AhnLab CPP

Purpose-built Workload Protection for Hybrid Cloud

Optimal security for various cloud workloads
Kubernetes-based container identification and image scan
Central management powered by a single agent

Overview

AhnLab CPP (Cloud Protection Platform) is a cloud workload protection platform (CWPP) that provides integrated protection for workloads operating across various cloud infrastructure, including physical and virtual servers, cloud VMs, Kubernetes clusters, and serverless containers. AhnLab CPP offers unified security management capabilities for cloud workloads by operating everything from host protection to identifying running containers and scanning container images within a single management interface.

- Unified Workload Management
- Container and Base Image Scan
- Malware Defense
- Network Attack Defense
- Application Control
- Monitoring File Modification

Key Features

Anti-malware	· Real-time, scheduled and manual scan of servers and cloud VMs (Windows/Linux) · Precise malware defense and multi-compressed file scan backed by top-notch engine · Deployed in Kubernetes using DaemonSet to protect container workloads and nodes
Host IPS & Firewall	· Optimal security for hosts, Kubernetes, and serverless environments · Signature-based network defense and user-defined rules · Flexible operating mode: Inline, Tap, Bypass, etc. · Firewall: IP, port and protocol control & Geo-IP block · Suspicious behavior detection: Port scan and host sweep
Application Control & Integrity Monitoring	· Allowing only authorized application to be executed · Defining authorization conditions and limiting access to critical files · Monitoring change of critical file, folder, registry, process, user, group, service, etc. · Real-time, manual, and scheduled scan
Container Security	· Kubernetes cluster integration and topology visualization · Pull and scan images by identifying running containers · Diagram of scanned images: cluster, namespace and pod deployment status

Host IPS

Host IPS is a host-based intrusion prevention module that analyzes inbound and outbound traffic, detecting and blocking suspicious patterns based on signatures. It protects servers from various network-based attacks, including those exploiting vulnerabilities in operating systems, web services, and applications. The module recommends optimal signatures based on known vulnerability of workloads for the best possible protection. It detects and identifies network attacks targeting the system and running containers.

Server-Optimized Signatures

· Industry-leading signatures based on our 30-year security intelligence and infrastructure
· Signature recommendation mapped to server vulnerabilities
· User-defined signatures for optimal defense
· Convenient signature settings (Snort and PCRE)

Firewall

· Allow and block traffic based on IPs, ports and protocols (XFF)
· Block inbound and outbound traffic with country-specific IPs

Features for Server Availability

· Various network engine modes: Inline, Tap, Bypass, etc.
· Supporting IDS mode and urgent termination
· Notification for detected devices under specific conditions (correlation rules)
· Disabling functions when specified CPU threshold is exceeded

Extended Visibility and Response

· View agent status, attackers, top signatures, and attack trends on the dashboard
· Detailed information on detected traffic
· Set exception IPs from detection events
· Apply specific signatures across all systems

Application Control

Application Control is a dedicated module for protecting server workloads that run only specific applications. It allows only authorized applications to run and blocks unwanted programs in advance, enabling more stable service operations. It enhances service reliability by supporting various operation modes such as maintenance mode and simulation mode. It also monitors changes to specific files, folders, registries, programs, and services to detect potential server attacks and risks in advance.

Optimized to Cloud Servers

· Optimal security for cloud workloads based on pre-built images
· Stable operations with minimal burden by allowing only trusted applications to run

Reducing Operational Burden

· Execution based on trust criteria defined by the admin (e.g., signer, vendor, cloud reputation)
· Various features designed for flexible management and server availability

Features for Server Availability

· Various operation modes prioritizing seamless service operation
#1. Lockdown mode
#2. Maintenance mode (for updates)
#3. Simulation mode (detection only)
· Alerts for devices with high detection volume and inventory reset (correlation rules)

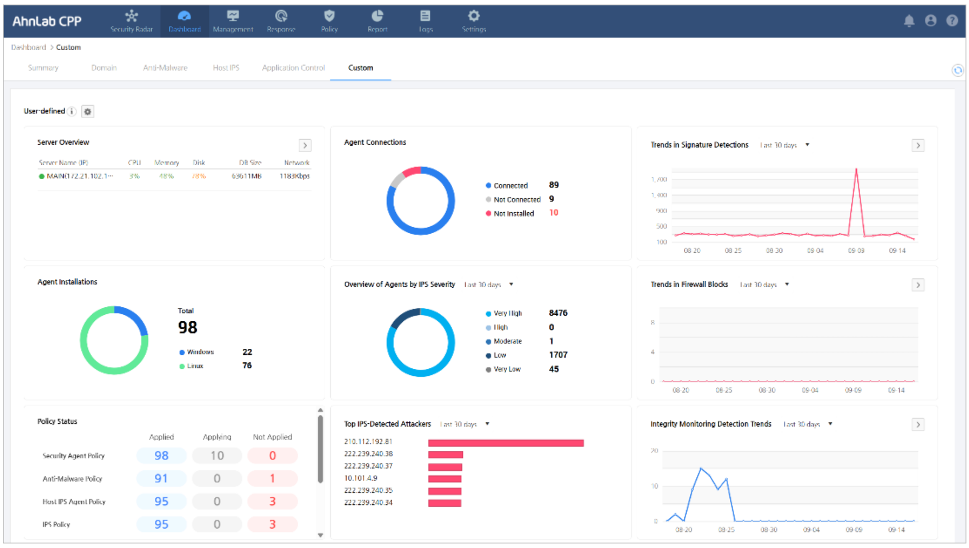
Detailed Visibility on the Dashboard

· Event visibility: Execution block trend, top blocking agents, top files, etc.

Integrity Monitoring

· Monitoring changes to critical file, folder, registry, service, process, port, user, group, etc.

· Default rules and user-defined rules



Server Overview

Server Name (IP)	CPU	Memory	Disk	DB Size	Network
MAIN(172.21.102.1···	3%	48%	78%	63611MB	1183Kbps

Agent Connections

● Connected	89
● Not Connected	9
● Not Installed	10

Agent Installations

Total 98

● Windows	22
● Linux	76

Overview of Agents by IPS Severity Last 30 days

● Very High	8476
● High	0
● Moderate	1
● Low	1707
● Very Low	45

Policy Status

	Applied	Applying	Not Applied
Security Agent Policy	98	10	0
Anti-Malware Policy	91	0	1
Host IPS Agent Policy	95	0	3
IPS Policy	95	0	3

Top IPS-Detected Attackers Last 30 days

210.112.192.81
222.239.240.38
222.239.240.37
10.101.4.9
222.239.240.35
222.239.240.34

Dashboard - AhnLab CPP

Container Security

Container Security is a module that identifies containers running in Kubernetes and provides topology visibility. It performs malware and vulnerability scans on the identified container images, helping enterprises strengthen container security and quickly detect and respond to potential threats.

Easy Integration: Kubernetes Cluster and Container Registry

· Kubernetes cluster integration: kubeconfig and account-based integration

· Container registry integration: Harbor, Nexus, Docker Hub, Amazon ECR, etc.

Kubernetes Topology Visualization

· Visualizing cluster, namespace and pod to gain visibility into resources and security status

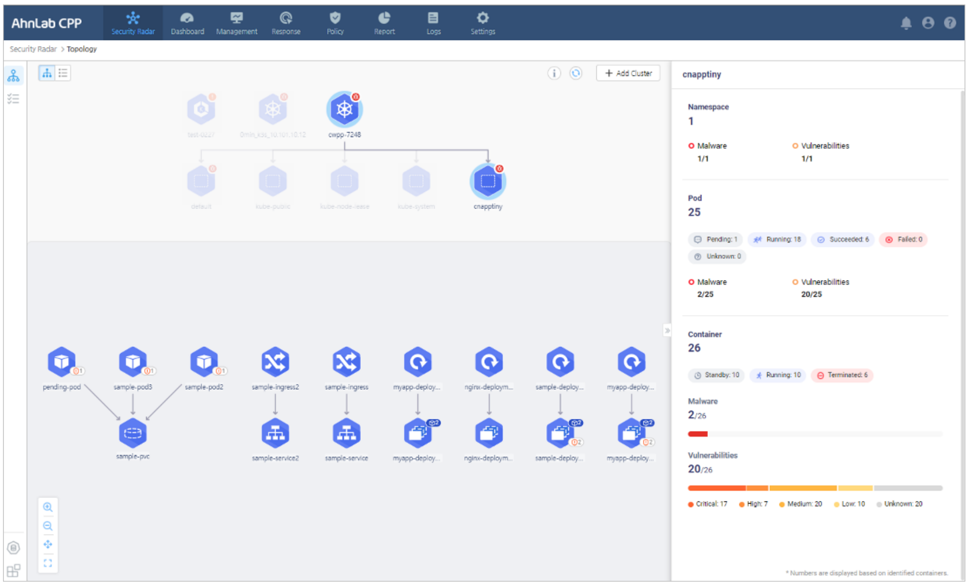
Identification and Scanning of Running Container

· Identify containers running in Kubernetes

· Scan container images for malware and vulnerability detection

· Provide status if the deployed image is not found in the integrated container registry

· Diagrams and lists showing the deployment status of scanned images



cnapptiny

Namespace
1

Malware 1/1 · Vulnerabilities 1/1

Pod
25

Pending: 1 · Running: 18 · Succeeded: 6 · Failed: 0 · Unknown: 0

Malware 2/25 · Vulnerabilities 20/25

Container
26

Standby: 10 · Running: 10 · Terminated: 6

Malware
2/26

Vulnerabilities
20/26

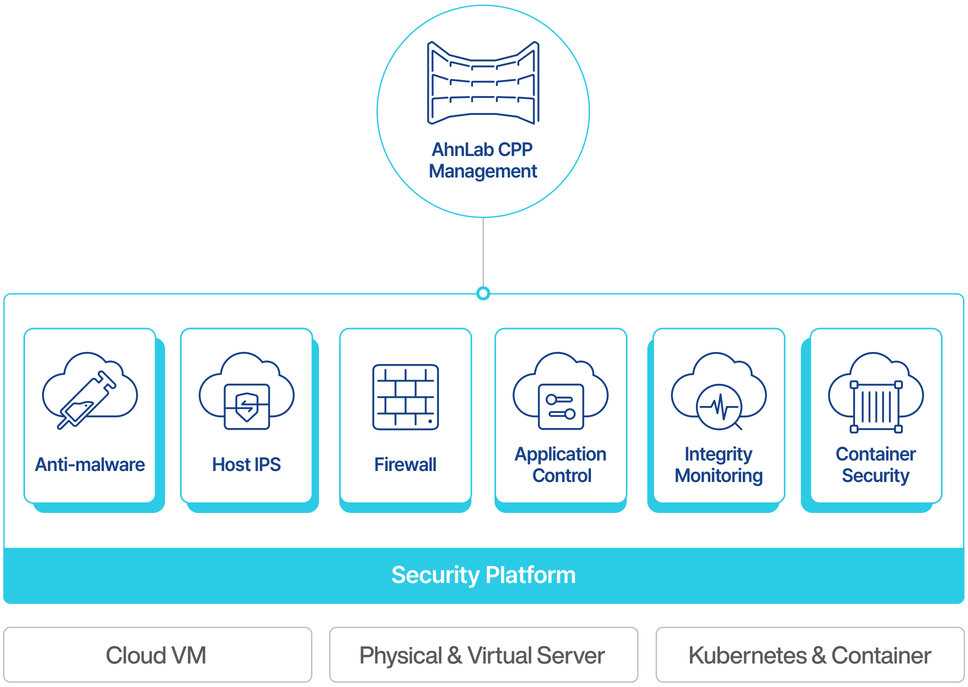
● Critical: 17 ● High: 7 ● Medium: 20 ● Low: 10 ● Unknown: 20

* Numbers are displayed based on identified containers.

Security Radar - AhnLab CPP

Central Management

AhnLab CPP supports customers in building an optimized platform for protecting hybrid cloud server workloads by integrating various security modules into a single agent for unified management.



Architecture of AhnLab CPP

Strengths

Unified Security	· Unified management of public cloud (AWS, Azure, etc.) and servers · Integrated operation of our server security modules through one agent
Risk Management	· Extended threat monitoring and visibility on the dashboard · Optimal response by offering correlation rules between security modules · Syslog and open APIs for flexible integration with third-party solutions
Flexible Operation	· Efficient operation by integrating modules via a single management · Improved cost efficiency by applying licenses only for modules needed

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com

AhnLab