アンラボ・セキュリティレター

Press Ahn

2022.8　Vol.104

クラウドセキュリティ、悩んだ時の第一歩

クラウドセキュリティ、悩んだ時の第一歩

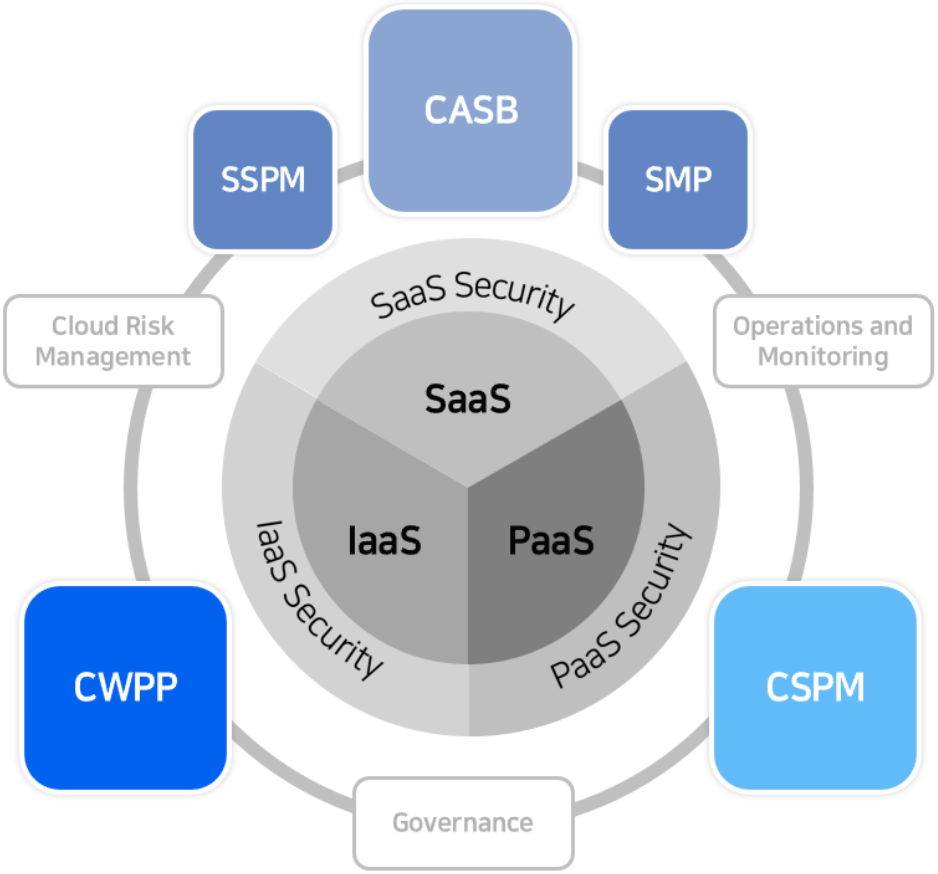
月刊レター「Press Ahn」の読者の中で、クラウドセキュリティという概念に馴染みのない読者はそういないだろう。しかし、クラウドセキュリティについて知れば知るほど、思ったよりも難しいという事実に気づく読者もいるはずだ。クラウドセキュリティのように、一筋縄ではいかなくとも必ず実施しなければならない場合、優先順位を決め、実際にできることから始めていくというアプローチが必要となる。

今回は、クラウドとオンプレミスの違いを掘り下げ、クラウドセキュリティを始める上で、まずは何から備えるべきかについて焦点を当てていく。

基本的に、クラウドセキュリティの導入は手軽に行えるものではない。構成要素が膨大であり、かつ保護すべき対象も変化し続けるからだ。クラウドセキュリティを適切に導入するための第一歩は、オンプレミスとクラウドの本質的な違いを理解することである。ここで言う理解とは、オンプレミスとクラウドの構造だけでなく、従来のセキュリティで分離されていたエンドポイントやネットワークに対する相互理解も含まれている。

クラウドセキュリティの構成

まず、クラウドセキュリティが基本的にどのように構成されているかを見てみよう。下記の図は、市場調査機関の「ガートナー（Gartner)」がまとめたクラウドセキュリティモデル、および各種セキュリティツールの役割だ。



[図1] クラウドセキュリティツールのカバレッジ（出典：ガートナー）

クラウドセキュリティツールの正式名称および役割

▲CWPP : Cloud Workload Protection Platform（クラウドワークロードセキュリティプラットフォーム）
▲CSPM : Cloud Security Posture Management（クラウドセキュリティ態勢管理）
▲CASB : Cloud Access Security Broker（クラウドアクセスセキュリティブローカー）
▲SMP : SaaS Management Platform（SaaS 管理プラットフォーム）
▲SSPM : SaaS Security Posture Management（SaaS セキュリティ態勢管理）

セキュリティツール	役割	保護領域
CWPP	クラウドワークロードセキュリティ	IaaS & PaaS
CSPM	IaaS・PaaS間におけるセキュリティ構成上の設定ミス防止	IaaS & PaaS
CASB	クラウドリソースへのアクセス制御、およびセキュリティポリシーの適用	SaaS
SMP	単一プラットフォームでの複数の SaaS ツール管理	SaaS
SSPM	SaaS アプリケーションのセキュリティ態勢管理、およびリスク評価	SaaS

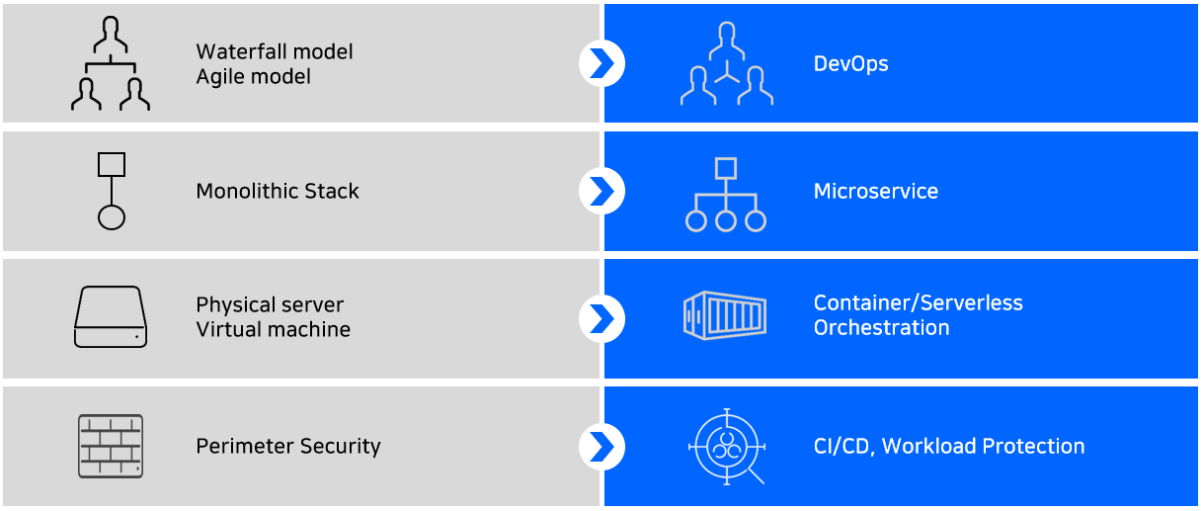
[表1] クラウドセキュリティツールの役割と保護領域

上記のクラウドセキュリティモデルは最も基本的なものであり、実際のクラウドセキュリティの区分領域はさらに細分化される。IaaS や PaaS を保護する CWPP と CSPM も、その領域を細分化してみると、保護対象が少しずつ異なってくる。そのため、上記の [図1] と [表1] は、クラウドセキュリティの構成を大きな枠組みで定義するという観点から理解してもらいたい。

クラウドセキュリティにおける重要なポイントは、1つの領域を 1つのソリューションでは完全にカバーしきれないことである。また、クラウドネイティブサービスのライフサイクルがますます短期化するにつれ、変化への迅速な対応が顧客ニーズとして浮上してきている。そのため、各種ソリューションは相互補完的なシステムを構築する方向へと再編されている。

オンプレミスとクラウド：概念の違い

クラウドセキュリティ構成の概念を理解すれば、従来のオンプレミスセキュリティとの本質的な違いに気づくだろう。ここで、両者のシステムには一体どのような違いがあるのか、概念的な側面から掘り下げてみる。



[図2] オンプレミスとクラウドの違い

まず、開発プロセスに焦点を当ててみよう。従来のオンプレミスは、特定の計画を中心として段階的に進めていく、「ウォーターフォール型」の開発手法が一般的だった。以降、一定周期ごとに開発を続け、変化に柔軟に対応できる「アジャイル型」へと変貌していった。また、クラウド環境への移行に伴い、迅速性や拡張性に対するニーズが増加するにつれ、開発から配布・運営までを統合する「デブオプス（DevOps）」方法論も脚光を浴びている。

アーキテクチャの観点から見てみると、オンプレミスではコンポーネント（Component）とデータが一つの空間で密結合された「モノリシックアーキテクチャ（Monolithic Architecture）」を活用してきた。モノリシックアーキテクチャの複雑性は比較的高くないが、些細な修正点にもアプリケーション全体が影響を受けてしまい、変化に対する柔軟性に欠けるという問題点がある。一方のクラウド環境では、コンポーネントを細分化し、それぞれを API で結合する「マイクロサービスアーキテクチャ（Microservice Architecture：MSA）」へと変化した。

こうした違いは、運用環境面においても変化をもたらすことになる。従来のオンプレミス環境では物理サーバーと仮想化技術を活用していたが、クラウドではマイクロサービスアーキテクチャを収容するため、コンポーネントを実行させる小さな単位ごとの環境が必要となった。これはやがて、コンテナとサーバーレス、およびオーケストレーションに対するニーズの増加へと繋がっていく。

まとめると、クラウド・デブオプス・マイクロサービスアーキテクチャのキーポイントは、アプリケーションの開発・運用に対する迅速さ、また変化への即時対応にある。近年の IT 環境では、こうした特性を備えることが求められており、より多くの企業がオンプレミスからクラウドに移行している状況だ。

オンプレミスとクラウド：マイグレーション（移転・移行）

オンプレミスを使用していた企業がクラウドを導入する際、「マイグレーション（Migration）」に向け様々な作業が行われる。クラウドマイグレーションは、移行するコンポーネントがクラウド環境にどれほど最適化されるかによって、大きく 4つの移行戦略に区分される。

クラウドマイグレーション - 4つの移行戦略

▲移行戦略 1：Rehost（リホスト）- Lift and Shift（リフト＆シフト）
▲移行戦略 2：Replatform（リプラットフォーム）- クラウド環境に合わせ開発ロジックを移行すること
▲移行戦略 3：Refactor（リファクタリング）- クラウドベースモデルに合わせコードを変更すること
▲移行戦略 4：Rewrite（リライト）-「クラウドネイティブ（Cloud Native）」に再設計すること

アンラボが本社を構える韓国では、多くの企業が迅速な移行を行うため、「リフト＆シフト」方式でクラウド環境を構築している。もちろん、新しく開発されたサービスの場合は該当しないが、サーバーアプリケーションのほとんどは「リフト＆シフト」形式で移行される。

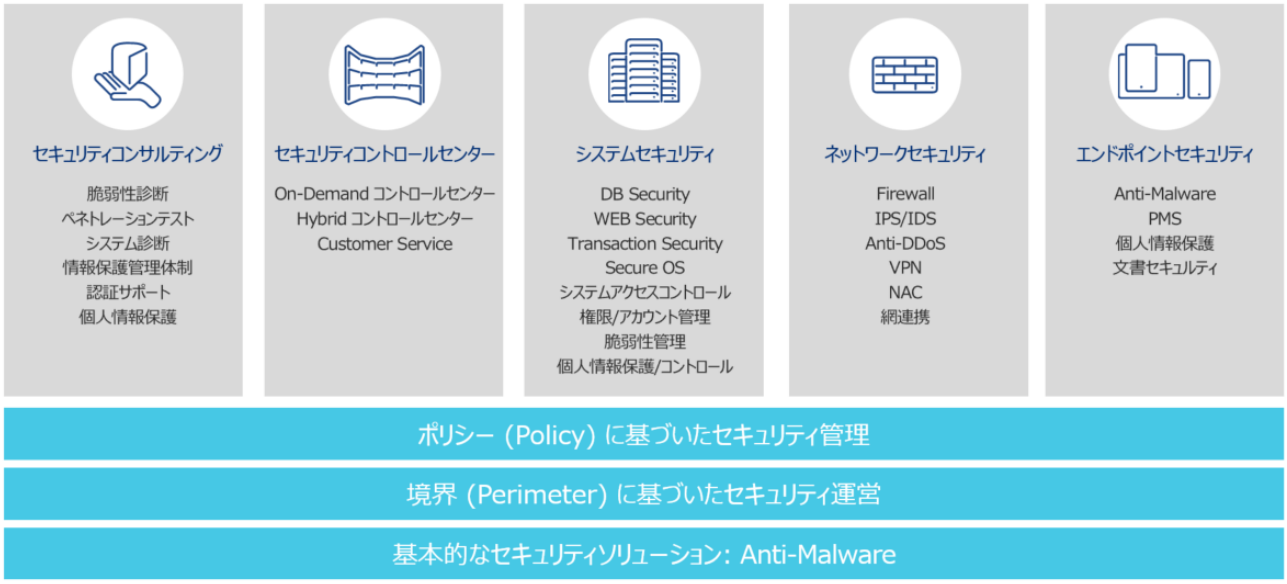
オンプレミスサーバーから仮想サーバーに移転する場合は、リフト＆シフト方式にさほど大きな懸念要素はない。しかし、従来の環境とは 180度変化するネットワークやクラウドインフラサービスの場合、この方式が運営に支障をきたすこともある。これは、セキュリティに関しても同様のことが言える。オンプレミスのセキュリティロジックをそのままクラウドに移行すると、長期的な観点から見たとき、構成面において困難に見舞われる可能性が高い。

クラウドを円滑に運用し、その利点を最大限得るためには、クラウド環境に合わせアーキテクチャを設計する、クラウドネイティブなマイグレーションが必要となる。もちろん、リフト＆シフト方式に比べ多くの時間と費用がかかるが、長期的なビジネス生産性や持続可能性を考慮した場合、クラウドネイティブがより良い選択と言えるだろう。

オンプレミスとクラウド：セキュリティの違い

このように、オンプレミスと構造的な違いを持つクラウドは、セキュリティを構成する上でも異なってくる。

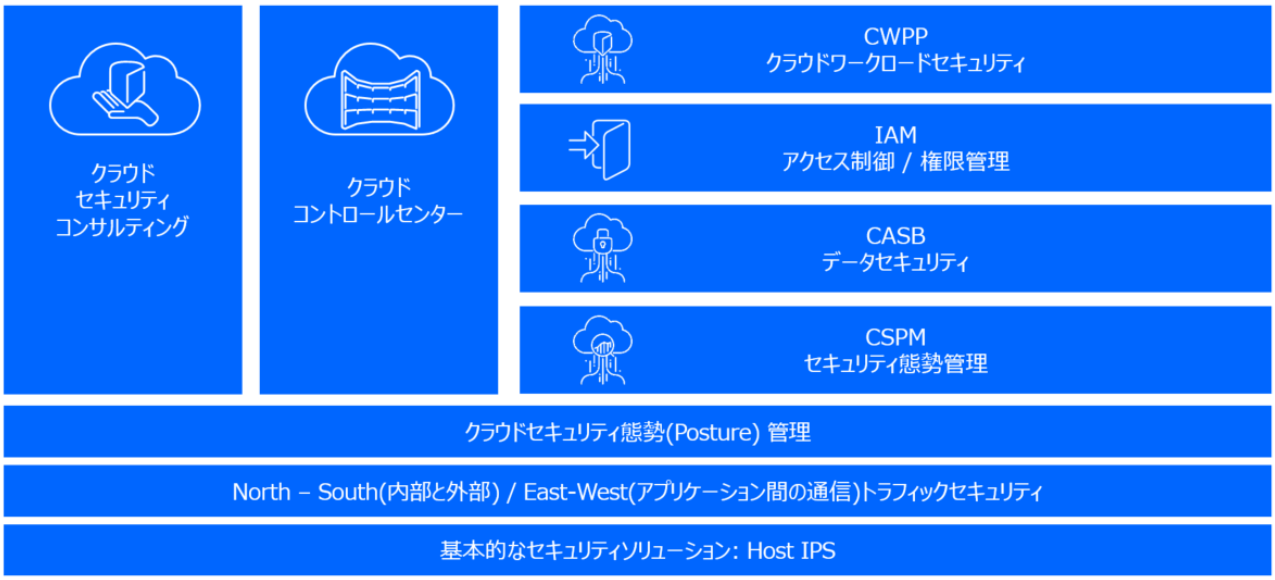
まず、オンプレミスのセキュリティフレームワークの場合、「境界（Perimeter）」を中心にセキュリティが運営される。境界とは、内部と外部、あるいはエンドポイントとネットワークなどの境目と考えれば理解しやすいだろう。オンプレミスの境界セキュリティは、保護対象とリソースが定義されている必要がある。定義されたリソースへの外部アクセスに対し強固な制御を行い、内部の重要リソースまたは外部からアクセスしているリソースに対し、セキュリティを別々に強化する形で行われる。言うなれば、ネットワークセキュリティを介して、強固なアクセス制御や脅威遮断対策を適用し、システムへのアクセスを制御する手法だ。



[図3] オンプレミスのセキュリティフレームワーク

オンプレミスのセキュリティ管理や適用は、ポリシー（Policy）に基づいて行われ、基本的なセキュリティソリューションとしては、ワクチンとして知られている「アンチマルウェア（Anti Malware)」が挙げられる。ワクチンをインストール後、エンドポイントセキュリティプラットフォームのコンポーネントを、ポリシーに基づき連結していく仕組みと捉えるといいだろう。

一方、クラウドのセキュリティフレームワークは、リソースを共有するクラウドの特性上、境界線が曖昧なものになってしまう。そのため、「ワークロード（Workload)」を中心にセキュリティの運営が行われる。ワークロードとは、OS・アプリケーションなど、ビジネスの価値を創出するリソースの集まりを意味する。強固なクラウドセキュリティシステムを構築するためには、境界を保護するよりも、クラウド上で運営されるリソース、すなわち、ワークロードに対する統合セキュリティがより効果的であると言える。



[図4] クラウドのセキュリティフレームワーク

クラウドセキュリティはオンプレミスとは異なり、セキュリティ態勢（Posture）管理が重要となる。セキュリティ態勢管理とは、クラウドコンポーネントの適正な設定を意味する。例えば、ネットワーク接続上の設定ミスや、あまりにも容易くアクセスできてしまうアカウントの設定管理などが挙げられる。ガートナーの調査によると、クラウドセキュリティ問題の約 80%が設定ミスにより発生している。それほどまで

に、セキュリティ態勢管理は、安全なクラウドセキュリティ環境を構築する上での重要なポイントとなるのだ。

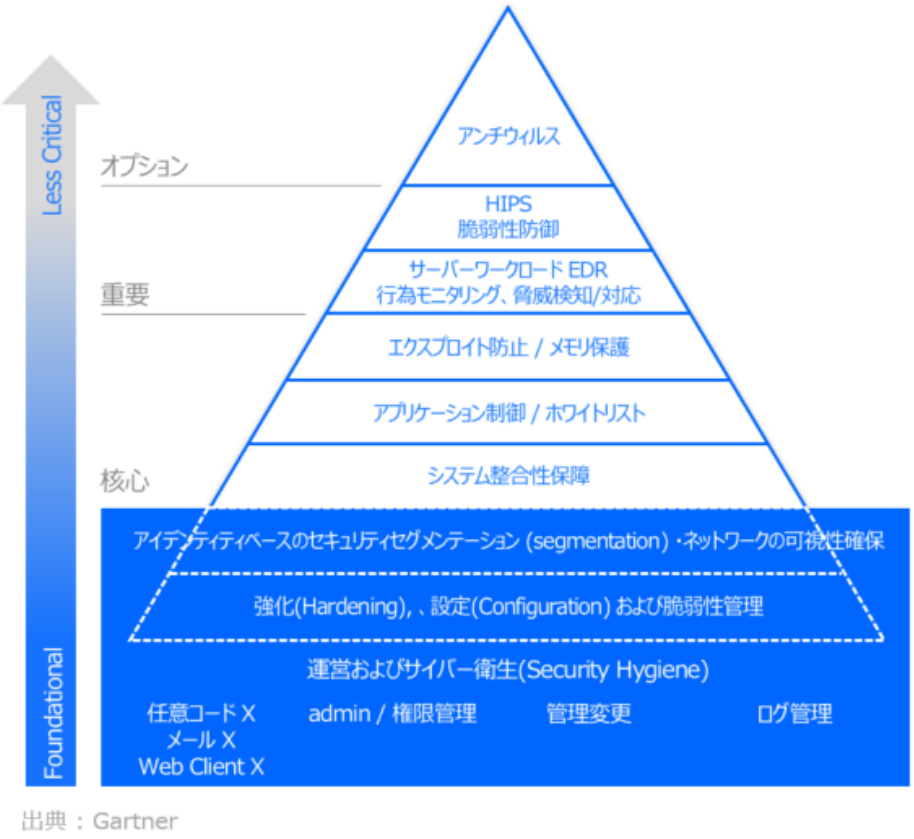
ソリューションの側面から見てみると、アンチマルウェアを活用するオンプレミスとは異なり、クラウドでは「ホスト型 IPS」が基本となる。マルウェアの遮断・駆除を行うアンチマルウェアは、クラウド環境においても重要なセキュリティ要素ではある。しかし、境界セキュリティとは異なるアプローチを有するクラウド環境では、オンプレミスのようにセキュリティの根幹を担うほどではない。

クラウド環境にてホスト型 IPS が基本となる理由としては、内部と外部の通信（North-South）だけでなく、サーバーとサーバー間、さらにアプリケーションとアプリケーション間の通信（East-West）トラフィックまでをも保護する必要があるからだ。特に、East-West トラフィックはクラウド環境上で頻繁に発生する。攻撃側も、内部被害拡散を狙いこれを悪用してくるため、ホスト型 IPS を介してトラフィックの流れや脆弱性を管理し、脅威を遮断していかなければならない。

CWPP & IPS から始めるクラウドセキュリティの第一歩

前述で説明した通り、クラウドのセキュリティフレームワークに関するキーポイントは、ワークロードの統合セキュリティにある。よって、クラウドセキュリティソリューションの優先順位においても、まず最初の一手に挙げられるのが、「クラウドワークロードセキュリティプラットフォーム（Cloud Workload Protection Platform：CWPP）」だ。

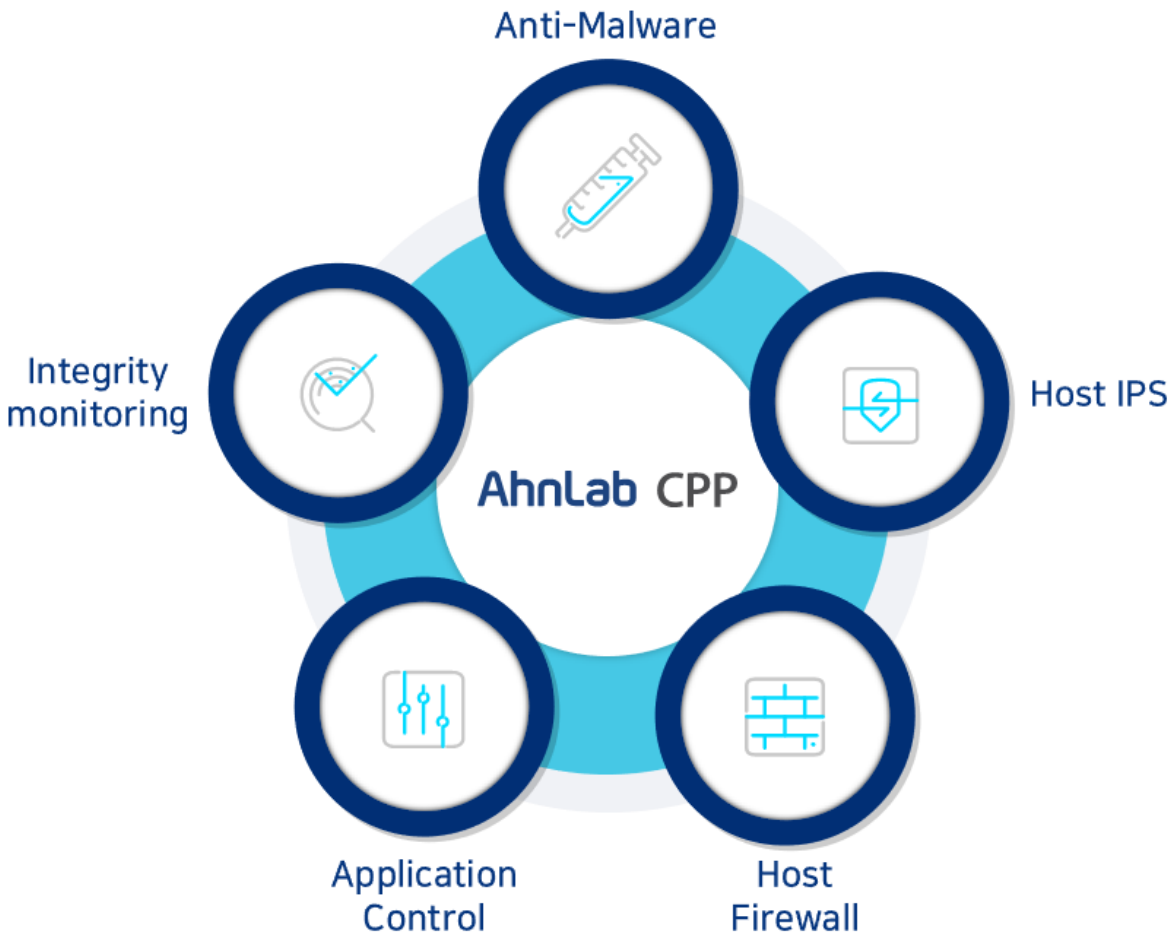
CWPP は、ハイブリッドおよびマルチクラウドアーキテクチャにて、サーバーワークロードを保護するセキュリティソリューションである。アプリケーションの開発から配布まで、あらゆる段階でセキュリティ状況を検知し、ワークロードの一貫した可視性や制御力確保に向け、様々な機能を提供している。サーバー・仮想マシン・コンテナなど、多様な環境を持つワークロードでの迅速な脅威検知・対応こそが、CWPP の核心的ポイント、かつ存在意義として挙げられる。



出典：Gartner

[図5] ガートナーが提示する CWPP 優先順位モデル

ガートナーの CWPP 優先順位モデルを見てみると、クラウドワークロードセキュリティは、運用や基本セキュリティの全般を指す「サイバー衛生」を筆頭に、強化・設定および脆弱性管理・アイデンティティベースのセキュリティセグメンテーション・ネットワークの可視性確保などを根幹としている。このように、実用性の高い機能が搭載されたセキュリティソリューションによる可用性の向上が、様々な機能が要求される状況では重要になってくる。



[図6] AhnLab CPP 構成図

アンラボは、クラウドセキュリティに対する顧客ニーズを徹底的に把握し、ニーズが反映された CWPP ソリューション「AhnLab CPP」をリリースした。「AhnLab CPP」は、CWPP の核心となるホスト型 IPS から、アプリケーション制御・整合性監視・ファイアウォール、そしてアンラボ独自の技術力とノウハウを誇るアンチマルウェアを搭載している。

続けて、「AhnLab CPP」の全機能に関する説明よりも、CWPP の基本となるホスト型 IPS に関する内容について補足していこう。

「AhnLab CPP」のホスト型 IPS、およびホストファイアウォール機能は、サーバー・アプリケーションの脆弱性を悪用したネットワーク攻撃からホストやコンテナ環境を防御する。さらに、境界ポイントに対する集中的な保護だけでなく、内部リソースの保護、すなわち攻撃に対するホストベースのネットワーク防御もサポートしてくれる。また、サーバーの送受信トラフィックを監視し、ファイアウォールの設定に従った許可・遮断や、適用された IPS シグネチャに従った攻撃検知・遮断も行う。

アンラボのホスト型 IPS は、自社の次世代侵入防止システムである「AIPS」を介すことで、韓国内で検証された数千余りのシグネチャを提供し、定期的なアップデートをサポートする。また、組織に必要なシグネチャを管理者側で直接設定することも可能だ。この際、従来の Snort (スノート) や PCRE など、様々な形態での登録もサポートしている。

ネットワーク型 IPS とは異なり、ホスト型 IPS の適用対象はサービスサーバーだ。そのため、全てのシグネチャを適用した場合、サービス提供時に性能上の問題が発生する可能性も出てくる。しかし、ホスト型 IPS は該当サーバーに必要なシグネチャのみを適用するよう設計されているため、サーバーへの負荷を軽減し、セキュリティパフォーマンスの向上を図ることができる。この際、各サーバーの環境情報をもとに分析することで、端末に適したシグネチャの推奨および自動割り当ても行う。

アンラボと二人三脚で行う“実用的な”クラウドセキュリティ

アンラボは、「AhnLab CPP」を中心としたクラウドセキュリティプラットフォームへの積極的な投資、また買収合併により、クラウド Web アプリケーションファイアウォール (WAF)・データ統合セキュリティ・コンプライアンスチェックの自動化など、幅広いセキュリティ力を保持している。さらに、セキュリティ特化型の次世代 MSP サービスである「AhnLab Cloud」をはじめ、クラウド脅威をリアルタイムで検知・対応するクラウドセキュリティ管制や、セキュリティニーズおよびコンプライアンス対策を提供するクラウド情報保護コンサルティングまで、包括的なクラウドセキュリティポートフォリオも有している。

クラウドセキュリティにおいてアンラボが目標に掲げるキーワード、それは「Actionable (アクショナブル：何らかの行動につながるの意)」である。複雑なクラウド環境にて、顧客がセキュリティを効果的に確立するためには、優先順位の適切な設定や、実際に適用可能なセキュリティ力の提供が必要不可欠であるからだ。実際、アンラボのポートフォリオは「Actionable」という目標を反映し、顧客が必要とする製品・サービスで構成されている。

アンラボの統合セキュリティ力は、顧客に様々なコミュニケーションルートも提供している。顧客はセキュリティソリューションやサービスを運用しつつ、コンサルティングを受けることで、クラウドのセキュリティインテリジェンスを確保することも可能だ。アンラボは、今後も顧客が本当に必要とする案件に重きを置き、最適なクラウドセキュリティパートナーとして発展への道を歩み続けていきたい。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)