AhnLab

AhnLab CPS PLUS

通过集成CPS安全实现数字化创新

融合了IT-OT的
CPS综合安全平台

背景

随着数字化的加快以及与IT领域的接触点增加，OT环境面临的网络攻击威胁也在不断上升。过去，由于OT环境具有严格控制外部访问的封闭性，相较于IT环境，一直被认为是相对安全的。然而，当前情况发生了变化，OT安全性不仅变得更加重要，而且迫切需要一种将OT与IT结合的全新的综合安全解决方案。

CPS（Cyber-Physical System，网络物理系统）是随着现有OT领域的外部连接的不断扩展而出现的概念，涵盖了OT、IT在内的广泛领域。为了有效保护涵盖多个环境的CPS，首先必须保障OT环境中优先考虑的“可用性（availability）”，并在提供资产可见性的基础上，通过多种安全模块之间的联动和集中管理来提高安全效率。

保障可用性

在涵盖IT与OT的CPS环境中，首先需要保护使用寿命长且难以进行安全补丁的OT环境中各种设备免受安全威胁，确保其安全运行。

确保可见性和检测/响应威胁

在可见性较低的OT环境中，需要确保对资产信息、网络状态、安全威胁及漏洞状况的可见性。并且，在保障各类设备可用性的前提下，进行安全威胁检测与响应。

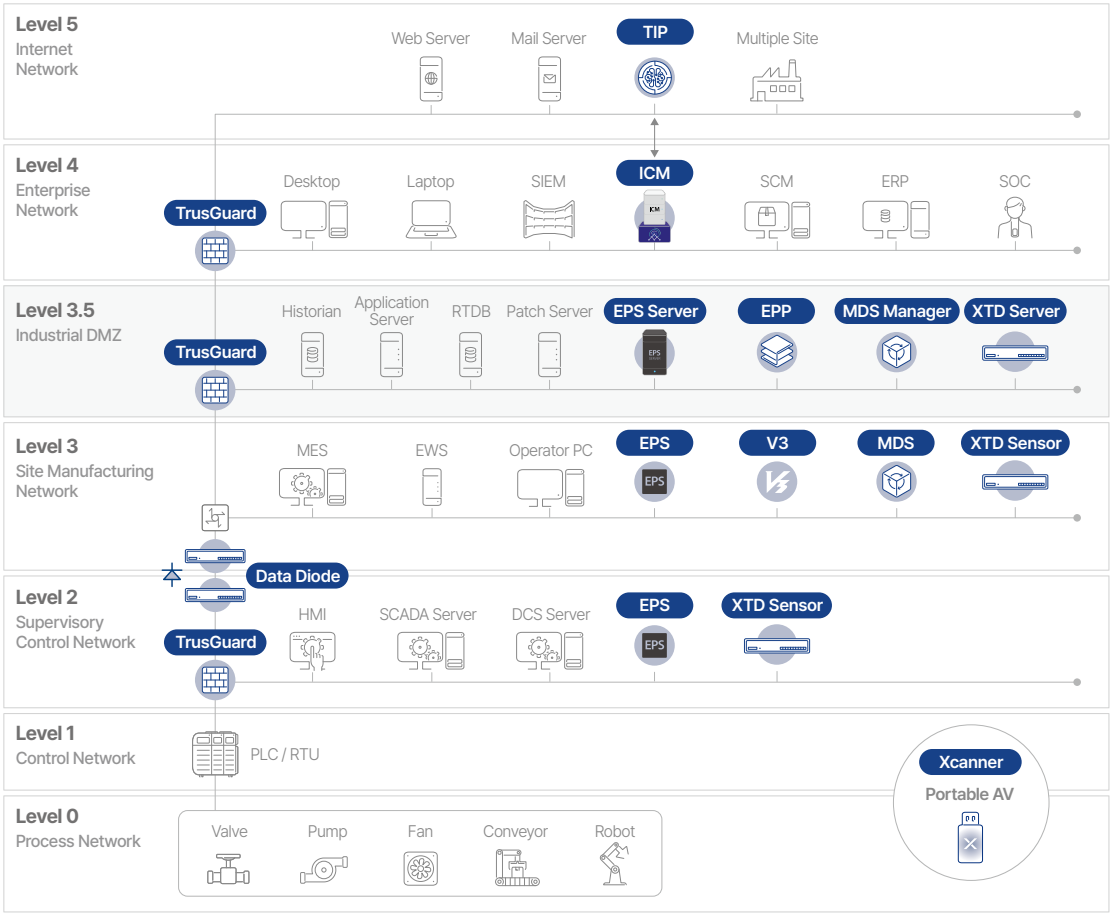
IT与OT融合安全

虽然OT网络是封闭的，但与IT网络系统的接触点日益增多，各种攻击频繁发生。因此，需要从CPS安全的角度来融合IT和OT的安全。此外，还需要一个支持安全模块之间联动和集中管理的综合安全平台，而不仅仅是单一的解决方案。

为什么选择 AhnLab CPS PLUS

AhnLab CPS PLUS是一个综合CPS安全平台， 广泛保护包括制造、炼油、运输等各个行业的OT端点和网络以及与OT连接的IT环境。它结合Ahnlab在威胁检测与响应方面的专业知识与OT技术实力，基于端点和网络安全技术，在覆盖IT和OT的CPS环境中提供了无缝的安全保护，包括：可见性、威胁检测与响应。平台内灵活联动的安全模块可以通过CPS安全集成管理解决方案“AhnLab ICM”进行有效地监控和运营。

AhnLab CPS PLUS是现有CPS安全平台中覆盖范围最广的平台。再加上卓越的技术实力和集成的协同效应，为客户提供差异化的CPS安全体验。



AhnLab ICM
基于CPS综合监控，提供可见性并管理安全模块

AhnLab EPS
OT端点进程和设备控制，恶意代码诊断

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

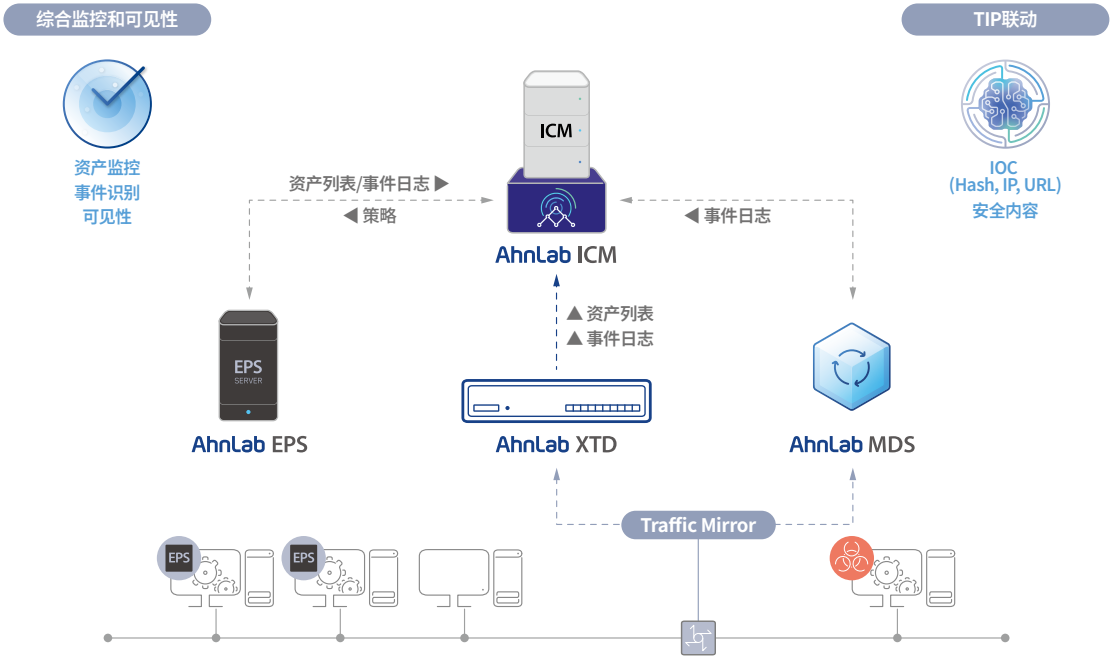
AhnLab TIP
覆盖IT和OT环境的CPS威胁情报

配置模块

1.AhnLab ICM（+TIP）

负责CPS安全集成管理的AhnLab ICM 通过仪表板一目了然地掌握联动模块的状态，从而确保对CPS环境的综合可见性。通过AhnLab EPS、XTD、MDS等覆盖整个CPS环境的模块状态、资产信息收集和事件监控，能够实时确认需要处理的问题。基于这种平台化中央管理能力，AhnLab ICM提供了综合可见性和全面威胁监控，不仅缩短了问题处理时间，还提高业务连续性和生产力。

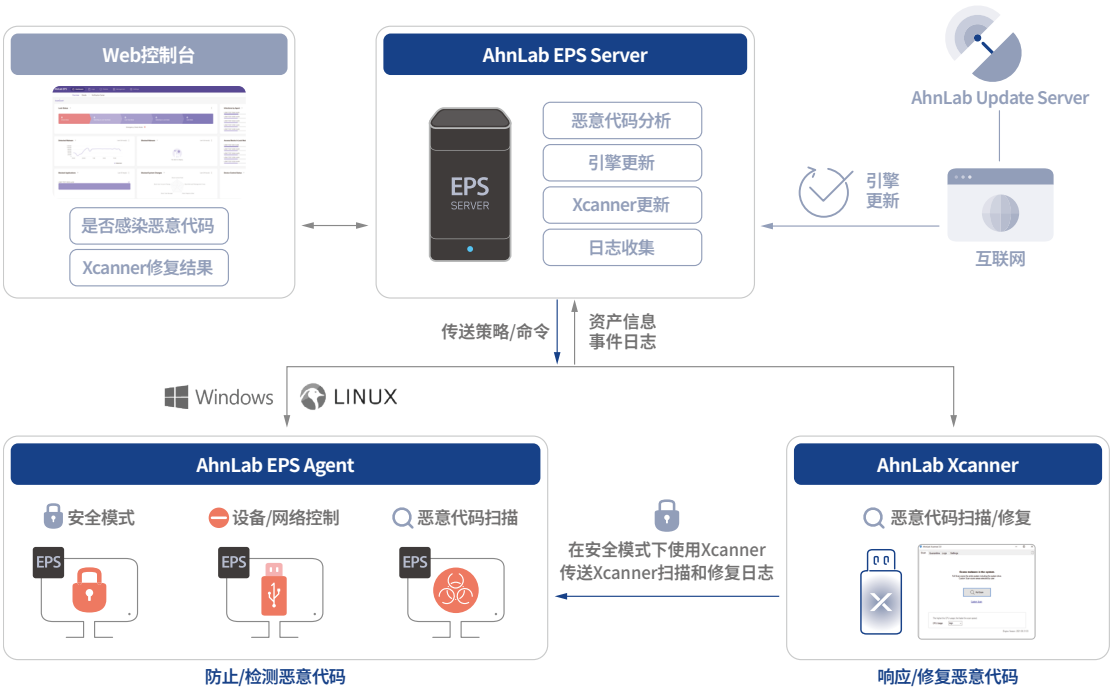
AhnLab TIP通过与AhnLab ICM联动，为CPS安全平台提供威胁情报。在AhnLab ICM中，用户可以通过覆盖IT和OT的CPS环境的入侵指标（IoC），实时获取更详细的信息。



2. AhnLab EPS & Xcanner

AhnLab EPS是专为OT网络设备安全优化的解决方案，通过阻止不受欢迎的程序、可移动设备、网络连接，保障业务连续性。此外，它支持从旧版本到最新版本的各种操作系统，如Windows、Linux、嵌入式系统，以适应设备的使用年限和环境特性。为了保障设备可用性，使用超轻量级Agent，最大限度地减少对系统资源的消耗，并在应用基于白名单的控制时，支持三个阶段的运营模式，以灵活应用策略。

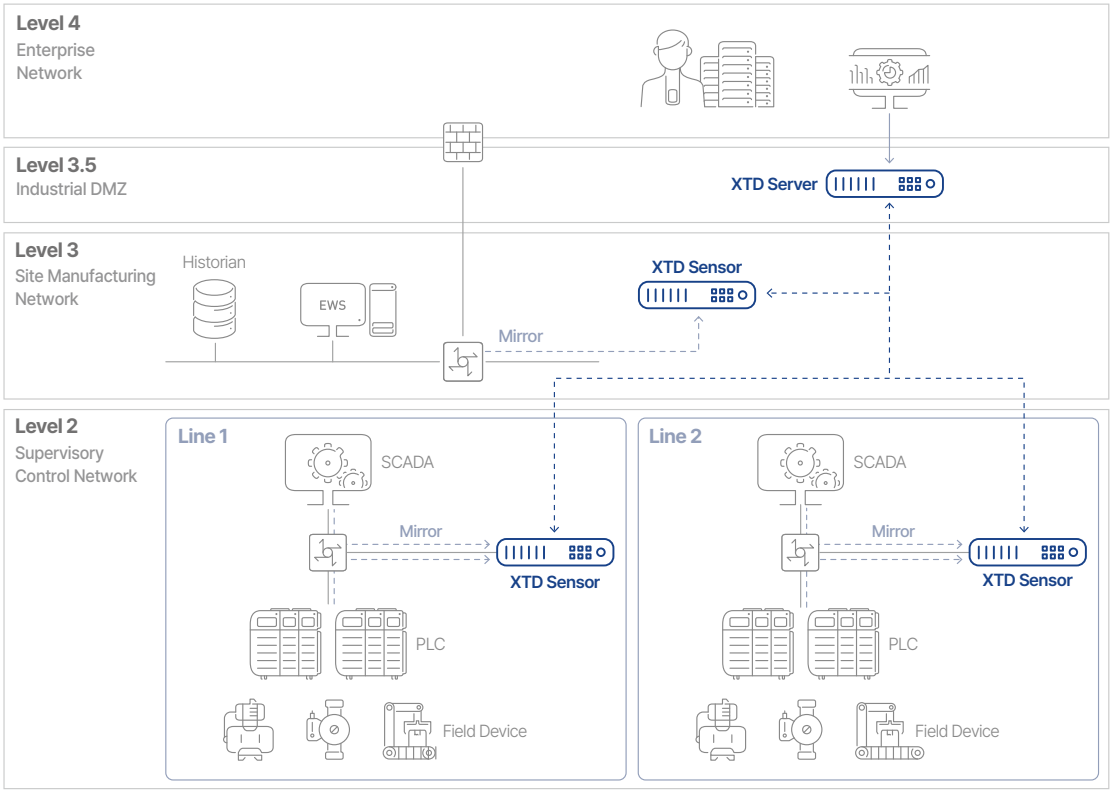
此外，对于疑似感染恶意代码的系统，可以利用OT便携式反恶意软件AhnLab Xcanner，无需另行安装解决方案，即可诊断并修复恶意代码。AhnLab Xcanner可以在授权的可移动存储设备上加载，或通过EPS Server发送到EPS Agent进行远程执行，扫描和修复情况可以通过EPS Server进行监控和管理。



3.AhnLab XTD

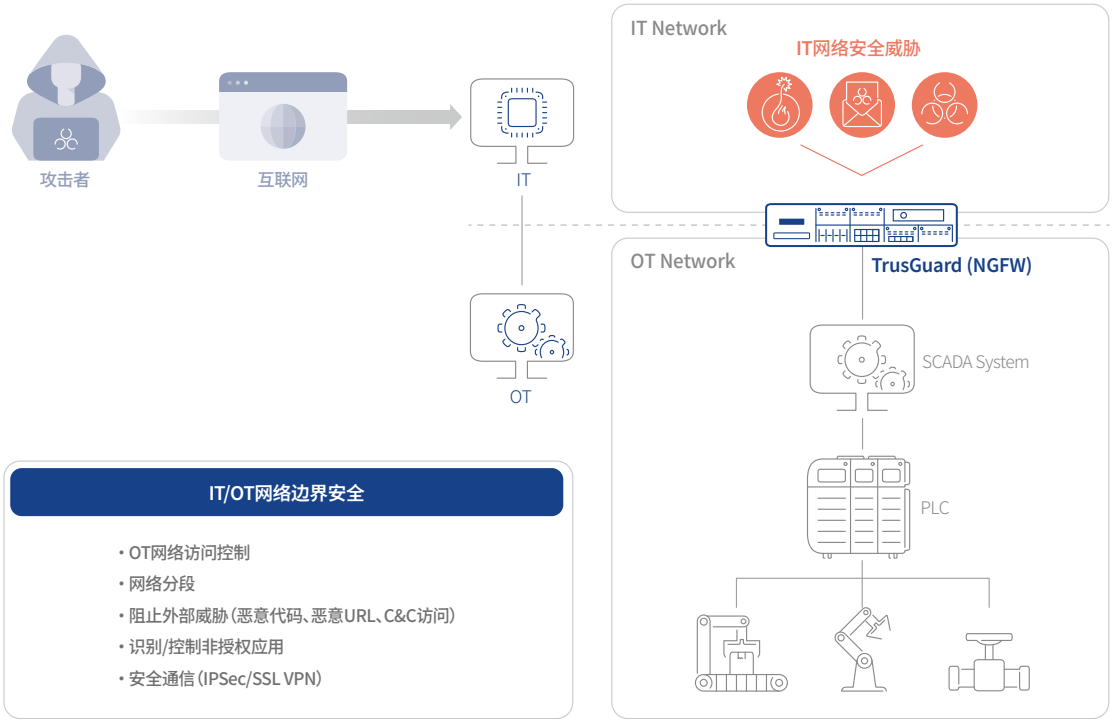
AhnLab XTD通过基于OT网络的可见性和威胁检测模块，为各种OT网络资产提供可见性。同时，能检测从IT网络流入或在OT网络内部系统之间传播的恶意代码或漏洞等安全威胁。AhnLab XTD采用了被动扫描（passive scan）方式，保障OT设备可用性，并基于自主研发的协议分析技术和深度数据包检测（DPI）功能，提供各种设备识别和异常控制逻辑的检测和分析。

此外，通过与OT端点安全模块AhnLab EPS的联动，可以整合EPS Agent识别的设备资产信息，提供广泛而详细的资产可见性。这两个模块的联动在检测和响应OT网络中传播的安全威胁方面发挥出色的能力。通过AhnLab EPS服务器的Restful API联动支持Xcanner远程扫描，当在网络中检测到恶意代码传播或恶意利用漏洞的有害流量时，会进一步对位于端点区域的可疑系统执行恶意代码扫描。



4.AhnLab TrusGuard

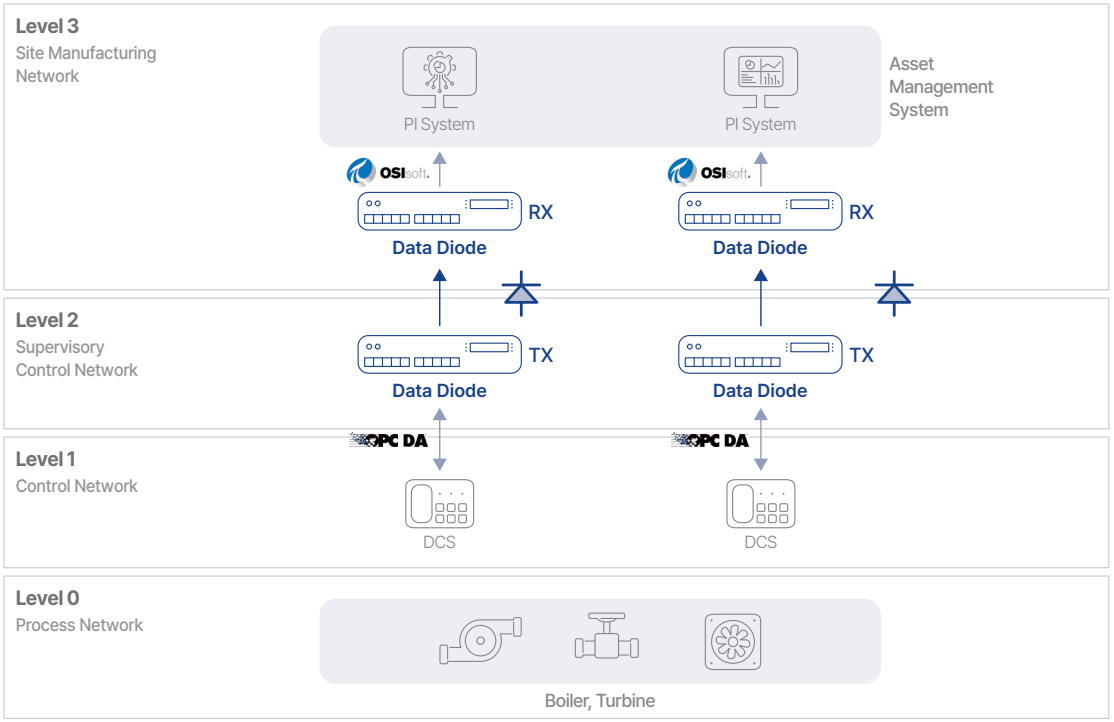
下一代防火墙AhnLab TrusGuard可在OT网络边界检测有害流量并阻止其访问，还支持IPSec/SSL VPN等安全通信和网络分段等功能。此外，可以识别Modbus、DNP3等OT协议，并可以详细控制功能码（function code）。



5.AhnLab 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。

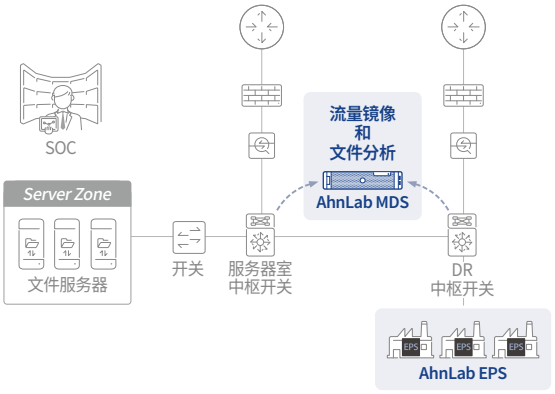
基于涵盖IT和OT环境的广泛协议支持技术，能够在多种环境中进行优化采用。还可以根据需要提供各种IT/OT协议、闭路电视流数据、数据库等多种应用场景。

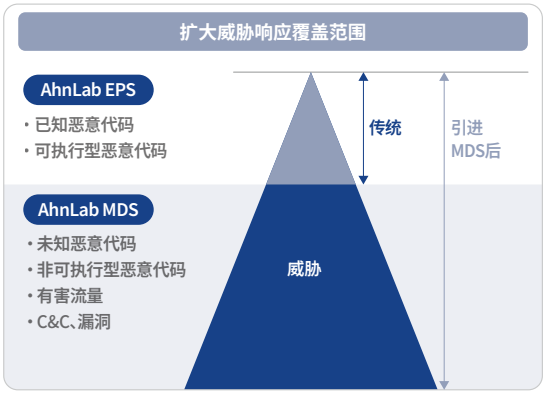


6.AhnLab MDS

网络沙箱模块AhnLab MDS专为响应日益复杂的新种和变种恶意代码而设计，通过收集生产网络中传输的文件，对恶意代码进行动态分析。MDS通过检测和监控各种安全威胁，如攻击者的C&C IP连接、恶意代码扩散和漏洞利用，提供卓越的响应能力。

此外，当与OT端点安全模块EPS联动时，基于MDS动态分析功能，可以防御新种、变种和未知恶意代码，从而扩大综合威胁响应覆盖范围。





7.AhnLab EPP/V3

在CPS环境中，不仅需要考虑OT安全，还要考虑与OT环境连接或管理OT环境的IT领域的安全。为确保全面安全，必须具备通过补丁管理来最小化漏洞，以及通过反恶意软件的强有力的拦截能力。

AhnLab EPP通过有机整合反恶意软件、补丁管理等多个模块，防止IT环境中的威胁渗透到OT环境。首先，它为多数端点系统提供稳定且广泛的补丁管理功能，从而实现端点强化（Hardening）。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最高水平的检测率，凭借经过验证的技术，提供全球最高水平的威胁拦截能力。

引进效果

AhnLab CPS PLUS通过IT-OT融合安全，能够有效满足CPS安全需求，帮助各位客户实现加速数字化创新。

保障运营可用性

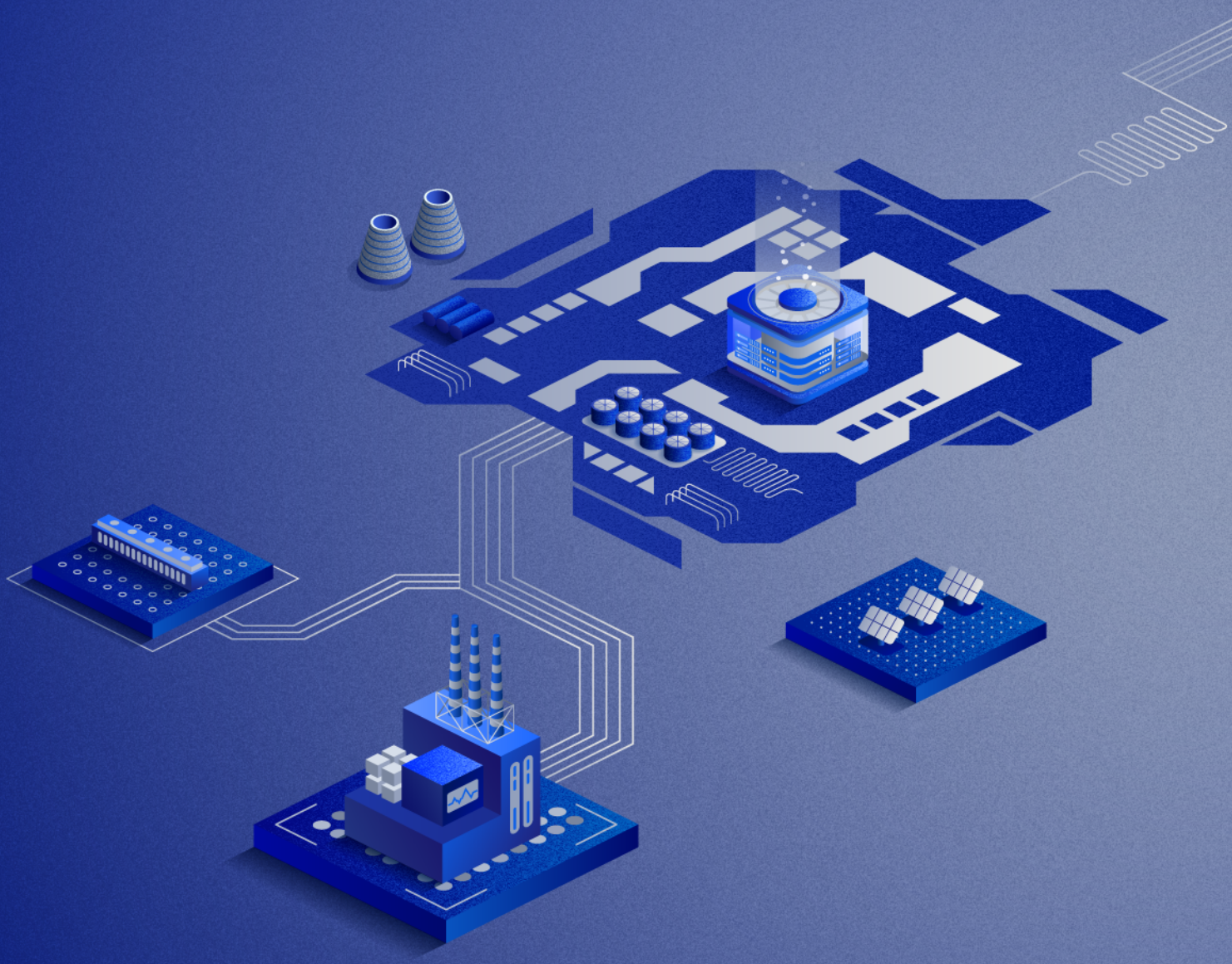
AhnLab CPS PLUS集成了反映CPS环境特殊性的多个安全模块， 在不增加系统负载的情况下实现强大的安全。

系统化的威胁管理流程

AhnLab CPS PLUS具备由“识别 > 检测 > 响应”的系统化威胁管理流程。精准识别CPS资产，检测异常迹象，并实施不影响工艺的最佳响应。

可见性和运营便利性

AhnLab CPS PLUS通过综合管理控制台AhnLab ICM，灵活地连接CPS端点、网络安全模块、SIEM和TIP。通过这种方式，在整个CPS环境中提供了更高的可见性和运营便利性。



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
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话：+86 10 8260 0932（北京）| +86 21 6095 6780（上海）

AhnLab