보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

클라우드 보안, 어렵다면 이것부터 시작하자

AhnLab 2022-08-01

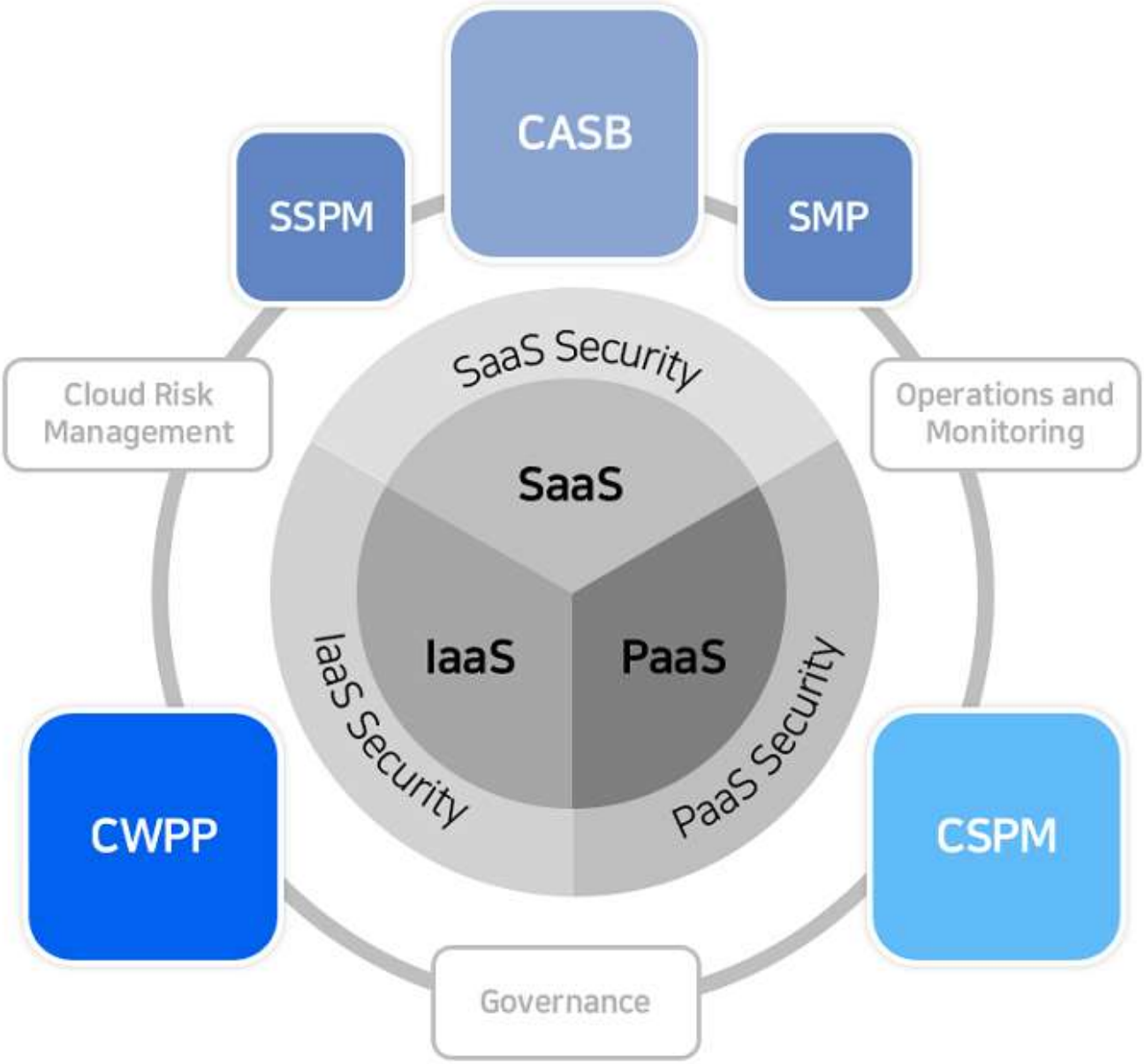
월간'안' 독자들에게 이제 클라우드 보안이라는 개념 자체가 생소한 경우는 많지 않을 것이다. 다만, 클라우드 보안에 대해 알면 알수록 생각보다 어렵다는 사실을 깨닫는 독자들도 있을 것이다. 클라우드 보안처럼 어렵지만 꼭 해야하는 일이 있다면, 우선순위를 설정하고 실제 할 수 있는 것부터 적용하는 접근 방식이 필요하다.

이번 글에서는 클라우드와 온프레미스의 차이점을 살펴본 뒤, 클라우드 보안에서 무엇부터 갖춰야 하는지 살펴본다.

클라우드 보안은 기본적으로 쉽지 않다. 구성되는 요소가 많고 또 보호해야 할 대상이 계속해서 바뀌기 때문이다. 클라우드 보안을 올바르게 시작하기 위해 가장 먼저 해야할 일은 온프레미스와 클라우드의 본질적인 차이를 이해하는 것이다. 여기서, 이해란 온프레미스와 클라우드의 구조 뿐만 아니라 기존 보안에서 분리되어 있던 엔드포인트와 네트워크에 대한 상호 이해까지 포괄한다.

클라우드 보안의 구성

우선, 클라우드 보안이 기본적으로 어떻게 구성되는지 살펴보자. 시장조사기관 가트너(Gartner)가 제시한 클라우드 보안 모델과 각 보안 툴의 역할을 정리하면 다음과 같다.



[그림 1] 클라우드 보안 툴 커버리지 (출처: 가트너)

클라우드 보안 툴 정식 명칭 및 역할

▲CWPP: Cloud Workload Protection Platform (클라우드 워크로드 보안 플랫폼)

▲CSPM: Cloud Security Posture Management (클라우드 보안 형상 관리)

▲CASB: Cloud Access Security Broker (클라우드 접근 보안 중개)

▲SMP: SaaS Management Platform (SaaS 관리 플랫폼)

▲SSPM: SaaS Security Posture Management (SaaS 보안 형상 관리)

보안 툴	역할	보호 영역
CWPP	클라우드 워크로드 보호	IaaS & PaaS
CSPM	IaaS와 PaaS에 걸쳐 잘못된 보안 구성 방지	IaaS & PaaS
CASB	클라우드 리소스 접근 제어 및 보안 정책 적용	SaaS
SMP	여러 SaaS 툴을 단일 플랫폼에서 관리	SaaS
SSPM	SaaS 애플리케이션 보안 형상 관리 및 리스크 평가	SaaS

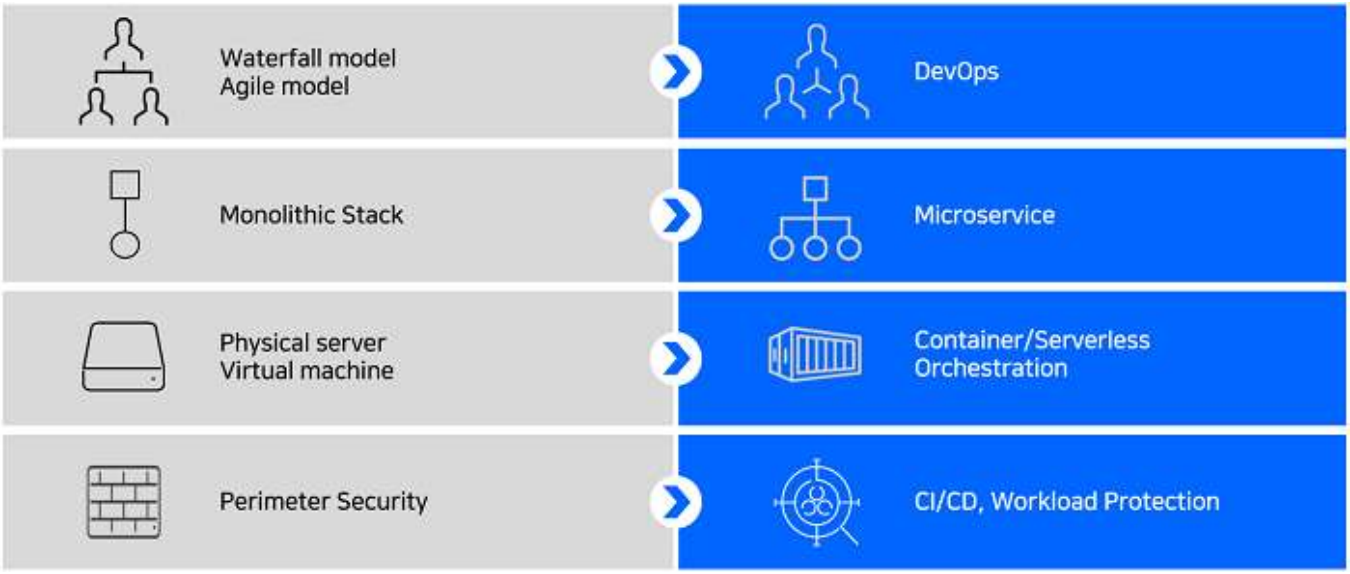
[표 1] 클라우드 보안 툴의 역할과 보호 영역

위 클라우드 보안 모델은 가장 기본적인 것으로 실제 클라우드 보안의 구분은 더 세분화되어 있다. IaaS와 PaaS를 보호하는 CWPP와 CSPM도 영역을 세분화해보면 보호하는 지점이 조금씩 다르다. 따라서, [그림 1]과 [표 1]은 클라우드 보안의 구성을 큰 틀에서 정의한다는 관점으로 이해하면 된다.

중요한 것은 클라우드 보안은 하나의 솔루션으로 온전히 한 영역을 커버할 수 없다는 것이다. 여기에 클라우드 네이티브 서비스의 수명주기가 점점 짧아짐에 따라 변화에 빠르게 대응해야 한다는 요구사항도 존재한다. 따라서, 각 솔루션들이 상호보완적 체계를 구축하는 방향으로 재편되고 있다.

온프레미스와 클라우드: 개념의 차이

클라우드 보안 구성의 개념을 이해하면, 기존 온프레미스 보안과 본질적으로 다르다는 것을 깨닫게 된다. 두 체계에 어떤 차이가 있는지 개념적인 측면에서부터 짚어본다.



[그림 2] 온프레미스와 클라우드의 차이

개발 프로세스부터 살펴보면, 기존 온프레미스에서는 특정한 계획을 중심에 두고 단계적으로 진행해 나가는 '워터폴(Waterfall) 방식을 흔히 채택해왔다. 이후에는 일정한 주기를 두고 끊임없이 개발하여 변화에 유연하게 대응할 수 있는 애자일(Agile) 방식으로 변모했다. 그리고 클라우드 환경으로 넘어오면서 신속성과 확장성에 대한 요구사항이 증가함에 따라, 개발부터 배포와 운영까지 통합된 '데브옵스(DevOps)' 방법론이 각광받고 있다.

아키텍처의 경우, 온프레미스에서는 컴포넌트(Component)와 데이터를 하나의 공간에 밀집시켜 연결한 '모놀리식 아키텍처(Monolithic Architecture)'가 활용되어 왔다. 모놀리식 아키텍처는 비교적 복잡성이 덜하지만, 작은 수정사항에도 애플리케이션 전체가 영향을 받아 변화에 유연하지 못하다는 단점이 있다. 클라우드 환경에서는 컴포넌트를 세분화하여 나누고 각각을 API로 연결한 '마이크로서비스 아키텍처(Microservice Architecture: MSA)'로 변화했다.

이와 같은 차이는 운영 환경에도 변화를 불러왔다. 기존 온프레미스 환경에서는 물리 서버와 가상화 기술을 활용했다면, 클라우드에서는 마이크로서비스 아키텍처를 수용하기 위해 컴포넌트를 실행시킬 작은 단위의 환경이 필요해졌다. 이는 곧 컨테이너와 서버리스 및 오케스트레이션 필요성 증가로 이어지게 된다.

정리하면, 클라우드와 데브옵스, 마이크로서비스 아키텍처의 핵심은 애플리케이션 개발 및 운영의 신속성과 변화에 대한 즉각적인 대응이다. 최근 IT 환경에서는 이 개념에 대한 필요성이 높아지고 있어, 점점 더 많은 기업들이 온프레미스에서 클라우드로 옮겨가고 있는 상황이다.

온프레미스와 클라우드: 마이그레이션

온프레미스를 사용하던 기업이 클라우드를 도입하면 '마이그레이션(Migration)'을 위한 다양한 작업들을 수행한다. 클라우드 마이그레이션은 이전하는 구성요소가 클라우드 환경에 얼마나 최적화 되는지에 따라 크게 4단계로 구분된다.

클라우드 마이그레이션 4단계

▲1단계: Rehost - Lift and Shift
▲2단계: Replatform - 개발 로직을 클라우드 환경에 맞게 옮겨오는 것
▲3단계: Refactor - 클라우드 기반 모델에 맞게 코드를 바꾸는 것
▲4단계: Rewrite - '클라우드 네이티브(Cloud Native)로 다시 설계하는 것

우리나라는 전환을 빠르게 하기위해 'Lift and Shift 방식으로 클라우드 환경을 구축하는 기업들이 많다. 물론, 새로 만들어지는 서비스의 경우는 그렇지 않지만, 서버 애플리케이션들은 대부분 Lift and Shift 형태로 이전되고 있다.

Lift and Shift 방식은 온프레미스 서버에서 가상 서버로 이전하는 것에 대해서는 큰 애로사항이 없다. 하지만, 환경이 기존과 완전히 바뀌는 네트워크나 클라우드 인프라 서비스의 경우 운영에 차질을 빚을 수 있다. 이는 보안도 마찬가지다. 온프레미스의 보안 로직을 클라우드에 그대로 옮겨오면 장기적인 관점에서 구성에 어려움을 겪을 가능성이 높다.

클라우드를 원활하게 운영하고 최대한의 혜택을 보기 위해서는 클라우드 환경에 맞게 아키텍처를 설계하는 클라우드 네이티브 마이그레이션이 필요하다. 물론, Lift and Shift에 비해 시간과 비용이 많이 소요되지만 장기적인 비즈니스 생산성과 지속가능성을 고려하면 클라우드 네이티브가 올바른 선택이라 할 수 있다.

클라우드 보안은 온프레미스와 어떻게 다른가?

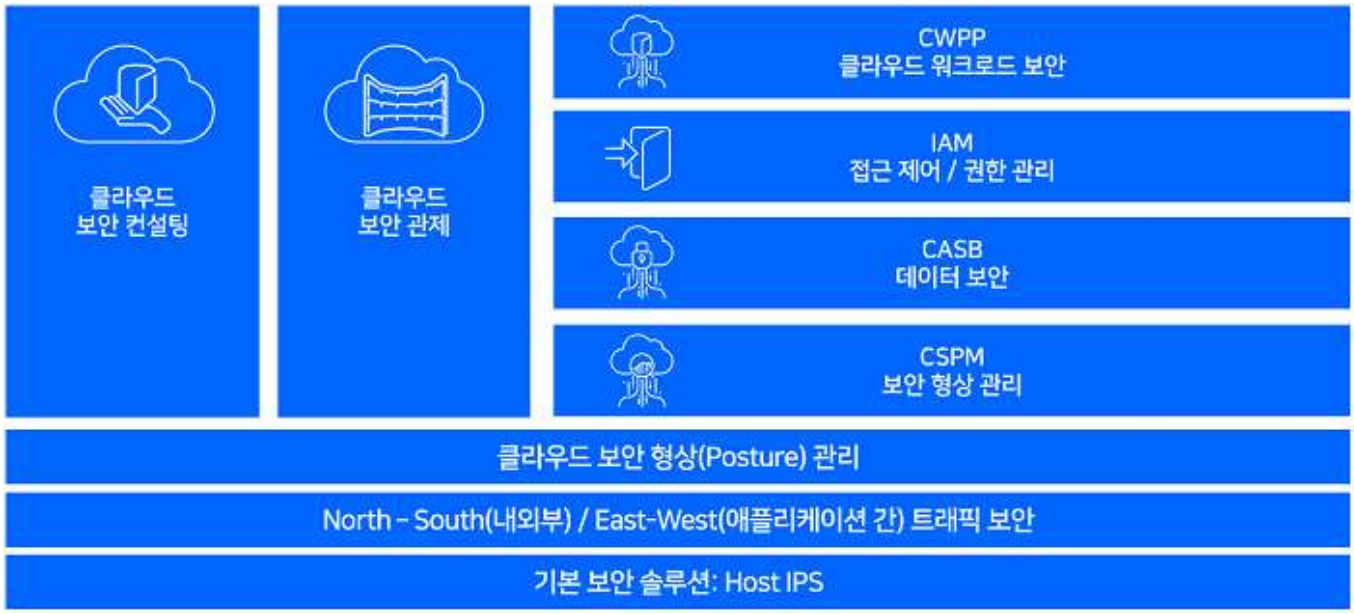
이처럼 온프레미스와 구조적인 차이를 가진 클라우드는 보안도 다르게 구성된다.

온프레미스 보안 프레임워크를 먼저 살펴보면 '경계(Perimeter)'를 중심으로 보안이 운영된다. 경계는 내부와 외부 혹은 엔드포인트와 네트워크 등의 경계로 이해하면 쉽다. 온프레미스의 경계 보안은 보호할 대상과 자원이 정의되어 있어야 한다. 정의된 자원에 대해 외부 접근을 강력하게 통제하고, 내부의 중요 자원 또는 외부와 연결된 자원에 대한 보안을 별도로 강화하는 형태로 진행된다. 이를테면, 네트워크 보안을 통해 강력한 접근 통제와 위협 차단을 적용하고 시스템에 대한 접근을 제어하는 식이다.

[그림 3] 온프레미스 보안 프레임워크

온프레미스 보안 관리와 적용은 정책(Policy)을 기준으로 하며, 기본 보안 솔루션으로는 백신으로 알려진 안티 멀웨어(Anti Malware)가 꼽힌다. 백신을 설치해두고 엔드포인트 보안 플랫폼의 구성 요소들을 정책을 기반으로 연결해 나가는 것으로 이해하면 된다.

반면, 클라우드 보안 프레임워크는 자원을 공유하는 클라우드의 특성 상 경계가 모호하기 때문에 '워크로드(Workload)' 중심으로 보안이 운영된다. 워크로드란 운영체제, 애플리케이션 등 비즈니스 가치를 창출하는 자원의 모음을 뜻한다. 즉, 견고한 클라우드 보안 체계 구축을 위해서는 경계를 지키는 것 보다 클라우드 상에서 운영되는 자원인 워크로드에 대한 통합 보안이 더 효과적이라 할 수 있다.



[그림 4] 클라우드 보안 프레임워크

클라우드 보안은 온프레미스와 달리 보안 형상(Posture) 관리가 중요하다. 보안 형상 관리란 클라우드 구성 요소의 올바른 설정을 의미하는데, 예를 들면 잘못 설정된 네트워크 연결이나 너무 쉽게 접근 가능하도록 설정된 계정 등을 관리하는 것 등이 있다. 가트너의 조사에 따르면, 클라우드 보안 사고의 약 80%는 설정 오류에 의해 발생했을 만큼 보안 형상 관리는 안전한 클라우드 보안 환경 조성의 핵심이라 할 수 있다.

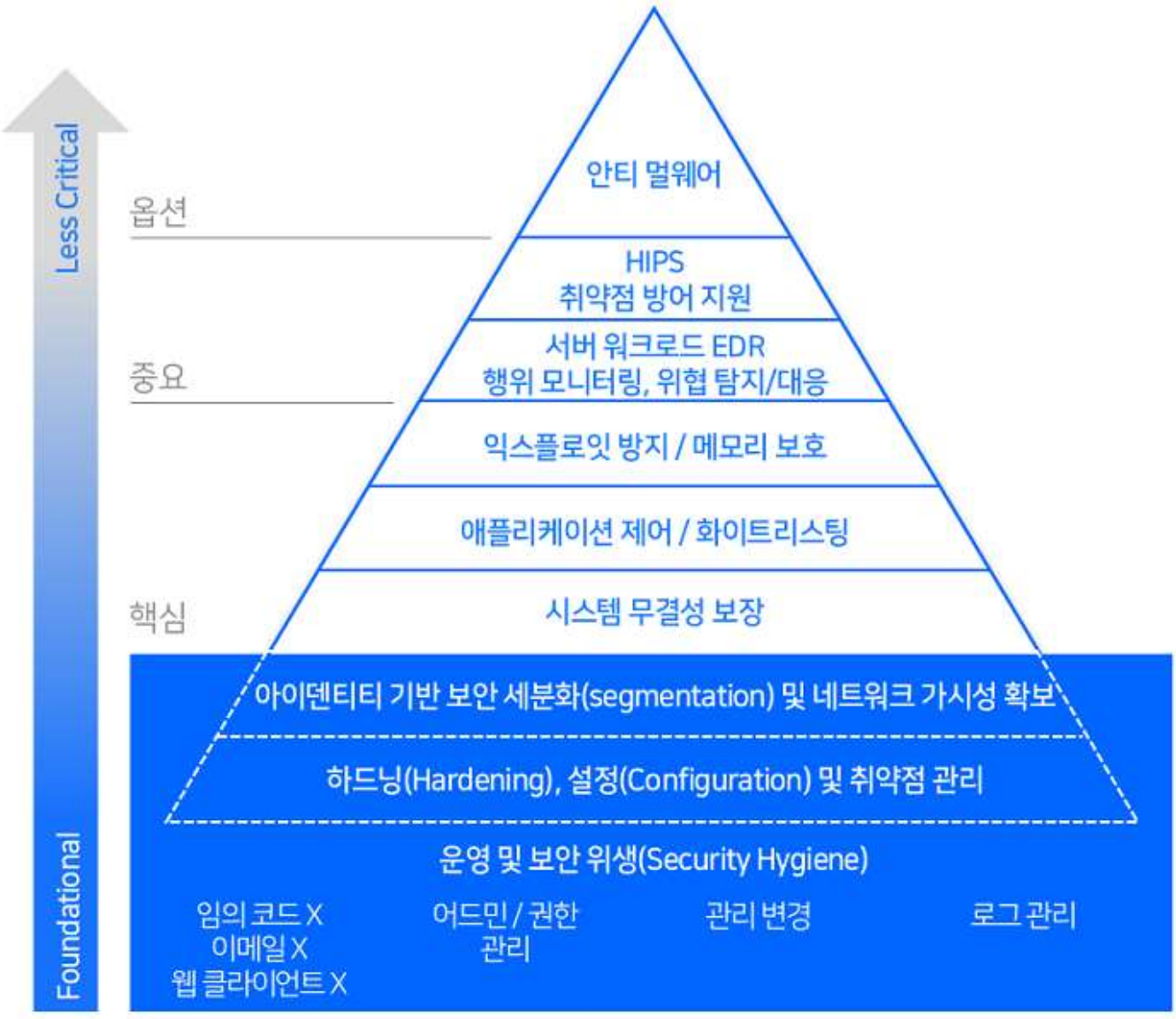
솔루션 측면에서 보면 온프레미스의 안티멀웨어와 달리 클라우드에서는 호스트 IPS가 기본이 된다. 악성코드를 차단하고 치료하는 안티멀웨어는 클라우드 환경에서도 중요한 보안 요소이지만 경계 보안과는 다른 접근법을 가져가는 클라우드 환경에서는 온프레미스에서처럼 보안의 근간을 이루는 정도는 아니다.

클라우드 환경에서 호스트 IPS가 기본이 되는 이유는 내부와 외부의 통신(North-South) 뿐만 아니라 서버와 서버 간, 그리고 애플리케이션과 애플리케이션 간 통신(East-West) 트래픽까지 보호해야 하기 때문이다. 특히, East-West 트래픽은 클라우드 환경에서 빈번하게 발생하고 공격자들도 이를 내부 피해 확산에 활용하기 때문에 호스트 IPS를 통해 트래픽의 흐름과 취약점을 관리하고 위협을 차단할 수 있어야 한다.

클라우드 보안, CWPP와 호스트 IPS부터

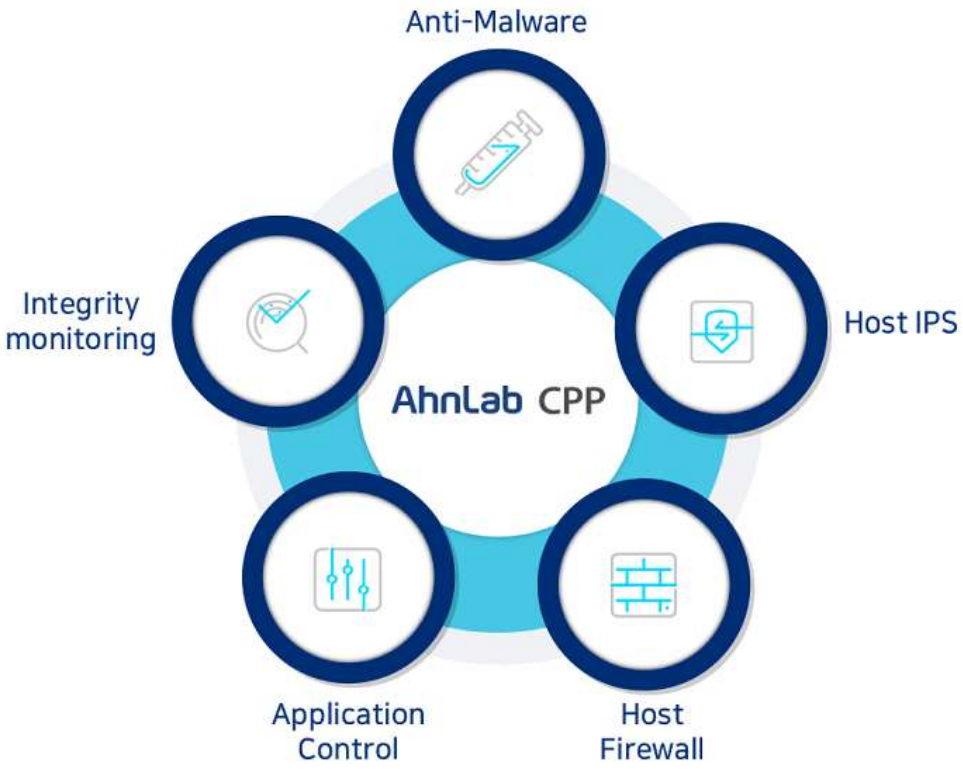
앞서 설명했 듯, 클라우드 보안 프레임워크에서 핵심은 워크로드 통합 보안이다. 따라서, 클라우드 보안 솔루션의 우선순위에서도 클라우드 워크로드 보안 플랫폼(Cloud Workload Protection Platform: CWPP)가 단연 첫 손에 꼽힌다.

CWPP는 하이브리드 및 멀티 클라우드 아키텍처에서 서버 워크로드를 보호하는 보안 솔루션이다. 애플리케이션의 개발부터 배포까지 모든 단계에서 보안 현황을 점검하고 일관적인 워크로드 가시성과 통제 역량 확보를 위해 여러 가지 기능들을 제공한다. CWPP의 핵심이자 존재 이유는 서버, 가상머신, 컨테이너 등 다양한 환경에서 워크로드 위협을 신속하게 탐지해 대응하는 것이다.



[그림 5] 가트너가 제시한 CWPP 우선순위 모델 (출처: 가트너)

가트너의 CWPP 우선순위 모델에 따르면, 클라우드 워크로드 보안은 운영과 기본적인 보안의 전반을 일컫는 '보안 위생'을 필두로 하드닝, 설정 및 취약점 관리, 아이덴티티 기반 보안 세분화, 네트워크 가시성 확보를 근간으로 한다. 이처럼 다양한 기능들이 요구되는 상황에서 중요한 것은 실질적으로 활용도가 높은 기능들을 탑재한 보안 솔루션을 통해 가용성을 향상시키는 것이다.



[그림 6] AhnLab CPP 구성도

안랩은 클라우드 보안에 대한 고객들의 요구사항을 면밀하게 파악한 뒤 이를 반영해 출시한 CWPP 솔루션 'AhnLab CPP'를 선보였다. AhnLab CPP는 CWPP의 핵심인 호스트 IPS부터 애플리케이션 제어, 무결성 모니터링, 방화벽, 그리고 안랩의 독보적인 기술력과 노하우를 자랑하는 안티 멀웨어를 탑재하고 있다.

이어서, AhnLab CPP의 모든 기능을 설명하기 보다는 CWPP의 기본이 되는 호스트 IPS에 대한 내용만 부연한다.

AhnLab CPP의 호스트 IPS, 그리고 호스트 방화벽 기능은 호스트와 컨테이너 환경을 대상으로 서버 및 애플리케이션 취약점을 악용한 네트워크 공격을 방어한다. 경계점에서의 집중 보호 뿐만 아니라 내부 자원, 즉 호스트 기반의 네트워크 공격 방어를 지원하는 것이다. 서버로 들어오거나 나가는 트래픽을 모니터링해서 방화벽 설정에 따라 허용/차단하거나, 적용된 IPS 시그니처에 따라 공격을 탐지/차단한다.

안랩 호스트 IPS는 자사의 차세대 침입방지시스템인 AIPS를 통해 국내에서 검증된 수천 여 개의 시그니처를 제공하며 주기적으로 업데이트를 지원한다. 또한 관리자는 조직이 필요한 시그니처를 직접 설정할 수 있다. 이때 기존 스노트(Snort), PCRE 등 다양한 형태의 등록을 지원한다.

네트워크 IPS 와 달리 호스트 IPS는 서비스 서버를 적용 대상으로 하여, 모든 시그니처를 적용할 경우 서비스 제공 시 성능 이슈가 발생할 수 있다. 이에 호스트 IPS는 해당 서버에 필요한 시그니처만을 적용하도록 설계되어, 서버의 부하를 줄이고 보안의 효율성을 높일 수 있다. 이 때, 각 서버의 환경 정보를 기반으로 분석을 진행해 단말에 적합한 시그니처를 추천, 자동 할당한다.

안랩과 함께하는 '실용적인' 클라우드 보안

안랩은 AhnLab CPP를 중심으로 한 클라우드 보안 플랫폼에 활발한 투자와 인수합병을 통해 클라우드 웹 애플리케이션 방화벽(WAF), 데이터 통합 보안, 컴플라이언스 점검 자동화 등 폭 넓은 보안 역량을 갖추고 있다. 여기에, 보안 특화 차세대 MSP 서비스 'AhnLab Cloud'를 비롯해 클라우드 위협을 실시간으로 탐지해 대응하는 클라우드 보안 관제와 보안 요구사항 및 컴플라이언스 준수 방안을 제공하는 클라우드 정보보호 컨설팅까지 포괄적인 클라우드 보안 포트폴리오를 갖추고 있다.

클라우드 보안에 관해 안랩이 지향하는 키워드는 'Actionable'이다. 복잡다단한 클라우드 환경에서 고객이 효과적으로 보안을 확립하기 위해서는 올바른 우선순위 설정과 실제 적용 가능한 보안 역량 제공이 필수적이기 때문이다. 실제, 안랩의 포트폴리오는 'Actionable'이라는 지향점을 반영하여 고객들이 꼭 필요로 하는 제품과 서비스들로 구성되어 있다.

안랩의 통합 보안 역량은 고객들에게 다양한 소통 경로를 제공하기도 한다. 고객들은 보안 솔루션과 서비스를 활용하면서, 혹은 컨설팅을 통해 클라우드 보안 인텔리전스를 확보할 수 있다. 안랩은 앞으로도 고객들이 실제 필요로 하는 사항에 우선순위를 두고 최적의 클라우드 보안 파트너로서 계속 발전해 나갈 계획이다.

AhnLab 이상국 마케팅본부장