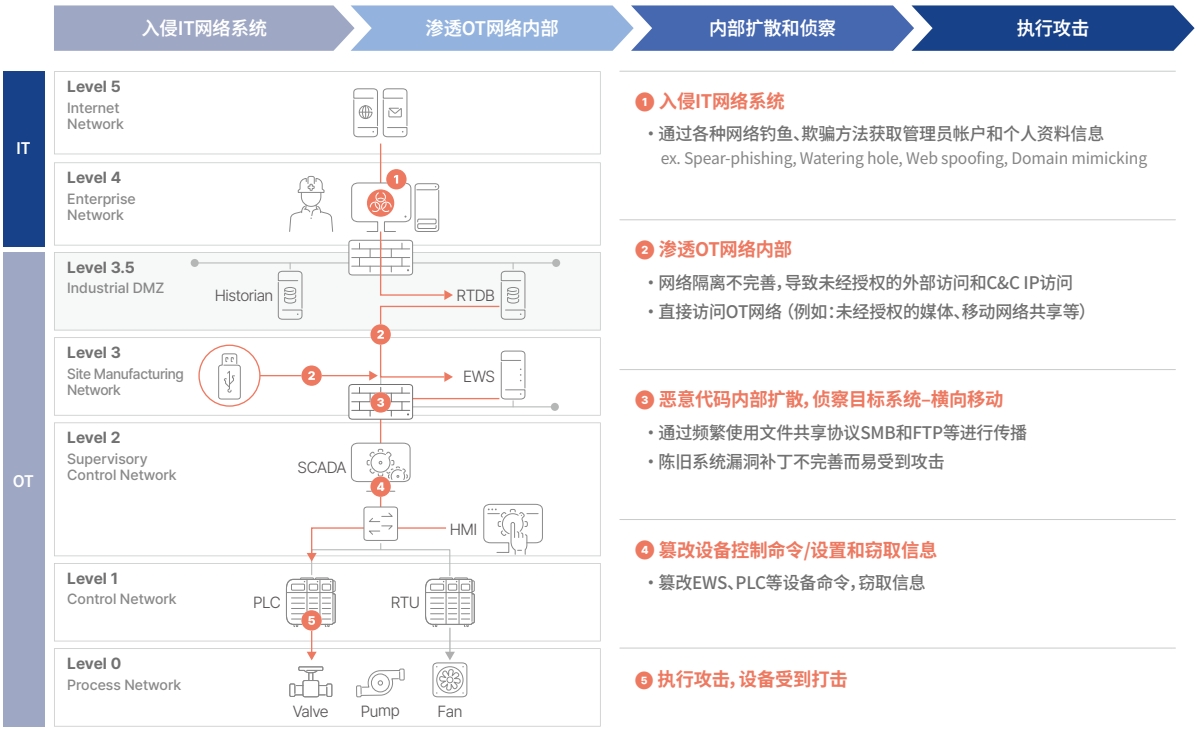
CPS攻击过程

从安全角度出发，以网络为准可对Level 0~Level 5划分为以下几类。大体上分为IT网络（Level 4~5）和OT网络（Level 0~3.5）。其中，OT网络进一步分为控制网络（Level 0~2）和运营网络（Level 3~3.5）。以下是OT环境的各层级及其网络结构和组成元素的汇总：

Level	Type	Key Components	Description
0	控制网络（OT）	• Sensors • Actuators • Production devices	现场设备，直接在现场执行作业的各种设备和机械。
1		• PLC • RTU	控制系统，向现场设备发出命令并进行控制的系统或装置。
2		• SCADA • HMI • DCS	远程管理和操作系统，负责对现场设备进行远程管理和操作的系统。
3	运营网络（OT）	• MES • PLM	生产系统管理与运营，对整个生产流程进行全面管理和运营的系统。
3.5	DMZ	• RTBD • Historian • Application servers	OT与IT的边界或缓冲区，连接OT与IT领域的接触点或缓冲区域。
4	企业网络（IT）	• ERP • SCM • CRM	企业业务管理系统，负责管理与生产流程相关的全公司级别的业务管理。
5	互联网（IT）	• Web servers • Mail Servers	外部网络连接资产，与外部网络直接连接的关键资产或设备。

【表1】网络各层构成要素和作用

根据上述内容，以下是对CPS环境中最新攻击的流程图：



【图2】针对CPS的攻击过程

CPS攻击通常从IT环境开始。虽然有时攻击者直接将未经授权的介质连接到OT网络，但大多数情况下，攻击是在IT网络系统被侵入后扩散到OT网络。OT环境通常是封闭的网络，通过气隙（Air-Gap）的网络隔离和网络分段（Segmentation）等措施来限制攻击面（Attack Surface）。但由于OT环境与IT网络管理系统相连接，当IT网络系统首先面临安全威胁时，攻击者可能会窃取OT网络系统的网络连接信息和账户信息。

攻击过程大致如下：攻击者通过网络钓鱼或高级持续性威胁（Advanced Persistent Threat，APT）等各种技术渗透到管理OT网络的IT系统中。接着，攻击者会窃取用于访问OT网络系统的管理员帐户、IP、URL等各种配置信息。利用这些信息，攻击者可能会通过网络隔离策略未完善或管理薄弱的对方进入OT网络。此外，通过没有安全管理的USB设备或通过移动网络共享连接未经授权的笔记本电脑，也可能导致恶意代码进入OT网络。

一旦入侵成功，攻击者会检测目标系统并传播恶意代码。由于OT环境的工作特性，例如频繁使用SMB端口、远程文件传输、远程访问，以及系统老旧且补丁不及时，这使得恶意代码能够快速传播。随后，攻击者会连接到SCADA（监控和数据采集系统）或HMI（人机界面）等运营系统，通过EWS（警报系统）或PLC（可编程逻辑控制器）发出异常控制命令或篡改设备设置等，从而直接影响运营。

以上，我们已经了解了CPS环境中的攻击展开过程。为了加强CPS环境的安全，必须采用IT和OT的综合安全战略。仅依赖IT安全无法充分防御OT环境的风险，因此需要加强两者之间的安全集成。

CPS安全需求和集成安全方法

CPS安全基本上需要遵循“识别 > 检测 > 响应”这一流程。需要注意的是，不仅OT领域、还应涵盖IT与OT的接触点、以及IT领域，建立一个“IT & OT融合安全”体系。IT & OT融合安全需要依据“识别 > 检测 > 响应”流程，全面涵盖端点、网络和ICS安全。以下是对整体流程和各安全领域要求进行整理的内容。

【图3】CPS安全流程与各安全领域需求

A.识别

在CPS安全中，“识别”指的是对运营中的资产和相关信息进行透明的“可见化”管理。CPS环境需要可视化的原因在与它是实现有效安全管理的基础。由于OT网络中存在多种资产且使用年限较长，资产的位置、状态和网络通信等综合管理起来难度较大。因此，如果不能准确识别资产，将很难检测到安全威胁或设备故障灯影响可用性的情况，并进行相应的响应。

可视化的标准可以从资产和网络的观点进行区分。从资产的观点来看，可以分为控制网络中的各种设备和运营网络中的各种服务器或工作站；从网络的观点来看，可以根据各资产间的网络会话及其使用的各种IT/OT应用协议进行划分。

由于OT网络的环境特点，资产或网络的变化没有IT环境那么频繁，因此可以将已识别的元素作为基线，进而检测未识别的安全威胁和异常行为。

以OT网络为例，从控制网络开始，需要监控资产的种类、供应商、软件版本等资产信息及设备的工业协议和流量会话。特别是，能够将不同的工业协议标准并整合分析的能力是必不可少的。

在进入运营网络后，各端点和网络区域都有相应的安全要求。首先，在端点区域，必须确保系统信息的可见性。系统信息包括系统类型、供应商、软件版本等多种信息。此外，还需要掌握整个工序中使用的应用程序、进程和可移动介质。在网络区域，要求对网络协议和流量会话进行监控。

B.检测

在通过识别确保可见性后，需要检测CPS环境中的威胁因素和异常情况。

首先，在控制网络中，需要识别OT设备的异常情况。应综合监控控制命令误操作、设备故障、未经授权的协议及流量会话，始终确保设备的稳定性。

在运营网络中，首先要求对端点区域进行恶意代码扫描。此外，还需要检查是否存在未经授权的应用程序和可移动介质。在网络区域，需要持续监控对恶意代码传播、未经授权的流量等威胁因素。

C.响应

最后，响应是指基于之前识别和检测到的内容，制定最佳的响应计划，以将对工序的影响降至最低。考虑到CPS环境的特殊性，为进行最有效的响应，需要设备管理员与安全专家的密切合作。CPS安全的首要任务是不阻碍运营连续性。

尽管OT环境在威胁应对方面较IT环境有更多限制，但在运营网络中可以进行主动响应。当检测到端点安全威胁时，可以通过恶意代码扫描和修复来最大限度地减少损害。还可以通过设备控制和漏洞修补来加强全方位的安全。对于网络安全威胁，可以通过“分段（segmentation）”对网络进行细分化，提高监控和威胁响应的效率。此外，通过IT与OT之间的网络隔离来有保护OT环境并加强访问控制也是一种有效的方法。

要构建系统化的安全架构，需要配备适当的安全模块。首先，在网络方面，需要专用IDS来检测网络威胁并确保资产可见性。此外，还需要通过防火墙进行网络分段。使用单向数据传输模块可以加强OT网络与外部网络之间的通信安全。

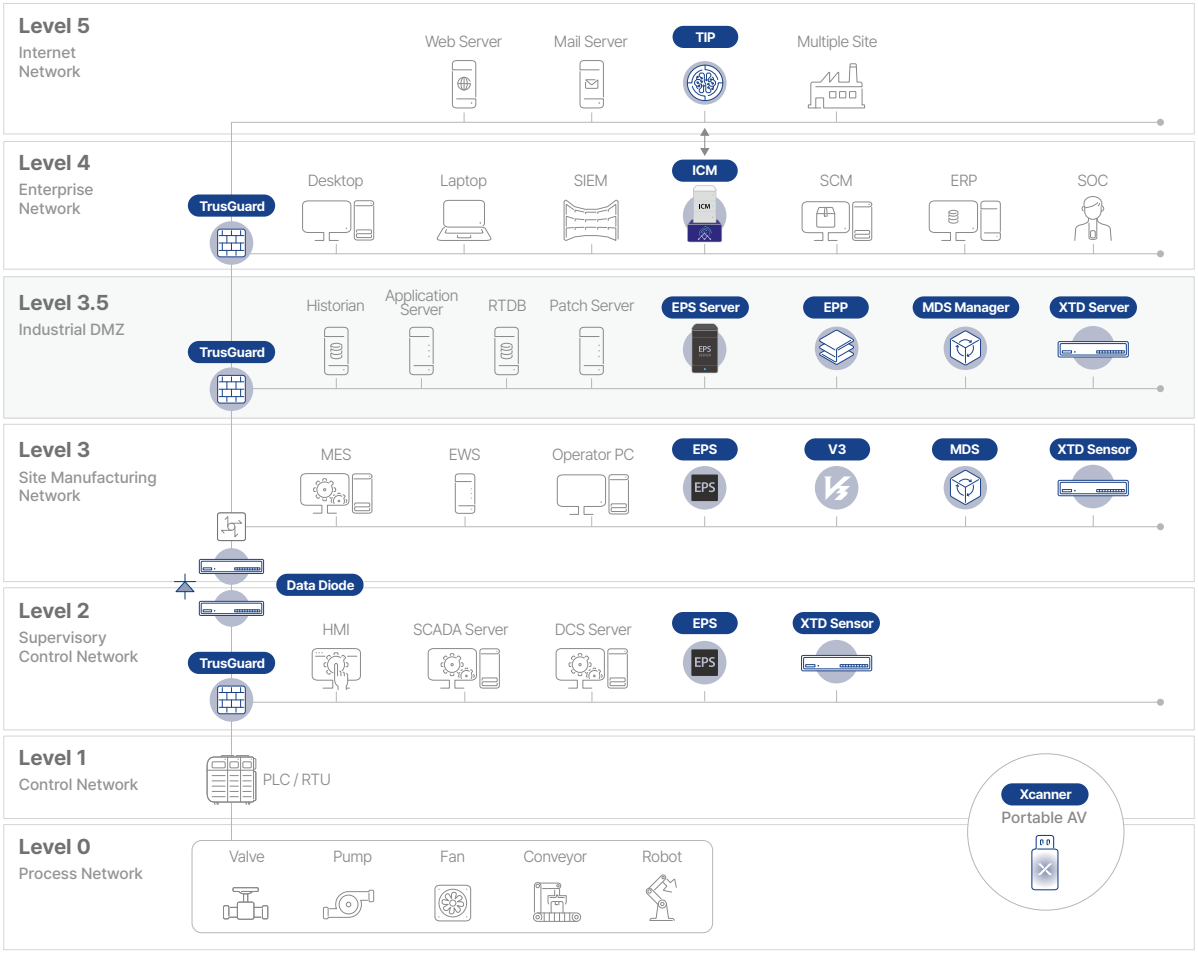
为了保护CPS环境的端点，需要基于允许列表的应用程序控制和设备控制，以防止未经授权的运行。漏洞管理和便携式反恶意软件模块有助于减少CPS设备的攻击面并响应恶意代码。此外，为了有效保护CPS环境，还需要确保所使用中的IT设备的安全。采用强大的EPP（端点保护平台）将是一个很好的起点。

在此其础上，需要对各安全模块进行集成管理。当前的CPS安全威胁难以通过单一解决方案响应，组织需通过基于平台化的方法，具备综合监控和管理能力。

AhnLab CPS PLUS：综合CPS安全平台

AhnLab的CPS综合安全平台“AhnLab CPS PLUS”保护包括OT端点、网络和与OT网络相连接的IT领域在内的CPS环境。该平台为制造、能源、运输等各产业客户的业务提供了保护。

AhnLab CPS PLUS的差异化在于其相较于其他竞争公司提供了最广泛的覆盖范围。基于模块间灵活联动的平台战略，为客户提供了强大的安全效率和业务生产效率。



【图4】AhnLab CPS PLUS结构图

AhnLab ICM
基于CPS综合监控提供可见性和安全模块管理

AhnLab EPS
OT端点进程和设备控制，诊断恶意代码

AhnLab XTD
确保OT网络可见性和检测异常行为等威胁

AhnLab Xcanner
专为检测并修复OT端点恶意代码而设计的便携式反恶意软件

AhnLab TrusGuard
OT网络安全和分段

AhnLab Data Diode
通过物理单向数据传输控制OT环境访问

AhnLab MDS
通过网络沙箱分析检测未知恶意代码

AhnLab EPP/V3
针对CPS环境中IT设备提供反恶意软件和综合补丁管理

AhnLab TIP
涵盖IT和OT环境的CPS威胁情报

AhnLab CPS PLUS结合了Ahnlab威胁检测&响应能力和OT安全技术，在整个CPS环境中构建了“识别 > 检测 > 响应”综合安全平台。该平台共由9个安全模块组成，并通过综合管理模块AhnLab ICM进行监控和集中管理。

Domain	Module	第1阶段：监控&识别	第2阶段：威胁检测	第3阶段：响应	第4阶段：后续措施
IT & OT	ICM	• 收集IT & OT资产列表	• 日志分析 • 查询详细分析报告	• 更改安全模式（Lockdown）例外项目 • 检查未应用恶意代码策略的Agent	• Checking Remediation Status • Applying Rest API Policy
Endpoint (OT)	EPS	• 识别生产设备资产	• 已知恶意代码	• 执行恶意代码扫描 • 阻止未经授权的进程 • 阻止设备运行	• 切换为安全模式（Lock） • 请求AhnReport分析
Network (OT)	XTD	• 识别OT资产 • 识别各资产流量	• 传播恶意代码 • 网络威胁，如漏洞 • 异常PLC逻辑	• 威胁检测/响应警报	
Endpoint (OT)	Xcanner			• 受感染设备上运行扫描并修复	
IT & OT	TrusGuard		• 网络威胁 • 未授权流量	• 基于ACL拦截未授权会话 • 拦截有害流量	• 设置防火墙策略 • 网络分段
Network (OT)	Data Diode			• 单向数据传输	
IT & OT	MDS		• 已知/未知恶意代码 • 受感染设备的网络异常行为 • 绕过行为分析	• 确认MDS误报 • Pinpoint扫描	
Endpoint (IT)	EPP/V3	• 补丁管理	• IT恶意代码	• 修复恶意代码	• EPP/防病毒策略设置
IT & OT	TIP				• 查询威胁信息

【图5】AhnLab CPS PLUS各模块的角色

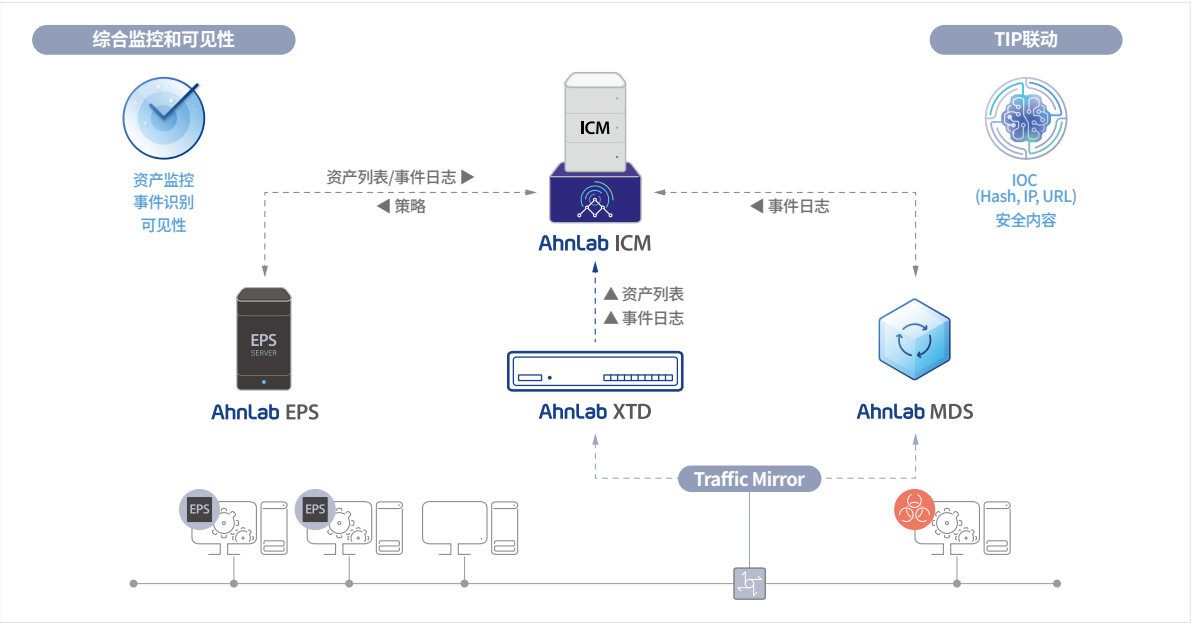
AhnLab CPS PLUS安全模块的作用

AhnLab CPS PLUS的9个安全模块拥有保护CPS的共同目标，并承担不同的角色。让我们看一下各安全模块的角色以及它们之间是如何联动的。

ICM（+TIP）

在安全平台中，最重要的能力是对联动的模块进行中和监控和管理。这便是AhnLab ICM在AhnLab CPS PLUS中扮演的角色。管理员可以通过直观的仪表板确保整个CPS环境的可见性，并对CPS安全的核心模块进行集中管理。

ICM与AhnLab EPS、XTD、MDS等CPS安全模块联动，提供各模块的状态和日志综合查询与搜索功能，使管理员能够立即识别需要采取措施的问题。客户可以利用ICM增强业务连续性、管理效率和生产效率，从而享受真正的“CPS安全平台”所带来的好处。

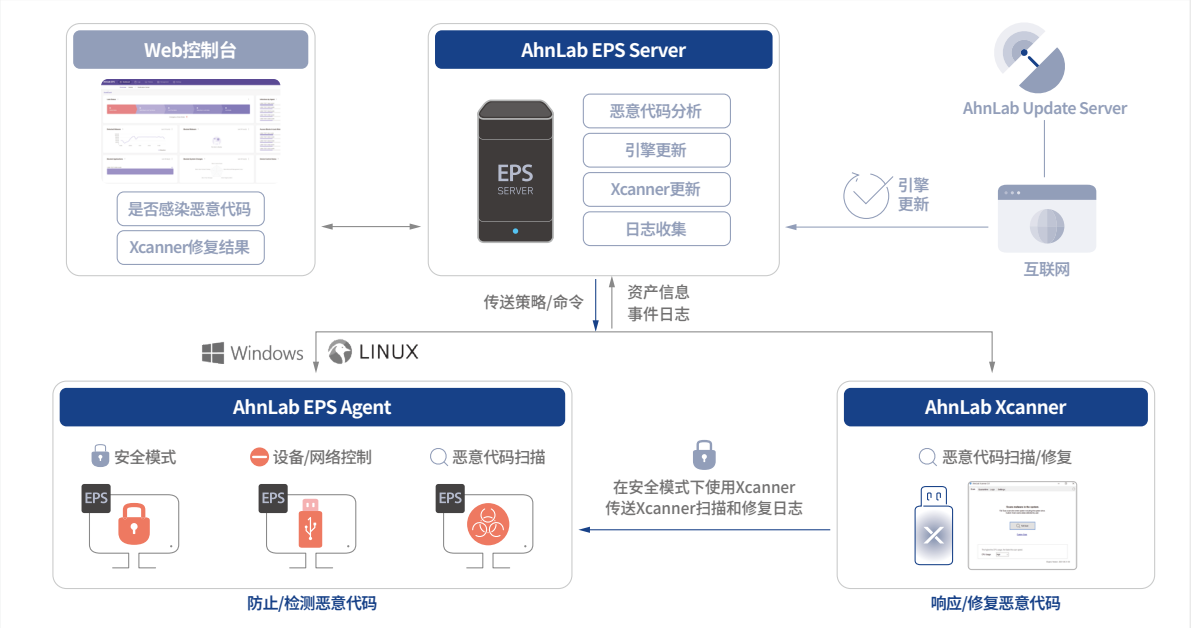


【图6】AhnLab ICM的集中管理架构

此外，ICM通过与自家的威胁情报平台AhnLab TIP联动，实现真正的基于情报的CPS安全。管理员通过涵盖IT与OT的CPS环境中的入侵指标（IoC），实时获取更详细的信息。

EPS（+Xcanner）

OT端点安全模块AhnLab EPS长久以来保护着制造企业、发电站等各行业企业的CPS环境。EPS基于Web的直观控制台能够准确识别和管理工厂内的OT设备。为保证OT设备的运营稳定性，将Agent尽可能实现轻量化，并在服务器执行各种扫描和分析等会造成负载的任务。EPS还能够顺利支持从Windows到Linux等操作系统，包括那些未及时进行安全更新和补丁的旧版本操作系统。



【图7】AhnLab EPS和Xcanner结构

EPS的核心能力在于应用了基于允许列表（allowlist）的控制技术，确保文件只有在授权的设备和网络上运行，从而最大限度地降低潜在的安全威胁。允许列表会自动生成和应用，因此减轻了管理员在策略设置方面的负担。

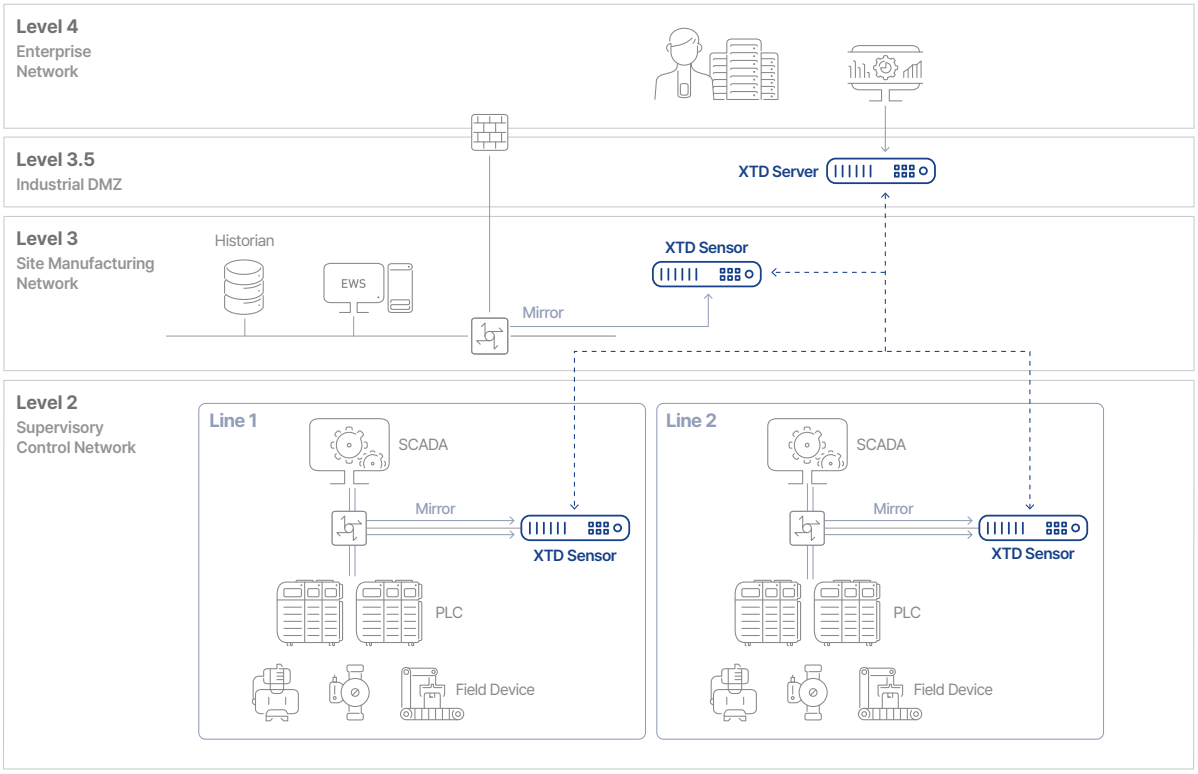
EPS支持三个阶段运营模式，以增强客户的运营便利性和安全设置的稳定性。首先，三个阶段运营模式包括：用安全模式（Unlock Mode），可以进行系统更新或维护共偶；安全测试模式（Lock Test Mode），为安全运营设备而在转换为安全模式之前进行模拟；安全模式（Lock Mode），不允许任何未授权的更改，以确保运营稳定性和连续性。

此外，EPS能够检测和拦截针对OT设备的已知恶意代码。Agent可以在本地检测恶意代码，并在服务器进行详细分析。通过这种方式，可以在不增加系统负载的情况下，实现对恶意代码的实时检测、分析和拦截。

如果OT设备感染了恶意代码，可以使用便携式防病毒软件AhnLab Xcanner来清除恶意代码。Xcanner可以安装在授权的USB上，或者通过EPS Agent下载。Xcanner的扫描和清除记录以及相关日志可以在EPS服务器上进行监控和管理。Xcanner的优势在于其恶意代码响应流程设计简易直观，即使是非专家也能轻松应对安全事件。

XTD

AhnLab XTD提供基于网络的OT网络可见性，并实时检测安全威胁和异常行为。考虑到OT环境对可用性的高度重视，XTD采用网络流量镜像“被动监控”方式运行，以保证设备运营的稳定性，不会影响设备的正常运行。



【图8】AhnLab XTD运营结构

XTD的特点是能够与OT端点安全模块联动，支持端点领域的可见性和恶意代码扫描和修复。此外，通过对多种OT协议的DPI（Deep Packet Inspection，深度包检测）分析技术，支持识别各类设备和针对异常控制逻辑的检测分析能力。

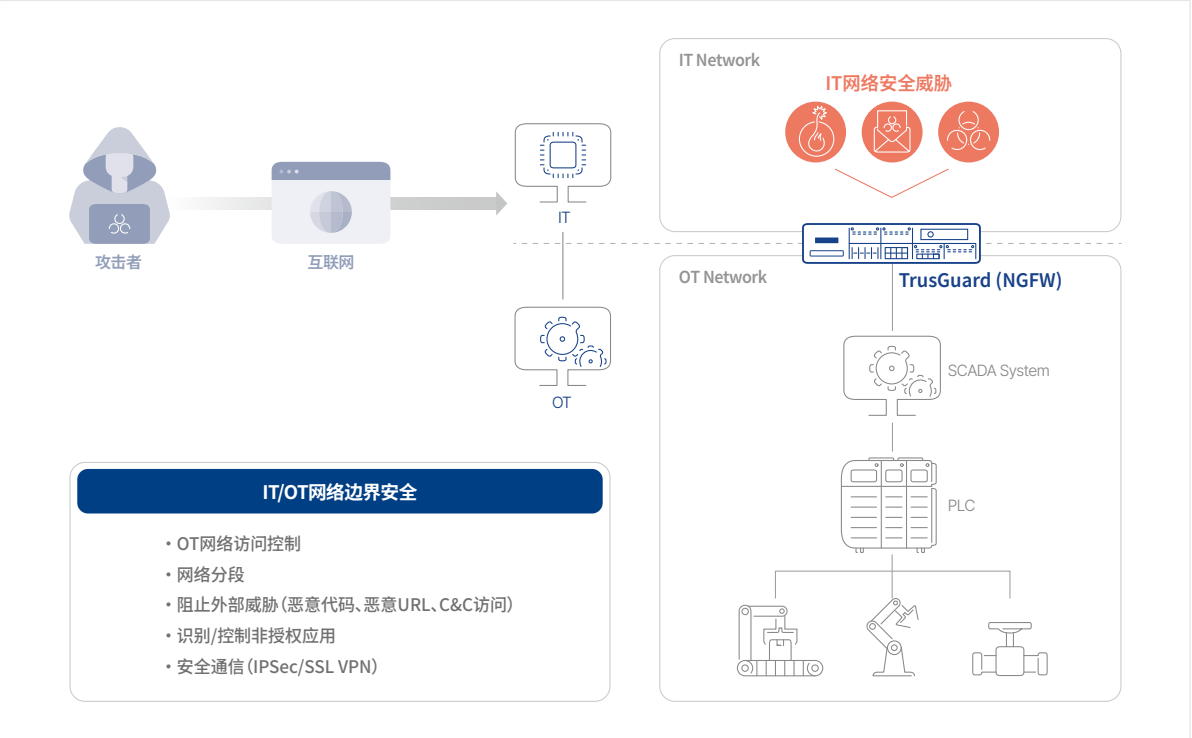
将XTD与EPS联动，可将可见性扩展到连接至OT网络的端点。一般的同类解决方案只提供至网络领域的资产状态。而XTD通过与EPS的联动，不仅可以提供网络领域，还可以提供连接到OT网络的服务器、工作站（Workstation）的操作系统补丁版本等详细的端点信息，扩大可视性。

与Xcanner联动时，还可以扩大恶意代码扫描领域。若初期在网络中检测到恶意代码传播或利用漏洞的恶意流量，则可以对位于端点领域的可疑系统再次执行恶意代码扫描。此外，不同于仅提供网络内安全威胁检测的大部分同类解决方案，还可以扫描恶意代码以查找威胁来源，从而实现更主动的威胁响应。

另外，还提供“威胁追溯（Threat Tracking）”功能，通过反向追踪检测到的威胁的传播路径，告知威胁信息。通过该功能，可以确定传播攻击的先前分发站点，从而识别攻击的传播和移动路径。由此用户可以确认检测到的威胁事件的传播路径和最初发生的资产等威胁之间的关联性，从而进行系统的威胁响应。

TrusGuard

防火墙模块AhnLab TrusGuard在OT网络边界控制入站和出站流量，拦截恶意代码、URL、C2连接流量等恶意流量，并支持IPSec/SSL VPN等安全通信和网络分段等功能。

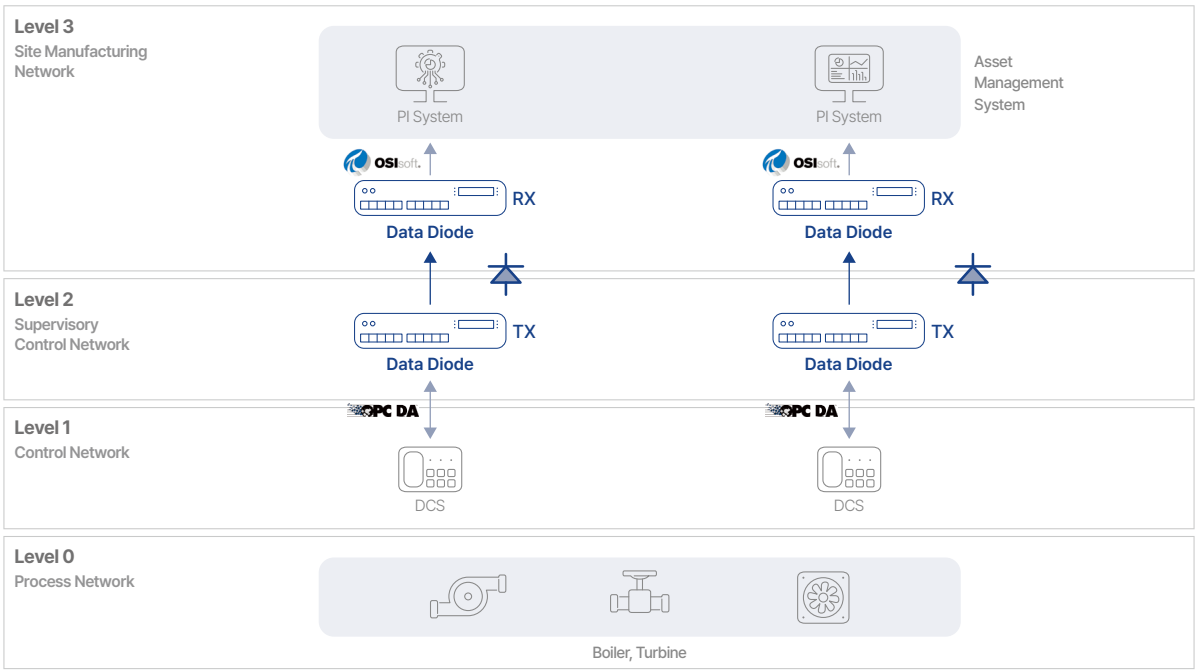


【图9】AhnLab TrusGuard的网络边界安全结构

此外还应用了OT协议分析技术，可以在OT网络内详细控制工业协议。具体来说，不仅可以控制Modbus、DNP3等各协议，还可以识别并控制功能代码（Function Code）。

Data Diode

AhnLab Data Diode强制将安全级别不同的网络之间的数据流向仅向单方向传输，从而在保持安全级别较高的OT网络的封闭性的同时，仅将必要的数据安全地传输到外面。对于传输的数据， 应用了经验证的加密模块。包括数据加密、前向错误纠正（Forward Error Correction, FEC）、数据传输错误控制和恶意代码扫描等技术，以最大化数据传输的可靠性和稳定性。



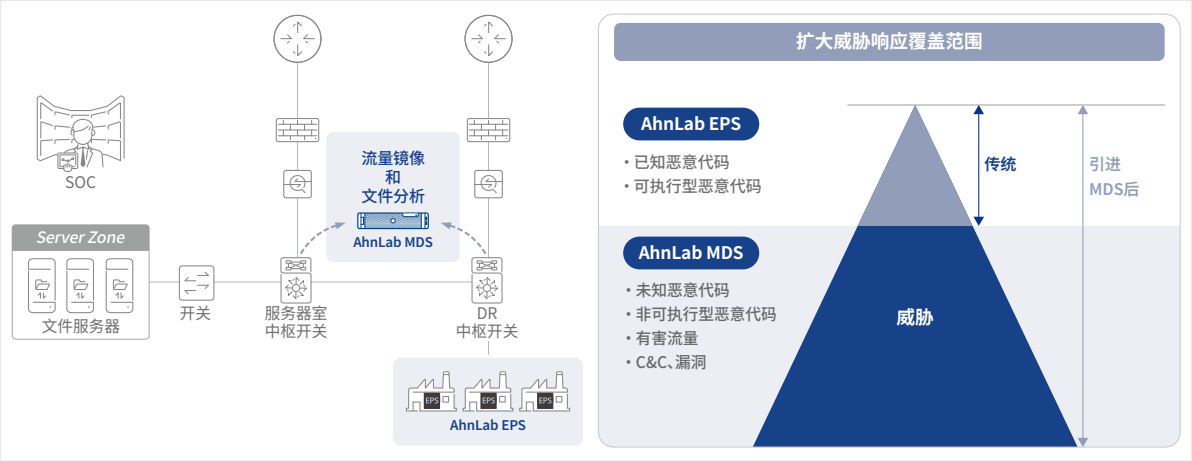
【图10】AhnLab Data Diode结构图

此外，基于涵盖IT和OT环境的广泛协议支持技术， AhnLab Data Diode能够以最优的形式部署在各种环境中。还具备了灵活性，可以根据不同的应用场景（如供各种IT/OT协议、闭路电视流数据、数据库等）提供定制化支持。

MDS

最近，随着网络威胁持续升级，高级持续性威胁（Advanced Persistent Threat: APT）和新/变种恶意代码的数量呈现日益增加趋势。因此，除了已知（Known）的恶意代码外，还需要对未知（Unknown）的恶意代码进行分析和响应。

网络沙箱模块AhnLab MDS通过收集和分析生产网络中的文件，对未知恶意代码进行动态分析。此外，还能够检测和分析攻击者的C&C IP连接，从而监控恶意代码在OT网络中的传播路径、C&C、漏洞等各种安全威胁，并提供对感染设备的修复和响应。

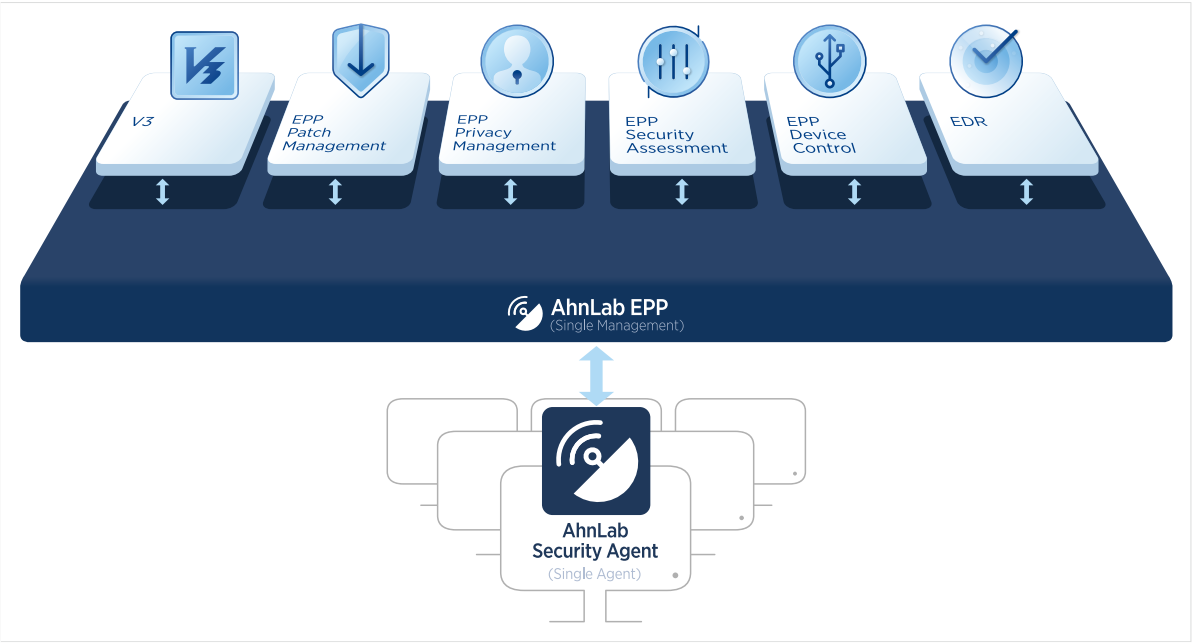


【图11】通过AhnLab EPS与AhnLab MDS的联动扩大威胁覆盖范围

特别是在与EPS联动时，基于MDS动态分析功能，能够防御所有新型、变种以及未知的恶意代码，从而扩大综合威胁响应的覆盖范围。

AhnLab EPP/V3

在CPS环境中，不仅需要考虑OT安全，还必须关注与OT环境相连接或管理OT环境的IT领域的安全。关键能力包括通过补丁管理最大限度地减少漏洞，以及通过反恶意软件来强力阻断威胁。



【图12】AhnLab端点平台（EPP）结构图

AhnLab EPP通过有机联动从反恶意软件到补丁管理的各种模块，防止IT环境中的威胁入侵OT环境。首先，为多数端点系统提供稳定且广泛的补丁管理功能，以减少端点攻击面。此外，反恶意软件模块（V3）在AV-TEST等全球认证评估中长期保持着顶级检测率，基于经验证的技术实力，提供全球最高水平的威胁拦截能力。

引进效果

AhnLab CPS PLUS基于IT-OT融合安全，有效地解决了CPS安全需求。通过这一平台，客户能够加速实现真正的数字化转型。

引进效果#1：保障运营可用性

CPS环境的首要任务是保障设备运营的可用性。AhnLab CPS PLUS通过多种优化于CPS环境特殊性的安全模块，在不增加系统负载的情况下，实现强大的安全防护。

引进效果#2：系统的威胁管理流程

AhnLab CPS PLUS采用了“识别 > 检测 > 响应”的系统化的威胁管理流程。它能够详细识别CPS资产，检测OT网络中传播的各种威胁和异常情况，提供不影响工序的最佳响应能力。

引进效果#3：便利的集成管理与监控

AhnLab CPS PLUS通过集成管理控制台AhnLab ICM，灵活联动CPS端点、安全模块、SIEM、TIP。由此，为有效管理CPS环境安全威胁，提供运营便利性。

结论

对于CPS环境的网络攻击正在持续增加，预计损损害规模也将逐渐扩大。虽然组织对OT安全的理解正在加深，但未来需要从整合IT和OT的安全视角出发进行思考。当然，这不是一个容易的事，但如果正确理解CPS安全的方法和架构，这个挑战并非是一个不可能的任务。

组织在推进CPS安全倡议时，应牢记以下三个建议：

#1.不仅要考虑OT安全，还要关注IT安全

正如本文中多次提到的那样，针对OT环境的威胁是从与OT连接的IT领域开始的。因此，为有效实现CPS安全，应采用融合IT与OT的整合安全方法。未来，CPS的连接点将超越IT和OT，扩大到更多领域。

#2.构建“识别 > 检测 > 响应”安全流程

资产识别、威胁检测与响应是CPS安全的基础。特别是在OT环境中，资产和网络的更改较少，因此如果基于充分的资产可见性和正确的检测威胁能力，构建威胁响应流程，从长远来看将带来很大的效果。

#3.倡导平台化而非单一解决方案

如今的CPS安全威胁早已超出了单一解决方案能够应对的范围，而且威胁将持续升级。因此，需要灵活联动各安全模块的CPS安全平台。提供优化的安全功能、综合可见性和管理能力的CPS安全平台是应对日益进化的CPS威胁的唯一方法。

Ahnlab已成为解决日益增加的CPS安全需求的最佳合作伙伴。AhnLab CPS PLUS集中管理和监控跨越IT和OT环境的各个安全模块，其广泛的安全覆盖范围在竞争对手中脱颖而出。覆盖多个行业的丰富的客户案例证明了该平台的卓越性。未来，AhnLab将继续增强各模块功能，并加强模块间的联动与整合，以支持面向未来的应用案例（use case）。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 (邮编: 100102) I 上海市闵行区万源路2158号 泓毅大厦1201室 (邮编: 201113)
https://www.ahnlab.com/cn
cn.sales@ahnlab.com
电话： +86 10 8260 0935/8（北京）I +86 21 6095 6780（上海）