AhnLab EPS

针对 OT 环境中各种专用系统优化的安全解决方案

保障专用系统可用性的轻量级 Agent
通过安全模式功能主动拦截新种与变种安全威胁

产品概要

AhnLab EPS（Endpoint Protection System）是一款专为 OT 环境中专用系统优化设计的安全解决方案，这些系统需要执行预定义进程并限制使用应用程序。AhnLab EPS 能够在保障生产设备系统（ICS）、销售终端设备（POS）、自主服务机（KIOSK）、自助发放机等各种专用系统的可用性的同时，为其提供全面的保护。

- 保障可用性
- 停机时间最小化
- 系统资源占有率最小化
- 限制使用应用程序
- 支持多种环境

特点及优势

基于允许列表（AllowList）的程序控制

- 通过创建允许列表（AllowList），仅运行运营所需的程序
- 支持系统安全模式功能，维持安全的系统运行环境
- 设置安全模式允许程序，可在安全模式（Lock Mode）下安装和更新运营所需程序

各种拦截策略以增强安全性

- 创建拦截列表（Blocklist）来阻止不必要的程序运行
- 阻断对系统重要设置的更改路径
- 阻止针对特定网络的攻击，设置基于主机的防火墙
- 控制 USB、CD/DVD、蓝牙等外部设备
- 通过基于 ASD（AhnLab Smart Defense）云端扫描大容量文件

提高客户端安全管理效率

- 搜索未安装客户端（Agent）的计算机
- 查看设备补丁信息（Windows KB、Linux RPM）
- 监控并阻止重要文件完整性更改

EPS 客户端集成管理和通过监控实现的运营便利性

- 通过监控中心（仪表板），进行实时综合监控
- 统一管理和查询安装在各种操作系统的 EPS 客户端策略
- 通过客户端远程控制提升管理便利性和维护效率

安全稳定的系统运营

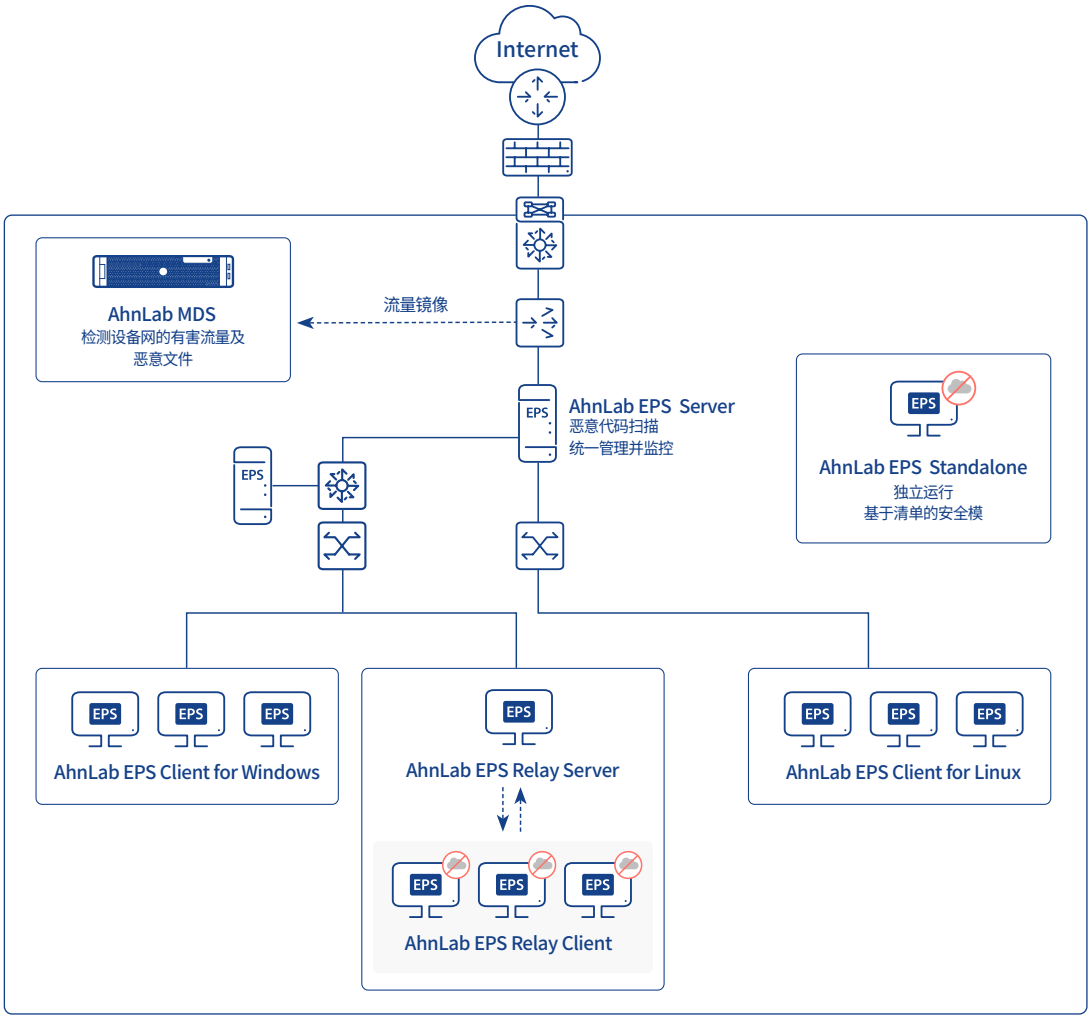
- 搭载稳定专用引擎的服务器（AhnLab EPS Server）和超轻量客户端（AhnLab EPS Client）
- 最小化系统资源占有率，构建以高可用性为核心的强大安全体系

高效的安全运营

AhnLab EPS 提供“三个阶段的运行模式”，有助于高效的专用系统安全运营和管理。通过安全模式功能的“禁用安全模式（Unlock Mode）> 安全测试模式（Lock Test Mode）> 安全模式（Lock Mode）”，实现稳定且优化的安全策略设置和管理，而无需中断系统运行。

引进方式和主要功能

根据客户环境，AhnLab EPS 提供“主从式架构（托管方式）”和“独立式架构（Standalone）”的两种方式。



1. 主从式架构（托管方式）

主从式架构由中央监控及策略管理的服务器（EPS Server）和安装在终端系统的轻量级 Agent（EPS Client）构成，可以确保专用系统的稳定运行。

在无法直接与 EPS 服务器通信的独立网络环境（如多台计算机一体式设备）中，可以通过中继服务器和中继客户端实现对终端的集中安全管理。

组成部分		主要功能
服务器	AhnLab EPS Server	• 统一管理和监控客户端、中继服务器、中继客户端的策略
客户端	AhnLab EPS Client for Windows	• 基于Windows操作系统的终端安全防护 • 安全模式、外部设备控制、系统控制、防火墙、网络攻击检测、恶意代码扫描
	AhnLab EPS Client for Linux	• 基于Linux操作系统的终端安全防护 • 安全模式、系统控制、恶意代码扫描
中继服务器	AhnLab EPS Relay Server for Windows	• EPS中继客户端与EPS服务器之间的通信中继 • 安全模式、外部设备控制、系统控制、防火墙、网络攻击检测、恶意代码扫描
中继客户端	AhnLab EPS Relay Client for Windows	• 与EPS Server无法直接通信的环境下的终端安全 • 安全模式、外部设备控制、系统控制、防火墙、网络攻击检测

2. 独立式架构（Standalone 方式）

独立式架构由独立的 Agent（AhnLab EPS Standalone）构成，可以保护在脱机状态下仅使用有限程序的专用系统。

组成部分	主要功能
AhnLab EPS standalone	• 基于Windows操作系统的脱机终端安全防护 • 管理策略设置、日志保存与查询 • 安全模式、外部设备控制

基于联动的 CPS 安全强化

随着 OT 环境的外部连接的日益增加，不仅是 OT 环境，覆盖与 OT 相连的 IT 环境在内的 CPS（Cyber-Physical System）安全概念逐渐受到关注。AhnLab EPS 与 AhnLab CPS 安全平台“AhnLab CPS PLUS”中的多个安全模块联动，有效应用 CPS 安全威胁，进一步强化安全防护能力。

AhnLab Xcanner	**非安装型便携式反恶意软件** • 检测并清除OT端点系统中的恶意代码 • 可通过AhnLab EPS远程运行
AhnLab MDS	**网络沙箱分析** • 动态分析ATP攻击和新/变种恶意代码 • 恶意代码分析结果发送到AhnLab EPS服务器
AhnLab XTD	**OT网络可视化与威胁检测** • IT/OT协议分析、资产识别以及OT网络中的恶意代码和漏洞检测 • 收集与AhnLab EPS联动的设备详细信息，并对可疑系统进行远程扫描（Xcanner）
AhnLab ICM	**CPS环境集成监控与管理** • 基于从各模块收集的信息，提供集成的可视化与监控 • 管理安装在多个站点（Multiple Site）的AhnLab EPS服务器

使用环境

1. 主从式架构（托管方式）

AhnLab EPS Server

类别		最低要求
硬件	CPU	Intel®Xeon®Processor E5 Family（16 core以上、3GHz以上、8MB Cache以上）
	内存	32GB或更多
	硬盘	操作系统专用：300GB x 2 （RAID 1）或更多可用空间 数据专用：2TB或更多可用空间（推荐RAID配置）
操作系统		Red Hat Enterprise Linux 9.2（64 bit）
VM 环境		VMware，AWS
WEB 控制台（浏览器）		Google Chrome 96或更高版本 Microsoft Edge 122或更高版本 ※ Internet Explorer仅用于下载客户端（Agent）安装文件

* 最低要求是最多安装20,000台 Agent环境下的标准，根据文件收集量可能会需要增设服务器。

AhnLab EPS Client for Windows

类别		推荐配置
硬件	CPU	Pentium 133Mhz以上
	内存	15MB或更多
	硬盘	100MB或更多可用空间
操作系统	嵌入式	Windows Embedded XP, Standard 2009, Standard 7, POSReady 2009, POSReady 7, 8.1 Industry, 10 IoT Enterprise, 11 IoT Enterprise
	客户端	Windows 2000, XP, Vista, 7, 8(8.1), 10, 11
	服务器	Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003, 2008, 2012, 2016, 2019, 2022

* 由于SHA-1代码签名终止支持，可用版本和功能可能会因操作系统而异。
* 上述操作系统均支持32/64 bit

AhnLab EPS Relay Server, AhnLab EPS Relay Client

类别		推荐配置
硬件	CPU	Pentium 133Mhz以上
	内存	15MB或更多
	硬盘	100MB或更多可用空间
操作系统	嵌入式	Windows Embedded Standard 2009, 7, 7 SP1 (KB4490628, 4474419 补丁环境) Windows Embedded POSReady 2009, 7 Windows Embedded 8.1 Industry Windows Embedded 10 IoT Enterprise, 11 IoT Enterprise
	客户端	Windows 2000, XP, XP SP3, Vista, Vista SP2 (KB4493730, 4474419 补丁环境), 7, 7 SP1 (KB4490628, 4474419 补丁环境), 8, 8.1, 10, 11
	服务器	Windows 2000, 2003, 2003 R2, 2008, 2008 SP2 (KB4493730, 4474419 补丁环境), 2008 R2, 2008 R2 SP1 (KB4490628, 4474419 补丁环境), 2012, 2016, 2019, 2022

* 上述操作系统均支持32/64 bit
* 仅支持在Relay Client上运行Windows 2000和XP
* 仅支持在Relay Server上运行Windows XP SP3

AhnLab EPS Client for Linux

类别		推荐配置
硬件	CPU	英特尔系列（32/64位）
	内存	1GB或更多
	硬盘	500MB或更多可用空间
操作系统		CentOS 3.3~8.1 / Red Hat Enterprise Linux 3.3~8.1, 8.4, 8.6~8.8 / Red Hat Linux 9 / antiX Linux 13.2, 15, 16.2, 17.2 / Ubuntu 10.04, 11.04, 11.10, 12.04, 14.04, 18.04, 20.04, 22.04 / Ruby Duck release 5.6(Marcy 5.1) / SUSE Linux 9.2, 10.3 / Fedora 8, 14

2. 独立式架构（Standalone 方式）

AhnLab EPS Standalone

类别		推荐配置
硬件	CPU	Pentium 233MHz以上
	内存	64GB或更多
	硬盘	1.5GB或更多可用空间
操作系统	嵌入式	Windows Embedded Standard 2009 / Standard 7 / POSReady 2009 / POSReady 7 / 8.1 Industry(Pro, Enterprise) / 10 IoT Enterprise
	客户端	Windows XP SP2, SP3 Professional / Vista(Enterprise, Ultimate) / 7(Professional, Enterprise, Ultimate) / 8, 8.1(Pro, Enterprise) / 10(Pro, Enterprise) / 11(Professional, Enterprise)
	服务器	Windows Server 2008(Standard, Enterprise) / 2012(Essentials, Standard) / 2016(Essentials, Standard) / 2019(Essentials, Standard) / 2022 (Essentials, Standard)

* 上述操作系统支持32/64 bit

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）