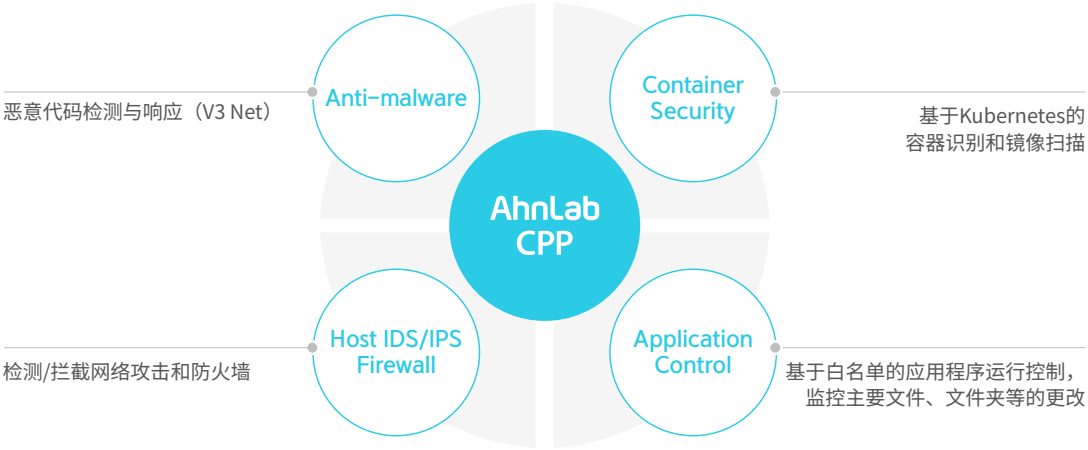
AhnLab CPP

混合 & 多云环境安全平台

提供对云工作负载的可视性
为服务器工作负载的特性提供优化的安全支持

产品概要

AhnLab CPP（Cloud Protection Platform）是为保护云工作负载而设计的平台（CWPP），为云计算资源上的物理服务器、虚拟服务器、云实例提供基于主机的运行时安全。其主要功能包括反恶意软件、IDS/IPS、防火墙、应用程序控制、完整性监控等。此外，CPP 能够识别在 Kubernetes 环境中运行的容器，支持拓扑结构可视化，并对已识别容器镜像进行恶意软件和漏洞扫描。通过统一管理平台，从主机保护到运行中的容器识别和镜像扫描，CPP 为云工作负载提供了集成的安全管理能力。



主要功能

Anti-malware **反恶意软件**	• 通过多个全球认证机构验证的V3进行恶意代码响应 • 基于特征码和信誉的强大的恶意代码检测（支持Windows和Linux服务器）
Host IPS & Firewall **主机IPS和防火墙**	• 基于经过验证的特征码，检测并阻止各种网络攻击 • 支持基于漏洞的特征码推荐和自定义特征码 • 支持防火墙和国家IP拦截
Application Control **应用程序控制**	• 通过应用程序运行控制，仅允许受信任应用程序运行 • 自定义多种信任条件并限制对重要文件的访问 • 监控对重要文件、文件夹、注册表、进程、用户、组、服务等的更改 • 支持实时、手动和计划扫描
Container Security **容器安全**	• 支持与Kubernetes集群联动及拓扑结构可视化 • 识别运行中的容器并进行镜像拉取和扫描 • 提供已扫描的镜像的集群、命名空间、Pod部署状态图表

Host IPS

Host IPS 是一种基于主机的入侵防御模块，通过分析进出系统的流量，基于特征码检测并拦截可疑模式的流量。它不仅能保护服务器免受操作系统、Web 和应用程序漏洞攻击，还能防御基于各种类型网络的攻击。此外，Host IPS 基于服务器工作负载的已知漏洞信息推荐合适的特征码，提供针对工作负载特性优化的保护方案。Host IPS 不仅能够检测并拦截针对系统的网络攻击，还能对识别并拦截针对运行中容器的网络攻击。

提供经过验证的特征码
- 基于AhnLab的威胁分析团队和基础设施，提供针对本地环境优化的特征码
- 推荐并应用与服务器漏洞匹配的特征码

支持自定义特征码
- 支持客户根据需求自行设置并应用特征码
- 自定义时，提供Snort和PCRE支持，简化配置过程

防火墙功能
- 基于IP、端口和协议进行阻止和允许设置（支持XFF）
- 支持针对特定国家IP进行入站/出站拦截

考虑服务器可用性的多种功能
- 除Inline模式外，还支持Tap、Bypass模式等多种网络引擎模式
- 提供IDS模式及紧急关闭功能
- 支持基于特定条件向检测终端发送警报（使用连接规则）
- 当CPU超过指定阈值时，支持自动关闭的功能

威胁可视化与响应便捷性
- 通过仪表板查看检测到的Agent、攻击者、Top特征码、攻击趋势等状态
- 提供检测到的流量的详细信息
- 支持在检测事件中设置例外IP
- 支持将特定特征码应用于整个系统

Application Control

应用程序控制（Application Control）是针对仅允许特定应用程序运行的服务器工作负载保护而优化的服务器工作负载应用程序控制模块。它仅允许受信任应用程序的运行，事先阻止与工作负载用途无关的不必要程序的运行，以支持更稳定的服务运营。此外，支持维护模式、模拟模式等多种运营模式，进一步增强服务的稳定性。监控特定文件、文件夹、注册表、启动程序和服务等的更改情况，以便提前检测到对服务器的攻击或潜在风险。

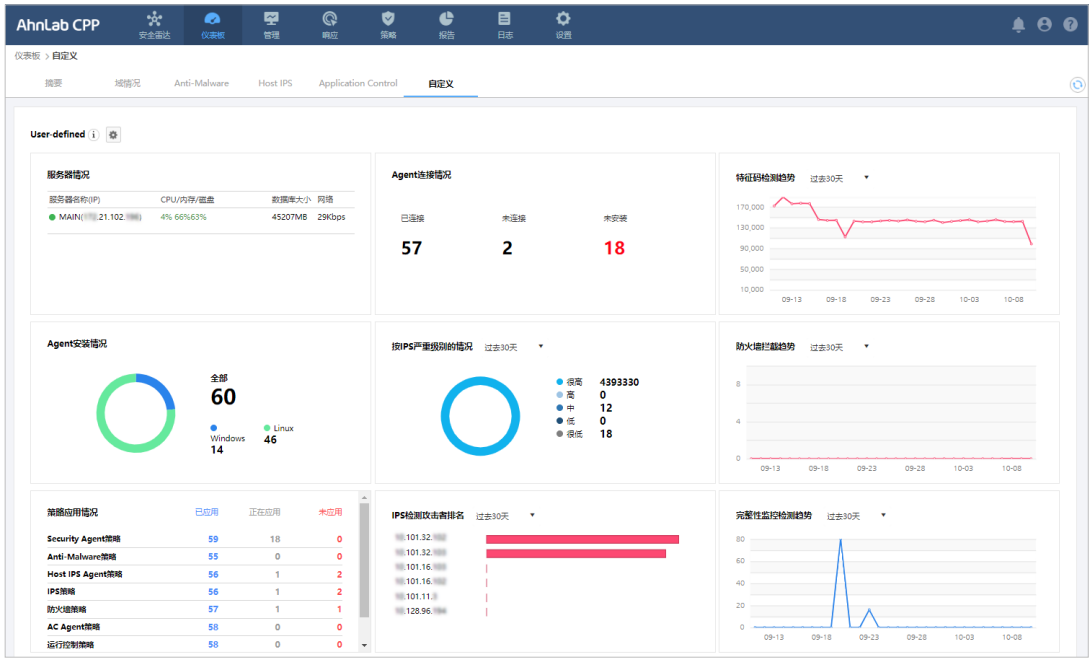
针对云服务器环境的优化
- 基于预先创建的镜像运行的云工作负载提供优化的安全支持
- 仅允许受信任应用程序的运行，以支持稳定的服务运营并减轻管理员的工作负担

减轻管理员的工作负担
- 基于管理员指定信任标准（签名者、提供者、云信誉）来允许运行，提供灵活管理支持

考虑服务器可用性的多种功能
- 支持以稳定服务运行为首要目标的多种运营模式
  #1.安全运营模式
  #2.维护模式（考虑更新）
  #3.模拟模式（仅支持检测而不拦截 - 判断策略的适用性）
- 支持对检测量多的终端发送警报及清单初始化（使用连接规则）

通过多样化的仪表板提供细化的可视性
- 提供对关键事件（如运行阻止趋势、运行阻止Agent排名、文件排名等）直观可视性

完整性监控
- 监控重要文件、文件夹、注册表、服务、进程、端口、用户、组、启动程序等的更改
- 支持基本规则和用户定义规则



AhnLab CPP仪表板

Container Security

容器安全（Container Security）是一种容器安全模块，能够识别在 Kubernetes 环境中运行的容器，提供拓扑结构可视化，同时对识别出的容器镜像进行恶意代码和漏洞扫描。该模块旨在增强企业的容器环境安全，快速识别潜在威胁并及时作出响应。

简便的Kubernetes集群与容器注册表连接

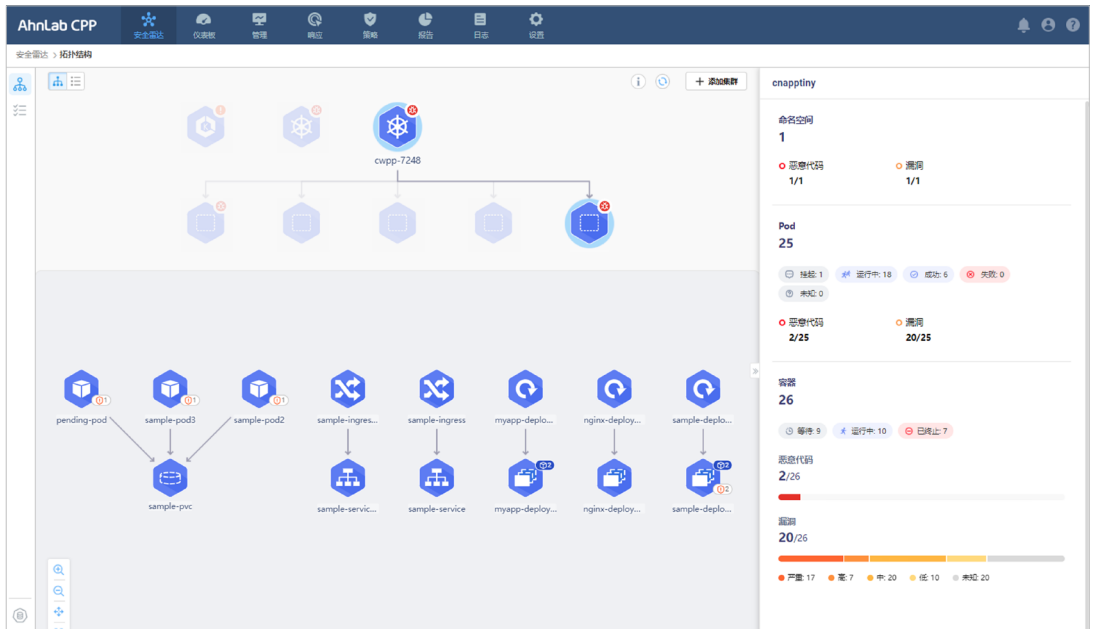
- 通过kubeconfig和帐户连接方式，轻松连接Kubernetes集群
- 支持与Harbor、Nexus、Docker Hub、Amazon ECR等多种容器注册表的连接

Kubernetes拓扑结构可视化

- 通过拓扑图形化展示集群、命名空间和Pod信息，能够一目了然地查看资源配置和安全状态

识别和扫描运行中的容器

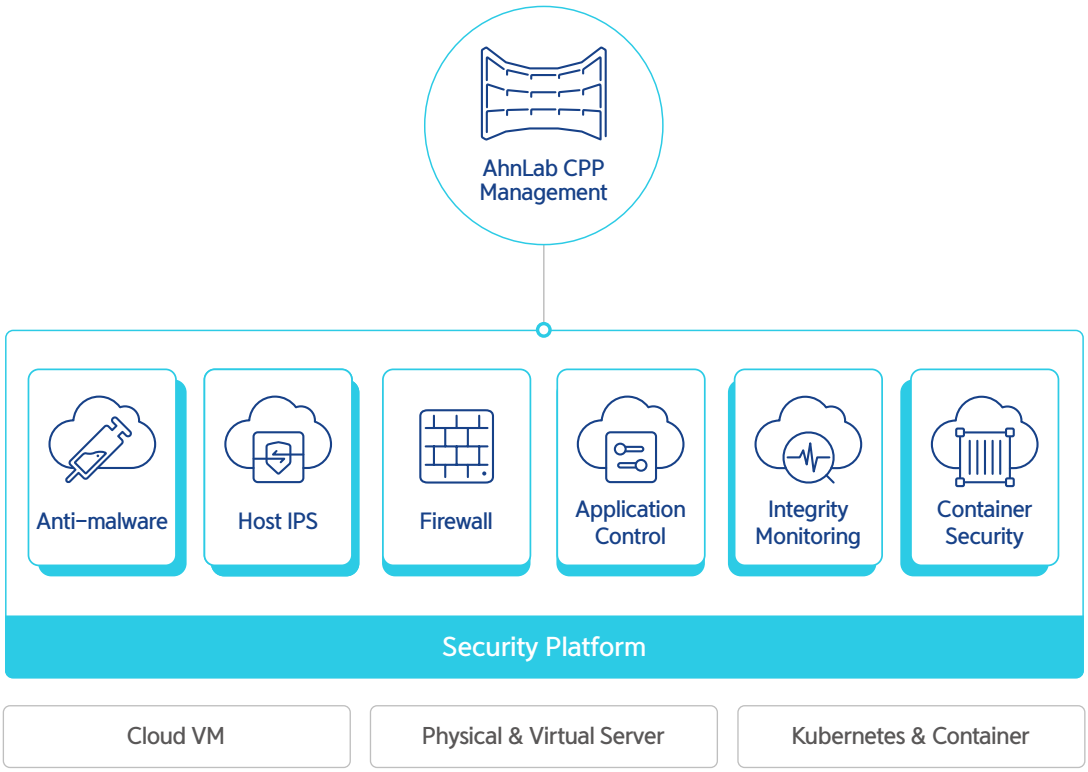
- 识别在Kubernetes环境中运行的容器，并对相应容器镜像进行恶意代码和漏洞扫描
- 当用于部署的镜像不存在于连接的容器注册表中时，提供状态信息
- 提供已扫描镜像的部署状态图表和列表



AhnLab CPP安全雷达

优化的安全运营与管理

AhnLab CPP 通过基于**单一 Agent（One Agent）**提供多种安全模块的集成运营与管理，支持构建针对混合云服务器工作负载保护的优化安全平台。



主要功能

高效的服务器安全集成管理	• 支持公共云（AWS、Azure、NHN、NCP等）与物理/虚拟环境服务器的集成管理 • 通过单一Agent（One Agent）提供对AhnLab服务器安全解决方案的集成运营与管理
针对服务器工作负载优化的威胁管理与响应	• 通过多种仪表板提供威胁监控与可视化 • 提供AhnLab服务器安全解决方案之间的连接规则，以建立符合组织需求的威胁响应体系 • 提供Syslog、开放API，方便与第三方解决方案（如SIEM、综合日志分析系统等）进行无缝对接
灵活的配置与成本节约	• 将Host IPS、Application Control、V3 Net、Container Security等多种功能在单一管理平台上进行集成运营，以满足客户的高效管理需求 • 仅针对工作特性所需的安全解决方案许可证进行部署，从而提高引进和管理的成本效率

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）

AhnLab