AhnLab

White Paper

How to Prepare for Cloud Security Threats

Overview

We are living in the era of the cloud. Cloud has become more important than ever as it played a key role in accelerating digital transformation during the COVID-19 pandemic. Organizations began to expand their perimeters to support remote work, and this has made them vulnerable to emerging cloud security threats. To gain visibility and maintain a high-level security for both on-premise and public clouds, many organizations and businesses are looking into adopting various security solutions. But with so many solutions already available in the market, what should be the main priority? The key to hybrid cloud security is to effectively protect server workloads. Solutions for cloud workload security is called 'CWPP (Cloud Workload Protection Platform).'

This whitepaper discusses the basic concepts of the cloud and cloud security measures that utilize 'AhnLab CPP,' an industry-leading workload security solution for hybrid cloud environments.

What are Cloud IaaS, PaaS, and SaaS?

Cloud is a lease-like rent service where the user uses the necessary IT resources through the internet and pays for the amount used. When taking various residence types as an example, on-premise can be owning your house whereas cloud is renting a place from an accommodation service provider. The latter means that you can stay and borrow the resources needed as long as you pay the accommodation service provider.

In order to build your own house, it takes a lot of time, effort, and money from designing to the completion of construction. And once it's built, it is difficult to expand or reduce the size or get rid of unnecessary space. Not only that, a lot of time, money, and effort goes into maintenance. By contrast, when renting a house, the construction and the maintenance of the building is mainly the accommodation provider's responsibility, and the user only needs to rent as much as they need whenever they want. It is comparatively easy to expand or reduce the size of the housing, and you can also cancel it when it is no longer needed. There is no need to be concerned about the maintenance or the management of the housing. This type of housing can be referred to as cloud services in the IT environment.

Renting cloud assets can be categorized into three different types: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). To refer to the concept of renting a house, as the previously mentioned example, IaaS is when you rent the house but have nothing inside it. Utilities such as electricity and water are there, but furniture and appliances must be purchased on your own. PaaS is when the house is furnished with furniture and appliances. For example, if you wanted to cook something, you have all necessities for cooking. SaaS is when the house is fully-furnished with built-in furnitures and appliances, like an actual restaurant. You only need to decide what you want to eat.

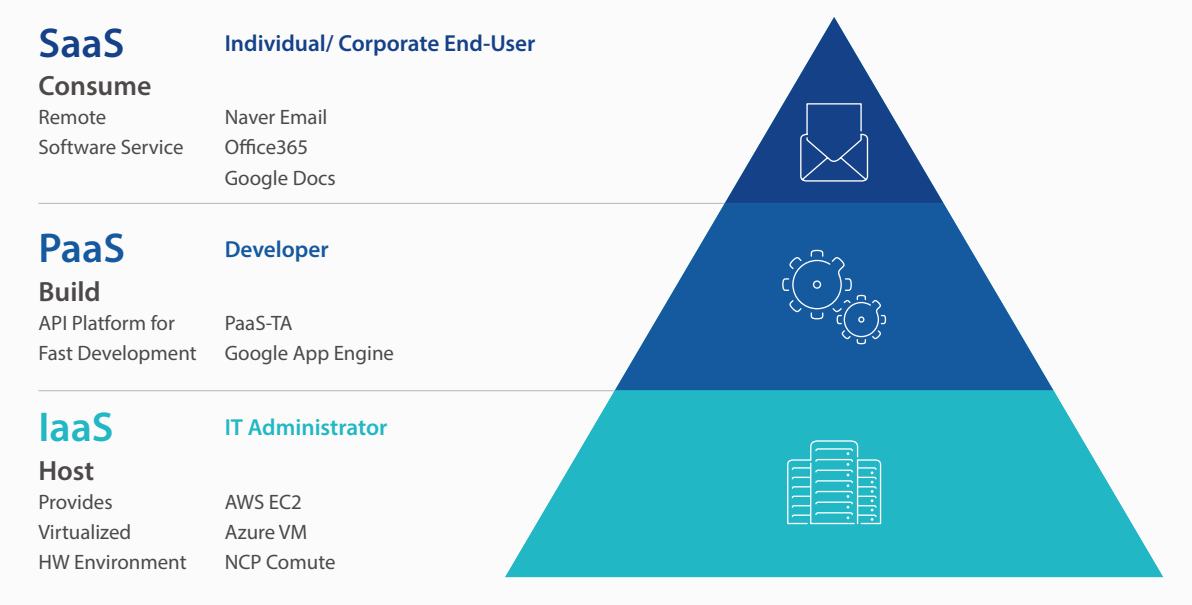

Figure 1. Cloud Service Structure

Hence in the cloud, IaaS is the renting of infrastructures, such as hardware or network. PaaS is providing of the development platform and environment, while SaaS is providing all services ready to be used out of the box.

Cloud offers cost reduction and increases work efficiency for users. In comparison with on-premise,

the cloud's advantage is that no initial cost is needed, and flexible expansion of resources is possible through autoscaling.

As a result, cloud migration is on the rise. According to Gartner, the global public cloud market in 2021 is valued at 396 billion dollars and it is expected to grow up to 482.1 billion dollars by next year.

Furthermore, Gartner predicted that the Korean public cloud market valued at 3,240 billion won in 2021 will increase to 3,723.8 billion won in 2022. These are the results of the sudden increase in cloud migration following the acceleration of digital transformation since the COVID-19 pandemic, and this increase is expected to continue post-COVID-19.

However, as hackers concentrate on financial benefits, attacks targeting the cloud environment are increasing as well as diversifying. Thus, security administrators are increasingly faced with cloud security challenges because the cloud environment is quite different from legacy environments in terms of resource sharing and the form of service provided.

Who is Responsible for Cloud Security?

The following discusses cloud security in detail. Security threats occur in the cloud environment just like they do on-premise. Let's take the residence type for example again.

If it is my house that I am in charge of, it would be my responsibility to manage the house. In the case of renting a house from an accomodation service provider, it is uncertain who has the responsibility. Defending against intrusions, such as robbery, or natural disasters would be the accomodation provider's responsibility. But what would happen if someone came into the room I rented and stole my wallet or important files? If my roommate stole it or misplaced the room key, then I, the tenant, would be held responsible. In such cases, one must consider the circumstances to decide who is responsible. This is the same for cloud environments.

If an accident occurs in an environment where infrastructure and service are provided by an actual cloud provider, who would be responsible? According to a research conducted by Thales Group and Ponemon Institute in 2019, 31% of the companies believed that they were responsible. The remaining 33% thought that both the company and the cloud provider were equally responsible, while 35% thought that the cloud provider was responsible in terms of responsibility for data security in the cloud.

Then what is the correct answer? The answer is that both the user and the service provider shares

responsibility depending on the type of cloud service. Although many companies are now aware of the answer, many still struggle in deciding which security control is shared, unlike on-premise environments.

When an error or a security threat occurs in a public cloud environment, responsibilities are assigned based on the range of services provided by the cloud service provider. Cloud service providers call this the 'shared responsibility model.' Shared responsibility is the concept of the user and cloud provider sharing the responsibility for security in the cloud environment.

Figure 2 from Amazon Web Services explains the range of responsibilities for security between the user and the cloud service provider. It shows that AWS is responsible for the areas, including hardware, network, and system. The user, on the other hand, is responsible for areas, such as network traffic-related security, firewall configuration, application and access control, and data security.

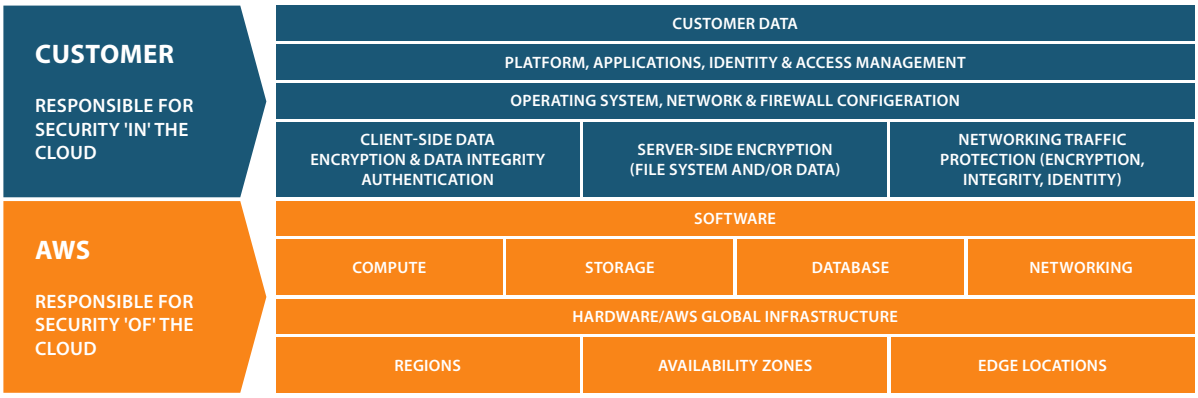

Figure 2. AWS Shared Responsibility Model (Source: AWS)

Figure 3 is Microsoft Azure's shared responsibility model. The areas highlighted in blue are the customer's responsibilities and the grey area represents Microsoft's responsibilities. It shows that the range of responsibilities varies based on the service types (IaaS, PaaS, and SaaS).

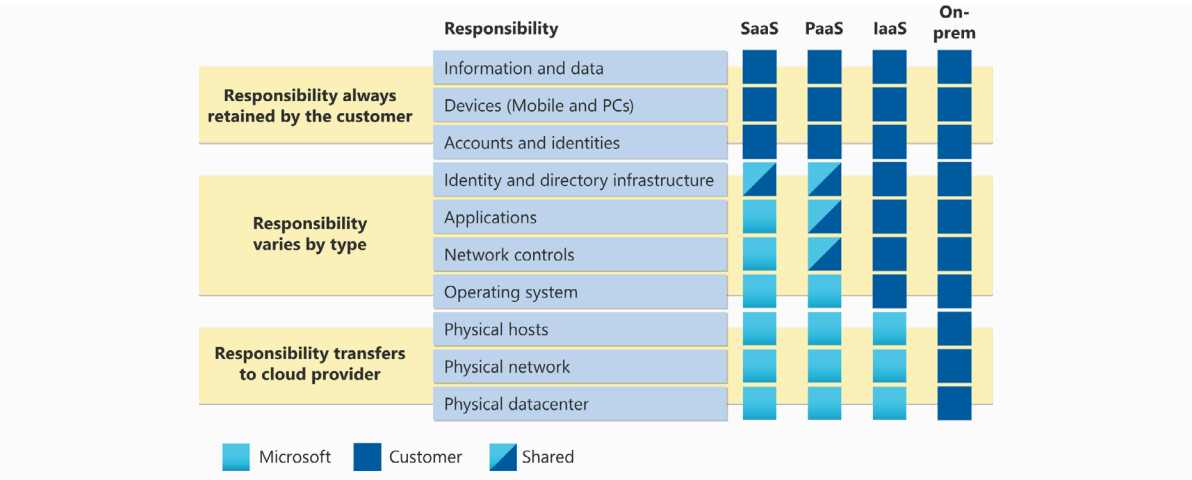

Figure 3. Azure Shared Responsibility Model (Source: Microsoft)

In conclusion, CSP (Cloud Service Provider) and the company must share the responsibility for cloud security, and it is crucial that the security managers are also aware of this model.

Cloud Security, Where to Start?

How can one start building a safe cloud environment? The current cloud environment has become highly complex with diversifying forms; there are various cloud services for physical, virtual, hybrid, and multi-cloud, server/virtual machine, container, and serverless environments.

Security starts from IaaS, which is the foundation of cloud services. Based on the shared responsibility model, the company must configure and operate all areas, excluding the hardware and the network. administrators in charge of the company's security will then have to follow the following requirements.

Firstly, the administrator must overlook and manage the on-premise and cloud servers at once. Secondly, logical access control must be easy and simple as physical access control or network control over the cloud server is difficult due to not being directly managed by the company. As growing numbers of threats exploit cloud configuration errors, protection against network attacks or access to the server is becoming increasingly important. Lastly, due to targeted attacks on the server, administrators must protect the server from security threats.

Cloud Workload Security Platform, AhnLab CPP

To address customer requirements, AhnLab released the cloud workload security platform 'AhnLab CPP.' AhnLab CPP provides efficient response through integrated management of cloud servers for both on-premise and virtual servers, enhanced security features for server workload protection, and seamless integration with third-party solutions.

AhnLab CPP provides integrated management and visibility across on-premise, virtual server, and cloud (AWS, Azure, Naver Cloud platform, Kakao i Cloud, and NHN cloud) in Windows/Linux servers. It also automatically identifies autoscaling devices by syncing with the cloud account.

AhnLab CPP manages security features and security products required for the protection of cloud server workload on a single, integrated console. AhnLab CPP provides whitelisting-based application execution/access control, application control for integrity monitoring, host IPS for IDS/IPS/Firewall features, and 'V3 Net' for malware detection and response.

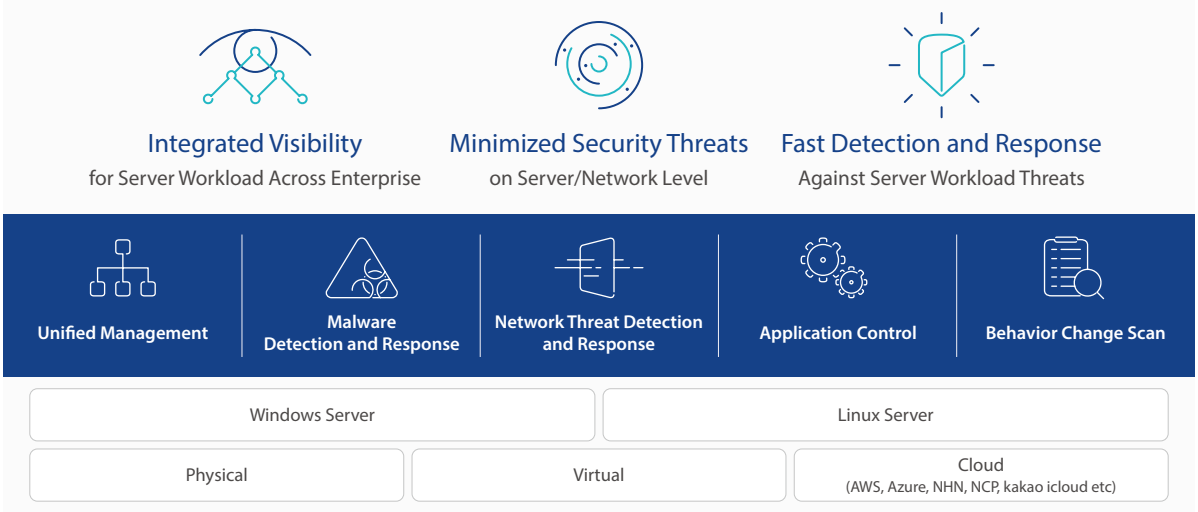

Figure 4. AhnLab CPP Security Architecture

Furthermore, it offers comprehensive visibility over server workload through various dashboards which allow the user to see the total security status of the company's server at a glance. AhnLab CPP is optimized for hybrid cloud environments, thus minimizing the security threats for server workloads. AhnLab CPP provides Syslog to help seamless integration with third-party solutions, such as SIEM.

Key Features of AhnLab CPP

AhnLab CPP includes application control, host IPS, and V3 Net. Application control allows stable operation of the server through whitelisting-based application execution and access control. It also helps respond to threats in advance and detect unauthorized system changes to key files/folders/registries. Signature-based, host IPS detects and blocks network attacks and provides firewall features. V3 Net protects the server from malware infection through real-time/manual server scans.

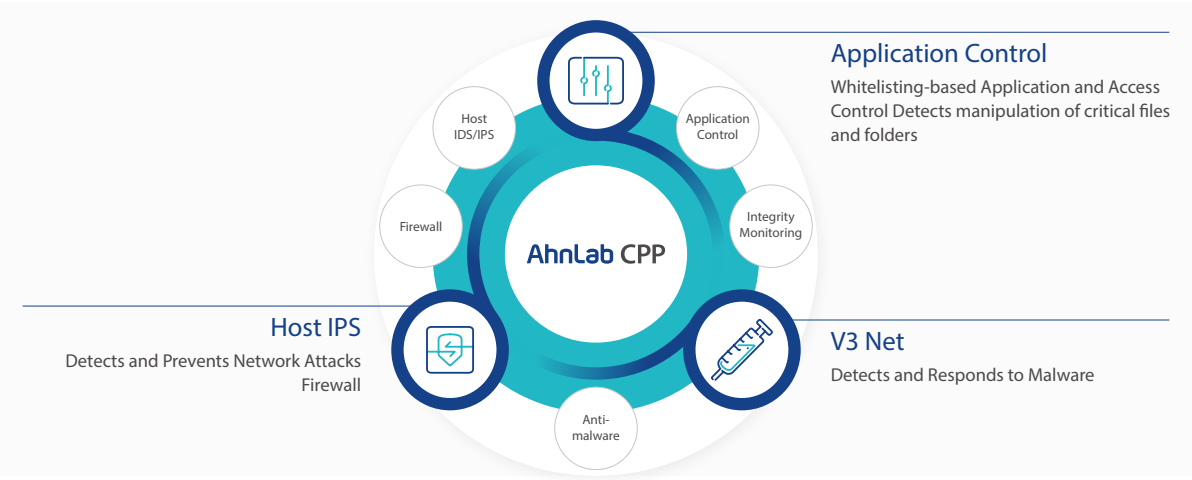

Figure 5. Structure of AhnLab CPP Key Features

1. Application Control & Integrity Monitoring

Application control allows execution of authorized applications only and blocks execution of everything else so that the server operates for its original purposes only to provide prevention against threats. As for the key files/folders, it only allows access from designated processes so that the service is not stopped due to unwanted changes.

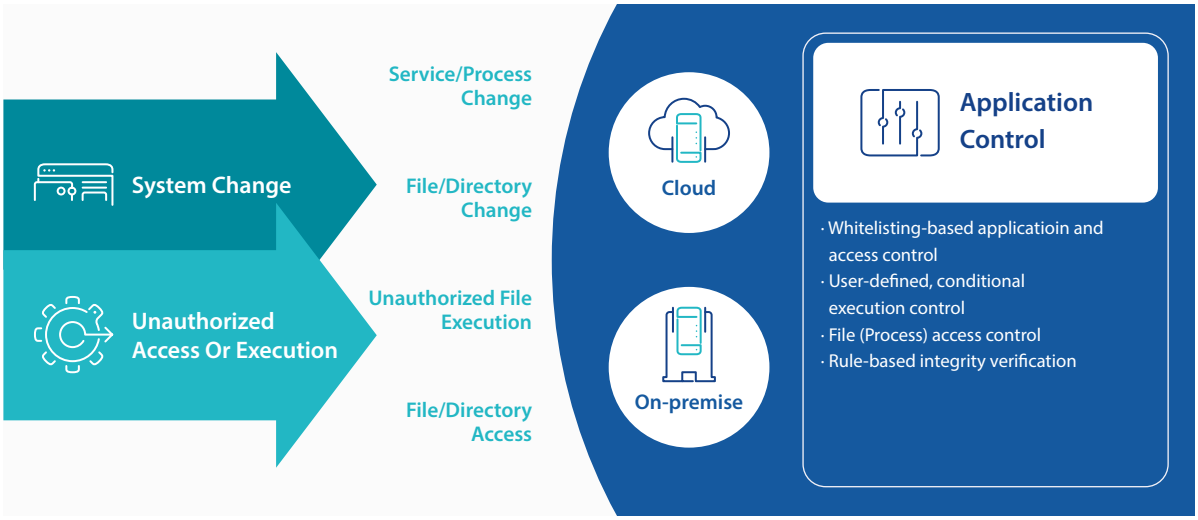

Figure 6. AhnLab CPP Application Control

The integrity monitoring feature scans for changes in specific locations, such as files/folders, registries, start programs, and services, where there should not be any changes normally. It also allows the user to optimize the feature to each specific environment by using user-defined rules and default rules.

Application control supports various operational modes, such as Lockdown and Maintenance Mode, to enable optimal service operation. Lockdown Mode is the default security mode, and Maintenance Mode is used when software installation or update is needed. During an update, changes may occur in many executables. However, this is not possible in Lockdown Mode. In this case, changing to the Maintenance Mode allows all changed executables to be automatically registered to the whitelist without being blocked. Simulation Mode does not block and only detect files that are not on the whitelist, and it can be used to evaluate the adequacy of security policies before Lockdown.

2. Host IPS & Firewall

AhnLab CPP's Host IPS monitors traffic that flows in and out of the server to allow or block traffic based on the firewall settings. It also detects and blocks attacks based on the applied IPS signature. AhnLab Host IPS provides thousands of signatures verified and periodically updated by AIPS, AhnLab's next-generation network intrusion prevention system. The administrator can also directly

configure signatures needed. The various forms of signatures include Snort and PCRE.

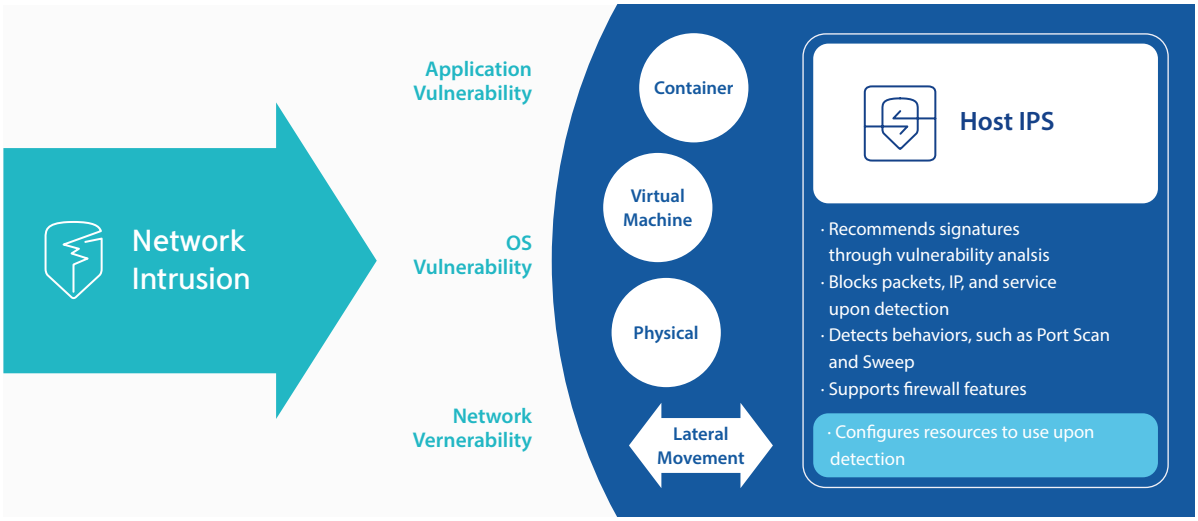

Figure 7. AhnLab CPP Host IPS & Firewall

Unlike network IPS, host IPS is applied to the service server, and thus applying all signatures can lead to performance issues when providing the service. Therefore, Host IPS is designed to apply minimal signatures that are required for the corresponding server, minimizing the load on the server and enhancing the security efficiency.

From the administrator's point of view, it is almost impossible to analyze the environment of each server in an environment where servers are added and deleted flexibly, almost like the cloud server. Also, it makes it difficult to apply appropriate signatures. AhnLab CPP's host IPS analyzes the environment information of each server to recommend and automatically assign signatures appropriate for the device.

Along with the normal firewall feature, it provides the feature of blocking incoming and outgoing traffic to a specific country based on the country's IP address. Although host IPS operates in inline mode, TAP Mode and Bypass Mode is supported; TAP mode considers server availability and Bypass Mode considers error environments.

3. Malware Response

V3 Net provides anti-malware features that are globally proven by numerous independent anti-malware software testing institutions. V3 Net allows the user to switch between manual scan, scheduled scan, and other scans depending on the server activity. It provides security capacities that are convenient for users, such as quick and accurate malware detection and remediation via its exclusive engine, efficient application of prevention measures via the scan exception settings, and various reporting on the detection and remediation.

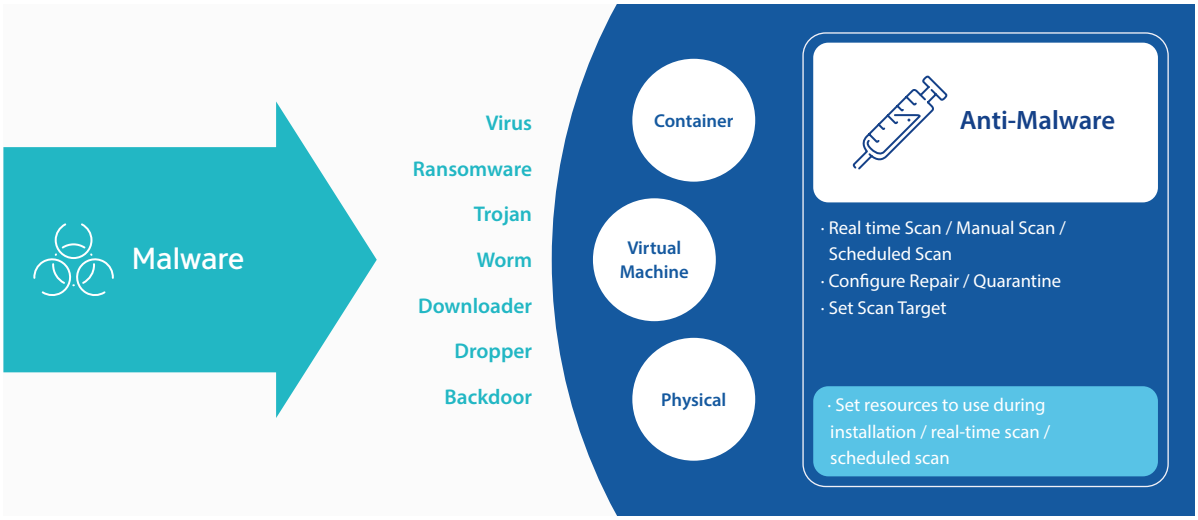

Figure 8. AhnLab CPP Anti-Malware

4. Container Security

AhnLab CPP detects and responds to malware in container files in the docker and k8s environment. It also detects network attacks to and from the container. AhnLab CPP also supports features for identifying the detected container file and the location of the network attack/communication. This allows the administrator to easily identify the container with security vulnerabilities and to bolster the security level of the service operational environment.

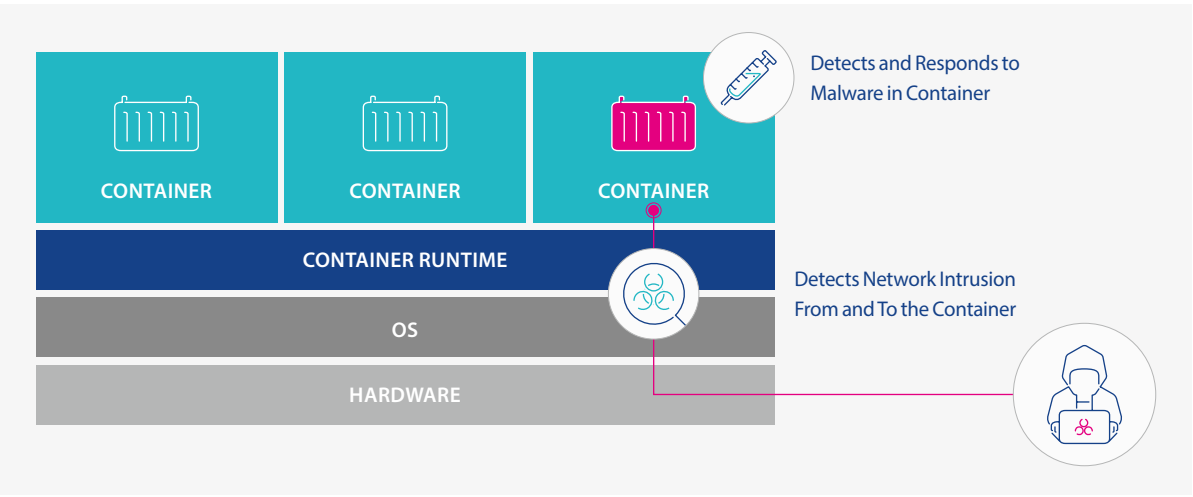

Figure 9. AhnLab CPP Container Security

Conclusion

To conclude, AhnLab CPP is a platform to protect Windows/Linux servers in on-premise and cloud environments. AhnLab CPP provides integrated visibility over servers in the organization as well

as application control, host IPS and firewall, anti-malware features, and container security. By providing efficient security management capabilities regardless of the server location, AhnLab enables businesses to secure server security in hybrid environments.

Along with cloud migration, the form and location of how cloud services are being provided are becoming increasingly diversified and complex. Thus, the cost for the management of server workload within the organization is increasing and administrators are struggling to secure workloads in various locations, such as on-premise, virtual, and cloud. Especially when migrating to the cloud, it is crucial to understand the organization's range of responsibilities and examine what kind of security capacities and solutions are needed to effectively protect assets and create a secure system.

In short, AhnLab CPP provides businesses with the technology and expertise needed to establish a stable hybrid cloud environment.

AhnLab

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