All about Cloud Security

클라우드 보안의 모든 것

paloalto NETWORKS®

Palo Alto Networks

팔로알토 네트웍스 소개

팔로알토 네트웍스는 세계적인 사이버 보안 리더로, 디지털 시대의 신뢰를 유지하는데 전념하고 있으며, 전 세계 5만개 이상 조직에서 모든 애플리케이션을 안전하게 보호하고 사이버 침입을 방어하고 있습니다.
팔로알토 네트웍스의 사이버 보안 분야에서의 전문성, 혁신을 위한 노력, 획기적인 보안 플랫폼은 공격 라이프 사이클의 모든 단계에서 고도로 자동화된 사이버 위협 예방 수단을 제공하고, 기존의 레거시 보안 기술보다 탁월한 보호를 가능하게 함으로써 사이버 침해 시대를 종식시키는데 일조하고 있습니다.

회사 간략 정보

- 150여 개국에서 다양한 업계에 걸쳐 5만개 이상 고객 확보
- 포춘 100대 기업 중 85개 이상, 글로벌 2000대 기업 63% 이상의 고객들이 팔로알토 네트웍스 솔루션을 활용해 사이버 보안 구현
- 2017회계년도 매출 18억 달러, 전년 동기대비 28% 성장–동종업계 최고 수준의 성장률
- 가트너 선정 2011년, 2012년, 2013년, 2014년, 2015년, 2016년(2017년 7월 간행) 기업 방화벽 시장 선도 기업
- 액센추어, 아마존 웹 서비스(AWS), 구글, 마이크로소프트, 프루프포인트, PwC, 스플렁크, 태니엄, VM웨어 등 업계 최고 기업과 협력 관계 구축
- 글로벌 서포트 조직 보유(북미·남미, EMEA, 아시아, 일본)
- 탁월한 서비스 품질 인증
  - *J.D. 파워, TSIA 선정 고객 지원 부문 'Outstanding Customer Support Experience'(2015, 2016, 2017)*
  - *TSIA 선정 고객 지원 헌신 부문 'Outstanding World– wide' 등급(2015, 2016, 2017)*
  - *포춘 매거진에 의해 세상을 변화시키는 Top50 회사(2017년 9월) 및 퓨처 50 리스트 선정 (2017년 10월)*
  - *전 세계적으로 5100여명의 직원을 두고 있으며, 〈SF 비즈니스 타임즈〉에 의해 베이 지역에서 '가장 일하기 좋은 직장'1위로 선정 (2016)*
  - *2012 7월 상장; 뉴욕 증권 거래소 Stock symbol: PANW*

CONTENTS

All about Cloud Security 클라우드 보안의 모든 것

paloaltonetworks.com I paloaltonetworks.co.kr I Tel : 02-6001-2900 I E-mail : Sales-KR@paloaltonetworks.com

가속화되는 클라우드로의 전환

비즈니스 가치 혁신시키는 클라우드

클라우드는 비즈니스 가치를 혁신할 수 있도록 도와준다. 클라우드를 도입하면 언제, 어디서나 데이터와 애플리케이션에 쉽게 액세스할 수 있으며, 프로젝트 확장도 쉽고, IT 소비 현황을 쉽게 추적할 수 있다. 가상화의 이점을 살려 사일로 형태로 분산된 비즈니스 프로세스를 매끄럽게 연결하고 필요에 따라 손쉽게 복제할 수 있다.

이러한 장점이 인정받으면서 클라우드 성장 속도가 가파르게 상승하고 있다. 시장조사기관 시너지 리서치 그룹이 발표한 2018년 1분기(1~3월) 전 세계 클라우드 인프라 서비스 매출은 150억 달러에 달하며, 이는 전년 동기 대비 51% 늘어난 수치다. IDC는 세계 퍼블릭 클라우드 서비스 시장이 2020년까지 연평균 20.4% 성장하며, 2020년 1950억 달러에 이를 것으로 예상했다.

CAPEX 절감시키는 클라우드

클라우드는 IT 운영 효율성을 향상시키고 CAPEX를 절감할 수 있다. 적은 수의 하드웨어 인프라를 이용해 많은 애플리케이션을 구동시킬 수 있으므로 하드웨어 구입과 관리 비용, 전력비용, 데이터센터 상면 비용 등을 절감할 수 있다. 또한 IT 소비현황을 정확하게 파악할 수 있어 예산 운용을 보다 용이하게 할 수 있다.

클라우드는 다이내믹 가상머신(VM) 프로비저닝 기능을 제공해 케이블 연결로 이뤄진 전통적인 방식보다 신속하게 애플리케이션을 제공할 수 있다. 또한 사용자는 언제, 어디서든 데이터와 애플리케이션에 액세스할 수 있으며, 프로젝트 확장이 쉬워 비즈니스 민첩성을 높일 수 있다.

또한 클라우드는 서비스 개발 속도를 빠르게 해 타임 투 마켓에 맞는 비즈니스 전략을 구현할 수 있다. 전통적인 방식으로 서비스를 개발하려고 한다면, 서비스를 기획하고, 설계한 후 자체 인력 혹은 외주개발사와 계약을 통해 실제 개발한다. 개발 완료 후 테스트와 수정, QA단계를 여러 차례 거치면서 문제가 없을 때 서비스를 시범적으로 오픈하고, 완벽하다고 생각될 때 정식 오픈한다.

이 과정이 몇 주 혹은 몇 달씩 걸리기 때문에 기업은 몇 개월 후의 상황을 예측하고 대비해야 한다. 시시각각 변하는 현재 비즈니스에서는 이와 같은 서비스 개발 프로세스는 맞지 않다.

클라우드를 이용한다면, 미리 개발된 애플리케이션 모듈을 플랫폼 위에 조립해 서비스를 완성하면 된다. 애플리케이션 모듈은 마켓 플레이스에서 구입하면 되기 때문에 개발과 테스트, QA 시간을 획기적으로 단축시킬 수 있다.

서비스 전체를 새로 개발하는 것이 아니며, 상당 부분의 소프트웨어 모듈은 다른 서비스에 활용돼 안정성을 검증할 수 있다. 장애를 줄이면서 짧은 시간에 완성된 서비스를 오픈할 수 있다.

하이브리드 클라우드로도 일관된 보안 정책 유지

이 같은 클라우드의 장점으로 인해 클라우드 전환 속도를 높이는 기업이 늘어나고 있다. 그러나 하나의 클라우드를 사용하는 기업은 거의 없으며, 기존에 운영하던 물리적 데이터센터를 완전히 버린 곳도 있다. 대부분 물리적 데이터센터와 프라이빗 클라우드, 그리고 여러 종류의 퍼블릭 클라우드를 함께 사용하는 복잡한 하이브리드 형태를 운영하고 있다.

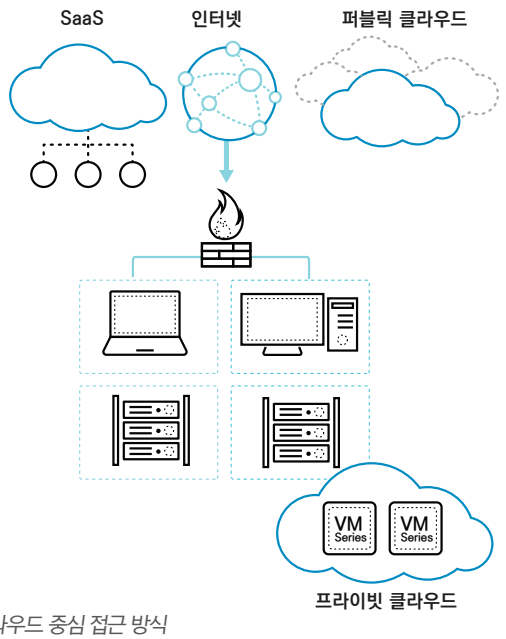
ZK리서치가 IT 담당자를 대상으로 실시한 설문조사에 따르면 응답자의 86%가 기업 데이터를 여러 제공업체의 클라우드 인프라에 두고 있는 것으로 나타났다.

글로벌 MSP 기업 라이트스케일의 보고서에서는 글로벌 기업의 멀티 클라우드 활용률이 81%에 달했고, 이 중 프라이빗과 퍼블릭 클라우드를 결합한 비율이 51%, 멀티 퍼블릭 클라우드를 사용하는 비율은 20%에 이르렀다.

기업이 하이브리드 클라우드로 전환했을 때 기대할 수 있는 이점은 다음과 같다.

- **소규모로 출발해 필요에 따라 확장**

하이브리드 클라우드를 채택하면 프로젝트 규모에 따라 IT 인프라 리소스를 라이선스 형태로 이용하다 필요에 따라



클라우드 중심 접근 방식

추가할 수 있다. 퍼블릭 클라우드가 아니라면 단기 프로젝트가 진행되는 동안 임시로만 사용되고 바쁜 시기가 끝나면 사용되지 않고 방치되는 하드웨어에 투자할 것이다.

하이브리드 클라우드를 사용하면 구성 요소를 바탕으로 하는 개발 방법론을 채택할 수 있으며, 새로운 애플리케이션을 개발하고, 테스트하고, 배포하는 과정을 간단하게 분리할 수 있다. 또한 트래픽 흐름을 중단하지 않고 강력한 보안 정책 시행을 유지하면서 필요에 따라 환경을 복제하고 스풀업한 다음 사용할 수 있다.

• 투명한 확장

하이브리드 전략을 채택하면 퍼블릭 클라우드가 IPSec VPN 연결을 통해 데이터센터가 확장된 것 같은 효과를 얻을 수 있어, 장소를 불문하고 워크로드를 안전하고 확실하게 배포할 수 있다.

또한 보편적으로 지원되는 라우팅 프로토콜을 사용해 내부 IP 주소 공간을 퍼블릭 클라우드로 투명하게 확장할 수 있다. 오버레이 네트워크는 네트워크 운영팀이나 보안 전문가에게 익숙하고 쉬운 분야기 때문에 보안 정책을 용이하게 확장할 수 있다.

• 일관된 보안 정책

클라우드는 보안에 취약하다는 인식이 있지만, 실제로는 네트워크부터 클라우드까지 일관된 보안 정책을 쉽게 적용할 수 있다.

사내 혹은 외부 클라우드에 있는 보안 정책을 중앙에서 관리할 경우 유사한 규칙, 보안 객체 등을 논리적으로 그룹화할 수 있다. 단일 인터페이스를 통해 퍼블릭·프라이빗 클라우드에 있는 모든 방화벽의 효율을 개선할 수 있다.

이를 가능하게 하는 기술의 한 예로 가상 방화벽을 들 수 있다. 가상 방화벽은 프라이빗 클라우드는 물론 여러 퍼블릭 클라우드의 애플리케이션과 데이터를 보호해 하이브리드 클라우드를 안전하게 운영할 수 있도록 한다.

• 컴플라이언스 준수

클라우드는 컴플라이언스 대응에도 도움이 된다. 신뢰할 수 있는 클라우드 서비스 사업자들은 전 세계 주요 보안 컴플라이언스를 충족시킨다. EU GDPR, ISO 27001, HIPAA, FedRAMP, SOC 1 및 SOC 2와 같은 광범위한 국제 및 업계 고유의 규정과 호주 IRAP, UK G-Cloud 및 싱가포르 MTCS를 비롯한 국가별 표준을 준수하고 있다.

국제 규제를 준수하는 퍼블릭 클라우드를 이용하면 해당 클라우드에서 운영되는 데이터의 안전성도 인정될 수 있다. 물론 고객이 책임져야 할 데이터 접근통제 등까지 클라우드 서비스 사업자가 책임지는 것은 아니지만, 사업자의 잘못으로 클라우드 데이터가 사라지거나 침해당하지 않도록 보안에 대비했다는 사실을 인정받을 수는 있다.

클라우드의 3대 보안 과제

서비스 사업자 –고객, 클라우드 보안 책임 공유

클라우드는 '특정한 장소(Location)'라기보다 자동화된 온디맨드 프로세스로 신속하게 프로비저닝되는 리소스 풀에 가깝다.

미국 국립표준기술연구소(NIST)는 클라우드를 '컴퓨팅 리소스 풀을 ▲최소한의 관리 작업으로 ▲신속하게 프로비저닝하고 쉽게 제공할 수 있으며 ▲편리한 온디맨드 네트워크 액세스가 가능하도록 한 모델'이라고 정의한 바 있다.

클라우드는 가상화 기술을 이용해 하드웨어 리소스를 효율적으로 사용할 수 있도록 도와주고, 다이내믹한 가상머신(VM) 프로비저닝을 통해 구매한다.

케이블 연결로 이뤄진 전통적인 방식에 비해 훨씬 신속하게 애플리케이션을 제공할 수 있다. 또한 애플리케이션 리소스 경합 문제를 해결하고 서버 활용을 극대화하는 효율적인 방법을 제공한다.

클라우드의 핵심 가치는 '민첩성'과 '유연성'이다. 그러나 이러한 특징은 숙련된 보안 전문가가 보기에 네트워크 보안의 철칙을 어기는 것이나 다름없다. 프라이빗이든 퍼블릭이든 클라우드의 보안 위협은 전통적인 데이터센터보다 훨씬 더 심각하다.

클라우드 보안 위협은 기업의 비즈니스에만 국한되는 것이 아니다. 스마트 홈, 스마트시티, IoT, 커넥티드 카 등 다양한 융합 서비스 역시 클라우드로 제공되며, 이러한 환경을 노리는 대규모 공격이 발생할 수 있다. 융합 서비스를 고도화하기 위해 머신러닝 분석을 클라우드에서 수행하는 경우, 이 인프라를 공격해 사회전체를 혼란에 빠뜨릴 수 있다.

클라우드는 컴플라이언스 위배 문제도 야기할 수 있다. 최근 인터넷을 기반으로 제공되는 서비스는 국경을 초월해 진행되며, 전 세계로 단숨에 확장할 수 있다. 그 대신 세계 각국의 다양한 컴플라이언스를 해결해야 한다는 문제에 직면하게 된다.

세계 각국은 개인정보 보호와 클라우드 관련 규제를 강화하고 있는데, 제대로 관리되지 못한 클라우드로 인해 막대한 벌금과 과징금, 대규모 소송에 휘말릴 수도 있다.

클라우드는 '남의 컴퓨터'

클라우드 보안에 대한 우려가 높아지면서 클라우드 사업자들은 '안전한 인프라와 서비스를 제공한다'는 점을 강조한다. 그러나 그들이 제공하는 보안은 자사의 인프라와 서비스를 보호하기 위한 것으로 고객 비즈니스 보호를 보장하지 않는다.

보안 문제를 자신하는 사업자 때문에 클라우드 보안은 오히려 더 취약해질 수 있다. 클라우드 사용자들은 사업자만을 맹신하고 클라우드에서 구동되는 비즈니스를 보호하는데 소홀하게 되기 때문이다.

클라우드를 사용하는 조직은 클라우드가 '남의 컴퓨터'이며, 클라우드 내 고객 애플리케이션과 데이터는 고객이 보호해야 한다는 점을 명심해야 한다. 공격자들은 목표로 삼은 서비스가 어떤 환경에서 운용되는지 상관없이 네트워크에 잠입해 공격을 진행한다.

리소스 공유 모델, 네트워크 분할 어려워

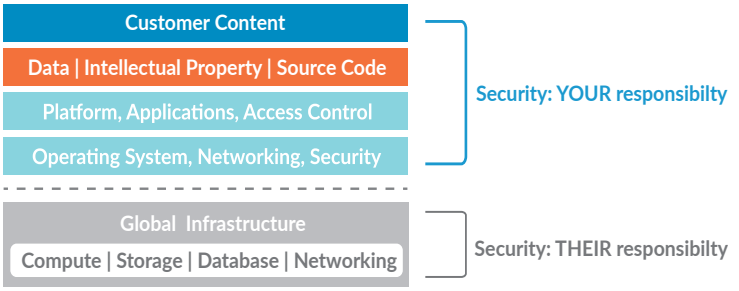
컴퓨팅 리소스를 공유하는 방식으로 인해 클라우드의 보안 위협이 높아진다. 보안을 위해서는 서비스의 종류와 중요도에 따라 네트워크를 분리하고 분할해야 하는데, 리소스를 공유하는 클라우드에서 적절한 분리·분할을 결정하는 것이 쉬운 일은 아니다.

클라우드는 단 몇 분 만에 가상 워크로드가 생성되거나 변경될 수 있지만, 변경된 워크로드의 보안 구성을 설정하는데 몇 시간, 며칠, 혹은 몇 주씩 걸릴 수 있다.

클라우드 전환 시 조직이 직면하게 될 3대 보안 과제는 다음과 같다.

- **애플리케이션 통제**

클라우드에서 네트워크 보안 위협은 한층 더 고도화된다. 다수의 데이터센터 애플리케이션이 광범위한 포트를 사용한다면, 포트 기반 정책을 사용하는 기존 보안 수단은 위장 악성 애플리케이션이나 암호화된 애플리케이션에 숨은 위협을



퍼블릭 클라우드 공동 보안 모델

탐지하지 못한다.

공격자는 포트와 무관하게 다수의 공격 경로를 사용하며, 정상 애플리케이션을 이용하고, 정상적인 접근으로 위장한다. 또한 다양한 공격 수단을 이용해 공격 목표에 접근한다.

그런데 기존과 같은 방식으로 TCP/80, TCP/443을 열어두면 프록시, 암호화된 터널, 원격 액세스 애플리케이션 등 거의 500개에 달하는 애플리케이션에 접근이 허용된다. 포트 기반 제어 정책은 애플리케이션 식별과 컨트롤 기능이 떨어지고 최신 공격을 제대로 차단하지 못한다.

• 분리와 분할

보안을 위해 데이터센터 워크로드는 서비스 중요도에 따라 분리·분할돼야 한다. 비즈니스에 핵심적인 애플리케이션과 데이터는 네트워크의 안전한 영역에 격리하고 '제로 트러스트(Zero Trust)' 정책을 적용해 보안을 한층 더 강화할 수 있다. 물리적 네트워크에서는 제로 트러스트가 애플리케이션과 사용자 ID 기반 정책을 통해 관리되는 방화벽이나 VLAN을 사용해 비교적 쉽게 구현할 수 있다.

그러나 클라우드에서는 서비스에 따라 네트워크를 분할하거나 철저한 '제로 트러스트' 정책으로 제어할 수 없다. 클라우드에서는 서버 내 가상머신(VM) 사이에서 직접 통신이 일어나며, 트러스트 레벨에 차이가 발생하는 애플리케이션 간 통신도 일어난다.

클라우드 애플리케이션을 트러스트 레벨 기준으로 분할하는 것이 원칙적으로 맞지만, 리소스를 공유하는 클라우드에서 중요한 서비스를 격리하는 것은 쉽지 않다. 가상화 포트 기반 보안 솔루션은 호스트 내부 트래픽 가시성이 부족하기 때문에 서로 다른 트러스트 레벨의 애플리케이션을 공유 리소스 풀 내에서 운영하면 보안 취약점이 높아진다.

워크로드 분리·분할이 제대로 돼있지 않고, 애플리케이션과 위협을 식별하지 못하면 공격자를 쉽게 허용하고, 모든 애플리케이션을 제어할 수 있도록 길을 열어준다. 네트워크에 잠입한 공격자는 별다른 저항없이 중요 시스템에 접근해 데이터를 유출하거나 서비스를 중단할 수 있다. 장기간 시스템에 잠복해 있으면서 사이버 스파이 역할을 할 수도 있다.

또한 클라우드는 다양한 서비스를 API로 연결하는데, 보안에 취약한 API는 공격자의 통로로 이용될 수 있다. 보안에 취약한 인증 방법이나 자격증명으로 인한 문제를 해결하기 위해 클라우스 사업자는 API 키와 임시 암호를 제공하고 있으나 공격자들은 이러한 보안 프로세스도 쉽게 우회할 수 있다.

• 동적 클라우드 정책 설정

클라우드는 동적으로 움직이며, 워크로드가 끊임없이 추가·제거·변경된다. 워크로드 수정은 클릭 몇 번으로 끝나지만, 그에 따른 보안 정책 변경은 복잡한 승인절차를 거쳐야 한다. 워크로드 변경에 따라 방화벽 정책을 바꾸고, 사용자의 권한이나 액세스 정책을 변경하며, 다른 시스템에 영향이 없는지 여부도 고려해야 한다.

클라우드의 동적 변화에 보안 정책을 맞추지 않으면 클라우드 워크로드 배포와 보안 정책 변경을 일치시키지 못하고 보안 홀을 방치함으로써 보안 상태를 약하게 만들고, 거버넌스 정책과 규정을 위반하는 원인이 될 수 있다.

클라우드 보안을 위한 10가지 권장사항

'제로 트러스트' 기반 보안 정책으로 클라우드 보호

클라우드는 공유된 컴퓨팅 리소스 풀을 사용하며, 동적으로 자동화된 환경이 구현되고, 언제 어디서나, 어떤 장치로든 애플리케이션 워크로드에 액세스 할 수 있도록 지원한다. 이 같은 특징으로 인해 전통적인 데이터센터의 보안·관리 모델을 적용할 수 없다.

클라우드 보안 모델은 클라우드 기술 혁신에 맞춰 새롭게 설계돼야 한다. 비즈니스에 영향을 미치지 않으면서 서비스 간 충돌되지 않는 클라우드 구축 옵션과 효과적인 보안 기능 관리가 필요하다. 또한 보안, 운영, 네트워킹, 개발 팀에서 요구하는 사항들에 민첩하게 대응할 수 있어야 한다.

클라우드를 운영할 때 반드시 지켜야 할 보안 권장 사항을 10가지로 간추리면 다음과 같다.

1. 공유 보안 모델

클라우드 사업자가 보장하는 것은 자사 서비스와 인프라의 보안일 뿐, 고객의 데이터와 애플리케이션을 보호하지는 않는다. 은행에 돈을 맡기면 그 돈은 은행이 보관하지만, 개인이 실수로 계좌이체를 잘못했거나 전자금융사기·보이스피싱을 당해 사기꾼에게 돈을 보냈다면 이는 은행이 책임지지 않는다. 이와 마찬가지로 클라우드에서 운영되는 기업의 자산은 기업의 책임이지, 사업자의 책임은 아니다. 이를 클라우드에서의 공유 보안 모델이라고 한다.

클라우드 내의 워크로드를 보호하는 것은 온프레미스 워크로드 보호와 다를 바 없다. 조직은 어떤 보안 방식을 사용할지 스스로 결정하고, 자체 고객 데이터와 지적 재산 같은 자사 콘텐츠를 안전하게 보호하는 조치를 취해야 한다.

2. 비즈니스 그룹·데브옵스 조기 참여

최근 클라우드 프로젝트는 데브옵스(DevOps) 같은 비즈니스 그룹이 주도한다. 새로운 제품과 기능의 프로토타입을 신속하게 구동하기 위한 방법으로, 개발과 운영팀이 함께 투입돼 새로운 애플리케이션 접근 방식의 일반적인 가용성과 구축을 지원할 수 있다.

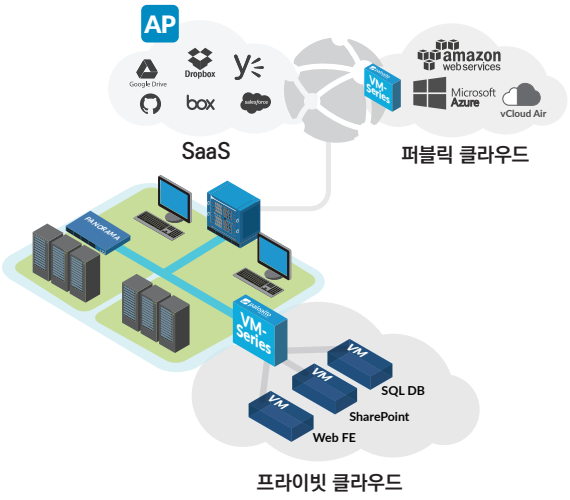
개발·운영팀이 함께 클라우드 프로젝트 범위를 파악하고, 애플리케이션 구축 아키텍처가 비즈니스 개발 요구를 만족시키는 동시에 보안 리스크를 최소화하도록 보장해야 한다.

3. 잠재적 노출 파악

클라우드에서 가장 관리가 어려운 부분이 '섀도우 클라우드(Shadow Cloud)'다. 특히 퍼블릭 클라우드는 계정 생성이 쉽기 때문에 관리 조직이 파악하지 못한 클라우드로 인한 보안 취약점이 발생할 수 있다.

보안 환경이 제대로 구성돼 있지 않은 섀도우 클라우드는 정상적인 권한을 가진 임직원의 정상적인 활동이라해도 보안홀을 만들 수 있다. 따라서 조직 내에서 누가 퍼블릭 클라우드를 사용하는지 파악하고 조직의 환경이 정확하게 구성되도록 보장하는 것이 필수다.

- **퍼블릭 클라우드 사용 모니터링:** 퍼블릭 클라우드 사용 현황을 신속하고 정확하게 하기 위해 네트워크 애플리케이션 트래픽을 기반으로 사용 내역을 알려주는 네트워크 가시성 툴을 활용하는 것이 좋다.
- **적절한 구성:** 보안 베스트 프랙티스를 염두에 두고 조직 보안 환경을 구성한다. 예를 들어 각각의 AWS 서비스는 공개 API 세트를 제공하는데, 사용하지 않을 경우 반드시 이를 비활성화해야 한다. 많은 AWS 신규 사용자들이 S3가 공개 서비스이며 잠금 정책을 설정해 놓지 않을 경우, 인터넷에 저장된 모든 것이 외부로 노출된다는 사실을 모르고 있다. 애저에서는 리소스 그룹 내에 처음 VNet 생성 시, 모든 아웃바운드 포트가 기본적으로 개방돼 있으며 원치 않는 노출이 발생할 수 있다는 점을 사용자가 반드시 인지하고 있어야 한다.
- **2팩터 인증 실행:** 버라이즌의 데이터 침해 조사 보고서에 따르면, 해킹 관련 보안 침해의 81%가 훔친 계정이나 취약한 패스워드를 활용한 것으로 나타났다. 공격자가 훔친 계정 정보를 사용해 접속하는 위험을 최소화하기



〈그림 1〉 팔로알토 네트웍스 솔루션을 통한 전통적인 데이터센터 및 클라우드 기반 애플리케이션과 데이터 보호

위해서는 2팩터 인증을 적용해야 한다.

- **SSH 잠금:** SSH(Secure Shell)는 클라우드 서비스를 안전하게 컨트롤하는 방법으로 선호되는 수단이지만, AWS와 애저 환경을 위협에 노출시키기도 한다. 조직이 암호화 키와 인증서 인벤토리를 정확히 이해하지 못하는 경우가 많고, 사이버 범죄자들은 이를 악용하는데 능숙하기 때문이다. SSH 액세스를 확보한 사이버 범죄자는 조직의 클라우드 인프라를 사용해 손쉽게 봇넷 공격을 실행할 수 있다.

4. 공격자 파악

공격자들은 자동화를 사용해 단 몇 분만에 잠재적인 타깃을 찾아낸다. 타깃을 식별한 다음, 공격자는 취약점 탐색, 기본 패스워드 체크, SSH 구성 오류 탐색 등을 실행한다.

팔로알토 네트웍스는 공격자 자동화 기능의 영향을 보기 위해 퍼블릭 클라우드 내에 SQL 데이터베이스와 워드프레스 서버 인스턴스가 있는 테스트 환경을 구현해 봤다. 8시간 동안 35개 이상의 국가에서 25개 이상의 다양한 애플리케이션으로 테스트 환경을 조사한 결과, 공개 노출에 대한 우려가 비교적 적은 프라이빗 데이터센터와는 달리, 퍼블릭 클라우드 내의 리소스는 광범위하게 노출된 것을 확인했다. 이 사례는 퍼블릭 클라우드 보안이 얼마나 중요한지 상기시킨다.

5. 보안 옵션 평가

클라우드로 전환했을 때 선택할 수 있는 몇 가지 보안 옵션으로 다음을 추천한다.

- **네이티브 퍼블릭 클라우드 보안:** 클라우드 서비스 사업자는 보안 그룹, 웹방화벽 등의 기본 보안 서비스를 제공한다. 이러한 툴이 공격 노출면을 줄이는데 도움을 주지만, 보안상의 틈이 여전히 존재한다.
  보안 그룹은 기본적으로 포트 기반 접근제어 목록으로 필터링 기능을 제공한다. 그러나 특정 허용 애플리케이션을 식별하고 효과적으로 컨트롤한다거나, 위협 방지 또는 파일 이동 컨트롤을 실행하는 것은 불가능하다.
  웹방화벽은 HTTP와 HTTPS 애플리케이션만 보호하고 다른 모든 트래픽은 무시한다. 링크, 쉐어포인트, 액티브 디렉토리 등 정상적인 작동을 위해 다양한 인접 포트를 사용하는 애플리케이션을 보호하지 못한다. 게다가 SSH, RDP 같은 원격 관리·액세스 툴을 식별하고 컨트롤하는 데 효과적인 수단이 아니다.
- **포인트 제품:** 호스트 기반의 포인트 제품은 클라우드를 보호하지 못한다. 예를 들어 IDS는 수동 개입과 치료가 필요하기 때문에 클라우드의 속도와 민첩성을 직관적으로 따라가지 못한다. 또한 IPS는 알려진 위협만을 탐지하며, 제로데이나 알려지지 않은 공격은 놓칠 수 있다. 이처럼 포인트 솔루션은 모두 퍼블릭 클라우드 환경에 대한 총체적인 뷰를 제공하지 못한다.
- **DIY 보안:** 일부 조직들은 스크립팅과 가시성 툴을 사용해 퍼블릭 클라우드 워크로드를 자체적으로 보호하는 방법을 선택한다.
  이러한 전략의 단점은 리소스 부족, 보안 구축과 운영 관리

의 전문성 결여, 보안 침해 발생 시 지원 미비 등이다. 대개 소수의 엔지니어들만이 조직 환경에 대해 잘 알고 있는데, 이들에게 적절한 문서화 또는 지식 공유 요구사항을 관리할 시간이 항상 주어지는 것은 아니다. 만약 이런 엔지니어들 가운데 한 사람만 퇴사하더라도 조직은 효과적인 보안 관리에 어려움을 겪게 될 수 있다.

- **인라인 가상화 어플라이언스:** 가상 차세대 방화벽 같은 인라인 가상화 어플라이언스는 클라우드 구축 환경 내 모든 트래픽의 가시성을 확보할 수 있게 해 준다. 조직은 차세대 통합 보안을 도입해 퍼블릭 클라우드 내 애플리케이션과 데이터 보호를 강화할 수 있다.

  차세대 통합 보안은 애플리케이션, 사용자, 콘텐츠 기반 식별 기술을 사용해 누가 어떤 목적으로 무엇에 액세스했는지 정확히 파악할 수 있도록 해준다. 이러한 이해를 바탕으로 동적 보안 정책을 실행해 위치에 관계없이 애플리케이션, 콘텐츠, 사용자를 안전하게 지원하고 퍼블릭 클라우드 내 데이터와 애플리케이션을 표적화된 위협과 우발적인 위협으로부터 보호할 수 있다.

6. 아는 것이 힘이다

클라우드 보안은 아는 것에서 시작된다. 모바일, 네트워크, 클라우드 전반의 모든 트래픽을 알아야 보호할 수 있다.

퍼블릭 클라우드의 네이티브 툴은 애플리케이션 레이어 가시성을 거의 제공하지 못한다. 게다가 어떤 경우에는 데이터를 정확히 해석하기 위해 보다 심층적인 네트워킹 정보가 요구되기도 한다. 정확한 해석을 하더라도, 344KB의 데이터가 소스 IP 주소와 포트에서 목적지 주소와 TCP 443으로 전송되고 있다는 것은 주목할 가치가 있는 데이터가 아니다. 왜냐하면 TCP 443을 사용할 수 있는 애플리케이션들이 수백 개가 있기 때문이다.

퍼블릭 클라우드가 IPSec VPN을 통해 기업에 연결된 하이브리드 환경에서는 TCP 80과 TCP 443에 대한 액세스만 제한하는 포트 기반 컨트롤만 사용해도 충분하다고 보고, 위협 노출은 기업 쪽에서만 발생한다는 주장도 있다. 이것은 근본적으로 잘못된 생각이다. 포트 컨트롤은 애플리케이션 트래픽, 콘텐츠, 사용자에 대한 컨텍스트 인식은 제공하지 않는다.

소스, 목적지 IP, 국가, 프로토콜, 해당 작업을 실행하는 사용자 또는 사용자 그룹, URL 카테고리, 애플리케이션 ID, 사용 중인 특정 애플리케이션 기능, 구체적인 파일네임 및 유형 등 트래픽 플로우에 대한 종합적인 컨텍스트를 이해해 보다 정확한 보안 정책 결정이 가능하다.

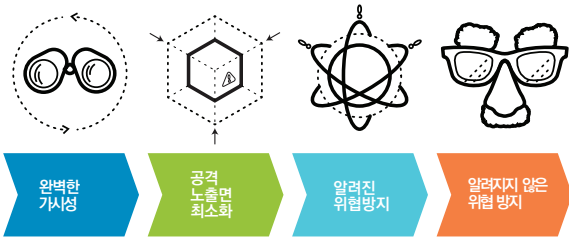
7. 방지의 중요성

'공격자가 이미 이겼다'고 판단해 탐지·치료에 주력하는 조직이 있다. 그러나 조직 환경을 제대로 파악한다면, 현실적으로 선제방어가 가능하다.

클라우드에서 사이버공격을 사전에 방어하기 위해서는 다음의 4가지 기능이 필요하다.

- **완벽한 가시성:** 가시성과 실행은 강력한 보안 툴이다. 포트, 프로토콜, 우회 기법이나 암호화에 관계없이 네트워크와 퍼블릭 클라우드의 애플리케이션들을 식별하는 것이 중요하다. 또한 애플리케이션 특성, 사용 중인 애플리케이션 기능과 관련 리스크를 파악해야 한다.

  이러한 정보를 바탕으로 일관된 보안 정책을 글로벌하게 배포함으로써 알려진/알려지지 않은 공격으로부터 네트워크를 보호할 수 있다.
- **공격 노출면 최소화:** 애플리케이션 ID를 사용해 허용된 애플리케이션만 실행하고 나머지는 모두 차단하는 포지티브 보안 모델을 실행함으로써 공격 노출면을 줄일 수 있다. 또한 비즈니스 요구에 맞게 애플리케이션 사용을 조정하고, 애플리케이션 기능을 컨트롤해야 한다. 예를 들어 쉐어포인트 문서는 모두에게 허용하지만 쉐어포인트 관리자 액세스는 IT 그룹에만 제한적으로 허용하도록 정책을 설정한다. 이로써 네트워크 내부에서 위협의 측면 이동(Lateral Movement)을 차단할 수 있다.



〈그림 2〉 사이버 공격 방어를 위한 4가지 기능

- **알려진 위협 방지:** 허용된 애플리케이션 플로우에 대해 애플리케이션별 위협 방지 정책을 적용하는 것이 방지 전략의 핵심단계다. 애플리케이션별 위협 방지 정책은 취약점 익스플로잇, 멀웨어, 멀웨어 C&C 트래픽을 비롯한 알려진 위협을 차단할 수 있다.
- **알려지지 않은 위협 방지:** 알 수 없는 파일, 악성일 가능성이 있는 파일들에 대해 수백 개의 행위를 기반으로 분석을 실행한다. 팔로알토 네트웍스 '차세대 보안플랫폼'은 파일이 악성으로 간주될 경우, 5분 내에 방지 메커니즘이 제공된다. 방지 기법이 제공된 다음에는 파일 분석을 통해 수집된 정보가 다른 방지 기능들을 지속적으로 향상시키는 데 사용된다.

8. 클라우드 중심 접근방식 사용

데이터센터 운영에 있어 클라우드 중심의 접근방식이 필요하다. 예를 들어 전통적인 하드웨어 기반 데이터센터와 같은 방식으로 고가용성(HA)을 구축하는 것은 아무 의미가 없다. 왜냐하면 운영 환경이 남의 컴퓨터에서 실행되고 있기 때문이다. 어떤 디바이스 인스턴스에서 다른 인스턴스로 페일오버를 실행하기 위해서는 해당 프로세스가 소프트웨어 내에서 이뤄져야 한다. 환경에 따라 최대 60초가 소요될 수 있으며, 다른 지역으로 확장되지 않을 수 있다.

클라우드 중심 접근방식은 클라우드 사업자 패브릭과 로드 밸런싱 등의 자체 복원 기능을 사용해 신속하고 완벽하게 HA 목표를 달성한다.

9. 자동화

급속한 변화가 일반적인 퍼블릭 클라우드에서 가장 중심이 되는 원칙이 자동화다. 보안 베스트 프랙티스 변경 컨트롤이 늦어지면 지연으로 인해 마찰이 발생하거나, 구축이 느려질 수 있다. 변경 컨트롤이 작동할 때까지 구축을 '대기'시키지 않을 경우에는 보안이 약화될 수 있다.

퍼블릭 클라우드 보안을 위한 자동화 툴은 다음과 같다.

- **써드파티 리소스와 양방향 통합:** API를 통해 써드파티 툴 및 데이터를 통합함으로써 보안 운영을 효율화할 수 있다. 예를 들어 서비스나우와 통합으로 서비스 티켓과 워크플로우 생성을 효율화할 수 있다.
- **터치리스 구축(Touchless Deployments):** 부트스트래핑 같은 기능은 단 몇 분만에 완벽하게 구성된 방화벽을 구축할 수 있도록 해준다. 따라서 애저 리소스 그룹이나 AWS 가상 프라이빗 클라우드와 같은 퍼블릭 클라우드 내 격리된 가상 네트워킹 환경을 안전하게 보호할 수 있다.
- **빠르고 정확한 정책 업데이트:** XML API와 Dynamic Address Groups 같은 자동화 기능은 워크로드 변경에 따른 보안 정책 동적 업데이트를 지원한다. 조직은 환경 변화에 따른 더욱 빠르고 정확한 보안 정책 업데이트를 통해 클라우드와 동일한 속도로 운영할 수 있다.

10. 중앙 관리

클라우드 내에서 데이터와 애플리케이션에 대한 효과적인 보안을 유지하기 위해서는 정책 일관성이 필수다. 분산된 물리·가상 방화벽 네트워크를 중앙에서 컨트롤하고 네트워크에서 퍼블릭 클라우드까지 일관된 보안 규칙을 적용하는 것이 보안 기능과 효율성 유지에 있어서 중요하다.

중앙 관리는 네트워크 전반의 트래픽과 위협에 대한 인사이트를 제공하며, 관리를 간소화하고 퍼블릭 클라우드 내 워크로드 변경에 따른 보안 정책 지연을 최소화한다.

멀티-하이브리드 클라우드 보호하는 팔로알토 네트웍스 보안 플랫폼

완벽한 자동화·오케스트레이션 지원하는 '시큐리티 오퍼레이팅 플랫폼'

중단 없는 하이브리드 클라우드 보호를 위해 팔로알토 네트웍스가 제안하는 '시큐리티 오퍼레이팅 플랫폼(Security Operating Platform)'은 네트워크, 엔드포인트, 클라우드 전반을 아우르는 완벽한 자동화 보안 운영과 최적화된 오케스트레이션을 지원한다.

성공적으로 사이버 공격을 방어하기 위해 데이터 기반 접근방식과 클라우드에서 제공되는 지능형 분석을 제공하며, 팔로알토 네트웍스가 제공하는 혁신적인 보안 앱과 써드파티 앱, 고객이 직접 개발한 앱을 활용해 빠르고 유연하게 클라우드 보안을 강화할 수 있도록 지원한다.

애플리케이션, 사용자, 콘텐츠에 맞춰 자동으로 변화되는 보안 정책을 지원하며, 네이티브 클라우드 서비스, 자동화 도구와 긴밀하게 연동해 멀티 클라우드 구축을 가속화하고 단순화한다.

선제방어 플랫폼: 네트워크·엔드포인트·클라우드 보호

팔로알토 네트웍스의 차세대 보안 플랫폼은 모든 공격을 선제적으로 방어하기 위해 공격면을 줄여 공격당할 가능성을 지속적으로 낮춰준다.

네트워크, 엔드포인트, 클라우드 전체에서 위협 데이터가 발견되면, 알려진 위협은 즉시 차단하고 알려지지 않은 것은 '와일드파이어(WildFire)'에서 분석한다.

머신러닝을 적용한 행위분석 기술 '매그니파이어(Magnifier)'를 이용해 위협 데이터를 분석하며, 유연하게 확장 가능한 '로깅 서비스(Logging Service)'를 이용해 하이브리드 클라우드 전체의 보안 이벤트를 수집·연계 분석해 은밀하게 진행되는 공격을 찾아낼 수 있다.

이러한 분석 결과는 네트워크, 엔드포인트, 클라우드 등의 정책에 추가해 공격 확산을 막고, 유사공격까지 미리 예방할 수 있다. 이처럼 알려지지 않은 공격을 알려진 공격으로 전환하는 시간을 5분 이내로 줄일 수 있어 공격이 시작되기 전에 차단해 '선제방어(Threat Prevention)'의 이상을 구현할 수 있다.

PAN-OS : 전용 보안운영체제로 클라우드 혁신 지원

팔로알토 네트웍스는 전용 보안운영체제 'PAN-OS'를 통해 하이브리드 클라우드 전반에서 일괄적인 혁신을 이룬다. 'PAN-OS'는 팔로알토 네트웍스가 제공하는 혁신적인 보안 기술을 클라우드 전체에서 구현하도록 지원하며, 클라우드 전체의 가시성을 확보하고 자동화된 운영을 지원한다.

'PAN-OS'는 멀티벤더 환경에서도 SSL 복호화를 간단하게 적용할 수 있으며, 콘텐츠 업데이트 배포와 오래된 룰을 찾아 현재 환경에 최적화하는 작업을 자동화·단순화해 대규모·분산 환경에서도 데이터센터를 안전하게 운영할 수 있도록 도와준다.

AWS, MS 애저, 구글 클라우드 플랫폼과 연동해 다중 클라우드 보안 기능을 향상하고, 고위험 SaaS 애플리케이션을 식별하고 제어한다.

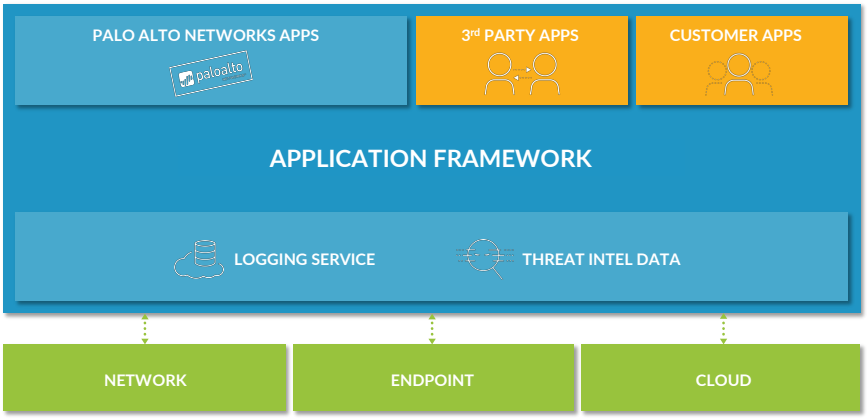
차세대 보안 플랫폼: 퍼블릭 클라우드까지 일관된 보안

팔로알토 네트웍스의 혁신은 2007년 차세대 방화벽(NGFW)을 세계 최초로 발표하면서부터 시작됐다. 차세대 방화벽은 기존의 포트 기반 단순 통제 정책만을 수행했던 방화벽의 한계를 극복하고 애플리케이션, 사용자, 콘텐츠를 기반으로 한 보안 정책을 제공해 전통적인 보안 솔루션을 우회하는 지능형 공격을 차단했다.

팔로알토 네트웍스의 NGFW는 진화를 거듭해 차세대 보안 플랫폼을 구성하는 주요 인프라로 발전했다. 물리적 어플라이언스나 가상 폼팩터로 구축돼 모든 물리적 데이터센터와 클라우드 데이터센터를 보호하고, AWS, 애저, 구글 클라우드 등 주요 퍼블릭 클라우드까지 일관된 보안을 보장한다.

하드웨어 어플라이언스 'PA' 시리즈는 고성능 네트워크 보안을 재정의한다. 업계 최고의 성능은 기본이며, 업계 최고 속도의 SSL 처리 성능, 고도의 안전성, 단순한 관리를 보장한다.

리모트 오피스부터 고속·대형 데이터센터까지 다양한 환경에 적합한 어플라이언스를 제공하며, 싱글패스 소프트웨어 엔진으로 포트에 상관없이 애플리케이션을 식별하고,



〈그림 1〉 팔로알토 네트웍스 '시큐리티 오퍼레이팅 플랫폼'

콘텐츠가 악성인지 여부와 사용자가 누구인지 동시에 파악한다.

PAN-OS에서 제공하는 부트스트래핑을 통해 최적의 방화벽 이미지를 만들 수 있으며, 이 구성을 사용해 다수의 물리적/가상 폼팩터 방화벽 구축을 자동화한다.

VM 시리즈: 모든 가상화·클라우드 환경 지원

클라우드 데이터센터를 위한 차세대 방화벽 VM 시리즈는 물리적 어플라이언스와 동일한 수준의 지능화 된 위협 방지 기능을 제공하며, 오토스케일링 기능으로 트래픽 양에 따라 리소스 사용을 자동으로 조절할 수 있도록 한다.

업계 최초로 AWS, 애저, 오픈스택 모두를 지원하고 있으며, 구글 클라우드 플랫폼, 앤서블 등의 지원을 추가하면서 모든 클라우드 환경을 보호할 수 있도록 도와주고, 위협 사전 방지 기능으로 네트워크에서 클라우드까지 비즈니스를 보호하게 해 준다.

VM 시리즈는 애플리케이션 제어 기능을 활성화 한 상태에서도 업계 최고의 성능을 제공하고, 클라우드를 우선 구축할 수 있도록 도와주며, 싱글 패스에서 모든 트래픽을 분석하고, 모든 포트에서 애플리케이션의 가시성을 제공한다.

VM 시리즈는 원격지 사무소와 모바일 장치 사용자까지 보호할 수 있도록 '엔드포인트용 글로벌프로텍트(Global-Protect Network Security for Endpoints)'와 연동할 수 있다. 워크로드 변경에 따른 정책 업데이트를 자동화해 클라우드 속도로 정책을 구성·배포할 수 있다. 아마존 람다, 애저 등 네이티브 클라우드나 앤서블, 테라폼 등의 기능·자동화 툴과 연동해 안전한 클라우드 운영이 가능하다.

파노라마: 클라우드에 직접 구축하는 중앙관리 솔루션

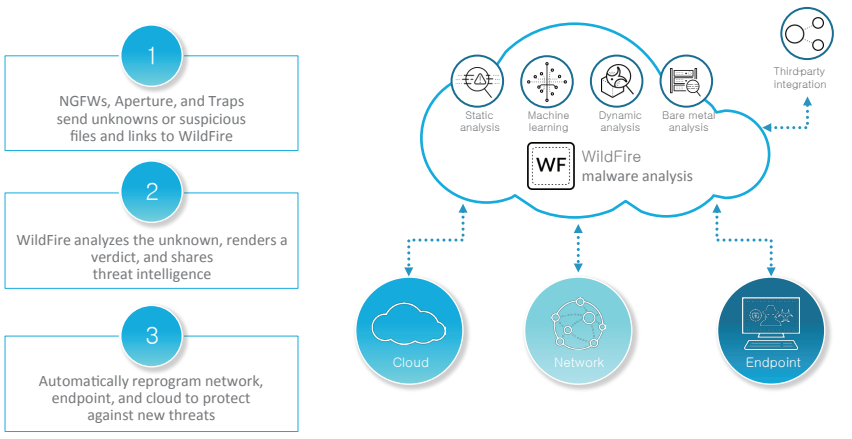
멀티·하이브리드 클라우드 보안 관리 자동화를 위한 '파노라마(Panorama)'는 클라우드 VM을 직접 설치해 방화벽 로그를 수집하며, 하나의 장비에서 여러 정책을 적용하고 통제한다.

방화벽 폼팩터나 위치에 관계없이 모든 팔로알토 네트웍스 차세대 방화벽과 VM 시리즈 가상 차세대 방화벽을 관리해 정책의 유기적인 일괄성을 보장한다. 새롭게 생성·변경된 보안 규칙을 파노라마를 통해 배포해 공유 정책을 실행하고 소프트웨어·콘텐츠 업데이트와 라이선스를 중앙에서 관리한다.

트랩스·섹도: EDR 뛰어넘는 XDR

팔로알토 네트웍스의 혁신은 네트워크에 국한되지 않는다. 엔드포인트 보호를 위한 지능형 위협 탐지 시스템 '트랩스(Traps)'와 2018년 인수한 '섹도(Secdo)'를 통합해 기존의 알려진/알려지지 않은 공격 도구 분석 기술을 한층 더 향상시켰다.

특히 섹도는 파일 없는 공격 분석·탐지에 뛰어난 기술을 가진 기업으로, 팔로알토 네트웍스 엔드포인트 보안 플랫폼



〈그림 2〉 시큐리티 오퍼레이팅 플랫폼의 자동화된 선제방어 프로세스

을 EDR에서 XDR로 한 단계 진화시키고 있다.

차세대 엔드포인트 보안 플랫폼 트랩스는 공격자들이 사용하는 공격도구를 미리 찾아내고 선제적으로 방어하는 특화된 장점을 갖고 있다.

트랩스는 취약성 프로파일링 기법으로 익스플로잇이 실행되는 것과 애플리케이션 공격이 시작되는 것을 선제적으로 인지하고 차단한다. 시스템 레벨 권한 상승 등을 통해 애플리케이션 단의 보안 솔루션 작동을 무력화하는 공격까지 차단할 수 있도록 커널 취약점 공격 방어 기술을 제공한다.

또한 트랩스는 데스크톱, 노트북, 서버, 가상머신에서도 구동되며 클라우드 워크로드상의 윈도우, 맥OS, 리눅스까지도 보호한다.

클라우드 기반 위협 분석 서비스 '와일드파이어'를 통해 분석된 위협 정보를 이용해 전 세계 모든 알려진 공격을 선제적으로 차단하며, 로컬에서 머신러닝을 이용해 신·변종 공격을 즉시 분석한다. 스크립트 엔진, 커맨드 쉘 등 합법적인 프로세스도 세밀하게 제어해 보안 솔루션을 우회해 진행되는 악성 차일드 프로세스까지 탐지한다.

시스템을 모니터링해 랜섬웨어 행위를 찾아내고 발견 즉시 해당 공격을 차단해 고객 데이터가 암호화되지 않도록 하며, 엔드포인트에 대한 정기적인 온디맨드 스캔으로 악성 파일이 활동을 시작하기 전에 사전 차단한다.

애플리케이션 프레임워크: 일관성 있는 SaaS 보호

클라우드의 최대 장점인 유연성을 해치지 않으면서 보안을 보장할 수 있는 방법으로 팔로알토 네트웍스는 '애플리케이션 프레임워크(Application Framework)'를 클라우드 보안 플랫폼의 핵심 위치에 뒀다. 애플리케이션 프레임워크는 팔로알토 네트웍스가 제공하는 다양한 보안 애플리케이션과 써드파티 SaaS 애플리케이션, 고객이 직접 개발한 커스텀 애플리케이션을 자유롭게 사용하면서 하이브리드·멀티 클라우드 전반에서 일관된 보안을 유지할 수 있도록 지원해주는 혁신적인 기술이다.

애플리케이션 프레임워크는 시큐리티 오퍼레이팅 플랫폼상에 구축되며, 다양한 보안 애플리케이션을 조직이 쉽고 단순하게 클라우드에서 사용할 수 있도록 지원한다.

운영되는 SaaS 애플리케이션은 팔로알토 네트웍스의 애플리케이션이든 써드파티·커스텀 애플리케이션이든 상관없이 보안 정책을 일괄적으로 적용할 수 있도록 자동화하며, 로깅 서비스를 통해 모든 보안 위협 정보를 수집하고 분석할 수 있도록 한다.

더불어 위협 인텔리전스 데이터를 활용해 전 세계에서 발생하는 위협 정보를 실시간으로 수집, 대조하고 대응해 공격자보다 한 발 앞선 방어 전략을 펼칠 수 있도록 한다. 네트워크, 엔드포인트, 클라우드 전반에 걸쳐 자동화된 보호를 제공해 진화하는 클라우드 기반 공격을 막을 수 있게 한다.

애플리케이션 프레임워크를 이용하면 자동화된 워크플로우로 보안운영(SecOps)의 요구를 만족시킬 수 있으며, 클라우드 오케스트레이션을 통해 보안 정책을 강화하고 위협

을 빠르게 격리할 수 있다. 여러 써드파티 애플리케이션을 조합해 보다 강력한 보안과 효율적인 클라우드 비즈니스가 가능하다.

애플리케이션 프레임워크는 IoT 환경에서 더욱 심화되는 위협까지 대응할 수 있다. IoT는 민첩성과 유연성을 극대화해 운영해야 하며, 실시간 대응 속도를 보장하는 것이 매우 중요하다. 다양한 OS와 플랫폼, 디바이스에서 수많은 종류의 애플리케이션이 운영되는 과정에서 일괄적인 보안 정책 유지는 무엇보다 중요한 일이다.

애플리케이션 프레임워크는 개방된 에코시스템을 통해 모든 환경의 애플리케이션에서 보안 정책을 운영할 수 있도록 지원한다. 여러 산업에서 이용하는 독특한 디바이스를 보호하고, 인가되지 않은 행위를 중단할 수 있다. 모든 보안 운영은 관리자의 개입 없이 자동화돼 관리자 업무를 줄이고 실수·고의로 인한 위협을 막을 수 있다.

어패처·에비던트: 컴플라이언스까지 완벽 지원

클라우드에서 컴플라이언스는 매우 취약한 부분으로 꼽힌다. 유럽 일반개인정보보호법(GDPR)과 같은 강력한 보안 규제로 인해 클라우드 운영은 더욱 복잡해진다. 기업은 여러 클라우드를 사용해 비즈니스 유연성과 민첩성을 높이고자 하지만, 클라우드에 분산 저장된 데이터를 완벽하게 가시화하고 통제하는 문제를 해결하지 못한다는 어려움에 봉착해 있다.

통제하지 않은 데이터가 유출되거나 위변조 돼 컴플라이언스 위반으로 판정되면 막대한 과징금을 부과 받게 되고, 기업 신뢰도 하락으로 인한 피해와 함께 대규모 소송까지 이어질 수 있어 비즈니스 연속성에 치명타를 입게 된다.

팔로알토 네트웍스의 클라우드 자원 검사·모니터링 서비스 '어패처(Aperture)'와 클라우드 기반 컴플라이언스 지원 서비스 '에비던트(Evident)'를 이용하면 이러한 문제에서도 해방될 수 있다. 어패처와 에비던트를 이용하면 멀티클라우드·서버리스 환경에서 보지 못했던 정책설정 오류, 규제위반, 보안위협 등을 종합적으로 탐색하고 개선 방안을 제안할 수 있다

어패처는 SaaS 애플리케이션에 직접 연결해 애플리케이션과 데이터를 직접 통제하는 서비스다. 관리자에게 데이터 분류, 공유, 액세스 권한 가시성, 위협 탐지를 제공해 SaaS 애플리케이션 보안 문제를 해결한다. 와일드파이어 클라우드 기반 멀웨어 분석 환경에 통합돼 SaaS 애플리케이션 내에 상주하는 회사 데이터를 외부 공격이나 후속 데이터 유출, 규정 위반 위협으로부터 보호한다.

에비던트는 미국 중앙정보국(CIA) 지원을 받은 클라우드 보안 스타트업 에비던트아이오에서 개발한 보안 플랫폼으로, 2018년 팔로알토 네트웍스가 인수해 시큐리티 오퍼레이팅 플랫폼에 포함시켰다.

에비던트는 클라우드 전반의 컴플라이언스를 지원하는 탁월한 제품으로, 클라우드 트랜스포메이션을 주저하는 기업들의 고민을 해결할 수 있는 서비스로 꼽힌다. '에비던트'는 단일 대시보드에서 기업이 사용하는 모든 클라우드의 보안 환경을 파악하고 잘못된 구성과 취약점을 탐색해 보안 규정 준수를 돕는다.

핵심 비즈니스에만 집중하게 하는 시큐리티 오퍼레이팅 플랫폼

팔로알토 네트웍스의 시큐리티 오퍼레이팅 플랫폼은 클라우드 전환을 주저하는 조직에게 명확한 해답을 제시한다. 모든 클라우드·데이터센터 환경을 포괄하는 자동화된 보안 운영 플랫폼을 통해 보안 고민 없이 혁신 기술을 신속하게 사용할 수 있게 하며, 기업이 핵심 비즈니스에만 집중해 경쟁력을 높일 수 있도록 도와주고, 진화하는 사이버 공격을 성공적으로 선제 방어해 안심하고 클라우드 전환을 촉진할 수 있도록 도와준다.

팔로알토 네트웍스의 클라우드 보안 오퍼링은 기존 투자를 최대한 활용하고 경계 없는 써드파티 기술 통합, 완벽하게 자동화된 오케스트레이션과 보안 운영을 보장해 보안 강화와 클라우드 효율성을 극대화 할 수 있다.

팔로알토 네트웍스 코리아
서울시 강남구 영동대로 517 아셈타워 37층
paloaltonetworks.com
paloaltonetworks.co.kr
Tel : 02-6001-2900
E-mail : Sales-KR@paloaltonetworks.com