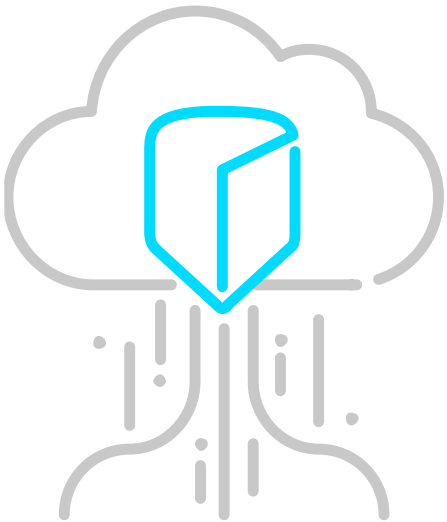
2020. 07. 07

More security,
More freedom

클라우드 워크로드 보안을 위한 제언

클라우드 보안 위협에 대비하는 방법

안랩 제품기획팀



AhnLab

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

1. 개요

안랩은 올해 초 '2020년 사이버보안 위협 Top 5'를 발표한 바 있다.

올해 예상되는 주요 보안 위협으로는 타깃형 랜섬웨어 공격 본격화, 클라우드 보안 위협 대두, 특수목적시스템 및 OT 보안 위협 증가, 정보 수집 및 탈취 공격 고도화, 모바일 사이버 공격 방식 다변화 등이다. 다양한 산업 분야에서 디지털 트랜스포메이션이 빠르게 진행되면서 클라우드 환경에 대한 사이버 공격 위협이 더욱 커지고 있다.

본 문서에서는 클라우드에 대한 기본 개념, 클라우드 환경에서의 보안 대책과 클라우드 워크로드를 보호하는 AhnLab CPP를 소개한다.

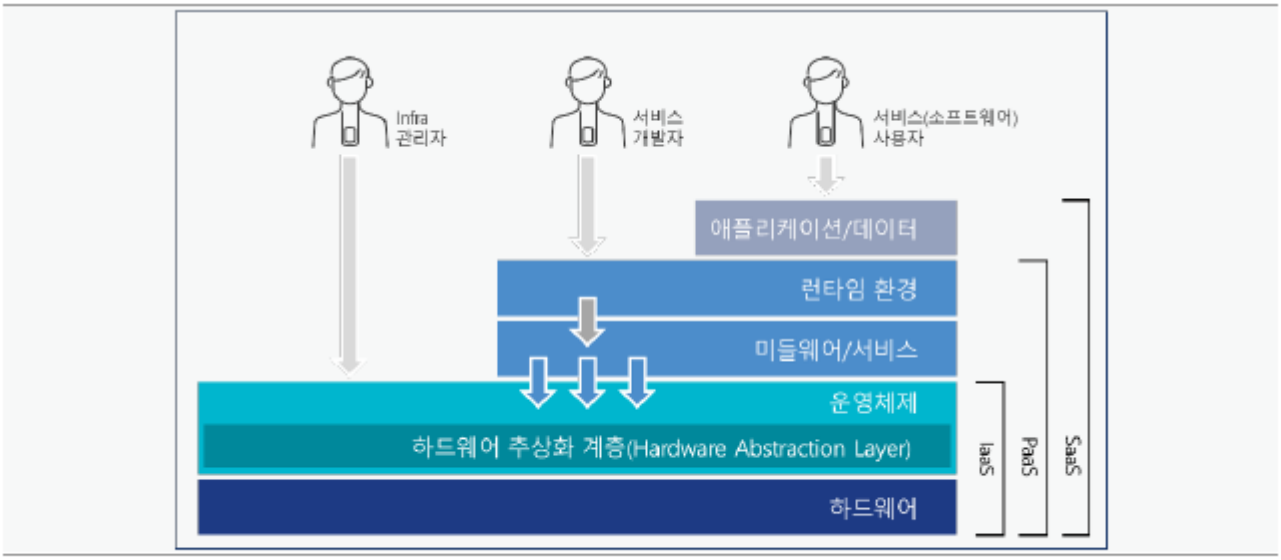
2. 클라우드 워크로드 보안 플랫폼 등장 배경

01. 클라우드 IaaS · PaaS · SaaS란?

최근 IT 환경이 클라우드로 많이 전환됨에 따라 클라우드 환경에서의 보안 위협이 더욱 커지고 있다. 보안 위협을 알아보기 전에 우선 클라우드가 무엇인지 개념부터 짚어보자.

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 기간만큼 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.



[그림 1] 클라우드 서비스 유형(출처: 클라우드혁신센터)

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, IaaS 는 집만 빌리고 그 안에는 아무 것도 없는 경우이다. 전기나 수도 등은 준비되어 있지만 가구나 가전 제품 등은 알아서 채워야 한다. PaaS 는 가구나 가전 제품까지 준비되어 있는 것이다. 예를 들어, 요리를 한다고 할 때 요리할 수 있는 기본적인 준비는 된 상태이다. SaaS 는 빌트인 된 가구 및 가전 제품과 함께 실제 뷔페처럼 모든 게 다 완비되어 있는 형태라고 할 수 있다. 무엇을 먹어야 할 지 준비만 하면 된다.

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

사업자는 클라우드를 통해 비용 절감, 업무 효율성을 얻을 수 있다. 이에 따라 클라우드로의 도입은 점점 증가하는 추세다. 글로벌 리서치 기관인 가트너에 따르면 2020 년 글로벌 퍼블릭 클라우드 시장은 약 293 조 원 규모로 예상하고 있다. 이 중 SaaS 서비스가 44%, IaaS 서비스가 19%를 차지하여 SaaS 중심으로 시장이 성장하는 것으로 파악된다.

국내 퍼블릭 클라우드 시장을 살펴보면, 2020 년 약 2 조 9 천억원 규모의 시장으로 15.9%의 성장을 예상하고 있다. 이 중 SaaS 서비스는 36%, IaaS 서비스는 34%를 차지한다. 국내에서는 해외와는 다르게 SaaS 와 IaaS 시장이 유사한 비율을 보이고 있다. 이는 해외 시장 대비 국내 클라우드의 전환이 '인프라' 중심으로 이루어지고 있기 때문으로 풀이된다. 즉 웹이나 개발 등 서버 환경을 클라우드에 네이티브하게 새로이 구축하기보다는 기존 환경 그대로 클라우드로 이전하거나 도입된 비율이 많은 것으로 볼 수 있다.

이는 클라우드 전환에 대한 기술적 이해의 어려움이나 국내 법규 자체가 온프레미스 중심으로 되어 있어 기존 환경을 그대로 전환하는 것이 구축 및 관리 측면에서 더 용이하기 때문이다.

이러한 현상은 다른 조사 결과에서도 볼 수 있는데, '클라우드 도입 시 느끼는 어려운 점'에서 꼽은 사유를 살펴보면 1 위가 보안에 대한 우려이다. 그 외 IT 기술 전문성 부족, 컴플라이언스 구축, 멀티/하이브리드 환경

관리의 복잡성 등을 꼽고 있다. 이는 클라우드 환경에 대한 관리에서부터 보안까지 전반적으로 어려움을 느끼고 있음을 알 수 있다.

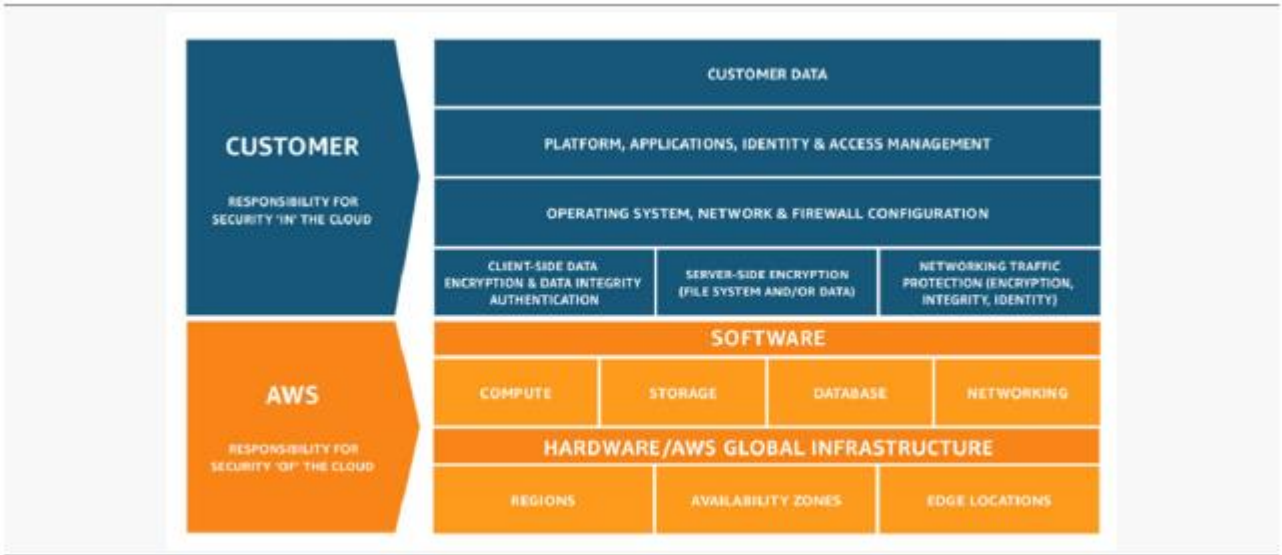
02. 클라우드 보안 책임은 누구에게 있나?

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 연구소에 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.

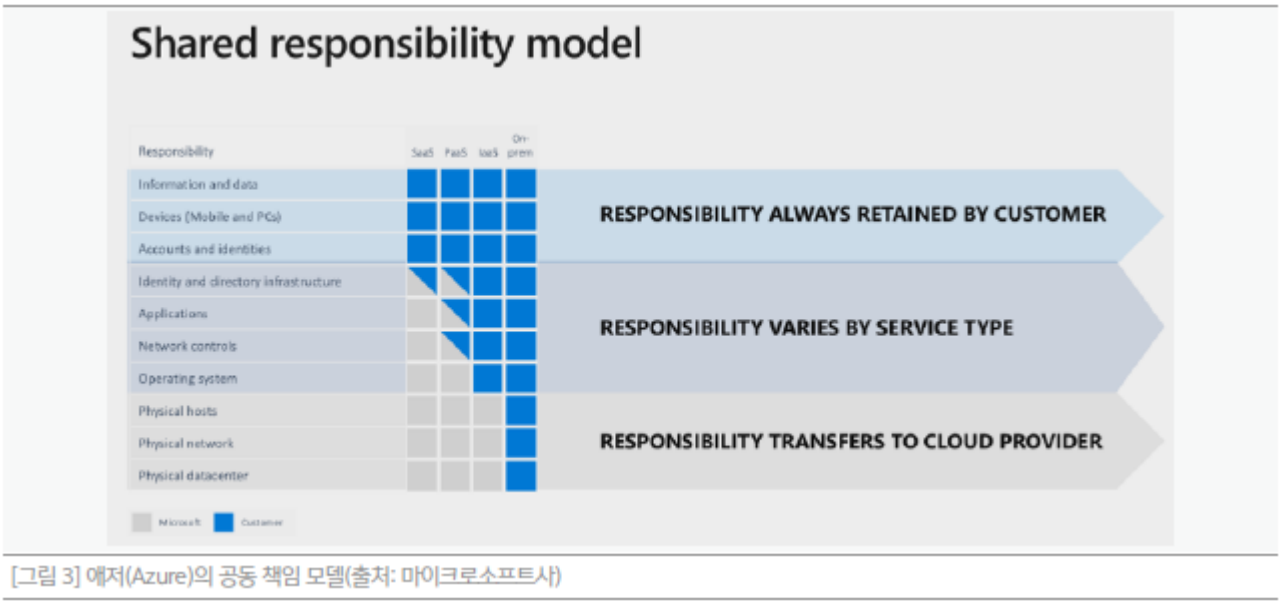
앞서 말한 것처럼, 퍼블릭 클라우드 환경에서 보안 사고나 장애 사고 발생 시 클라우드 서비스 공급 업체가 제공하는 서비스가 어디까지인지 보고, 누구의 책임인지를 확인해야 한다. 이것을 클라우드 서비스 공급자는 '공동 책임 모델(Shared Responsibility)'이라고 설명하고 있다. 공동 책임 모델이란 클라우드 환경에서 보안은 클라우드 사업자와 기업이 함께 책임을 공유한다는 개념이다.

[그림 2]는 아마존웹서비스(이하 AWS)에서 기업과 클라우드 서비스 사업자 간의 보안 책임 범위를 설명한 것이다. AWS 가 서비스하는 하드웨어, 네트워크, 시스템 등은 AWS 의 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 책임이라고 이야기하고 있다.



[그림 2] AWS 공동 책임 모델(출처: aws.amazon.com)

[그림 3]은 애저(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(Azure)의 공동 책임 모델(출처: 마이크로소프트사)

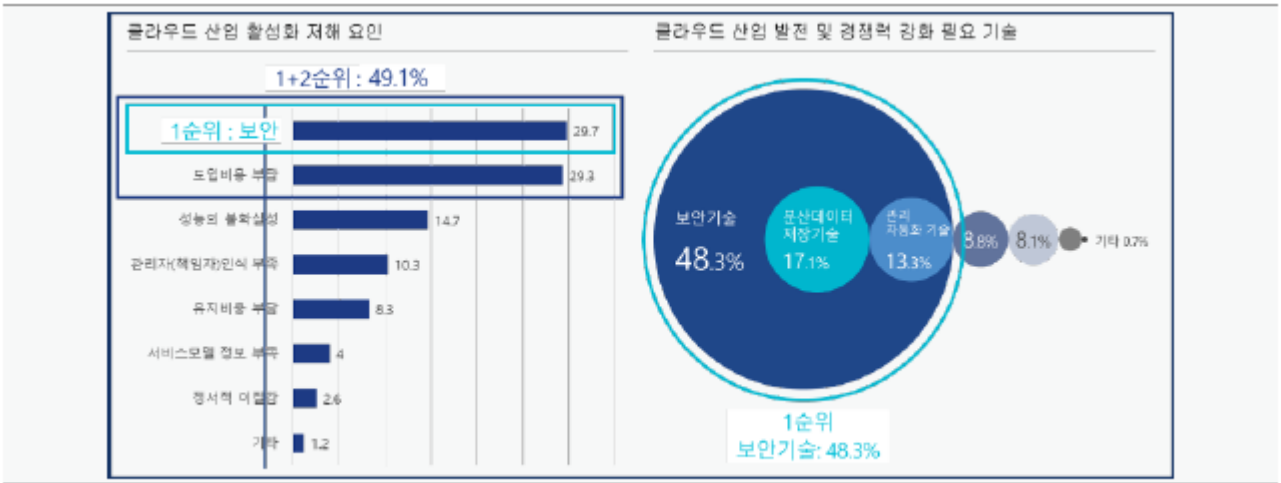
결론적으로 기존의 온프레미스 환경에서는 기업이 모든 책임을 지지만, 클라우드 환경에서는 CSP(Cloud Service Provider)와 기업이 각 범위를 나누어서 보안을 책임져야 하며, 이를 보안 담당자는 명확히 인지해야 한다.

03. 클라우드 보안 어떻게 해야 할까?

IT 전문 매거진인 네트워크타임즈가 국내 보안 담당자를 대상으로 한 설문 조사 결과에서 따르면, 클라우드 적용 현황에 대해 응답자의 44.7%가 클라우드를 적용했다고 답변했다. 이 가운데 중요 업무에는 17.7%, 중요하지 않은 업무에는 27.6%를 적용했다고 조사되었다. 더불어 43.0%의 응답자가 '적용 가능한 업무를 검토하고 있다'까지 밝혔다. 따라서 조사 응답자의 87.7%가 클라우드를 적용하거나 계획이 있는 것으로 나타났다. 반면 클라우드 보안 체계를 살펴보면 가장 많이 차지하는 것이 보안 체계 마련을 위해 검토 중이라는 답변이 51.8%로, 클라우드는 적용하지만 클라우드 전환 시 보안은 고민하지 않았다는 것을 보여주고 있다. 그리고 5.4%는 전혀 보안을 고려하지 않은 것으로 나타났다. 이 외에도 온프레미스 상의 보안을 그대로 적용한 것이 14.9%이고, 컨설팅 기업이 권고하는 대로 적용, 클라우드 전담 부서에 일임, 매니지드 서비스에 위임이 22%로 대부분이 클라우드 환경에서의 보안에 대해 그대로 위임한 것으로 보인다.

이는 최근 몇 년 사이에 클라우드 환경으로 급격하게 전환된 것에 비해 클라우드 환경에서의 보안은 기존 온프레미스처럼 정형화되어 있지 않다 보니 관리자 입장에서는 보안 솔루션 적용에 어려움을 겪고 있는 것으로 풀이된다.

이러한 현상은 정보통신산업진흥원(NIPA)에서 실시한 클라우드 산업 실태 조사에서도 나타난다. 클라우드 산업 활성화에 있어 저해 요소를 살펴보면 1 순위가 보안에 대한 우려였으며, 클라우드 산업 발전을 위해 우선적으로 개발되어야 할 기술에서도 보안 기술이 48.3%로 1 순위였다. 클라우드 관련 서비스와 기술이 빠르게 변화하고 있어 그에 맞게 보안도 빠른 변화가 필요하다는 시사점을 보여준다.



[그림 4] 클라우드 산업 활성화 저해 요인 및 경쟁력 강화 필요 기술 (출처: 정보통신산업진흥원)

그렇다면 클라우드, 특히 IaaS 기반의 클라우드 환경에서는 어떤 보안을 해야 할까? 기업들은 클라우드를 도입하고 있지만 100% 클라우드로 전환하기보다는 필요한 서비스에 한하여 도입하고 있는 실정이다.

이렇다 보니 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 심각한 노출이 될 수 있다. 따라서 서버로의 네트워크 접근이나

네트워킹 공격으로부터 보호 필요성이 증가하고 있다. 셋째, 서버로의 표적화된 공격이 존재하므로 악성코드 등 보안 위협으로부터 서버를 보호할 수 있어야 한다.

3. 클라우드 워크로드 보안 플랫폼 AhnLab CPP

안랩은 고객의 이러한 요구 사항을 해결하기 위해 AhnLab CPP 를 출시했다. AhnLab CPP 는 클라우드 워크로드 보안 플랫폼으로 ▲ 온프레미스 서버와 함께 클라우드 서버에 대한 통합 관리 ▲ 서버 워크로드 보호를 위한 보안 기능 제공 ▲ 서드파티 솔루션과의 연동을 통해 효율적 대응을 지원한다.

[그림 5] AhnLab CPP 개념도

AhnLab CPP 는 클라우드 서버 워크로드 보호에 필요한 보안 기능과 보안 제품을 하나의 콘솔에서 통합하여 관리한다. 화이트리스트 기반의 애플리케이션 콘트롤(Application Control), 침입방지시스템(IPS)과 방화벽 기능을 담당하는 Host IPS, 악성코드를 탐지/차단하는 V3 Net 제품 등을 하나의 콘솔에서 관리하는 것이다.

AhnLab CPP 는 온프레미스 상의 윈도우/리눅스(Windows/Linux) 서버, 그리고 AWS, 애저(Azure) 클라우드 상의 윈도우/리눅스 서버에 대한 가시성과 함께 통합 관리를 지원한다. AWS, 애저 클라우드 계정과의 연동을 통해 오토 스케일링되는 단말에 대해서 자동 식별을 지원한다.

또한 서버에서 발생하는 보안 이벤트에 대한 로깅과 함께 다양한 대시보드를 제공해서 관리자가 보안 상태를 직관적으로 파악할 수 있도록 한다. 시스로그(Syslog) 제공으로 SIEM 등의 서드파티(3rd party) 솔루션과의 연동을 통해 신속한 탐지 및 대응이 가능하다.

AhnLab CPP 를 통해 관리되는 보안 제품은 AhnLab Application Control(안랩 애플리케이션 콘트롤), AhnLab V3 Net(안랩 V3 Net), 그리고 AhnLab Host IPS(안랩 호스트 IPS)가 있다.

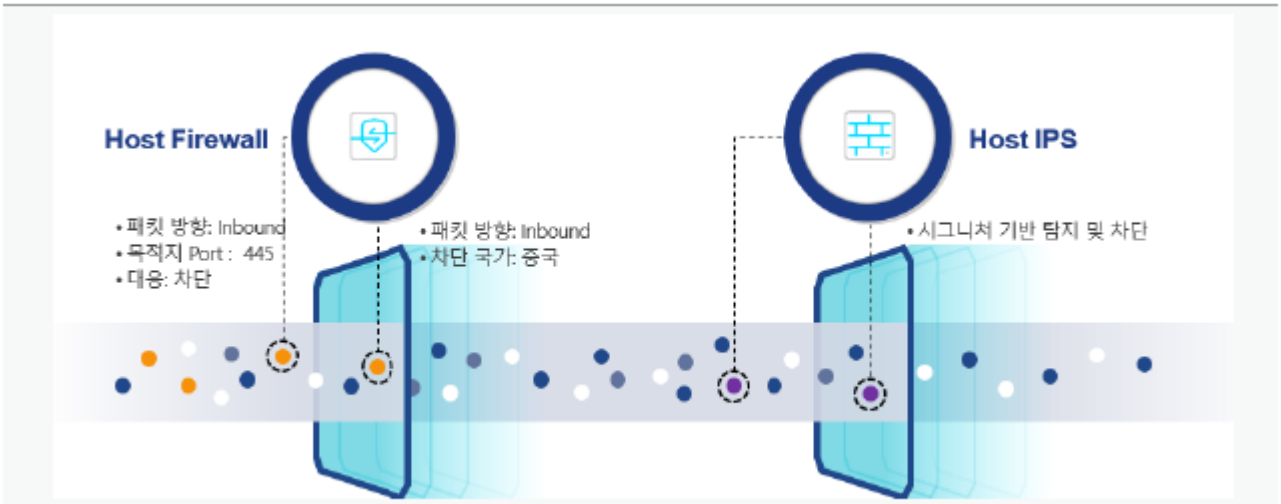
[그림 6] AhnLab CPP 주요 기능

안랩 애플리케이션 콘트롤은 화이트리스트 기반의 애플리케이션 실행 제어 및 접근 제어로 서버가 보다 안정적으로 운영되도록 한다. 안랩 V3 Net 은 서버 내 악성코드에 대해 실시간 검사 및 수동 검사를 통해 악성코드 감염으로부터 서버를 보호한다. 안랩 호스트 IPS 는 시그니처 기반으로 네트워크 공격을 탐지/차단한다. 그리고 방화벽 기능을 함께 제공한다.

각 보안 제품의 특징을 살펴보면, 먼저 안랩 애플리케이션 콘트롤은 허가된 애플리케이션만 실행을 허용하고 그 외는 모두 실행을 차단해서 원래의 용도로만 서버가 운영되도록 한다. 실제 허가되지 않은 애플리케이션은 실행이 차단되어 사전 방역 효과를 제공한다. 이와 함께 중요 파일로 지정된 프로세스만 접근을 허용해서 부적절한 변경으로 서비스가 중지되지 않도록 한다.

안랩 애플리케이션 콘트롤은 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 메인터넌스 모드로 변경해주면 차단 없이 변경되는 모든 실행 파일이 화이트리스트로 자동 등록될 수 있다. 시뮬레이션(Simulation) 모드 화이트리스트에 없는 파일에 대해 차단이 아닌 탐지만하는 모드로, 락다운 전에 보안 정책의 적절성을 판단하는 용도로 쓸 수 있다.

안랩 호스트 IPS 는 서버로 들어오거나 나가는 트래픽을 모니터링해서 방화벽 설정에 따라 차단하거나, 적용된 IPS 시그니처에 따라 공격을 탐지/차단한다. IPS 는 시그니처 기반으로 네트워크 공격을 탐지/차단하는 것인데 안랩 호스트 IPS 는 자사의 차세대 침입방지시스템인 AIPS 를 통해 국내에서 검증된 수천여 개의 시그니처를 제공하며 주기적으로 업데이트를 지원한다. 또한 관리자는 조직이 필요한 시그니처를 직접 설정할 수 있다. 이때 기존 스노트(Snort), PCRE 시그니처가 있다면 손쉽게 적용할 수도 있다.



[그림 7] AhnLab Host IPS 동작 방식

네트워크 IPS 와 달리 호스트 IPS 는 모든 시그니처를 적용하는 게 아니라, 해당 서버에 필요한 시그니처만을 적용하도록 설계되어 있는데, 이것은 서버의 부하를 줄이고 보안의 효율성을 높이기 때문에 서버 부하와 보안의 효율성 측면에서 호스트 IPS 라는 점은 매우 중요한 이점이 있는 것이다. 관리자가 각 서버의 환경을 분석하고, 그에 맞는 시그니처를 직접 적용하기란 쉽지 않다. 특히 서버 대수가 많거나 클라우드처럼 서버가 유연하게 추가/삭제되는 경우는 더욱 어렵다. 안랩 호스트 IPS 는 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 IPS 는 기본적으로 인라인(Inline) 모드로 동작하지만, 서버의 가용성을 고려한 탭(TAP) 모드와 장애 환경을 고려한 바이패스(Bypass) 모드도 지원하고 있다.

정리하자면, AhnLab CPP 는 온프레미스와 클라우드 상의 윈도우/리눅스 서버를 보호하기 위한 플랫폼으로, 조직 내 서버에 대한 통합된 가시성과 함께 애플리케이션 콘트롤, 호스트 IPS 및 방화벽, 안티멀웨어 기능 등을 제공한다. AhnLab CPP 는 서버 위치와 무관하게 일관성 있는 보안 관리 지원으로, 보다 안전한 서버 보안 환경 구축을 가능하게 한다. 클라우드로의 전환 시, 조직의 책임 범위가 어디까지인지 파악과 함께 조직 내 자산 보호에 무엇이 필요한지 검토하여 보안 체계를 함께 마련해가는 것이 가장 중요한 부분이다.

