멀티클라우드 시대
차세대 보안 플랫폼 전략

'마이크로소프트 애저' 사용 기업을 위한 효과적인 보안 방안

SPECIAL REPORT
BylineNetwork

멀티클라우드 시대
차세대 보안 플랫폼 전략

퍼블릭 클라우드 서비스 제공업체들은 '책임공유(Shared Responsibility)' 모델이란 보안정책을 운영하고 있다.

클라우드 인프라부터 애플리케이션, 데이터까지 모든 보안을 책임지는 것이 아니라 클라우드 인프라 보안만 책임진다. 클라우드 애플리케이션과 데이터 보안은 고객사의 몫이다.

클라우드 제공업체들이 제공하는 인프라 보안에만 의지한다면 자칫 큰 보안 사고를 부를 수 있다. 기업은 클라우드 애플리케이션과 데이터 사용 현황에 대한 가시성과 통제 능력을 반드시 확보해야 한다.

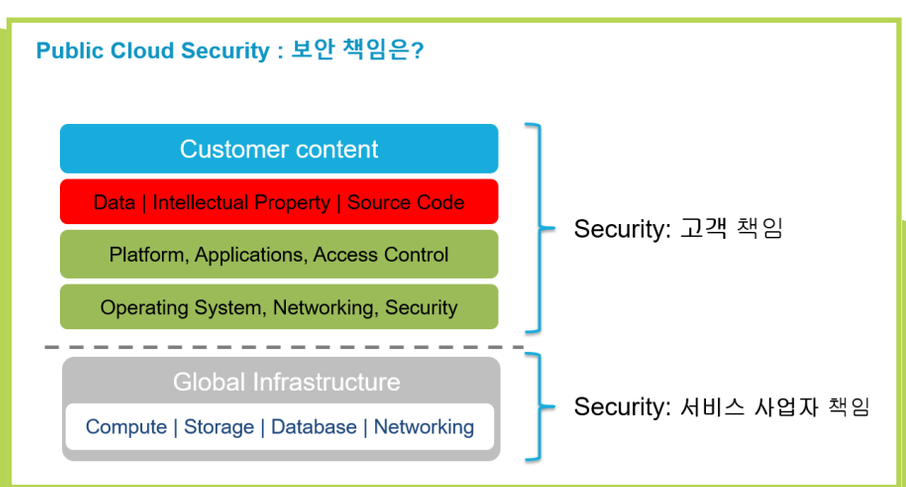
만일 기존 온프레미스에 적용했던 방식을 클라우드 환경에 그대로 적용하려 한다면 효율적이고 효과적인 보안을 구축할 수도 없다. 클라우드 환경에 적합한 보안 방안이 필요하다.

클라우드 확산으로 기업은 온프레미스(On-Premise)와 프라이빗 클라우드, 퍼블릭 클라우드까지 서로 다른 인프라와 서비스 환경이 혼재되고 있다. 퍼블릭 클라우드도 하나만 이용하는 것이 아니라 여러 서비스를 채택하는 경향이 두드러지는 추세다.

하이브리드·멀티클라우드 환경을 운영하는 기업이 지속적이고 효과적인 보안을 유지하기란 쉽지 않다.

그 방안으로 팔로알토 네트웍스는 '멀티클라우드 차세대 보안 플랫폼'을 제시하고 있다. 다양한 퍼블릭 클라우드 서비스를 동시에 이용하면서도 온프레미스·프라이빗 클라우드 환경을 한꺼번에 운영하는 기업이 일관된 보안 수준을 유지하면서도 통합적이고 간소화된 방식으로 보안관리할 수 있도록 지원한다.

퍼블릭 클라우드는 마이크로소프트 애저(Microsoft Azure), 아마존웹서비스(AWS), 구글 클라우드 플랫폼까지 글로벌 선두 퍼블릭 클라우드 서비스를 모두 지원한다.



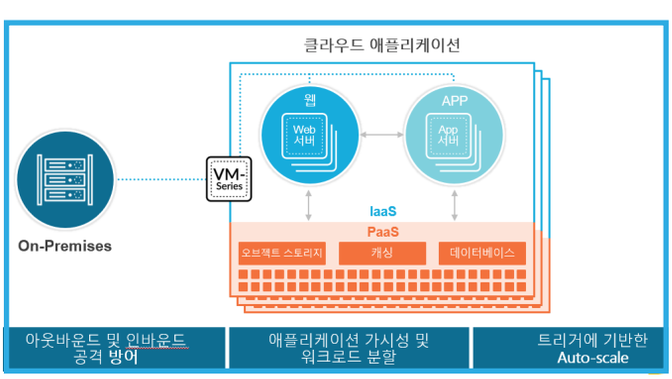
클라우드 보안 해법은 무엇인가

인라인·API·호스트 기반 보호

클라우드 환경에 보안을 적용하는 것은 쉬운 일이 아니다. 물리적 환경과는 달리 무형의 자산과 데이터에 보안을 적용해야 한다. 기존 데이터센터에 적용해온 보안 프로세스와 정책, 제품을 클라우드에 그대로 활용하고자 하는 경우 다양한 문제가 발생한다.

팔로알토 네트웍스 코리아의 클라우드 보안 스페셜리스트인 김민석 이사는 최근 열린 '클라우드 앤드 시큐리티 세미나'에서 "가시성이 애매모호한 클라우드 무형 자산 때문에 클라우드 보안에 대한 큰 오해가 발생하고 있다"는 화두를 던졌다.

김 이사는 "많은 기업들이 퍼블릭 클라우드에 수동적인 보안 접근 방식과 기존에 사용해온 물리적 보안 제품을 인위적으로 적용하고 있다"라면서 "클라우드 트래픽을 우회시키거나 가상머신(VM)을 태깅하며 불필요한 작업을 취하고 있는 상황이다. 하지만 클라우드 환경에 최적화된 전용 보안 제품을 적용하지 않으면 다양한 문제가 발생한다"고 지적했다.



클라우드 환경은 물리적 환경과는 차이가 있다. 또 계속 진화한다.

예를 들어 기존 데이터센터와는 달리 동-서(East-West) 간 트래픽이 많이 발생한다. 물리적 보안 장비로는 클라우드 자원(VM)의 동-서 트래픽을 정확하게 확인하거나 통제하기 어렵다. 또 네트워크 컨피규레이션의 변화만으로 보안 정책이 적용된 동-서 트래픽을 처리하려면 수동적이 되거나 복잡해진다.

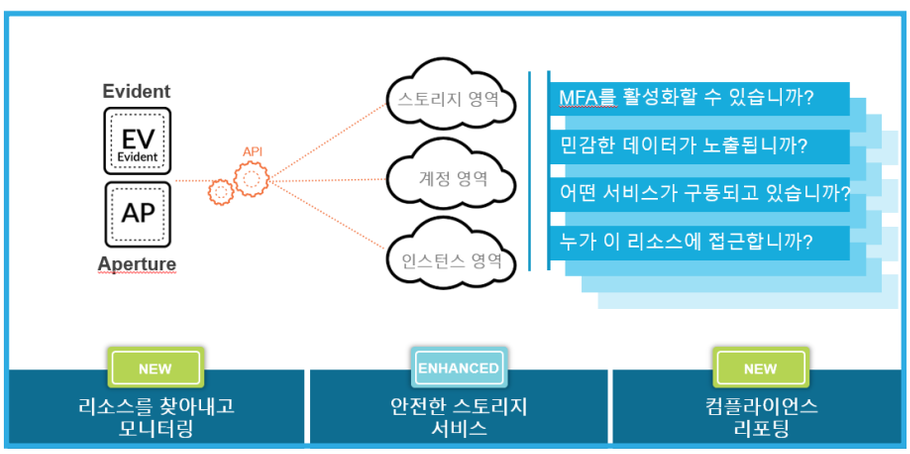
가상 방화벽으로 클라우드 통제, 정책 구현·관리 자동화

팔로알토 네트웍스는 클라우드 트래픽 통제 정책을 손쉽게 적용할 수 있도록 차세대방화벽의 클라우드 버전(가상 차세대방화벽)인 'VM시리즈(VM-Series)'를 제공하고 있다. 지난 2013년 첫 출시한 'VM시리즈'는 퍼블릭 클라우드 인입점에 설치돼 클라우드 환경을 보호하는 게이트웨이 방식의 차세대 보안 솔루션이다.

'VM시리즈'는 온프레미스 환경과 퍼블릭 클라우드(IaaS·PaaS) 사이에 오가는 인바운드·아웃바운드 트래픽을 제어해 공격을 방어한다. '마이크로소프트 애저'와 같은 퍼블릭 클라우드에 인입되는 모든 애플리케이션에 대한 가시성을 확보하며, 자동화된 정책을 바탕으로 통제할 수 있도록 제공한다.

애플리케이션 인지 기능을 바탕으로 필요한 리포트를 손쉽게 출력할 수 있다는 점도 장점이다.

또한 클라우드 트래픽이 급격하게 증가할 경우 서버 자원이 확장됨에 따라 가상방화벽도 자동 확장되는 '오토스케일(Auto-Scale)' 기능



도 제공하는 것이 특징이다.

'VM시리즈'는 앱 컨트롤 기능과 인증서버 연동을 위한 사용자 아이디(User ID) 연동 기능을 무상 제공하며, 고객이 원할 경우 침입방지시스템(IPS), 안티바이러스(AV), 지능형공격방지(ATP), 가상사설망(VPN) 서비스를 서브스크립션 방식으로 선택해 적용할 수 있도록 제공한다.

김 이사는 "팔로알토 네트웍스는 2013년부터 시작해 5년 이상 지속적으로 클라우드 보안에 투자하면서 제품을 꾸준히 고도화하고 있다"라면서 "'VM시리즈'는 최근 2년 사이에 템플릿 기반 자동화 기능을 크게 강화했고, 사용자인터페이스(GUI)도 고도화했다. 깃허브에서 제공하는 스크립트를 사용, 애저 포털에 연동해 클릭 몇 번으로 토폴로지에 맞게 손쉽게 자동 배포할 수 있는 기능을 지원한다"고 설명했다.

이어 김 이사는 "XML API를 통한 양방향 연동 기능을 제공, 인바운드 트래픽을 XML 파일로 자동 통제 처리할 수 있도록 정의할 수 있는 동시에 아웃바운드 트래픽은 애저 시큐리티센터 등 모니터링 툴킷과 통합해 처리할 수 있다"라면서 "팔로알토 네트웍스 차세대 방화벽은 마이크로소프트 애저와는 별동부대처럼 따로 동작되는 것이 아니라 마치 하나의 제품처럼 통합돼 사용할 수 있도록 제공한다"고 부각했다.

API 기반 서버리스 영역 보호, 호스트 기반 보호까지 완비

팔로알토 네트웍스는 스토리지와 계정, 인스턴스를 포괄하는 '서버리스(Serverless)' 영역을 보호할 수 있는 기술도 제공한다.

클라우드상의 '서버' 인프라 영역은 가상 차세대방화벽인 'VM시리즈'가 인라인 기반 보호 기능을 제공한다면, '서버리스' 영역은 API 기반 보호 기능을 제공하는 '어패처(Aperture)'와 '에비던트아이오(Evident.io)'가 담당한다.

'어패처'와 '에비던트'는 소프트웨어서비스(SaaS) 애플리케이션과 데이터 등 클라우드 자원에 대한 검사, 모니터링, 데이터유출방지(DLP), 잘못된 보안구성을 통한 위협을 방지하며, 컴플라이언스를 준수할 수 있도록 지원한다.

클라우드 스토리지 사용자 설정 오류로 중요한 데이터가 유출·노출되거나 악성코드가 업로드 되는 사고도 이들 솔루션으로 방지할 수 있다.

클라우드 애플리케이션 가시성과 정보유출 방지는 '어패처'가, 클라우드 설정오류와 보안 컴플라이언스 위반사항을 탐지해 보안위험을 사전에 제거하는 기능은 '에비던트'가 수행한다.

팔로알토 네트웍스는 클라우드 보안 스타트업인 에비던트아이오를 지난 3월 인수해, 클라우드 보안 제품군을 강화했다.

김 이사는 "게이트웨이 방식의 가상 방화벽으로는 눈에 보이지 않는 서버리스 영역과 스크립트를 컨트롤하고 보호하기 어렵다"라면서 "API 기반의 무형자산과 스크립트 기반 자원은 서버리스 보안 솔루션이 보호해야 한다"고 말했다. 이와 함께 "서버리스 자원을 찾아내 모니터링하고 계정의 킷값을 바꾸거나 스토리지 암호화를 적용하고 컴플라이언스 리포팅까지 수행하는 서버리스 보안 솔루션은 앞으로 성장성이 더욱 커질 것으로 예상된다"고 전망하면서 "마이크로소프트 애저를 포함해 다양한 퍼블릭 클라우드 제공업체들과 긴밀히 협력해 지원하고 있다"고 밝혔다.

호스트 기반 보호는 차세대 엔드포인트 보안 제품인 '트랩스(Traps)'가 담당한다. '트랩스'는 알려진 위협뿐 아니라 알려지지 않은 악성코드, 익스플로잇 등의 위협으로부터 엔드포인트를 보호하는 솔루션이다.

팔로알토 네트웍스는 클라우드 환경 보호를 위해 최근 '트랩스'에 클라우드 기반 관리 서비스 기능을 추가했다. 또 클라우드상의 윈도우 워크로드 뿐만 아니라 리눅스까지 지원을 확장했다.

이밖에도 팔로알토 네트웍스는 중앙집중화된 방식으로 온프레미스와 클라우드 환경에 차세대방화벽을 쉽게 배포하고 관리할 수 있게 하는 '파노라마(Panorama)'도 제공한다.

김 이사는 "팔로알토 네트웍스는 게이트웨이 방식의 차세대방화벽과 서버리스 보안, 엔드포인트 보안까지 아우르는 통합형 클라우드 보안 플랫폼을 제공하고 있다"라면서 "마이크로소프트를 포함해 주요 퍼블릭 클라우드 제공업체들의 전문 보안 파트너로 클라우드 환경을 2중 3중으로 방어하고 클라우드 보안을 손쉽게 접목할 수 있도록 지원한다"고 강조했다. By

마이크로소프트 애저와 팔로알토 네트웍스 차세대방화벽,

“이렇게 활용하세요”

클라우드 컴퓨팅은 이제 피할 수 없는 현실이 됐다. 기업이 보유한 자체 데이터센터가 아닌 마이크로소프트 애저와 같은 퍼블릭 클라우드 환경을 이용하는 것은 일상이다. 문제는 보안이다. 기업의 생명줄 같은 보안을 외부에 맡겨만 둘 수는 없다. 퍼블릭 클라우드상에 있어도 데이터와 애플리케이션을 정책에 따라 보호할 수는 없을까.

팔로알토 네트웍스는 이런 문제를 해결하기 위해 퍼블릭 클라우드 업체와 글로벌 본사 차원에서 밀접한 협력을 맺고 있다. 마이크로소프트 애저의 경우 임원들이 분기마다 만나서 양사 기술과 서비스의 융합을 논의하고 있으며, 엔지니어링과 제품 팀이 능동적이고 지속적으로 협력하는 것은 물론, 현장에서의 고객응대도 함께 한다.

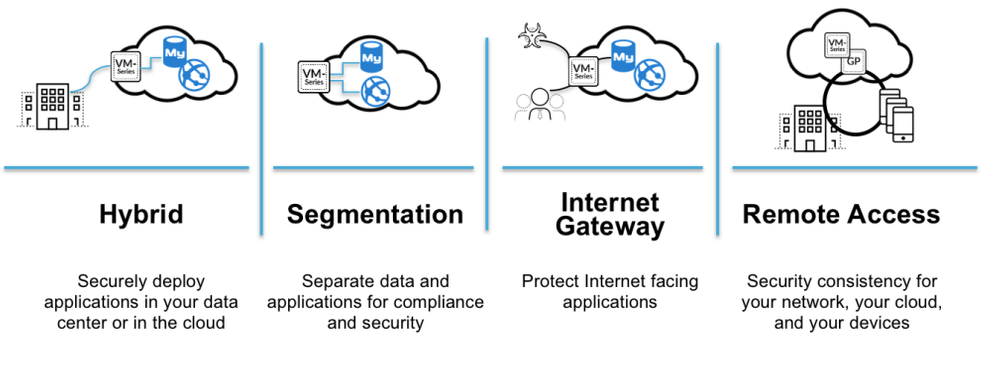
이를 통해 애저 보안 센터와 팔로알토 네트웍스 차세대방화벽 기술 통합, 애플리케이션 인사이트 및 지능형 보안 그래프, 또 가상 네트워크와 스케일아웃 구조로 전환 등이 가능하다.

팔로알토 네트웍스 코리아 김민석 이사는 ‘클라우드 앤드 시큐리티 세미나’에서 마이크로소프트 애저에서 팔로알토 네트웍스의 차세대방화벽을 활용하는 전략과 사례를 소개했다.

김 이사에 따르면, 애저 클라우드를 위한 차세대방화벽 ‘VM시리즈’를 활용하면 크게 세 가지의 이점을 얻을 수 있다.

VM 시리즈 활용 시 세가지 이점

1. 클라우드 환경을 손상시키려는 외부 해커의 공격을 방지할 수 있다. 워크로드 내부에서 손상된 경우에도 데이터 유출을 방지할 수 있다.
2. 포트를 넘어 애플리케이션 레벨에서 송수신 되는 모든 트래픽을 컨트롤 할 수 있다.
3. 클라우드 특성에 맞게 트래픽에 따라 가상 머신이 늘어나면 가상 방화벽도 스케일아웃 할 수 있다.

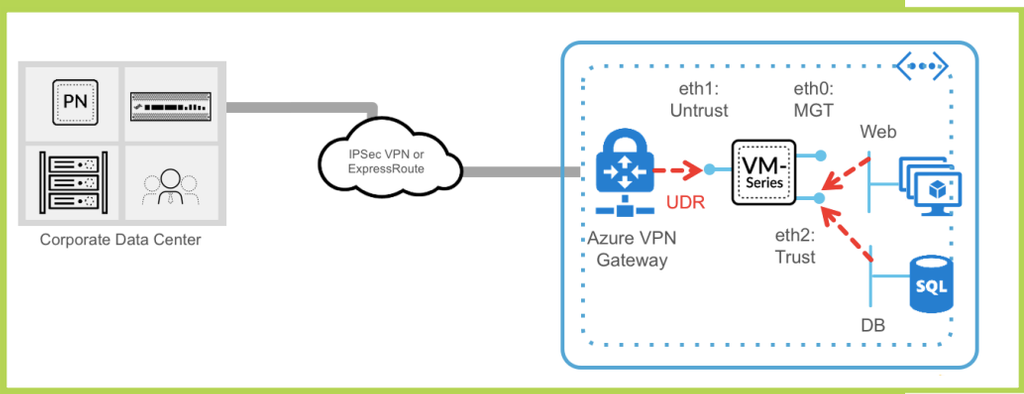


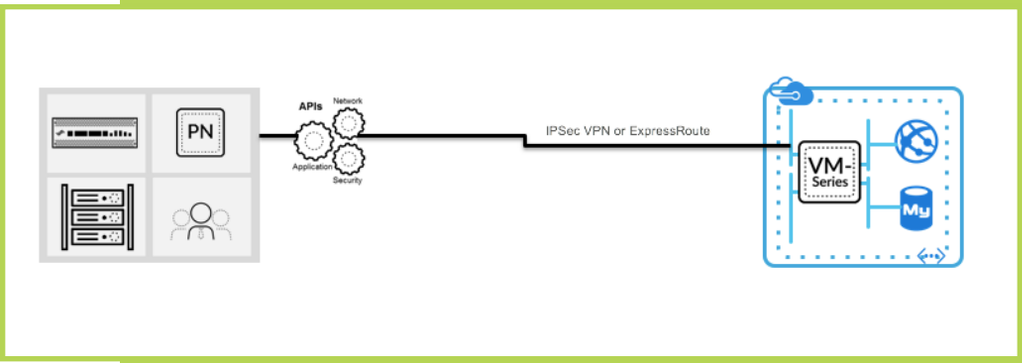
VM시리즈의 활용사례는 크게 네 가지로 분류할 수 있다.

우선 하이브리드 클라우드에 적용할 수 있다. 대다수의 기업들은 자체적인 전산환경을 보유하고 있다. 한꺼번에 퍼블릭 클라우드로 이전하는 회사는 거의 없다. 원하든 원치 않든 기업들은 자체적인 전산환경과 퍼블릭 클라우드 환경을 병행 운영해야 한다. 이 경우 물리적인 자원과 퍼블릭 클라우드에 모두 방화벽을 세워야 하고, 두 방화벽은 함께 운용돼야 한다. 팔로알토 네트웍스는 기존 차세대방화벽과 마이크로소프트 애저 가상머신을 위한 협업을 지원한다.

두번째는 클라우드 내에서의 분할 관리다. 마이크로소프트 애저 위의 VM이라고 하더라도 DB영역과 웹 영역은 다른 수준의 보안이 필요하다. 팔로알토 네트웍스 VM시리즈는 애저 상에서 DB와 웹에 다른 보안정책을 적용할 수 있다. DB라고 하더라도 담고 있는 데이터의 종류에 따라 다른 보안정책을 적용하는 것도 가능하다.

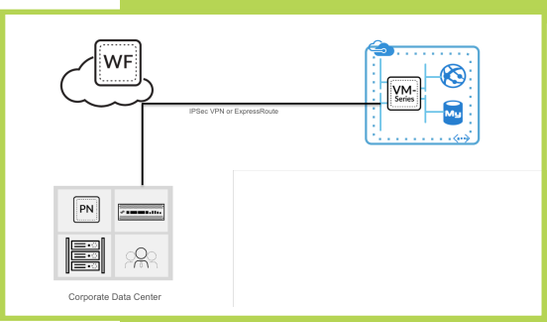
보안 정책을 중앙에서 간편하게 관리하는 것도 특징이다. 1번부터 50번까지의 VM은 A정책을 따르고, 51번부터 100번까지의 VM은 B정책을 따르도록 미리 정해놓을 수 있다. VM이 늘어날 때마다 관리자가 일일이 설정할 필요가 없다.





세번째는 인터넷 게이트웨이다. 애저에 적용한 VM시리즈를 인터넷 게이트웨이로 활용하면, 알려진 위협과 알려지지 않은 위협 모두로부터 웹 기반 애플리케이션을 보호할 수 있다. 알려지지 않은 공격이 들어오면 팔로알토 네트웍스의 사이버위협 인텔리전스 '와일드파이어'로 보내 알려지지 않은 위협을 알려진 위협으로 전환한다. 와일드파이어는 알려지지 않는 악성코드를 최소 5분 내에 분석, 테스트를 완료해 방화벽에 자동 업데이트 해준다.

네번째는 원격접근이다. VPN을 바탕으로 원격 사용자가 서버로 들어올 때 가상방화벽을 통해 들어오도록 할 수 있다. 가상데스크톱환경(VDI) 등에 유용하다. 예를 들어 보험설계사가 아이패드로 보험가입을 받고, 마이크로소프트 애저의 가상 데스크톱으로 데이터를 전송할 때 가상방화벽을 통하게 된다.



보안 로그관리를 위해서는 팔로알토 차세대 방화벽 관리 솔루션인 '파노라마'를 이용할 수 있다. 클라우드에서 파노라마 VM을 설치해 방화벽 로그를 수집하며, 하나의 장비에서 여러 정책을 적용하고 통제한다. 기본적으로 25대의 방화벽에서 최대 24테라바이트까지 로그를 수집할 수 있다. 더 확장 하고 싶으면 파노라마를 로그 수집기로 사용하고, 별도의 저장소에 저장할 수도 있다.

김민석 이사는 "마이크로소프트 애저의 VM에 들어오고 나가는 모든 트래픽을 팔로알토 차세대방화벽이 컨트롤 할 수 있다"면서 "이를 통해 클라우드 위협의 가시성을 확보하고, 체계적인 보안 정책을 적용해 안전한 클라우드를 운영하도록 지원한다"고 말했다. By

클라우드 보안 5가지 '오해'와 '진실'

이 다섯가지는 '참'일까, '거짓'일까? 글로벌 클라우드 서비스 제공업체인 마이크로소프트의 보안 전문가가 이에 대한 해답을 내놨다. 위 예 탄(Wee Yeh Tan) 마이크로소프트 아태지역 보안 담당 매니저의 얘기를 요약한다.

클라우드로 옮긴 데이터는 안전하다.

클라우드 때문에 내 일자리가 없어질 수 있다.

클라우드 서비스 제공업체는 내 데이터에 접근할 수 있다.

클라우드상의 데이터에 대한 통제력과 가시성은 확보할 수 없다.

클라우드는 컴플라이언스 준수를 지원한다.

01 클라우드로 옮긴 데이터는 안전하다? 거짓

한 설문조사에 따르면, 클라우드를 도입하기 전에 응답자들의 60%는 데이터 보안에 큰 우려를 나타냈다. 45%는 클라우드로 데이터를 옮기면 통제가 불가능해질 것을 걱정했다. 하지만 클라우드를 채택한 이후엔 정반대의 결과가 나타났다. 응답자의 94%는 오히려 기존에 온프레미스 환경에서는 누릴 수 없던 장점을 얻었고, 62%는 오히려 통제력이 개선됐다고 답했다.

실제로 신뢰할 수 있는 클라우드 서비스는 IT 운영과 보안에 많은 이점을 제공한다.

하지만 클라우드 보안은 '파트너십' 체제가 기본이다. 클라우드 서비스 제공업체는 '책임공유' 모델을 채택하고 있다.

물리적 환경과 서비스형인프라(IaaS)를 위해 제공하는 패브릭은 클라우드 서비스 제공업체가 책임지지만 가상화엔진과 운영체제(OS) 윗단은 고객사 책임이다. 클라우드 서비스에 접속하는 계정관리, 데이터 보안, 서비스에 사용되는 장치와 브라우저가 모두 해당된다.

탄 매니저는 "마이크로소프트 보안팀은 '블루팀'과 '레드팀'으로 나뉜다. '레드팀'은 마이크로소프트 클라우드를 뚫기 위해 끊임없이 침투 공격을 시도한다. 보안운영팀인 '블루팀'은 방어 역할을 담당한다. '블루팀'은 마이크로소프트 내에서 하드웨어와 소프트웨어 설계와 구입 단계부터 폐기까지 라이프사이클 전 단계에 걸쳐 보안관리를 수행한다"라면서 "클라우드로 데이터를 옮기면 안전할 것이라는 믿음은 이같은 클라우드 보안 강화를 위한 노력에서 나온다"고 설명했다.

02 클라우드 때문에 내 일자리가 없어질 수 있다

거짓

'엘리베이터 보이'와 '전화국 교환원', '공룡'의 공통점은 현재는 존재하지 않는다는 것이다. 기술 발전으로 엘리베이터 버튼을 누르는 것도, 전화를 연결시켜주는 사람도 필요 없는 시대가 된 지 오래다. 혹시 클라우드가 확산되면서 내 일자리가 줄어드는 것은 아닐까 하는 걱정과 우려가 많다.

보안 담당자도 마찬가지다. 클라우드 서비스 제공업체들과 보안책임과 역할을 나눌 수 있기 때문에 기존에는 직접 통제하고 책임져야 했던 관리 영역과 범위가 줄어들 수 있다.

기업은 방대한 모든 자산을 보호할 수 있는 충분한 자원을 운영하기 어렵다. 우선순위에 주력하다보면 보안 허점과 구멍이 생긴다. 우수한 인력을 보안효과를 높일 수 있는 업무에 집중시키거나 재배치할 수 있다. 클라우드 환경에서는 보안과 통제 요구수준이 높아질 수 있기 때문에 일자리가 사라지진 않을 것이다.

마이크로소프트도 7년 전부터 클라우드 여정을 운영하고 있다. 마이크로소프트 내부 이메일과 파일공유 시스템 표준으로 '오피스365'를 사용하면서 기존 익스체인지와 셰어포인트 운영자가 타격을 받을 수 있는 상황이 됐다. 이들은 다들 회사를 그만뒀을까? 단 한 명도 그만두지 않았다. 뛰어난 기술전문가들이었던 만큼 부가가치를 창출할 수 있는 아키텍처팀으로 재배치돼 일하고 있다.

03 클라우드 서비스 제공업체는 내 데이터에 접근할 수 있다

일부 참

애저 서비스를 이용하는 기업의 데이터에 마이크로소프트가 접근할 수 있을까? 어느 정도는 사실이다. 고객 데이터에 접근할 수 있지만 운영자들이 함부로 접근하지 않도록 다양한 통제 정책을 적용하고 있다.

만일 고객사 서비스에 문제가 생겨 마이크로소프트 고객사 데이터에 접근해야 할 경우에는 승인 절차를 거쳐야 한다. 티켓을 발행해 기술 매니저가 엔지니어의 요청을 받아 허용 여부를 결정한다. 허용 시간도 2~4시간으로 통제한다. 운영 담당자가 아닌 경우엔 고객 데이터에 접근할 수 없다. 마이크로소프트는 내부 인력이 고객사 데이터에 접근하는 기회를 최소화하기 위해 자동화를 확대하는 전략을 운영하고 있다.

사실 마이크로소프트가 클라우드 서비스를 운영하는 데이터센터는 100여곳이 넘을 만큼 방대하다. 센터마다 서버가 수만대다. 인력이 뛰어다니며 다 관리할 수 없기 때문에 자동화를 많이 구현하고 있다.

마이크로소프트는 고객들이 사용하는 클라우드 애플리케이션과 서비스에 사용하는 키를 비용효율적이면서 손쉽게 보호할 수 있도록 '애저 키 볼트(Azure Key Vault)'를 제공한다. 저장·이동·사용 중인 모든 데이터를 안전하게 암호화하며, 키에 대한 접근을 모니터링한다.

허용되지 않은 데이터 접근을 막기 위해 고객들은 이같은 기술을 별도로 활용하면 된다.

이밖에도 마이크로소프트는 최근 애저 클라우드에 고객이 매우 중요한 기밀 데이터를 안전하게 보관할 수 있는 보안영역(TEE, Trusted Execution Environments)을 제공한다. 또한 '올웨이즈 인크립티드(Always Encrypted)' 애저 SQL 데이터베이스 기술도 제공해 중요한 고객 데이터를 암호화된 상태를 유지한다. 이 데이터는 복호화 될 수 없다.

04
클라우드 상 데이터에 대한 통제력과 가시성은 확보할 수 없다

거짓

'애저는 위협을 탐지·방지하고 대응하기 위한 다양한 보안관리 툴을 제공해 고객이 데이터를 직접 통제하고 보호할 수 있도록 지원한다.

▲클라우드 기반 디렉토리·계정접근관리 기술인 '애저 액티브 디렉토리(AD)'와 ▲사이버위협에 대한 가시성을 높여 이를 방지·탐지·대응하는 '애저 시큐리티센터' ▲온프레미스와 클라우드로부터 생성되는 데이터를 수집·검색·시각화하는 '애저 로그 애널리틱스' ▲데이터를 안전하게 백업하는 '애저 백업' ▲애저 리소스를 배포·제어하는 '애저 소스 매니저' 등 다양하다.

최근 마이크로소프트는 그래프 보안 애플리케이션프로그래밍인터페이스(API)를 제공해 애저 파트너 업체들의 보안 솔루션을 간소한 방법으로 통합해 사용할 수 있도록 지원한다.

예를 들어 위협이 발생한 경우 이 API를 통해 연동돼 있는 팔로알토 네트웍스 보안 제품에서 즉각 대응조치를 취할 수 있다.

05
클라우드는 컴플라이언스 준수를 지원한다

참

마이크로소프트 애저는 고객이 다양한 컴플라이언스를 준수할 수 있도록 지원한다. ISO 27001 개인정보보호 국제표준을 비롯해 미국 정부·산업계·지역별(국가별) 규정 72개를 지원하는 툴과 기능을 제공한다.

컴플라이언스는 보안과 마찬가지로 클라우드 서비스 제공업체와 고객사가 책임을 공유해야 한다. 고객사는 필요한 경우 애저에서 제공하는 컴플라이언스 관련 기능을 적용(설정)하면 된다.By

멀티클라우드 시대
차세대 보안 플랫폼 전략

'마이크로소프트 애저' 사용 기업을 위한 효과적인 보안 방안

바이라인네트워크

발행 | 바이라인네트워크
배포 | https://byline.network/
취재/글 | 이유지 기자 yjlee@byline.network
심재석 기자 shimsky@byline.network
문의 | byline@byline.network

SPECIAL REPORT
BylineNetwork