Akamai

백서

포괄적인 세그멘테이션을 통한 AWS의 워크로드 보호 - 보다 간편하고 빠른 보안

보안이 염려되어 클라우드 도입을 망설이고 계신가요? 하나의 솔루션으로 AWS에서 가시성, 측면 이동 방지, 유출 탐지 및 대응 기능을 제공할 수 있습니다.

전 세계 기업 중 60% 이상이 클라우드를 도입하지 못하는 주된 이유로 보안을 꼽았습니다. 중요한 워크로드를 AWS로 이전하면 인프라 비용과 유지 관리 부담이 줄고 거의 무제한의 리소스와 전력으로 확장성과 탄력성을 높이며 머신 러닝 및 AI와 같은 최신 혁신 기술을 활용해 성능과 애널리틱스를 향상시킬 수 있습니다. 그러나 보안 문제 때문에 많은 기업이 망설이고 있습니다.

AWS의 보안 과제

완전히 새로운 환경을 고려할 때 보안을 처음부터 다시 검토하는 것은 당연한 일입니다. 클라우드를 완전히 새로 도입하는 상황이거나 다른 벤더사에서 전환하거나 새로운 하이브리드 솔루션을 선택하거나 기존 생태계에 AWS를 추가할 수도 있습니다. 어느 쪽이든 클라우드에는 이 인프라가 안고 있는 고유한 과제를 해결하기 위해 고유한 툴 세트가 필요합니다. 모든 클라우드 벤더사에서 공통되는 요소도 있지만, Azure, GCP(Google Cloud Platform) 또는 AWS에만 해당되는 요소도 있습니다. 다음은 AWS 기술이 포함된 클라우드 또는 하이브리드 클라우드를 사용하는 비즈니스가 안고 있는 주요 우려 사항입니다.

책임 공유 이해: 워크로드를 AWS로 이전할 때 여전히 많은 일을 책임져야 한다는 점을 알고 있어야 합니다. 고객 데이터, 애플리케이션 및 플랫폼의 보안을 유지해야 합니다. Gartner가 2025년까지 클라우드 보안 실패 중 99%가 고객의 잘못이 원인이 될 것이라고 예측한 이유도 바로 책임 공유 모델에 대한 이해 부족 때문입니다.

가시성 부족: 볼 수 없으면 제어할 수도 없습니다. 클라우드에서 가시성은 동서 및 남북으로 이동하는 네트워크 트래픽을 보호하고 시각화하는 경우 훨씬 더 복잡합니다. 흐름을 살펴보는 것만으로는 부족합니다. 중요한 자산이 여러 AWS 계정, 컨테이너 또는 네트워크 보안 그룹에 분산되어 있을 수 있으며, 이러한 모든 상황을 파악하지 못하면 흐름과 상호 의존성을 정확하게 이해할 수 없습니다.

정책 생성의 제한된 제어: 레이어 7 온프레미스에서 인사이트를 얻는 데 익숙하다면 이제 워크로드가 클라우드에 존재하므로 세부 인사이트와 제어 기능을 잃으면서까지 레이어 4 가시성으로 물러나고 싶지는 않을 것입니다. Amazon 보안 그룹은 레이어 4로의 트래픽 제어를 지원합니다. 하지만 레이어 7의 가시성과 제어 기능을 사용하는 경우 기본 인프라에 관계없이 포트 및 IP에만 의존하는 방법보다 더 많은 장점이 있습니다. 포트와 IP만으로는 문제 해결이나 유출 탐지에 크게 부족합니다.

컨테이너 보안: AWS는 Amazon 보안 그룹을 사용해 컨테이너 보안을 위한 정책을 적용하지만 개별 포드(Pod)가 아닌 클러스터로 제한됩니다. 통신에 대한 완전한 인사이트를 얻기 위해서는 최상위에서 실행되는 오버레이 네트워크의 맥락을 파악하고 세분화된 방식으로 포드 수준에서 드릴다운할 수 있는 솔루션이 필요합니다. VM과 컨테이너를 모두 포함하는 네트워크 정책을 생성할 때 작업은 더욱 복잡해지며 종종 기업에서 두 가지 보안 제어 세트를 처리해야 합니다.

올인원 보안 플랫폼으로 이러한 문제 해결

Amazon은 Amazon 보안 그룹과 같이 인프라를 클라우드로 전환할 때 발생하는 몇 가지 과제를 해결하기 위해 내장된 특정 툴을 제공합니다. 그룹을 사용해 권한을 할당하고 정기적으로 인증정보를 변경하며 IAM 그룹으로 단순성을 보장하는 등 기업이 AWS IAM(Identity and Access Management)을 최대한 활용하는 것이 좋습니다. 하지만 오늘날의 동적 퍼블릭 클라우드에서, 특히 레거시 인프라에서 멀티클라우드 및 컨테이너 기술에 이르기까지 모든 것을 포괄하는 하이브리드 환경을 고려하는 경우 이러한 툴은 시작 단계에 불과합니다. 정교한 보안 솔루션을 갖추어야 하이브리드 환경에서도 사각 지대를 없애고 나머지 보안 스택과 원활하게 작동하는 기술로 AWS 서비스를 보완할 수 있습니다. Akamai Guardicore Segmentation이 제공하는 이점은 다음과 같습니다.

AWS 인스턴스에 대한 완벽한 가시성

IT 인프라가 복잡해질수록 심층적이고 자동화된 가시성을 확보하는 것이 더욱 중요합니다. 수동 이동, 추가, 변경 및 삭제는 신뢰할 수 없을 뿐 아니라 격차와 오류가 발생하기 쉬우며, 속도 저하로 이어져 클라우드 도입에 걸림돌이 됩니다. 이와 달리 자동화된 뛰어난 가시성을 갖추면 모든 애플리케이션과 흐름을 검색해 개별 프로세스 수준까지 인스턴스에 대한 가시성을 추가적으로 확보할 수 있습니다.

Akamai Guardicore Segmentation에는 오케스트레이션 데이터를 가져오는 강력한 AWS API가 포함되어 있어 레이블링 및 애플리케이션 매핑에 사용할 수 있는 소중한 맥락을 제공하고 EC2 태그를 자동으로 가져와 EC2 인스턴스를 시각화합니다. 인프라 기준을 수립할 때 애플리케이션의 상호 통신 방식, 상호 의존성의 위치, 유동성과 민첩성을 지원하기 위해 정책을 생성하는 방법을 완전히 이해하는 데 필요한 세부 정보를 얻을 수 있습니다. 사용자는 각 클라우드 벤더사나 환경에 대해 별도의 보안 솔루션 없이도 기본 클라우드 정보와 AWS 관련 데이터를 모두 동일한 대시보드에서 시각화할 수 있습니다. Akamai 솔루션은 플랫폼, 인프라 및 클라우드 전반에서 작동하므로 사각지대를 없앨 수 있습니다.

세그멘테이션 및 적용 - 워크로드를 따르는 하나의 정책

모든 환경에서 이러한 '단일 창' 보기를 확보한 후에 보안 정책을 설계하고 배포할 수 있습니다. 애플리케이션 인식 정책은 레이어 4의 세분화와는 반대로 레이어 7을 제공하며 Amazon 보안 그룹만 사용할 때보다 더 강력한 보안을 지원합니다. 일부 기업은 측면 이동을 제한하기 위해 온프레미스에서 차세대 방화벽을 사용하기도 하지만, 이 방식은 동서 트래픽의 대략적인 세그멘테이션만 지원합니다. 방화벽을 통과해 트래픽을 다시 라우팅하기 위해서는 대규모 인프라와 네트워킹 변경이 필요하기 때문에 세분화된 세그멘테이션 제어를 제공하는 솔루션으로는 감당하지 못할 정도로 굉장히 어려운 작업입니다. 온프레미스 옵션이라 하더라도 기업이 클라우드에서 이러한 수준의 제어를 유지해야 한다는 문제가 생깁니다. 레이어 7 마이크로세그멘테이션은 기본 네트워크 인프라를 변경하지 않고도 동적 워크로드를 위해 구축된 정책을 지원하므로 이 문제의 해답이 될 수 있습니다. 정책이 워크로드 자체를 따르기 때문에 수동으로 변경할 필요가 없으며 민첩성과 빠르게 움직이는 DevOps를 수용하는 기업의 역량도 향상됩니다. 하나의 마이크로세그멘테이션 정책은 하이브리드 환경을 간소화하며 지역, VPC, 컨테이너, VM, 온프레미스 모두에서 하나의 일관된 정책 표현으로 룰을 적용할 수 있습니다. 먼저 Akamai가 제공하는 가시성을 기반으로 몇 분 안에 세그멘테이션 정책을 정의하고 적용할 수 있습니다. 퍼블릭 클라우드에서 최고의 보안 프로토콜을 제공하는 자동 정책 권장 사항을 통해 정책 생성 프로세스도 향상됩니다.

AWS 클라우드에서 유출 탐지 및 인시던트 대응

Akamai Guardicore Segmentation과 같은 풀 서비스 솔루션을 선택하면 AWS 보안에서 세그멘테이션 또는 가시성을 한층 더 강화할 수 있습니다. 정책 위반 탐지는 유출 탐지의 중요한 부분이며, 이를 통해 애플리케이션 수준의 세부 정보를 기반으로 잠재적인 사이버 위협에 실시간으로 대응할 수 있습니다. Akamai는 하이브리드 클라우드 환경에서 악의적인 의도를 즉시 알릴 수 있는 다음과 같은 다양한 유출 탐지 방법을 제공합니다.

- **평판 분석:** 도메인 이름 및 IP 주소에서 파일 해시 및 명령줄에 이르는 흐름 내에서 의심스러운 정보를 자동으로 탐지합니다.
- **동적 디셉션:** 공격자의 행동을 안전하게 파악할 수 있는 높은 상호 작용의 허니팟 환경으로 전환함으로써 공격자 모르게 공격자를 추적합니다.
- **인시던트 대응의 속도를 높여주는 툴:** AWS와의 통합을 통해 모든 정책 위반 또는 보안 인시던트를 AWS Security Hub에 실시간으로 전송할 수 있습니다.
- **맞춤 위협 추적:** Akamai Guardicore Segmentation의 인프라와 Akamai의 대규모 글로벌 위협 인텔리전스를 활용해 하이브리드 클라우드 환경에서 Akamai Hunt 서비스로 가장 교묘한 위협을 차단합니다.

AWS 보안 강화 이상을 지원하기 위한 통합 솔루션

클라우드로 전환한다고 해도 기업이 온프레미스에서 이용하던 보안, 가시성 또는 제어 기능을 포기해야 하는 것은 아닙니다. Akamai Guardicore Segmentation을 사용하면 전체 인프라에서 AWS 인스턴스에 대한 가시성을 완벽하게 확보할 수 있습니다. 이 기본 맵을 사용하면 정책을 원활하게 생성할 수 있으며 수동 지원 없이도 세분화된 제어를 제공할 수 있도록 AWS 보안 그룹을 개선합니다. 유출 탐지 및 인시던트 대응으로 보완한 하나의 엔드 투 엔드 플랫폼으로 AWS 클라우드에서 모든 기반을 보호할 수 있습니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.