

클라우드 시대 워크로드 보안, 네트워크 보안, 컨테이너 보안 방안

5G와 AI로 가중되는 보안위협, 세가지 도전과제	2
IT인프라 진화에 대처하는 보안 방식	4
클라우드 네이티브 워크로드 보안 방법, 'CI/CD 보안'	6
단순하고 효율적인 클라우드 네트워크 보안	8
통합 서버보안의 진화, OS부터 컨테이너 플랫폼까지 총체적 위협 보호	10



5G와 AI로 가중되는 보안위협, 세가지 도전과제

세계는 5G, 사물인터넷(IoT), 클라우드, 머신러닝 등으로 빠르게 변하고 있다. 5G 통신기술은 기기와 사람이 커뮤니케이션하는 방식을 바꾼다. 앞으로 펼쳐질 미래를 예측하려면 5G 이전의 과거를 돌아켜보면 알 수 있다.

5G 이전의 시대

2G나 2.5G 시대에는 통신망에서는 전화나 문자만 할 수 있었다. 3G 시대가 되자 스마트폰이 생겼다. 이 스마트폰을 잘 활용하기 위해 서비스 품질을 보장하는 네트워크가 필요하게 됐다. 이를 통해 스마트폰이나 태블릿, 다양한 OS 등이 보급되게 됐다.

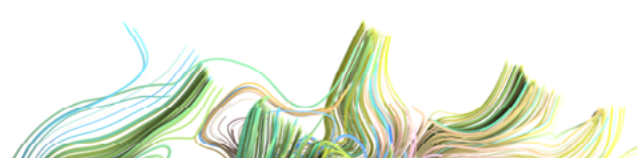
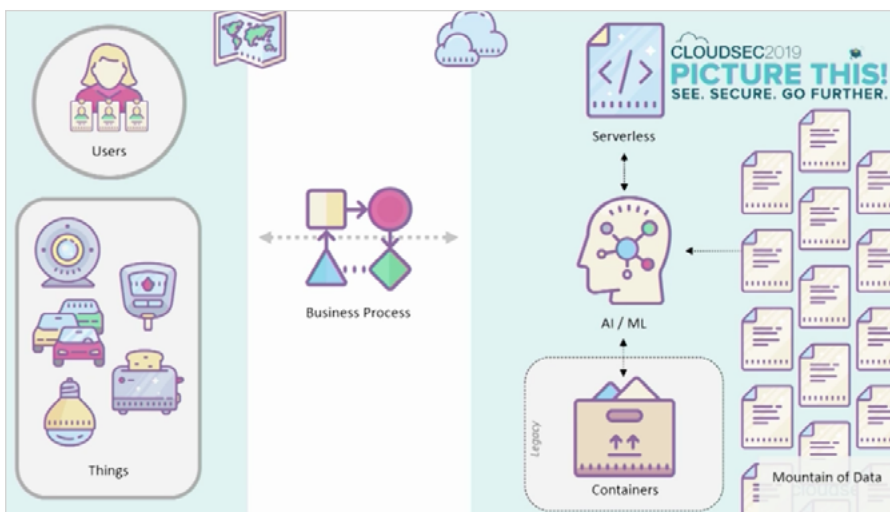
4G는 콘텐츠 소비 패러다임을 바꿔 놓았다. 넷플릭스, 스포티파이, 애플뮤직과 같은 스트리밍 서비스가 늘어났고, 모바일에서 실시간 온라인 게임을 사용할 수 있게 됐다. 소비자 중심의 변화인 셈이다. 이 발전은 백그라운드 운영에도 큰 변화를 가져왔다. 콘텐츠를 만들어 네트워크에서 어떻게 운영하는지가 중요해졌다.

5G는 산업혁명으로 부를 수 있을 정도로 중요한 변화다. 서비스 지연(Latency) 현상이 적어 이전 세대 통신망에 비해 반응이 빠르다. 따라서 혁신과 변화가 모든 산업에서 일어나고 있다.

예를 들어 미국에 있는 의사가 한국에 있는 환자를 로봇으로 실시간 수술할 수 있다. V2V(Vehicle to Vehicle), V2I(Vehicle to Infrastructure), V2E(Vehicle to Environment) 등을 통해 센서를 실시간으로 가져오고 다른 차량과 통신하는 자율주행차를 운영할 수 있

다. 교통과 물류, 산업 등에서도 혁신이 일어날 것이다. 공장끼리 더욱 많이 연결되고, 공장 내부 기기들끼리도 연결될 것이다.

5G 시장의 유일한 부작용은 기기 수가 너무 많이 늘어난다는 점이 될 것이다. 현재 5G나 IoT 기기들에게 할당되고 있는 IPv6 차세대 주소는 지구 모든 원자를 다 채우고도 서너 번 더 채울 수 있을 정도로 많지만, 절대 채우지 못할 것 같았던 하드디스크 20MB를 다 쓴 것처럼 언젠가는 동나게 될 것이다. 센서, 사물, 기기, 액추에이터, 제조업체, 차량, 컴포넌트가 모두 연결되고 이것이 5G의 혁신이 될 것이다.





5G 이후 시대의 보안 위협

이렇게 폭발적으로 늘어나는 기기는 보안담당자에게 위협이 된다. 사용자의 모든 기기는 하나당 위치나 시간, 현재 담당하는 업무 등에 따라 여러 개의 프로파일을 갖게 될 것이다. 이 모든 프로파일을 관리하는 것 역시 보안담당자에 큰 위협이 될 것이다. 기기를 모두 분류하고, 인증하고, 정상적인 행동이 아닌 것을 인지해야 하기 때문이다. 그 이유로 앞으로는 인력이 아닌 AI와 머신러닝이 보안의 해답이 될 것이다. 물론 보안 작업을 잘한다고 해서 비즈니스가 성공할 수 있는 것은 아니다. 쌓여가는 데이터를 통해 비즈니스 중심으로 접근해야 한다.

앞으로의 시대에서 레거시 인프라스트럭처들은 컨테이너에 담겨 사용하게 될 것이며, 컨테이너를 통해 모던 인프라로 다시 태어날 것이다. 그리고 서버리스(Serverless) 환경에 진입할 것이다.

이같은 5G를 결합하면 기술에서 위협이 발생한다. 우선 현재와 다르게 미래의 데이터 보안 시장은 하드웨어 정의 네트워크가 아닌 소프트웨어 정의 네트워크 아키텍처로 변화해야 할 것이다. 현재는 사람과 기계의 통신만 지원하면 되지만, 미래에는 엄청난 규모의 IoT 기기들이 기기 간 통신을 필요로 할 것이다. 이 매시브 통신의 시대가 다가오기 전에 기존 직원들이 새로운 기술들을 빠르게 학습해야 한다. 지난 10년간의 변화는 단 5년 만에 일어날 것이다.

AI는 당신의 상상보다 빠르게 발전했다

2001 스페이스 오디세이가 실제로 벌어지고 있다. 영화처럼 AI가 사람을 공격하는 시대가 실제로 올 수 있다. 이는 사실 인간의 편견이 반영된 것이므로 트레이닝하는 데이터셋에 따른 결과다.

자동화 무기를 떠올려보자. 사람이 조작하는 드론이 아니라, 앞으로의 자율 무기는 공중에 띄우면 사전에 탑재된 룰을 따라 스스로 타격을 설정하고 공격할 것이다. 있어서는 안될 일이지만 현재의 기술로 불가능하지 않다. 같은 방식으로 자율 사이버 무기가 등장해 기업의 서버를 공격할 수 있다. 이 악성코드는 네트워크 트래픽을 파악하고 상황을 인지해 사람을 사칭할 것이다.

실 사례로 이모텟(Emotet)이 등장했다. 머신러닝으로 구현한 무기다. 지난 2018년 10월 이메일 정보를 해킹해 보유하고 있다가, 2019년 4월 해킹한 사람의 이메일 쓰레드에 악성 파일을 첨부해 타인에게 보냈다. 사람의 이름으로 이메일이 왔으므로 악성코드에 감염된 사람은 스팸이라고 인지하고 못하고 있었다.

최근에는 인공지능망을 활용해 사람의 외모도 만들어낼 수 있다. 최근의 스타워즈에는 레아공주 캐릭터가 1977년 과거의 모습 그대로

로 등장한다. AI는 이미 실존하지 않는 사람의 얼굴을 만들어낼 수 있고, 음성파일을 확보하면 그 사람이 하지 않은 말의 음성을 만들어낼 수 있다. 모나리자의 사레처럼 사진 하나로 그 사람의 표정을 모사하는 동영상도 만들 수 있고, 16개만 있으면 완전히 동일한 이미지를 만들어낼 수도 있다. 디지털 영생을 판매하는 Eterni.me와 같은 사이트에서는, 사용자의 소셜 미디어를 분석해 사용자 사후 사용자가 살아있는 것처럼 포스팅을 하고 메시지를 보낼 수도 있다고 한다.


이러한 방식은 실제로 해킹에 악용된다. 한 기업 고위층을 AI가 사칭해 재무팀에게 ‘긴급한 상황이니 빠른 지급을 요청’해서 실제로 재무팀에게 돈을 받아낸 사례가 있었다. 몇 년 동안 기업들이 총액 150억 달러를 손해 볼 정도로 흔한 사례다. 앞으로는 임원급 인물의 얼굴과 표정, 목소리를 훔쳐 페이스타임이나 스카이프 등으로 돈을 요구할 수도 있을 것이다. 그러나 우리의 보안 센터들은 이러한 위협에 제대로 대처하지 못하고 있다.

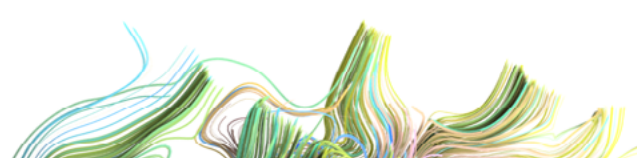
트렌드마이크로의 분석에 따르면, 보안담당자 60% 정도가 하루에 10만건 이상의 경고메시지를 처리한다고 한다. 10만명은 인기 미식축구팀의 만원 관객 수준의 수다. 경고메시지 하나에 소요되는 평균 시간이 25분이므로, 250만분의 시간이 필요하고, 이를 진단과 분류하는 데만 217명의 보안 요원이 24시간 3교대로 일해야 한다. 향후 이런 위협이 등장하면 보안담당자들은 어떻게 해야 할까?

앞으로의 보안위협 도전과제 세가지

비즈니스 중심 머신러닝(Business Oriented Machine Learning). 보통 머신러닝은 벤더에게 받아온다고 생각하기 쉽지만, 보안 담당자가 머신러닝을 통해 기업 보안을 어떻게 강화할지를 생각하고 적용 여부를 고민해야 한다. 비즈니스 애널리틱스나 보안센터에 어떻게 적용할지 모르기 때문이다. 데이터는 자꾸 늘어나므로 적응하고 채용하고 투자하자.

보안 오케스트레이션(Security Orchestration). 취약점 보고, 패치 매니지먼트 등 다양한 방법을 통합하고 일관성을 갖게 하는 조치가 해야 한다. 이를 통해 전반적인 영역에서 효과를 보도록 해야 한다. 통합하는 방법으로는 오케스트레이션이 필요하다.

자율 대응(Autonomous Response). 보안을 준비하고 오케스트레이션했다면 인간이 직접 대응하지 말고 자율대응을 하도록 한다. 머신러닝과 인간이 함께 보안을 준비하는 것이다. 언젠가는 머신러닝의 민감성이 인간을 넘는 시기가 올 것이며, 그렇다면 훨씬 더 높은 수준의 보안을 갖출 수 있을 것이다. 



IT인프라 진화에 대처하는 보안 방식

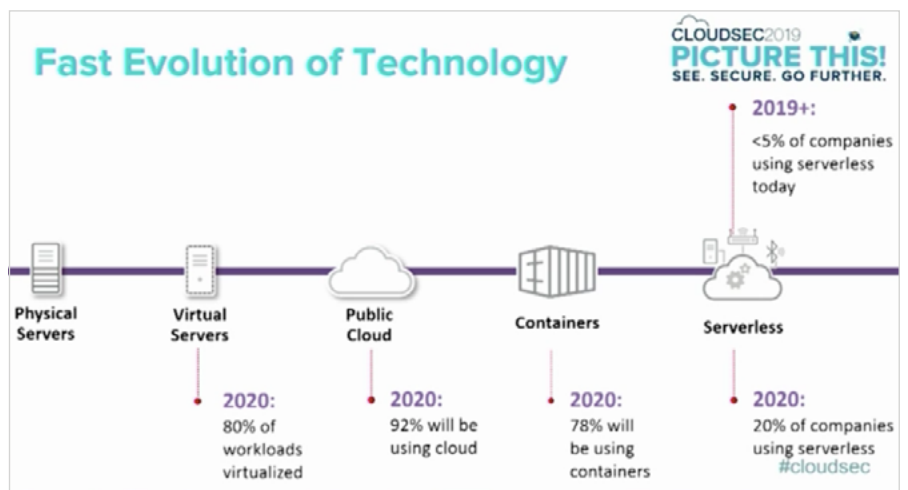
지난 7월 미국 대형 은행인 캐피털원 (Capital One)에서 1억600만명에 이르는 개인정보가 유출된 사실이 뒤늦게 알려졌다. 캐피털원 고객의 이름, 주소, 전화번호 등 신상정보와 신용점수, 신용한도 등 각종 금융 관련 데이터가 해커에 의해 유출됐다.

캐피털원의 데이터는 아마존웹서비스 (AWS) 클라우드에 저장돼 있었다. 캐피털원의 데이터를 빼낸 해커는 웹 서버의 방화벽 취약점을 뚫고 데이터에 접근했던 것으로 전해졌다. 해커의 기술이 뛰어났던 것이 아니라 방화벽 설정이 잘못됐다는 분석이 나왔다.

클라우드상 보안은 온프레미스의 보안과 달라야 하는데, 기존의 보안 환경을 그대로 유지했던 것이 문제였던 것으로 알려졌다. 캐피털원의 사례는 클라우드와 같은 새로운 환경에는 기존의 온프레미스 환경과는 차별화된 보안 시스템이 필요하다는 교훈을 전해준다.

최근 기업의 IT 인프라 환경이 급변하고 있다. 물리적 서버나 가상 서버(VM) 수준을 넘어 퍼블릭 클라우드, 컨테이너, 서버리스 등 새로운 애플리케이션 인프라가 등장했다.

한 조사에 따르면, 2020년이 되면 워크로드의 80%는 가상화된 환경에서 구동되고, 이 가운데 90% 이상은 클라우드에서 운영된다. 또 78%는 컨테이너를 활용할 것이



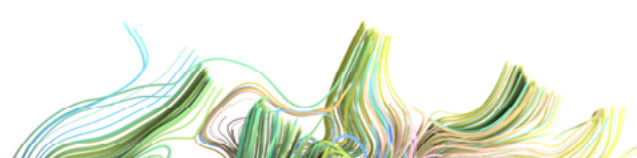
고, 현재 5% 미만에 불과한 서버리스로 구동되는 워크로드도 20%에 달할 전망이다.

IT 인프라가 다변화 된다는 것은 위협도 다변화 된다는 것을 의미한다. 애플리케이션 개발과 배포, 운영은 점차 편해지고 빨라지겠지만 IT 운영 입장에서 보면 보안 등의 리스크가 커진다.

워크로드 보안을 살펴보자. 전통적으로 워크로드 보안 방법은 대부분 서버, 호스트 중심 보안이다. 기존의 IT인프라가 호스트 단위로 구성됐기 때문이다. 그러나 이제는 달라졌다. 호스트 중심의 보안 시스템은 다변화한 현재의 IT 인프라를 다 지켜낼 수 없다. 기업들은 디지털 트랜스포메이션을 위해 IT 환경을 혁신하고 있기 때문에 이에 맞는 보안 시스템이 구성돼야 한다.

예를 들어 대다수의 기업은 CI/CD (Continuous Integration and Continuous Deployment)를 추구한다. 도커 컨테이너를 기반으로 한 마이크로서비스 아키텍처를 대부분 지향한다. 데브옵스(DevOps)라는 빠른 형태의 배포 방법이 일반화 되고 있다.

이런 환경에서 기존 호스트 기반 보안은 모든 워크로드를 보호할 수 없다. 전체 워크로드 보안을 위해서는 도커 컨테이너 개발부터 배포, 구동까지 일관된 보안을 제공해야 한다. 최근 모든 개발환경이 데브옵스와 CI/CD를 따르고 있기 때문에 개발과 배포 단계에서 취약점과 악성코드 감염, 컴플라이언스 위반까지 살펴봐야 한다. 지금까지처럼 실행되는 환경에 뿐만 아니라 개발과 배포 단계에도 보안을 적용해야 한다. 또 도커와





컨테이너 환경에서 호스트뿐 아니라 컨테이너 풀 스택도 보안이 필요하다.

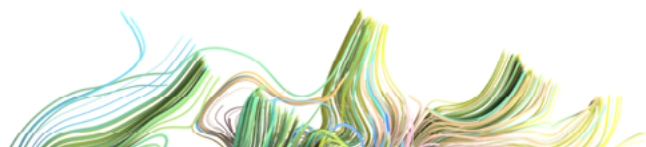
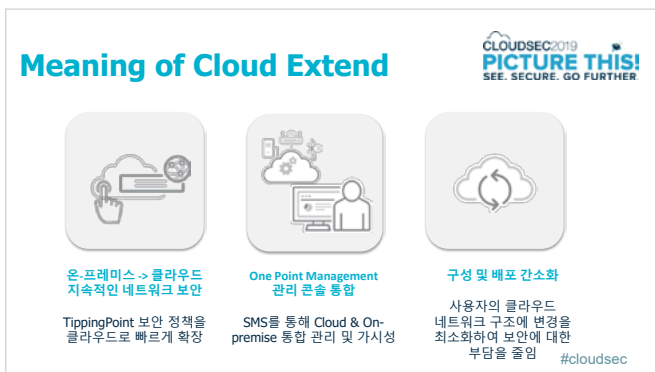
네트워크 보안도 달라져야 한다. 클라우드, 컨테이너 등 새로운 워크로드 환경은 네트워크 구성에도 어려움을 가져다주기 때문이다. 많은 기업들이 가상사설클라우드(VPC)를 활용하는데 있어 어려움을 겪는다. 이 때문에 VPC마다 네트워크 어플라이언스를 구성하는 방식은 그 자체로 복잡하다. 성능 이슈로 로드밸런서 구성도 해야 했다. 최근 트랜짓게이트웨이(TGW)를 활용하는 방법이 떠오르고 있다. TGW를 통해서 다양한 VPC를 컨트롤 할 수 있어 네트워크 보안도 보다 손쉽게 할 수 있게 됐다.

서버리스 컴퓨팅도 보안에 있어 새로운 도전과제다. 아마존 람다(Lambda)와 같은 서버리스 환경은 전통적인 보안으로는 접근할 수 없다. 코드 기반으로 서비스를 제공하는 서버리스 환경에서 보안은 데이터 플로우의 안전성이 매우 중요하다. 서비스가 다양화되면 데이터 플로우가 증가하기 때문에 모니터링과 보호가 어렵다.

서버리스에서 중요한 것은 코드의 퀄리티다. 애플리케이션이 스스로 데이터를 검수하고, 사용자의 행위를 검사해야 한다. 이를 런타임 애플리케이션 셀프 프로텍션(Runtime application self-protection)이라고 부른다. 라이브러리 형태의 보안코드 삽입하고 전체 애플리케이션의 행위를 모니터링하는 것이 서버리스 보안 방법이다.

IT인프라는 변화하고 있다. 계속 진화하는 환경에서 보안에는 어떻게 대처해야 할까.

김진광 트렌드마이크로 지사장은 “비즈니스 혁신을 이끄는 디지털 트랜스포메이션을 위해서는 보안이 기본이 되어야 한다”면서 “클라우드나 컨테이너와 같은 새로운 IT환경의 보안을 위해서는 온프레미스 보안과 다른 클라우드 전문 솔루션과 기술이 필요하다”고 말했다. **By**





클라우드 네이티브 워크로드 보안 방법

클라우드 환경은 계속해서 변한다. 물리서버에서 시작해 가상서버, 가상화 데스크톱, 퍼블릭 클라우드와 컨테이너, 서버리스까지 쉬지 않고 새로운 형태의 플랫폼이 등장하고 있다. 이는 기업의 핵심 서비스나 애플리케이션 역시 변화하는 클라우드 환경 위에서 제공해야 한다는 뜻이다.

지금까지 기업의 캐시카우 역할을 해왔던 애플리케이션은 물론, 앞으로 먹거리를 책임질 새로운 서비스들은 모두 하이브리드 클라우드 환경을 기반으로 발전해가고 있다. 기술이 이렇게 빠르게 변할 때 기업이 가장 신경 써야하는 부분 중 하나는 ‘보안’이다.

지난해 ‘엔터프라이즈 스트레티지 그룹(Enterprise Strategy Group, 이하 ESG)’이 백서를 통해 발표한 내용을 살펴보면, 클라우드 플랫폼 지형의 변화를 예상할 수 있다. 예컨대 전체의 35%를 차지하는 베어메탈 서버에서 서비스되는 애플리케이션의 수는 2년 후 그 비중이 26% 정도로 줄어든 것으로 보인다. 가상서버의 경우에는 46%에서 41%로 비슷한 수준이지만, 컨테이너 환경에서 돌아가는 애플리케이션의 수는 19%에서 33%로 크게 늘어날 전망이다.

이는 클라우드 지형이 ‘하이브리드’로 바뀌고 있다는 걸 보여준다. 바뀌는 클라우드 환경에서 애플리케이션과 서비스를 빠르게 적용하기

위해 많은 기업이 데브옵스(DevOps)를 택한다. 데브옵스의 툴도 개발 단계에 쓰이는 깃허브나 젠킨스, 쿠버네티스같은 것들부터 IT 서비스 관리에 이용하는 슬랙이나 지라 소프트웨어 등 다양하다. 기술 개발의 기반이 되는 클라우드 서비스 제공업체도 여럿이다.

그렇다면 이와 같은 환경에서는 과연 어떠한 보안 영역이 중요하게 될까. ESG 보고서는 ▲소프트웨어 취약점에 대한 스캐닝과 조치 방안 ▲래터럴 무브먼트(Lateral Movement)에 대해 발생하는 공격 탐지와 방어 ▲소프트웨어 취약점에 대한 탐지 ▲컨테이너 간 통신 액세스 제어 ▲컨테이너에 대한 모니터링 ▲컨테이너의 비정상적 동작에 대한 탐지 등 6가지 영역을 보안의 주요 화두로 꼽았다.

이렇게 다양한 플랫폼과 데브옵스 툴을 함께 연결하려면 반드시 ‘클라우드 네이티브 워크로드 보안’이 필요하다.

지금까지는 하이브리드 클라우드 환경임에도 불구하고, 여전히 서버 백신으로만 보안 환경을 유지하고 있는 곳이 많다. 필연적으로 문제가 일어날 수 있는 상황인데, 이 경우 개발과 빌드, 검증, 배포 등 각 단계에서 보안을 분리 적용해 문제에 대한 부서 간 공유가 어려워진다. 보안을 하나의 애플리케이션 관점에서 살펴야 하는데 서버에만 집중하게 되는 상황이 발생할 수도 있다. CI/CD 프로세스에

클라우드 보안 요구사항의 변화

Automation With Pipeline & Workload Security

PIPELINE MANAGEMENT & DEPLOYMENT: GitHub, Jenkins, ANSIBLE, CHEF, PUPPET, SALTSTACK, KUBERNETES, AWS OpsWorks

IT SERVICE MANAGEMENT: slack, Jira Software, now, Amazon SNS

Environments: aws, Azure, Google Cloud, docker, OPENSHIFT, vmware

Monitoring Tools: New Relic, AWS CloudTrail, AWS Config

#cloudsec

새로운 접근의 워크로드 보안

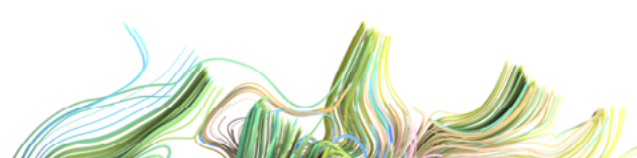
SINGLE STRATEGY FOR MULTIPLE PLATFORMS

자동화 DevOps에 사용되는 SDKs와 APIs를 자동화하고 간소화

위협 방어 연계 네트워크, 플랫폼개발 프로세스 과정 그리고 애플리케이션을 넘어 위협 정보를 공유하고 대응하는 체계

보안 범위 확대

#cloudsec





새로운 접근의 CI/CD 보안 - Build Pipeline



SHIFT-LEFT APPROACH



DEVELOPMENT PIPELINE

취약점 스캔	Pre-registry 검사	빌드 이미지 검증	
안티멀웨어 스캔	Container Registry 검사	컴플라이언스 검증	#cloudsec

서 서로 분산된 서비스 개발이 여전히 이뤄지면서, 그런 어떤 문제적인 이슈에 대한 공유가 부족한 부분도 있다.

이 때문에 다양한 멀티 플랫폼에 맞는 단일한 보안 전략을 세우는 것의 중요성이 대두되고 있다. 키워드는 자동화와 위협 방어 연계, 그리고 보안 범위 확대다. 데브옵스에 사용되는 소프트웨어개발킷(SDK)들과 애플리케이션프로그래밍인터페이스(API)를 자동화하고 간소화하는 것이 중요하다. 또 네트워크, 플랫폼, 애플리케이션의 각 레이어를 넘어 취약 정보를 공유하고 대응할 수 있는 위협 방어 연계 체계가 반드시 필요하다는 것이다. 운영 단계에 그치지 않고 개발 프로세스 과정까지 보안 범위를 확대할 수 있어야 한다.

이러한 새로운 접근의 CI/CD 보안을 ‘시프트-레프트(SHIFT-LEFT)’ 어프로치라고 부른다. 이는 커밋(commit)부터 빌드(build), 푸시(push), 배포(deploy), 그리고 운영(run)까지 전 과정에 걸쳐서 보안이 적용되어야 한다는 걸 뜻한다. 이런 빌드 파이프라인 과정에서 취약점 스캔, 안티멀웨어 스캔, 그리고 프리 레지스트리 검사, 컨테이너 레지스트리 검사, 빌드 이미지 검사, 컴플라이언스 검사 등이 모두 필요하다.

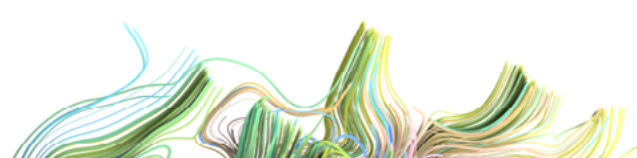
예컨대 커밋된 소스를 가지고 빌드할 때, 빌드된 이미지를 컨테이

너로 배포하기 위해 푸시가 진행된다. 이때 푸시된 이미지에 대해 스캐닝 보안을 적용, 취약점이나 멀웨어 여부 등을 검사하게 되는 것이다. 검사 결과는 자동으로 개발 그룹이 공유하는 젠킨스나 슬랙 같은 툴에 공유되며, 해당 내용 알람을 받은 개발 그룹은 결과 내용을 상세하게 조회해 문제 해결을 위한 협력을 할 수 있게 된다.

이 경우 개발자들은 이 과정에서 빌드된 이미지의 배포 시급성에 따라 운영 단계에서 취약점에 대한 보안을 적용하거나, 혹은 새로 빌드한 다음 배포를 하는 과정 등을 선택할 수 있다.

운영단계에서도 물론 보안이 적용되어야 한다. 컨테이너도 호스트 위에서 돌아가는 하나의 애플리케이션인 만큼 보안이 필요한데, 운영체제(OS) 레벨에서 보안을 적용하거나, 혹은 애플리케이션 컨테이너처럼 보안 소프트웨어 자체를 컨테이너로 배포하는 방법 등을 고려할 수 있다.

김석주 트렌드마이크로 부장은 “전체적인 클라우드 워크로드가 변화하고 있고 이 환경에 맞는 클라우드 네이티브한 보안이 꼭 필요하다”면서 “다양한 툴들과 같이 연계해서 유기적으로 동작 해야만 반드시 제대로 된 클라우드 워크로드 보안을 적용할 수가 있다”고 강조했다.



단순하고 효율적인 클라우드 네트워크 보안

트렌드마이크로는 티핑포인트를 인수하면서 네트워크 보안 지원을 클라우드 환경으로 확장했다.

티핑포인트 침입방지시스템(IPS)을 사용하는 기업 고객들은 트렌드마이크로가 최근 선보인 ‘클라우드 네트워크 프로텍션(Cloud Network Protection Powered by Tipping Point)’을 활용해 온프레미스 환경과 퍼블릭 클라우드 환경의 워크로드까지 일관된 보안을 간편하게 적용할 수 있게 됐다.

클라우드를 사용하는 기업들은 보안 우려가 여전히 크다. 클라우드 보안을 적용하려고 해도 걱정이 많다. 보안을 적용하더라도 우선 제공하는 클라우드 애플리케이션 서비스에 영향을 미치지 않는 것이 중요하기 때문이다. 그 이유로 서비스 이용자가 적은 새벽 시간에 서비스를 중단한 후 보안을 적용해야 한다는 부담을 갖고 있다.

클라우드 네트워크 보안 적용 걸림돌

기존 보안 솔루션을 클라우드에 올려서 사용할 경우엔 비용도 많이 들고 성능 요구를 충족하지 못하는 문제도 발생한다. 복잡하고 비효율적인 구성으로 적용되고 있는 상황이다.

대개 기존에 널리 사용돼온 차세대방화벽(NGFW)을 클라우드 환경에서 사용할 경우, ‘NGFW 샌드위치’ 구성이 이뤄진다. VPC마다 두 개의 NGFW를 배치한다. 로드밸런서도 VPC 앞뒤로 구축해야 한다. 인터넷 게이트웨이 피어링으로 인해 복잡해진다. 유연성도 떨어진 다. 성능과 확장성에 제한이 있어 더 많은 인스턴스가 필요하다.

빠르고 간편하게 서비스를 이용·확장하고, 사용한만큼 비용을 지불해 효율성을 높일 수 있다는 클라우드 이점이 반감된다.

그 점에서 보안도 클라우드 환경에 적합한 구성, 가용성과 비용효율성 등을 지원하는 솔루션을 사용하는 것이 중요하다.

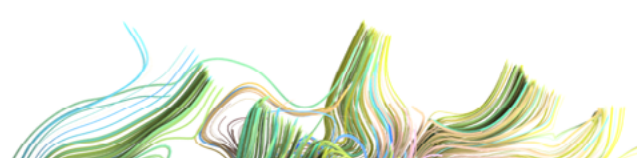
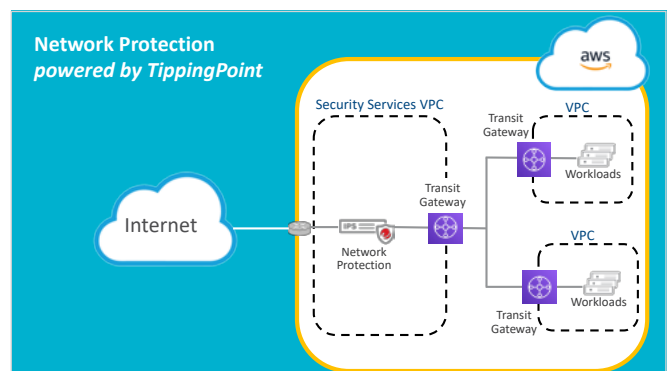
클라우드 친화적 보안 제공

트렌드마이크로가 선보인 새로운 티핑포인트 클라우드 네트워크 프로텍션은 퍼블릭 클라우드 환경과 하이브리드 클라우드 환경에 친화적인 보안을 적용할 수 있다.

초기 설치, 구성시 사용자의 클라우드 네트워크 구조 변경 등 영향을 최소화해 부담을 줄인다. 그리고 클라우드 환경 변화에 따라 민첩하게 보안정책을 확장 적용할 수 있다.

티핑포인트 클라우드 네트워크 프로텍션은 구성할 때 서비스를 중단할 필요없이 인라인 또는 탐지 모드로 즉각 적용할 수 있다.

또한 클라우드 네트워크 보안을 적용하기 위해 VPC마다 IPS를 넣을 필요 없이 앞단에만 한 대만 간단하게 설치하면 된다. 물론 사용



자가 원할 경우 액티브-스탠바이(Active-Stanby) 구성도 가능하다.

아마존웹서비스(AWS) 환경에서 티핑포인트 클라우드 네트워크 프로텍션은 트랜짓게이트웨이(TGW) 기능을 사용한다. TGW는 AWS 가 새롭게 선보인 서비스로, VPC를 상호 연결하는데 사용되는 일종의 네트워크 전송 허브다. 기존에 1대1만 지원하는 VPC 피어링 통신 제약을 해소한다. 자체 라우팅 테이블이 있어 라우터와 비슷한 역할을 수행한다.

AWS TGW 사용으로 복잡성 제거

그동안 클라우드 네트워크를 구성하려면 어려움이 있었다. VPC 피어링(Peering)을 통한 다수의 VPC 연결에 제약이 있었다.

만일 A, B, C 세 개의 VPC가 있고 각 VPC간 피어링을 할 경우, A와 B 간, A와 C 간 피어링으로 통신할 수는 있어도 B와 C 간 통신은 불가능하다. VPC는 한 번에 하나씩, 중복되는 CIDR 블록이 없어야 한다. 그리고 전이적 피어링 관계가 설정되지 않아 다수의 VPC간 통신 제한이 있었다.

각 서비스에 존재하는 VPC 연결을 TWG가 수행하는 구조에서는 드나드는 모든 트래픽을 인터넷 게이트웨이 구간에서 클라우드 IPS

살펴볼 수 있다. 따라서 VPC마다 IPS를 설치하지 않아도 한대의 IPS로 간단하게 구성할 수 있게 된다. 로드밸런서를 추가하지 않아도 되고, 인스턴스도 클라우드 IPS용 하나만 필요하다.

하이브리드 클라우드 환경 통합관리, 가시성 확보

하이브리드 클라우드 환경에서도 구성은 비슷하다. 트래픽 정책에 따라 라우팅 테이블이 길어질 수 있다는 차이만 있다.

티핑포인트 클라우드 네트워크 프로텍션은 온프레미스 IPS와 똑같은 관리콘솔을 사용할 수 있도록 제공한다. 관리콘솔이 통합되어 데이터센터(온프레미스) 환경에서 이미 티핑포인트 IPS를 사용하고 있다면 기존 보안정책을 클라우드로도 빠르게 확장할 수 있다. 온프레미스와 클라우드 환경에서 일관된 보안관리와 가시성을 확보할 수 있다.

트렌드마이크로는 DV랩스(DVLabs)와 제로데이 이니셔티브(ZDI)를 통해 최신 보안 취약점과 제로데이 위협을 능동적으로 방어할 수 있는 기능을 제공한다. 티핑포인트 IPS는 평판 기반 위협 방어, 악성코드 위협 방어, 가상패치, 위치·사용자 ID 기반 제어 기능 등을 제공한다. **By**

Delivering industry leading security

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- ✓ Network based virtual patching
- ✓ Zero day protection
- ✓ Integration into Trend Micro



Threats



Vulnerabilities & Exploits



Targeted Attacks



AI & Machine Learning



IoT



OT / IIoT



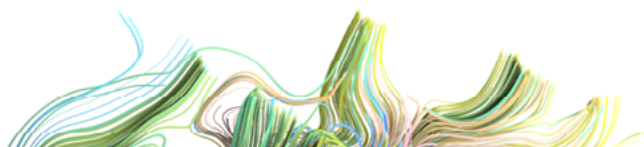
Cybercriminal Undergrounds



Future Threat Landscape



#cloudsec



통합 서버보안의 진화, OS부터 컨테이너 플랫폼까지 총체적 위협 보호



리눅스, 윈도우, 자바 등 다양한 플랫폼에서 발견되는 취약점은 꾸준히 증가하고 있다. 트렌드미크로의 ZDI(Zero Day Initiative) 분석에 따르면, 지난 2009년 한 해 동안 발견된 제로데이 취약점 수는 101건이었다. 10년 뒤인 2019년에는 1500개에 달하는 제로데이 취약점이 발견돼 15배나 증가했다.

해커들은 이같은 취약점을 이용해 공격을 시도하고 있다. 취약점이 발견되는 동시에 익스플로잇 공격이 발생하고 있다. 공격 효과를 높이기 위해 취약점 패치가 제공되기 전에 재빨리 공격을 수행하는 것이다.

이같은 제로데이 취약점은 이전까지는 주로 운영체제(OS) 관련 취약점이 많았다. 최근에는 OS 외에도 도커(Docker) 컨테이너, 컨테이너 오케스트레이션 툴인 쿠버네티스, 데브옵스 툴인 젠킨스 등 취약점이 발견되는 플랫폼들이 다양해지고 있다.

리눅스를 가장 많이 사용하는 기업의 데이터센터 서버를 취약점을 이용한 다양한 공격으로부터 안전하게 보호하기 위해서는 컨테이너, 쿠버네티스와 같은 새로운 플랫폼까지 보호할 수 있어야 한다.

이에 따라 서버보안은 백신을 설치하고 보안패치를 설치하는 것에서 나아가 애플리케이션 빌드부터 실행하는 전 단계에서 요구되는

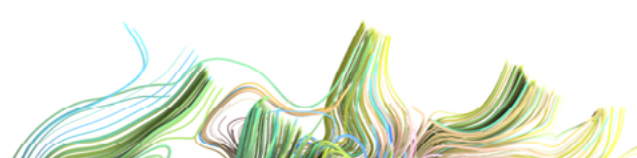
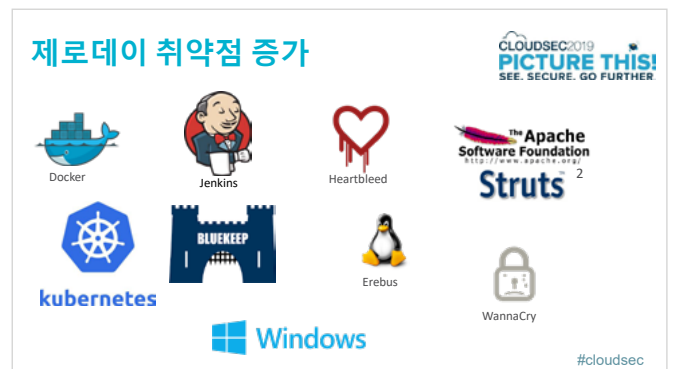
다양한 위협에 대응하고 보호하는 것이 점점 중요해지고 있다.

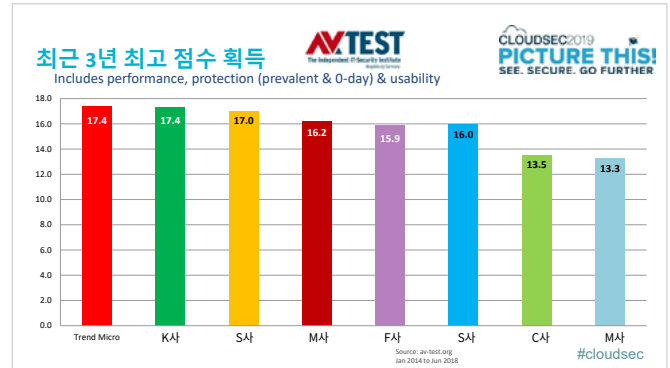
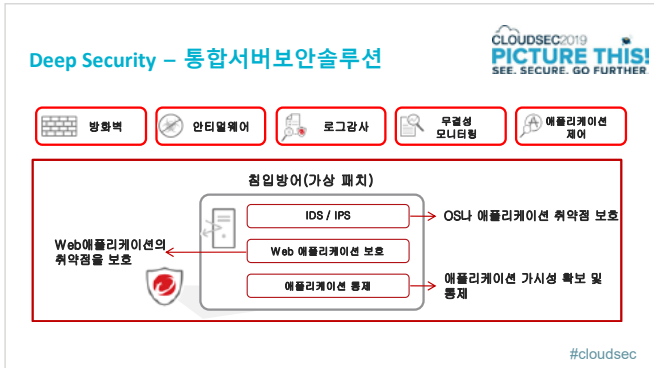
이미지를 배포하기 전에 취약점과 악성코드를 갖고 있는지 점검하는 것부터 네트워크 보안, 시스템 보안, 악성코드 대응까지 모두 가능해야 한다.

트렌드미크로의 ‘딤시큐리티’는 악성코드를 방어 기능부터 방화벽, 취약점 검사, 침입방어, 애플리케이션 제어, 무결성 모니터링, 로그감사 등의 기능을 모두 제공하는 통합 서버보안 솔루션이다.

악성코드 방어 기능은 알려진 멀웨어를 탐지, 차단하는 안티멀웨어 기능뿐 아니라 행위분석과 머신러닝, 샌드박스 분석 기술로 의심스러운 파일과 행위를 탐지한다. 여기에 더해 악성 URL로부터 서버를 보호하기 위해 웹사이트 평판 탐지, 차단 기능도 제공한다. 이를 바탕으로 표적공격을 수행하는 악성코드, 랜섬웨어, 제로데이 공격과 명령제어(C&C) 및 악성 URL로부터 서버를 보호한다.

애플리케이션 제어 기능은 서버 내에 있는 모든 실행파일을 인지해 모니터링한다. 화이트리스트 기능으로 허가된 애플리케이션만 사용하도록 하고, 허가되지 않은 애플리케이션이 실행될 경우 서버를 잠가버려(Lockdown) 실행을 차단한다. 이 경우는 변경이 적은 서버에서 사용할 때 유용하다.





무결성 검증 기능은 서버 내에 파일이나 폴더, 디렉토리, 레지스트리 프로세스, 통신 포트 등을 체크해 무단 액세스 통해 수정이나 변경 작업이 발생할 경우 경고를 통해 조기 발견할 수 있게 한다.

‘딥시큐리티’는 가상패치 기능도 제공한다. 크게 늘어나는 취약점으로 인한 제로데이 위협을 방어할 수 있는 기능이다. 취약점이 발견됐으나 정규 패치가 나오지 않았거나 사용자가 미처 패치를 하지 못했을 경우, 가상패치 기능이 해당 취약점을 이용한 공격을 방어해 패치(보안업데이트)를 적용한 것과 동일한 효과를 내는 기능이다.

자동으로 취약점을 스캔해 감사를 수행하고 방어 룰을 적용한다. 이를 통해 서버 네트워크와 OS, 애플리케이션 취약점을 방어해 관련 위협으로부터 보호한다.

윈도우XP처럼 출시된 지 오래됐지만 보안 패치와 업데이트를 제공할 수 없는 OS를 운영하고 있는 시스템을 효과적으로 보호할 수 있다.

가상패치는 취약점 발견 즉시 적용할 수 있다는 장점을 제공한다. 위험성이 큰 취약점이 새롭게 발견돼 긴급 패치가 나왔지만 테스트를 거쳐 데이터센터에서 운영되는 전체 서버에 적용할 때까지 생기는 보안 공백으로 인한 위험을 없앨 수 있다.

‘딥시큐리티’는 다양한 OS 플랫폼과 가상환경을 지원한다. 윈도우 유닉스와 우분투, 레드햇, 수세 등 리눅스와 리눅스 커널은 물론이고 VM웨어, KVM, 오픈스택, 도커 컨테이너까지 다양하게 지원하고 있다.

도커 컨테이너 보안 기능은 큰 차별점이다. 도커에서 실행되는 컨테이너 애플리케이션은 호스트 커널에 공유된다. 도커 호스트가 손상되면 모든 컨테이너 위협이 될 수 있는데, 트렌드미크로의 ‘딥시큐리티 에이전트(DSA)’로 컨테이너와 도커 컨테이너가 설치·구동되는 도커 호스트 영역 전체를 보호한다.

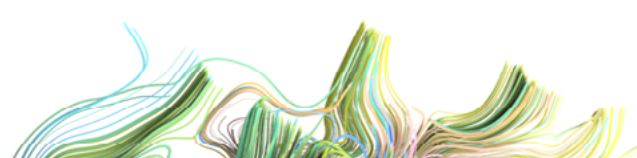
DSA는 도커 컨테이너와 쿠버네티스를 자동 감지해 소프트웨어 업그레이드와 다운그레이드 또는 삭제, 실행파일 속성 변경, 실행 중인 프로세스와 데몬, 주요 설정 파일 등을 모니터링하고 안전하게 보호한다.

‘딥시큐리티’가 제공하는 기능 가운데 안티멀웨어 기능과 침입방지 시스템(IPS), 무결성 보호 기능을 제공해 악성코드와 취약점 공격으로부터 컨테이너와 내부 애플리케이션을 보호한다.

트렌드미크로 ‘딥시큐리티’는 시장조사기관인 IDC의 분석 결과 전세계 시장 점유율 30%로 매년 글로벌 서버보안 시장 리더로 꼽히고 있다.

AV테스트(AVTEST)가 수행한 안티바이러스(AV) 성능, 보호, 사용성 등의 테스트(2014~2018년)에서는 트렌드미크로가 시만텍, 맥아피, 소포스, 사일런스, 마이크로소프트 등 경쟁사를 제치고 가장 우수한 점수를 받았다.

가트너가 2018년 발표한 클라우드 워크로드 보호 플랫폼(CWPP) 시장 가이드에서 정의한 26가지 중요 항목 가운데 트렌드미크로는 23가지로 가장 많은 항목을 충족하고 있는 것으로 인정받았다.



클라우드 시대 워크로드 보안, 네트워크 보안, 컨테이너 보안 방안

Byline Network SPECIAL REPORT

발행 바이라인네트워크
취재 / 글 이유지 기자 yjlee@byline.network
심재석 기자 shimsky@byline.network
이종철 기자 jude@byline.network
남혜현 기자 smilla@byline.network
문의 02 761 1928, byline@byline.network
주소 서울시 영등포구 국제금융로6길 33 맨하탄빌딩 1010호

Copyright © 2019 BylineNetwork