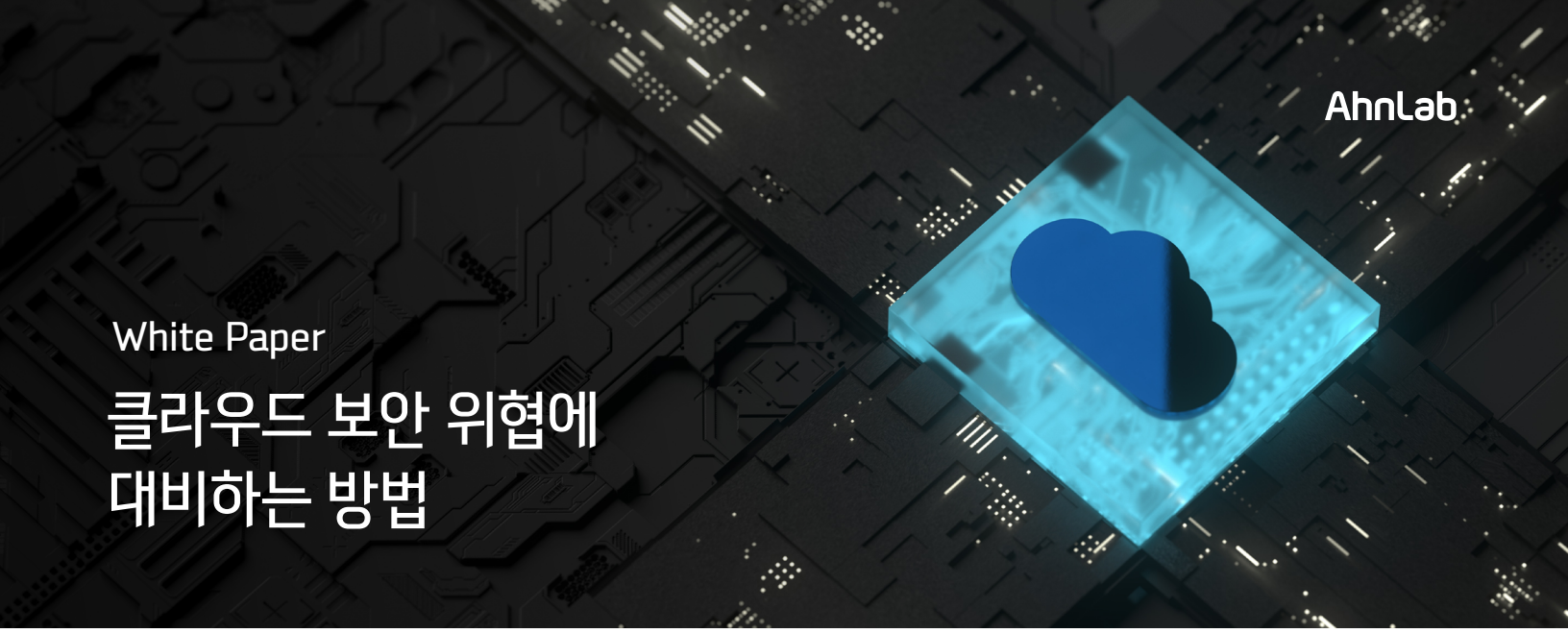


White Paper

클라우드 보안 위협에 대비하는 방법

개요

바야흐로 클라우드 전성시대다. 수 년 전부터 대세의 입지를 다져온 클라우드는 코로나19 팬데믹으로 디지털 트랜스포메이션이 가속화되면서 필수불가결한 존재로 자리 잡았다. 많은 기업들이 기존의 온프레미스(On-premise)와 퍼블릭 클라우드를 혼합해 사용하는 '하이브리드' 환경을 마주하게 되면서 두 환경에 걸쳐 통합 가시성을 확보하고 동등한 수준의 보안을 구축할 방안을 모색하고 있다. 이러한 측면에서 하이브리드 클라우드 보안의 핵심이자 첫 걸음은 서버 워크로드를 효과적으로 보호하는 것이다. 시장에서는 이와 같은 클라우드 워크로드 보안 솔루션을 'CWPP(Cloud Workload Protection Platform)'라 한다.

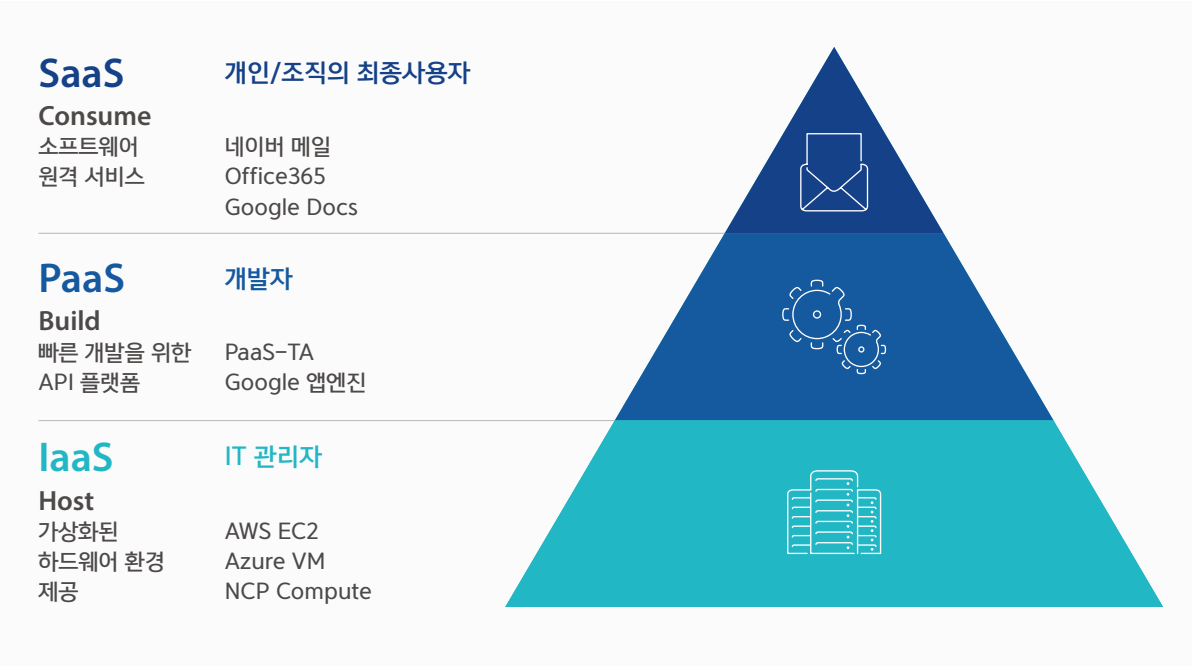
본 백서에서는 클라우드의 기본적인 개념부터 안랩의 하이브리드 클라우드 워크로드 보안 솔루션 'AhnLab CPP'를 활용한 클라우드 보안 방안에 대해 알아본다.

클라우드 IaaS · PaaS · SaaS란?

클라우드는 인터넷을 통해 IT 리소스가 필요할 때마다 필요한 만큼 쓰고 비용을 내는 일종의 리스 같은 임대 서비스라고 할 수 있다. 주거 형태로 친다면 기존의 온프레미스(On-premise)는 내 집이고 클라우드는 숙박 업체에 비유할 수 있다. 즉, 필요한 만큼 빌리고 필요한 기간 만큼 사용하고 그 비용을 업체에 지불하는 것이다.

내 집을 짓기 위해서는 설계부터 완공까지 많은 시간과 노력, 비용을 들여야 한다. 한번 짓고 나면 사이즈를 줄이거나 늘리고 필요 없는 공간이 생겨도 없애기 힘들다. 집을 짓는 것뿐만 아니라 유지보수에도 엄청난 시간과 비용을 들여야 한다. 이에 반해 임대는 건물을 짓고 유지보수하는 건 모두 숙박 업체의 몫이고, 사용자는 필요할 때 필요한 만큼만 빌리면 된다. 빌리고자 하는 공간을 쉽게 줄이거나 늘릴 수 있고 필요 없을 땐 취소할 수도 있다. 공간을 유지보수하고 관리하는 것 역시 전혀 신경 쓰지 않아도 된다. 이러한 개념을 IT 환경에서 구현한 것이 클라우드다.

클라우드 자산을 빌릴 때 그 유형은 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 등으로 구분할 수 있다. 앞서 집을 빌리는 걸 예로 들자면, IaaS는 집만 빌리고 그 안에는 아무 것도 없는 경우이다. 전기나 수도 등은 준비되어 있지만 가구나 가전 제품 등은 알아서 채워야 한다. PaaS는 가구나 가전 제품까지 준비되어 있는 것이다. 예를 들어, 요리를 한다고 할 때 요리할 수 있는 기본적인 준비는 된 상태이다. SaaS는 빌트인 된 가구 및 가전 제품과 함께 실제 뷔페처럼 모든 게 다 완비되어 있는 형태라고 할 수 있다. 무엇을 먹을지 선택만 하면 된다.



[그림 1] 클라우드 서비스 구조

이처럼 클라우드에서는 하드웨어나 네트워크 등의 인프라만 빌려주는 것을 IaaS라 하고 개발 플랫폼, 개발 환경까지 제공하는 것을 PaaS, 그리고 실제 그대로 서비스 이용만 하면 될 수준까지 제공하는 것을 SaaS라고 말한다.

사용자들은 클라우드를 통해 비용 절감, 업무 효율성을 얻을 수 있다. 온프레미스와 비교했을 때 초기 비용이 들지 않고, 오토 스케일링(Auto Scaling)을 통해 리소스를 유연하게 확장 가능한 점은 클라우드의 분명한 장점이다.

이에, 클라우드 도입도 점점 증가하는 추세다. 시장조사기관 가트너(Gartner)에 따르면, 2021년 글로벌 퍼블릭 클라우드 시장 규모는 약 3,961억 달러(약 463조 원)이며, 내년에는 약 4,821억 달러(약 562조 원) 수준까지 성장할 전망이다.

또한, 가트너는 2021년 3조 2400억 원 규모로 형성된 한국의 퍼블릭 클라우드 시장 규모가 2022년에는 3조 7238억 원까지 늘어날 것으로 예측했다. 코로나19 팬데믹 이후 디지털 트랜스포메이션이 가속화되면서 클라우드 도입이 급증한 결과이며, 클라우드 도입 확대는 포스트 코로나 시대에도 계속될 것으로 보인다.

다만, '경제적 이득'을 취할 수 있는 곳으로 몰리는 해커들의 특성에 따라 클라우드 환경을 노리는 공격 역시 증가 및 다변화되고 있다. 특히 기업의 보안 담당자들은 자원 공유, 서비스화 등 기존 레거시 환경과는 다른, 클라우드가 가진 특성 때문에 보안을 고민하지 않을 수 없게 되었다.

클라우드 보안 책임은 누구에게 있나?

지금부터 본격적으로 클라우드 보안에 대해 살펴보자. 온프레미스와 마찬가지로 클라우드 환경에서도 보안 위협은 발생한다. 앞서 클라우드 개념과 마찬가지로 주거 형태로 예를 들어 보자.

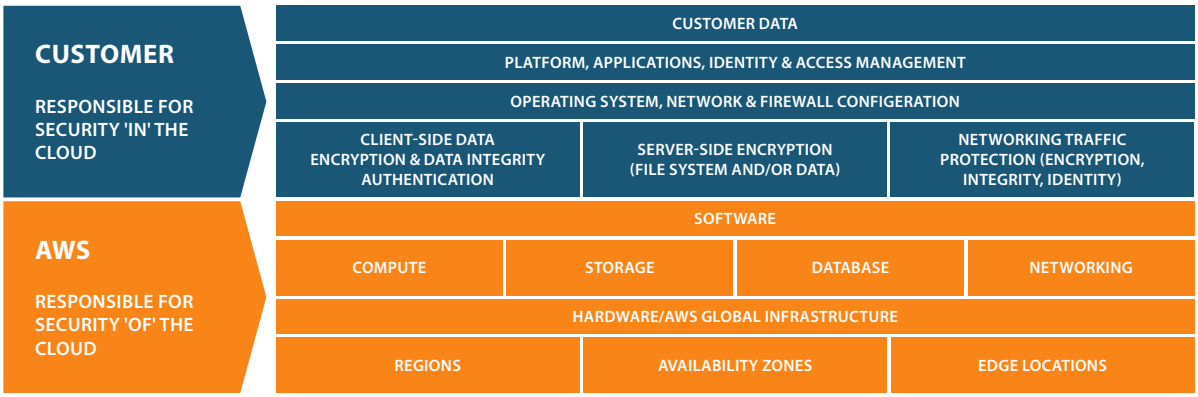
내가 관리하는 내 집인 경우 그 관리 책임은 자신이겠지만 숙박 업체의 경우에는 책임의 주체가 애매모호하다. 외부적인 침입, 즉 건물로 아무나 못 들어오게 하거나 홍수, 재해 등의 위험으로부터 방어하는 것은 숙박 업체의 몫일 것이다. 그런데 내가 빌린 방에 누군가 들어와서 지갑이나 중요 파일을 훔친다면 어떻게 될까? 예를 들어 같이 숙박하던 친구가 훔쳤거나 또는 내가 방 키 관리를 잘못했다면 빌린 사람의 책임이기도 하다. 이런 경우에는 상황을 고려하여 누구의 책임인지를 따져야 한다. 이는 클라우드 환경에서도 마찬가지다.

실제 클라우드 공급 업체에서 제공하는 인프라와 서비스를 사용하는 환경에서 만약 사고가 발생한다면 누구의 책임일까? 글로벌 보안 기업 탈레스와 포네몬 연구소가 2019년 말 조사한 결과에 따르면, 클라우드에서 데이터 보호의 책임에 대해 조사 대상 기업의 31%는 자신의 책임으로, 33%는 기업과 클라우드 공급 업체의 공동 책임으로, 35%는 클라우드 공급 업체의 책임으로 인식하는 것으로 나타났다. 즉 35%에 달하는 많은 기업이 클라우드 활용 시 클라우드 사업자가 모든 책임을 질 것으로 생각하고 있다는 것이다.

참고로, 정답은 '클라우드 서비스의 형태에 따라 사용자와 서비스 제공자가 책임을 공유한다'는 것이며, 현재는 이에 관한 인식이 많이 높아졌다. 하지만, 온프레미스와 달리 보안 통제권을 나누는 구조에 대해 어려움을 겪는 기업들이 여전히 많은 것이 사실이다.

퍼블릭 클라우드 환경에서는 보안 사고나 장애 사고 발생 시 클라우드 서비스 공급 업체가 제공하는 서비스가 어디까지인지 보고, 누구의 책임인지를 확인해야 한다. 이것을 클라우드 서비스 공급자는 '공동 책임 모델(Shared Responsibility)'이라고 설명한다. 공동 책임 모델이란 클라우드 환경에서 보안은 클라우드 사업자와 기업이 함께 책임을 공유한다는 개념이다.

[그림 2]는 아마존웹서비스(이하 AWS)에서 기업과 클라우드 서비스 사업자 간의 보안 책임 범위를 설명한 것이다. AWS가 서비스하는 하드웨어, 네트워크, 시스템 등은 AWS의 책임 범위이고 그 위에 고객이 직접 관리하는 영역에서의 보안, 예를 들어 네트워크 트래픽 관련 보안, 방화벽 설정, 암호화, 애플리케이션, 접근 제어, 데이터 보안 등은 모두 고객의 책임이라 밝히고 있다.



[그림 2] AWS 공동 책임 모델 (출처: AWS)

[그림 3]은 마이크로소프트 애저(Microsoft Azure)의 공동 책임 모델이다. 그림에서 파란색으로 표기된 것이 고객, 회색이 마이크로소프트사의 책임 범위이다. IaaS, PaaS, SaaS 등의 서비스 유형에 따라서 마이크로소프트사와 고객의 책임 범위가 달라진다는 것을 보여주고 있다.

[그림 3] 애저 공동 책임 모델 (출처: 마이크로소프트)

결론적으로 기존의 온프레미스 환경에서는 기업이 모든 책임을 지지만, 클라우드 환경에서는 CSP(Cloud Service Provider)와 기업이 각 범위를 나누어서 보안을 책임져야 하며, 보안 담당자는 이를 명확히 인지해야 한다.

클라우드 보안, 어떻게 해야 할까?

그렇다면 안전한 클라우드 환경 조성은 어떻게 시작해야 할까? 현재의 클라우드 환경은 물리, 가상, 하이브리드 및 멀티 클라우드의 혼합 뿐 아니라 서버/가상머신 외 컨테이너, 서버리스 등 서비스 제공 형태가 다양해지면서 복잡성이 심화된 상황이다.

여기서 보안은 클라우드 서비스의 근간을 이루는 IaaS에서부터 출발하게 되는데, 공동 책임 모델을 기준으로 IaaS는 하드웨어와 네트워크를 제외한 나머지 모든 영역을 기업이 설정하고 운영해야 한다. 이 때, 기업의 보안을 담당하는 관리자 입장에서는 보안에 대해 다음과 같은 요구 사항을 갖게 된다.

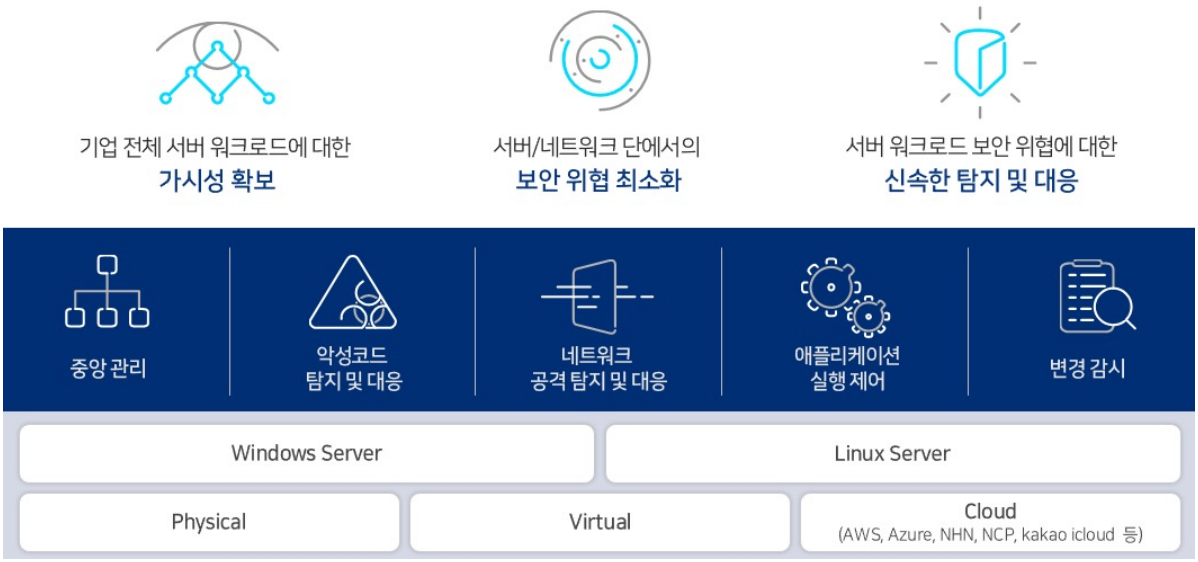
첫째, 온프레미스 서버와 함께 클라우드 상의 서버를 한꺼번에 보면서 관리할 수 있어야 한다. 둘째, 조직 내에서 직접 관리하지 않는 클라우드 서버에 대해 물리적인 접근 제어나 네트워크 접근 제어가 어렵기 때문에 논리적인 접근 제어가 용이해야 한다. 이 경우 잘못된 설정으로 인해 자산이 노출 될 수 있어, 서버로의 네트워크 접근이나 네트워킹 공격으로부터 보호해야할 필요성이 높아지고 있다. 셋째, 서버로의 표적화된 공격이 존재하므로 악성코드 등 보안 위협으로부터 서버를 보호할 수 있어야 한다.

클라우드 워크로드 보안 플랫폼 AhnLab CPP

안랩은 고객의 이러한 요구 사항을 해결하기 위해 클라우드 워크로드 보안 플랫폼 'AhnLab CPP'를 출시했다.

AhnLab CPP는 ▲온프레미스 & 가상 서버와 함께 클라우드 서버에 대한 통합 관리 ▲서버 워크로드 보호를 위한 보안 기능 제공 ▲서드파티 솔루션과의 연동을 통해 효율적 대응을 지원한다.

AhnLab CPP는 온프레미스, 가상 서버, 그리고 AWS, 애저, 네이버 클라우드 플랫폼, kakao icloud, NHN 클라우드 등 다양한 클라우드 상의 윈도우/리눅스 서버에 대한 가시성과 함께 통합 관리를 지원한다. 또, 클라우드 계정과의 연동을 통해 오토 스케일링되는 단말을 자동으로 식별한다.



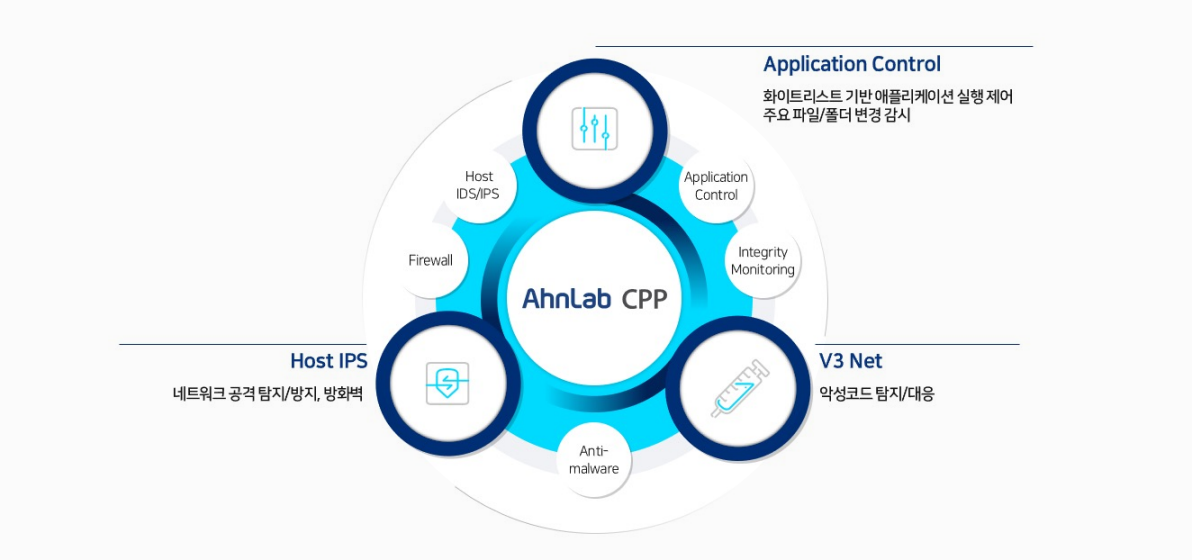
[그림 4] AhnLab CPP 보안 개념도

AhnLab CPP는 클라우드 서버 워크로드 보호에 필요한 보안 기능과 보안 제품을 하나의 콘솔에서 통합하여 관리한다. 화이트리스트 기반의 애플리케이션 실행/접근 제어, 무결성 모니터링을 담당하는 '애플리케이션 컨트롤(Application Control)', 침입탐지/방지시스템(IDS/IPS)과 방화벽 기능을 담당하는 '호스트 IPS(Host IPS)', 악성코드를 탐지/차단하는 'V3 Net'을 하나의 콘솔에서 관리하는 것이다.

또한 기업 전체 서버 보안 상태를 한눈에 파악할 수 있는 다양한 대시보드를 통해 서버 워크로드에 대한 통합된 가시성을 제공한다. AhnLab CPP 대시보드는 하이브리드 클라우드 환경을 고려하여 서버 워크로드에 대한 보안 위협을 최소화하며, 특히 시스로그(Syslog) 제공으로 SIEM 등의 서드파티(3rd party) 솔루션과의 연동을 통해 관리자의 신속한 탐지 및 대응에 기여한다.

AhnLab CPP의 주요 기능

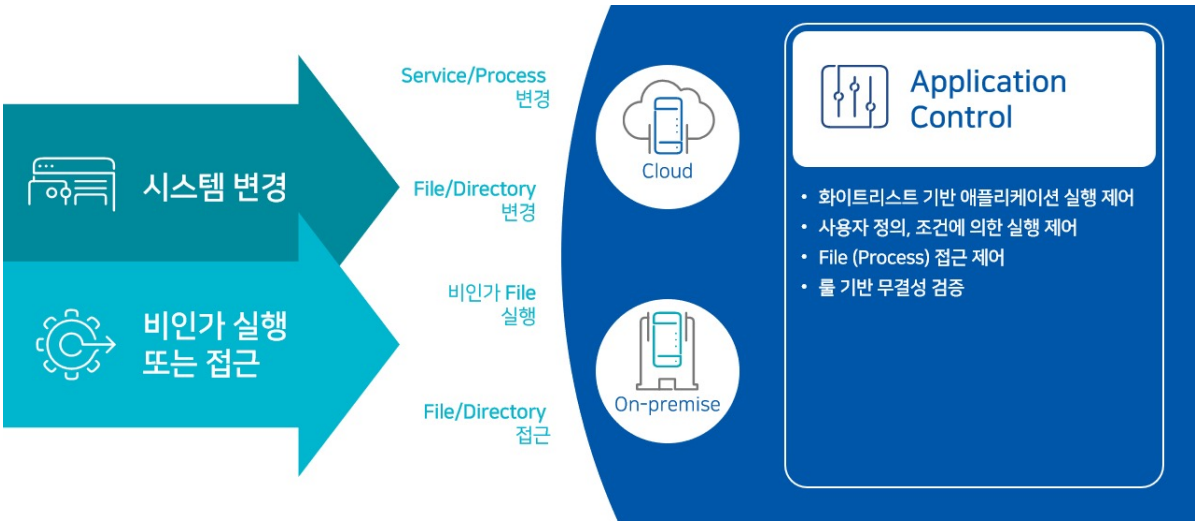
AhnLab CPP를 통해 관리되는 보안 솔루션은 크게 애플리케이션 컨트롤, 호스트 IPS, V3 Net이 있다. 애플리케이션 컨트롤은 화이트리스트 기반의 애플리케이션 실행 제어 및 접근 제어로 서버가 보다 안정적으로 운영되도록 한다. 또한 중요 파일/폴더/레지스트리 등에 대한 변경 감시를 통해 부적절한 시스템 변경을 탐지, 사전에 위협에 대응하도록 한다. 호스트 IPS는 시그니처 기반으로 네트워크 공격을 탐지/차단하며, 방화벽 기능을 함께 제공한다 V3 Net은 서버 내 악성코드에 대해 실시간 검사 및 수동 검사를 통해 악성코드 감염으로부터 서버를 보호한다.



[그림 5] AhnLab CPP 기능 구조도

1. 애플리케이션 컨트롤 & 무결성 모니터링

각 보안 솔루션의 특징을 살펴보면, 먼저 애플리케이션 컨트롤은 허가된 애플리케이션만 실행을 허용하고 그 외는 모두 실행을 차단해서 원래의 용도로만 서버가 운영되도록 하고, 사전 방역 효과를 제공한다. 중요 파일/폴더로는 지정된 프로세스만 접근을 허용해 부적절한 변경으로 서비스가 중지되지 않도록 한다.



[그림 6] AhnLab CPP 애플리케이션 컨트롤

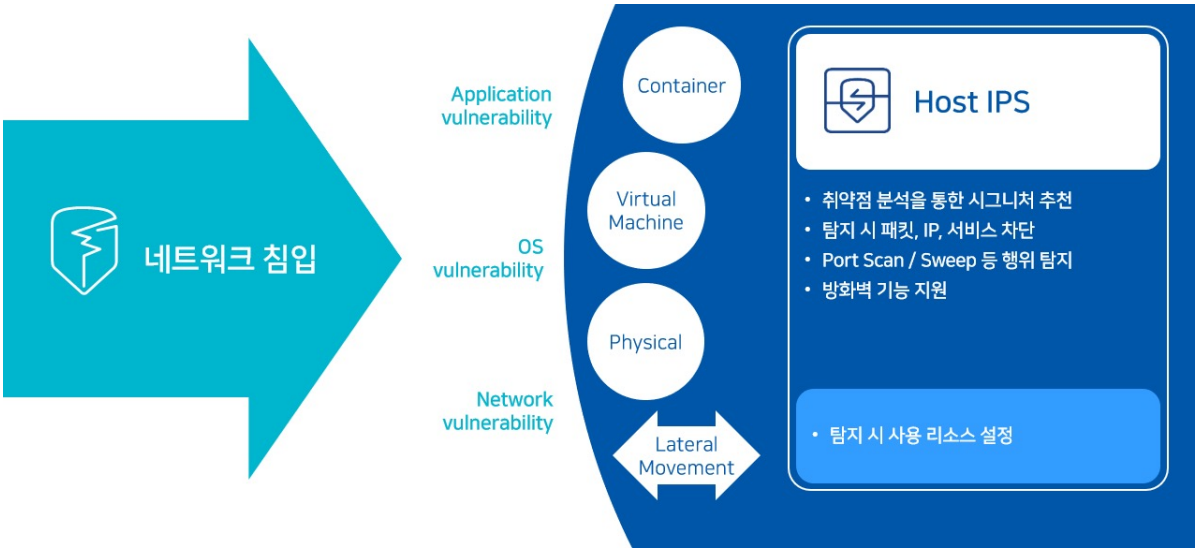
아울러, 무결성 모니터링 기능은 일반적으로 변경이 없어야 하는 특정 파일/폴더, 레지스트리, 시작 프로그램, 서비스 등에서 변경이 있는지 감시한다. 기본 배포된 규칙과 함께 사용자 정의 규칙을 함께 지원하여 사용자가 환경에 맞게 기능을 최적화할 수 있도록 했다.

애플리케이션 컨트롤은 서비스 운영을 고려해서 다양한 운영 모드를 지원하고 있다. 락다운(Lockdown)은 일반적인 보안 모드이고, 메인터넌스(Maintenance) 모드는 소프트웨어 설치나 업데이트가 되는 경우를 고려한 것이다. 업데이트가 이루어질 때는 많은 실행 파일의 변경이 이루어지는데, 락다운 상태에서는 패치가 불가능하다. 이때 메인

터넌스 모드로 변경해주면 차단 없이 변경되는 모든 실행 파일이 화이트리스트로 자동 등록될 수 있다. 시뮬레이션(Simulation) 모드 화이트리스트에 없는 파일에 대해 차단이 아닌 탐지만 하는 모드로, 락다운 전에 보안 정책의 적절성을 판단하는 용도로도 쓸 수 있다.

2. 호스트 IPS & 방화벽

AhnLab CPP의 호스트 IPS는 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.



[그림 7] AhnLab CPP 호스트 IPS & 방화벽

네트워크 IPS 와 달리 호스트 IPS는 적용 대상이 서비스 서버로, 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.

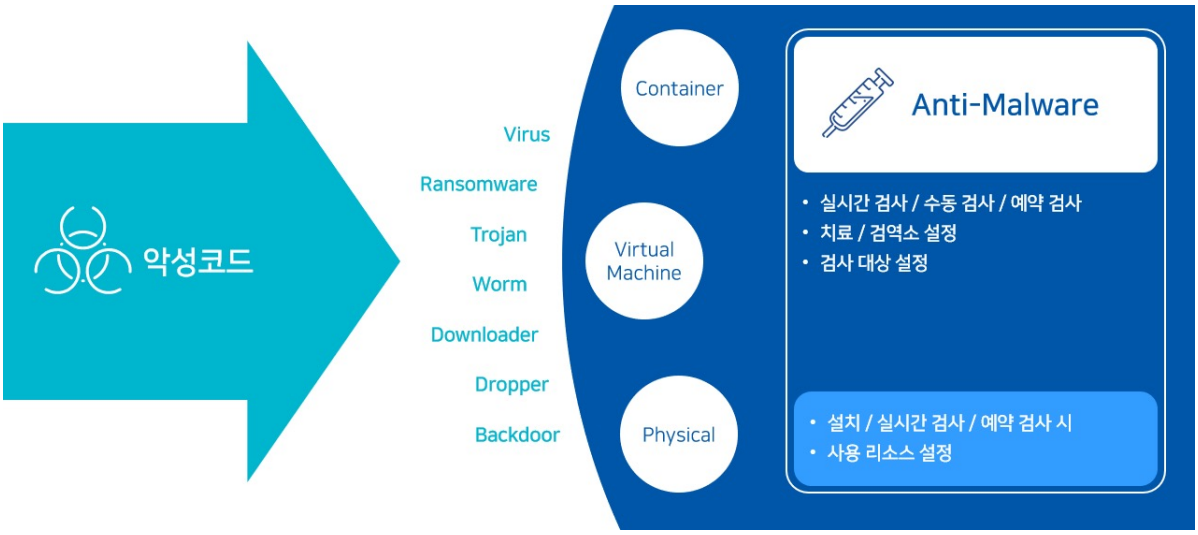
관리자 입장에서 서버 대수가 많거나 클라우드처럼 서버가 유연하게 추가/삭제되는 환경에서 각 서버의 환경을 분석하고, 그에 맞는 시그니처를 직접 적용하는 것은 불가능에 가깝다. AhnLab CPP의 호스트 IPS는 각 서버의 환경 정보를 기반으로 분석해서 단말에 적합한 시그니처를 추천, 자동 할당을 지원한다.

또한 일반적인 방화벽 기능과 함께, 국가별 IP 기반으로 특정 국가에 대한 들어오거나 나가는 트래픽의 차단을 지원한다. 호스트 IPS는 기본적으로 인라인(Inline) 모드로 동작하지만, 서버의 가용성을 고려한 탭(TAP) 모드와 장애 환경을 고려한 바이패스(Bypass) 모드도 지원하고 있다.

3. 악성코드 대응

V3 Net은 다수 고객 및 글로벌 인증 기관을 통해 이미 검증된 안티 멀웨어(Anti-malware) 기능과 서버 활용성을 고려한 수동 검사, 예약 검사 등의 설정이 가능하다. 독보적인 엔진으로 신속하고 정확한 악성코드 진단 및 치료를 지원

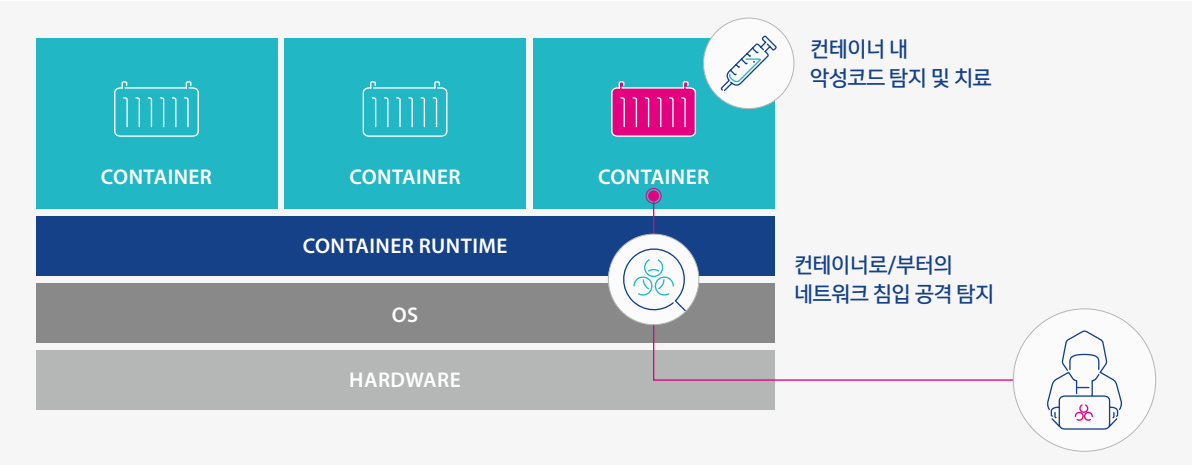
하며, 검사 예외 설정 기능으로 효율적인 방역 정책 적용이 가능하고 검사 및 치료에 대한 다양한 리포트를 제공하는 등 사용자 입장에서 편리한 보안 역량을 갖추고 있다.



[그림 8] AhnLab CPP V3 Net

4. 컨테이너 보안

AhnLab CPP는 도커, k8s 환경에서 컨테이너 파일에 대한 악성코드 탐지 및 대응 역량을 제공한다. 또한 컨테이너를 향한 또는 컨테이터로부터의 네트워크 공격에 대한 탐지를 지원한다. 특히 탐지된 컨테이너 파일과 네트워크 공격 및 통신이 어느 컨테이너에서 발생했는지 식별할 수 있다. 이를 통해 관리자는 보안상 취약점을 가진 컨테이너를 손쉽게 파악해 보다 안전한 서비스 운영 환경을 조성할 수 있다.



[그림 9] AhnLab CPP 컨테이너 보안

결론

정리하자면, AhnLab CPP는 온프레미스와 클라우드 상의 윈도우/리눅스 서버를 보호하기 위한 플랫폼으로, 조직 내 서버에 대한 통합된 가시성과 함께 애플리케이션 컨트롤, 호스트 IPS 및 방화벽, 안티 멀웨어 기능 등을 제공하며 컨테

이너에 대한 보안도 함께 지원한다. AhnLab CPP는 서버 위치와 무관하게 일관성 있는 보안 관리 역량을 제공해, 하이브리드 환경에서 보다 안전한 서버 보안 환경 구축을 가능하게 한다.

클라우드 도입과 함께 서비스 제공 형태 및 위치가 다양해지고 복잡해지면서, 조직 내 서버 워크로드에 대한 관리 부담이 증가하고 있다. 그 와 함께 온프레미스, 가상, 클라우드 등 다양한 위치 서버 워크로드를 어떻게 일관된 기준으로 안전하게 보호할 것인지 관리자의 고민이 있을 수 밖에 없다. 특히 클라우드로 전환 시, 조직의 책임 범위가 어디까지인지 파악하고 조직 내 자산 보호에 어떤 보안 역량과 솔루션이 필요한지 면밀히 검토하여 보안 체계를 마련해가는 것이 가장 중요하다.

위와 같은 이유로 안정적인 하이브리드 클라우드 환경 조성을 위해 CWPP의 다양한 보안 역량들이 요구되고 있으며, 안랩의 오랜 기술력이 축적된 AhnLab CPP는 고객들에게 좋은 선택지가 될 수 있다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901