AhnLab EPS

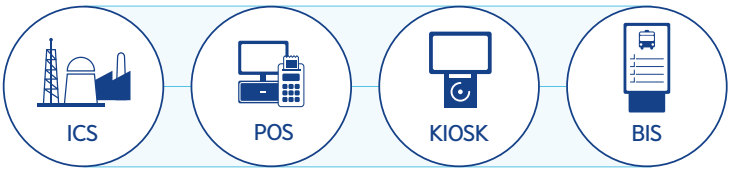
优化于工控系统的安全解决方案

轻量级的 Agent 最大程度地降低对系统可用性的影响
通过安全模式功能防止恶意代码扩散

轻量级　系统可用性　安全模式　检测与拦截

产品概要

AhnLab EPS(Endpoint Protection System) 是一款运行预定义的进程并使用明确而有限的应用程序的安全解决方案。AhnLab EPS 优化于诸如工控系统 (ICS), 销售终端设备 (POS), 自助服务机 (KIOSK) 和自助发证机等，不影响这些系统的可用性并保护其安全。



- 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

AhnLab EPS 基于 AhnLab 独有的白名单 (Whitelist) 技术，通过阻止一切不必要或未经授权程序的运行，诸如外部媒体连接，系统更改，网络连接等，可以提前预防因恶意代码或职员非业务行为导致的安全威胁和系统障碍，从而实现工控系统的不间断且稳定运行。

基于白名单的安全模式

- 通过阻止文件生成，删除，更改及运行等，可实现强有力的保护
- 通过使用三个阶段运营模式，可实现有效运营

在确保系统可用性的前提下，检测恶意代码并防止其扩散

- 通过轻量级的 Agent, 最大程度地降低终端系统的资源占有率
- 通过专用引擎，可实现稳定且精确的恶意代码检测
- 阻止运行和删除检测到的恶意文件

各种拦截策略以强化安全

- 阻止黑名单程序的运行
- 阻断系统的重要设置更改路径
- 拦截网络特定攻击，设置基于主机的防火墙
- USB, CD/DVD, 蓝牙等可移动设备控制

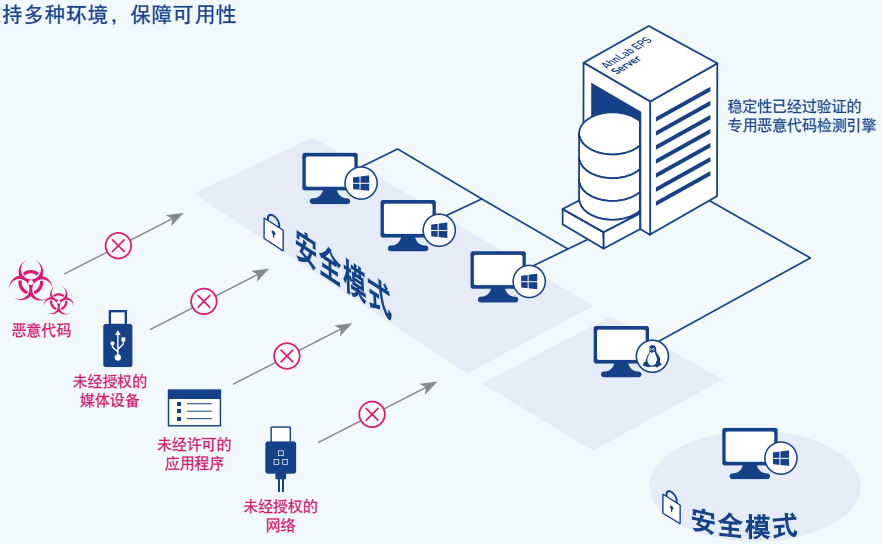
通过对 EPS 客户端的集成管理和监控以提供运营方便

- 通过仪表板 (Dashboard)，实现中央管理和实时监控
- 统一管理各种操作系统上的 EPS Agent 策略
- 通过远程控制客户端，提升管理便捷性

安全稳定的系统可用性

AhnLab EPS 具有优化于工控系统环境的恶意代码检测技术，提供对终端系统的安全模式功能。通过搭载了稳定的专用引擎的服务器（AhnLab EPS Server）和超轻量级 Agent(AhnLab EPS Client)，使系统资源占有率最小化，以及有效检测并拦截恶意代码，实现以可用性为中心的强大的安全体系。

- 终端资源负担最小化，强有力的安全模式功能
- 基于专用引擎的恶意代码检测
- 支持多种环境，保障可用性



高效的安全运营

AhnLab EPS 提供“三个阶段运营模式”，保障工控系统运营的稳定性和安全性。通过安全模式功能中的“禁用安全模式 > 安全测试模式 > 安全模式”，实现稳定且最优化的安全策略设置和管理，而无需中断系统运行。

禁用安全模式

- Agent 首次安装在客户端 PC 的状态
- 可进行系统更改及系统维护工作

安全测试模式

- 转换为安全模式前，定义安全策略
- 安全模式模拟(记录日志)
- 验证可用性 及设置例外

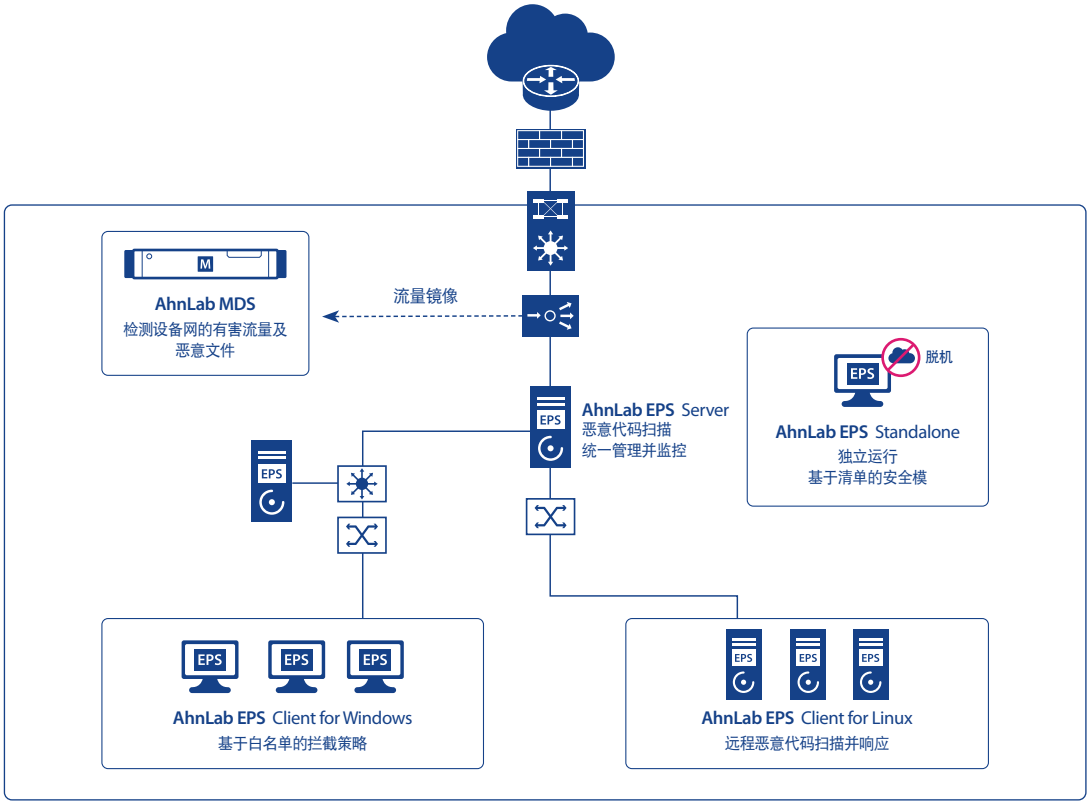
安全模式

- 转换为安全模式
- 根据已定义的策略，不允许系统任何更改
- 基于各种安全策略进行拦截

紧急检查模式
(可保持特定拦截策略)

引进方式及主要功能

AhnLab EPS 根据系统的运行环境，提供“主从式架构 (托管方式)”和“独立式架构 (Standalone)”。



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 服务器）和安装在终端系统的轻量级 Agent(EPS 客户端）构成，可以稳定地运营工控系统。

组成部分		主要功能
服务器	AhnLab EPS Server	· 统一管理EPS客户端策略 · 基于仪表板的统一监控 · 恶意代码扫描并响应 · 引擎更新管理 · 日志查询，远程控制 · 与基于沙箱的APT解决方案AhnLab MDS联动
Agent	AhnLab EPS Client for Windows	· 基于Windows操作系统的终端安全防护 · 提供三个阶段运营模式 · 基于白名单安全模式 · 控制媒体设备、阻止系统更改、阻止程序运行 · 基于主机的防火墙设置 · 检测网络攻击 · 恶意代码实时扫描、手动扫描及计划扫描
	AhnLab EPS Client for Linux	· 基于Linux操作系统的终端安全防护 · 恶意代码手动扫描及计划扫描 · 根据安全策略响应恶意文件

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应用程序的工控系统。

组成部分	主要功能
AhnLab EPS standalone	· 独立运行　基于Windows操作系统的脱机终端安全防护 · 提供三个阶段的运营模式 · 基于清单的安全模式 · 设置管理策略、导入/导出策略 · 保存和查询日志

使用环境

1. 主从式架构 (Managed 方式)

AhnLab EPS Server

项目		最低配置要求
硬件	CPU	Intel®Xeon®Processor E5 Family(8 core 以上, 3GHz 以上, 8MB Cache 以上)
	内存	16GB以上
	HDD	操作系统专用：300GB x 2 (RAID 1)以上 DATA专用：1TB以上(推荐RAID配置)
操作系统		RHEL 7.6(64 bit)
控制台 (浏览器)		Internet Explorer 8.0 以上

* 该要求是使用8,000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

区分		推荐配置
硬件	CPU	Pentium 133MHz以上
操作系统	嵌入式	Windows Embedded XP / Standard 2009 / Standard 7 / POSReady 2009 / POSReady 7/ 8.1 Industry(Pro, Enterprise)
	客户端	Windows 2000 Professional / XP(Home, Professional) / Vista (Enterprise, Ultimate) / 7(Professional, Enterprise, Ultimate) / 8, 8.1(Professional, Enterprise) / 10(Professional, Enterprise) / 10 IoT Enterprise
	服务器	Windows Server 2000(Server, Advanced Server) / Windows Server 2003(Standard, Enterprise) / 2008(Standard, Enterprise) /2012(Essentials, Standard) / 2016(Essentials, Standard) / 2019(Essentials, Standard)

* 上述操作系统支持32/64 bit
* 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。

AhnLab EPS Client for Linux

区分	推荐配置
硬件 (CPU)	Intel系列(32/64 bit)
操作系统	CentOS 3.3 ~ 8.1
	Red Hat Enterprise Linux 3.3 ~ 8.1
	antiX Linux 13.2, 16.2

2. 独立式架构 (Standalone 方式)

AhnLab EPS Standalone

项目		推荐配置及详细版本
硬件	CPU	Pentium 233MHz以上
	内存	剩余空间大于64MB
	硬盘	剩余空间大于1.5GB
操作系统	嵌入式	Windows Embedded Standard 2009 / Standard 7 / POSReady 2009 / POSReady 7 / 8.1 Industry(Pro, Enterprise)
	客户端	Windows XP SP3(Home, Professional) / Vista(Enterprise, Ultimate) / 7(Professional, Enterprise, Ultimate) / 8, 8.1(Pro, Enterprise) / 10(Pro, Enterprise)
	服务器	Windows Server 2008(Standard, Enterprise) / 2012(Essentials, Standard) /2016(Essentials, Standard) / 2019(Essentials, Standard)

* 上述操作系统支持32/64 bit

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 | 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）