

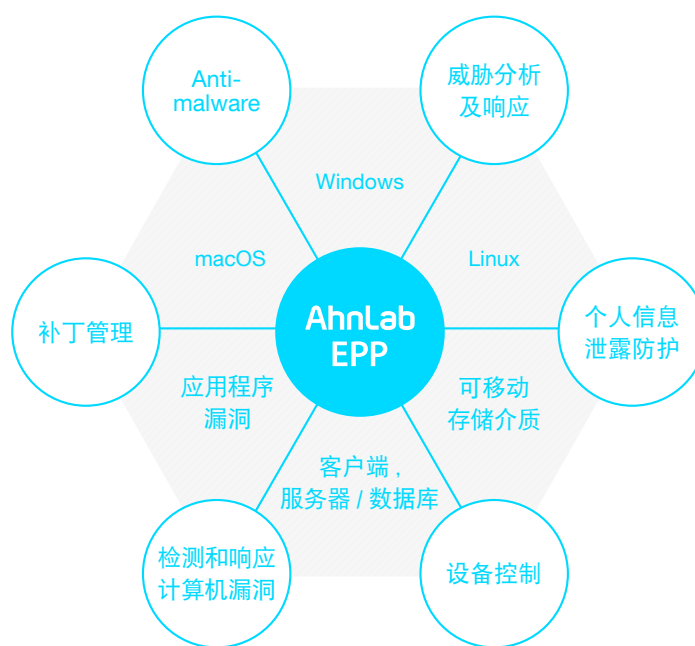
AhnLab EPP

下一代端点集成安全平台

基于单一 Agent, 单一管理控制台的统一安全运营及管理
通过连接规则的强大的威胁应

产品简介

AhnLab EPP 是威胁管理及响应观点的下一代端点安全平台 (Endpoint Protection Platform)。基于单一 Agent, 单一管理控制台有效管理复杂的端点环境, 并更好地响应越来越高级的安全威胁。



特点

高效的端点综合管理	<ul style="list-style-type: none">· 通过单一管理控制台(Single Management Console) 的有效且统一的安全运营· 通过基于Web管理员控制台及各种管理功能实现简化运营
优化的威胁管理和响应	<ul style="list-style-type: none">· 通过防病毒软件(V3) 和EDR等各种安全解决方案来监控和响应威胁· 通过Syslog联动第三方解决方案最大限度地提高安全管制效果
灵活的扩展性及运营稳定性	<ul style="list-style-type: none">· 软件方式的灵活的构建和扩展· Scale-out方式的简单的向外扩展服务器

独特的安全体系

通过 AhnLab EPP 的单一 Agent 和单一管理控制台 轻松管理防病毒软件、补丁、个人信息泄露防护和安全漏洞检查以及端点威胁检测和响应解决方案，并即时采取措施。



通过单一Agent和单一管理控制台轻松简单运营各种安全解决方案！

 V3 产品群	最佳的防病毒解决方案 <ul style="list-style-type: none">· 受到许多国际认证机构认可的世界最高级水准的威胁响应技术· 通过多维度分析平台的强大的检测技术· 基于各种操作系统(Multi OS) 的PC和服务器安全<ul style="list-style-type: none">-桌面版版：V3 Internet Security 9.0, V3 Endpoint Security 9.0(提供媒体控制功能), V3 for Mac-服务器版：V3 Net for Windows Server, V3 Net for Unix/Linux Server-虚拟化系统：V3 for VDI(Agent)
 EPP Privacy Management	个人信息泄露可疑文件的检测和拦截解决方案 <ul style="list-style-type: none">· 检测响应通过各种端点渗透的个人信息泄露可疑文件· 使用神经网络的搜索技术最大限度提高检测准确性和使用方便性· 使用文档变换技术检出各种文档文件中的个人信息
 EPP Patch Management	独门的补丁管理解决方案 <ul style="list-style-type: none">· 提供由Patch Lab验证的安全的补丁· 自动化的补丁管理可防止安全事件· 可以设置各种补丁管理策略
 EPP Security Assessment	计算机漏洞检测和响应解决方案 <ul style="list-style-type: none">· 提供同类产品中最高级别的检查项目· 可以通过管理员定义的检查功能添加检查项目· 方便的自动响应功能最大限度地提高用户便利
 EDR	端点威胁检测和响应解决方案 <ul style="list-style-type: none">· 同类最佳端点安全企业的下一代端点威胁检测和响应解决方案· 基于行为分析引擎收集和分析端点的所有行为和信信息· 提供持续监控和端点威胁可见性

强大的威胁响应

通过 AhnLab EPP 有机连接多个端点安全解决方案之间的规则和响应措施,更有效地应对安全威胁。根据安全管理员的需求可以应用各种安全策略,从而实现客户驱动型和主动型安全运营。

- 连接规则设置: 利用 and 和 or 条件将连接各产品的规则
- 连接响应设置: 针对违反连接规则的系统设置单独或共同的响应策略

连接规则设置示例

规则设置

共同	Agent版本	
V3	上次扫描日	10
APM	所有补丁安装率	70

OR +

V3	恶意代码检测次数	5
----	----------	---

在特定版本的所有Agent中, 检测满足如下条件的Agent

- ▲在一定期间未使用V3进行系统扫描(and)
- ▲补丁安装率不及70%(or)
- ▲V3检出恶意代码次数超过阈值

连接响应设置示例

响应设置

共同	选择响应	+	↓	↑
V3	扫描	×	↓	↑
APM	检查软件安装	×	↓	↑
EDR	检索文件	×	↓	↑

文件名:

哈希值:

文件大小: =

文件路径:

针对违反连接规则的Agent, 做出如下响应措施

- ▲发送通知
- ▲使用V3进行系统扫描
- ▲根据补丁策略安装软件
- ▲通过EDR确认是否存在具有特定哈希值的文件

优化的安全运营

通过 AhnLab EPP 的多样且方便的功能, 可以根据企业和组织的业务环境 and 安全需求构建优化的安全运营系统。

自动化Syslog联动



- 与各种第三方解决方案(SIEM,ESM,综合日志)轻松方便实现联动
- 同时支持Syslog UDP 和TCP, TCP over SSL - 安全管理员可选择指定联动信息
- 通过连接诸如AhnLab EDR等各种AhnLab安全解决方案和第三方解决方案, 实现丰富的威胁情报

自动收集端点威胁信息



- 分析端点的可疑系统
- 通过Agent自动收集威胁信息(通过AhnReport收集文件)
- 通过连接AhnLab专家服务(AhnLab Professional Service), 进行事后威胁分析和入侵事故响应 - 提供详细分析报表、响应指南

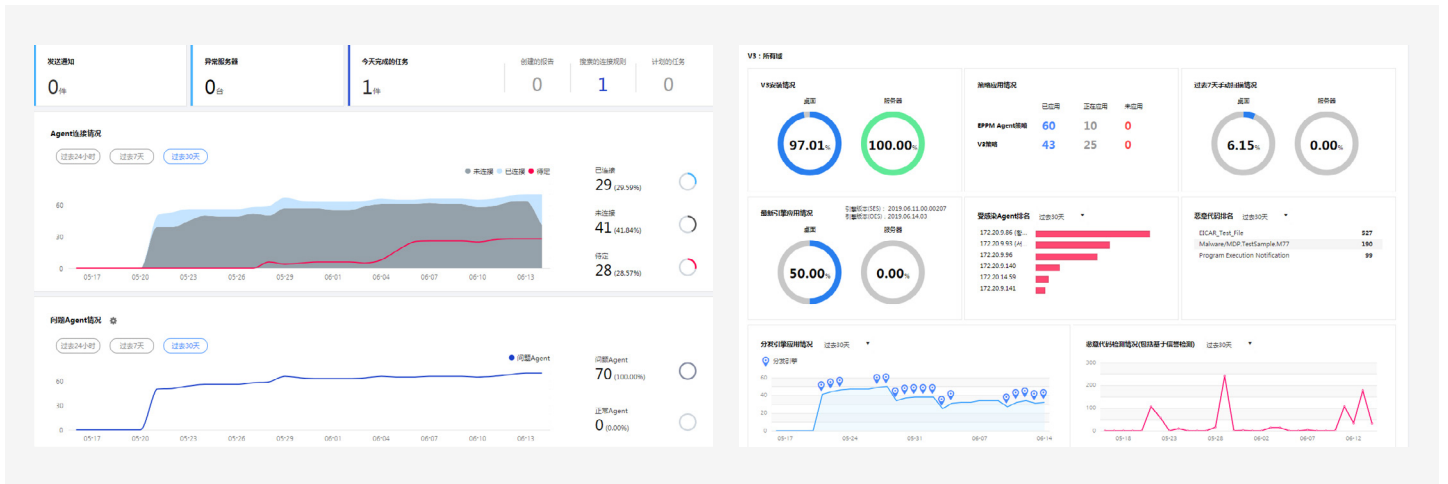
灵活扩展性和运营稳定性



- 可以根据客户企业规模和环境灵活配置
- 基于模块化配置方式的多样的构建和灵活的扩展性
- 基于负载均衡(Load Balancer, Active-standby)防止性能过载和通过流量分散处理的运营稳定性

出色的
可管理性

AhnLab EPP 提供基于 Web 的管理控制台和各种管理菜单，便于安全解决方案的运营。基于动态 UX 的直观的仪表板可以一目了然地提供端点可见性，以便安全管理员的有效管理和及时响应威胁。



AhnLab EPP 仪表板

使用环境

AhnLab EPP 由 AhnLab EPP Management（基于 Web 的中央管理控制台）和安装在端点系统上的 Agent 组成。

组成部分	类别	详细版本
管理控制台	网页浏览器	· Google Chrome(Windows, Mac)最新版本
Agent	操作系统	<ul style="list-style-type: none"> · Windows 8(8.1) / 10 / 10 IoT Enterprise · Windows Server 2012(包含R2) / 2016 / 2019 * 支持上述操作系统的64位兼容模式 · macOS Sierra(10.12) ~ Catalina(10.15), 11(Big Sur)

* Windows7和Windows Server 8(包含R2)在支持SHA-2的环境中可用。
有关更多信息，请访问 <https://cn.ahnlab.com/site/support/notice/noticeList.do>