포괄적인 세그멘테이션을 통해 AWS 의 워크로드를 더 간편하고 빠르게 보호

서론

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

AWS(Amazon Web Services)에서 PaaS(Platform as a Service) 리소스를 사용하고 중요 워크로드를 오프프레미스로 전환해 얻을 수 있는 이점은 인프라 비용과 유지 관리 부담이 줄고, 거의 무제한의 리소스와 전력으로 확장성과 탄력성을 높이며, 머신 러닝 및 AI와 같은 최신 혁신 기술을 활용해 성능과 애널리틱스를 향상할 수 있다는 것입니다. 그러나 보안 문제 때문에, 특히 클라우드 리소스가 사이버 공격의 주요 대상이라는 점에서 많은 기업이 망설이고 있습니다.

AWS의 보안 과제

완전히 새로운 환경이라면 당연히 보안을 처음부터 다시 검토해야 합니다. 현재 클라우드를 완전히 새로 도입하거나, 다른 벤더사에서 전환하거나, 새로운 하이브리드 솔루션을 선택하거나, 기존 생태계에 AWS를 추가하는 상황일 수 있습니다. 어느 쪽이든 클라우드에는 이 인프라가 안고 있는 고유한 도전 과제를 해결하기 위해 고유한 툴세트가 필요합니다. 모든 클라우드 벤더사에 공통으로 적용되는 요소도 있지만 Azure, Google Cloud Platform 또는 AWS에만 해당하는 요소도 있습니다. 다음은 AWS 기술이 포함된 클라우드 또는 하이브리드 클라우드를 사용하는 기업들의 핵심 우려사항입니다.

책임 공유 이해: 워크로드를 AWS로 이전하거나 빌트인 PaaS 리소스를 활용하는 경우 여전히 많은 책임이 있다는 점을 이해해야 하며, 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 생성에 대한 제한된 제어: 레이어 7 온프레미스에서 인사이트를 얻는 데 익숙하다면 이제 워크로드가 클라우드에 존재하는 상황에서 세부 인사이트와 제어 기능을 포기하면서 레이어 4 가시성으로 물러나고 싶지 않을 것입니다. Amazon 보안 그룹은 레이어 4의 트래픽 제어를 지원합니다. 하지만 레이어 7의 가시성과 제어 기능을 사용하는 경우 기본 인프라에 관계없이 포트 및 IP에만 의존하는 방법보다 더 많은 장점이 있습니다. 포트와 IP에만 의존하면 문제를 해결하고 유출을 탐지하기 매우 어렵습니다.

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 파악할 수 있고 세분화된 방식으로 포드 수준에서 드릴다운할 수 있는 솔루션이 필요합니다. 가상머신(VM)과 컨테이너를 모두 포함하는 네트워크 정책을 생성할 때 작업은 더욱 복잡해지며 종종 기업에서 두 가지 보안 제어 세트를 처리해야 할 수 있습니다.

PaaS 도입: 중요한 워크로드를 클라우드로 전환하는 것 외에도 PaaS 리소스를 도입하는 트렌드가 크게 확산하고 있으며, 이는 클라우드 중심 기업의 진화하는 요구사항을 반영합니다. 하지만 이러한 PaaS 리소스는 에이전트를 지원할 수 없기 때문에 대부분의 에이전트 기반 보안 솔루션은 PaaS 리소스에 대한 전체 보안 기능을 확장하기에는 매우 제한적입니다. 이로 인해 클라우드 보안 정책이 세분화되어 추가 오버헤드가 발생할 수 있으며 공격자들이 악용할 수 있는 보안 격차가 발생할 수 있습니다.

올인원 보안 플랫폼으로 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 그룹을 사용해 간편함을 보장하는 등 기업이 AWS ID 및 접속 관리(IAM)를 최대한 활용하는 것이 좋습니다. 하지만 오늘날의 동적 퍼블릭 클라우드에서, 특히 레거시 인프라부터 컨테이너 기술에 이르기까지 모든 것을 포괄하는 하이브리드 환경과 다양한 퍼블릭 클라우드 환경에서 사용되는 PaaS 리소스를 고려하는 경우 이러한 툴은 시작점에 불과합니다.

정교한 보안 솔루션은 하이브리드 환경에서도 사각지대를 없애고 나머지 보안 스택과 원활하게 작동하는 기술로 AWS 서비스를 보완할 수 있습니다. Akamai가 제공하는 것은 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.

제로 트러스트를 위한 Akamai Guardicore Platform의 핵심 제품인 Akamai Guardicore Segmentation에는 자산, 흐름 및 태그 정보 수집을 위한 전용 구성요소와 함께 오케스트레이션 데이터를 수집하는 강력한 AWS API가 포함되어 있어 레이블링 및 애플리케이션 매핑에 사용할 수 있는 유용한 맥락이 제공됩니다. 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 없이 기본 클라우드 정보와 AWS 관련 데이터를 모두 동일한 대시보드에서 시각화할 수 있습니다. Akamai 솔루션은 플랫폼, 인프라 및 클라우드 전반에서 작동하기 때문에 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 4가 아닌 레이어 7의 정밀함을 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 않고 동적 워크로드를 위해 구축된 정책을 지원하기 때문에 이 문제의 해결책이 될 수 있습니다. 정책이 워크로드 자체를 따르기 때문에 수동으로 변경할 필요가 없으며 민첩성과 빠르게 움직이는 DevOps 프로세스를 수용하는 기업의 역량도 향상됩니다. 하나의 마이크로세그멘테이션 정책은 하나의 일관된 정책 표현으로 리전, VPC, 컨테이너, VM 및 온프레미스 모두에 룰을 적용해 하이브리드 환경을 간소화할 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 개선됩니다.

AWS 클라우드에서 유출 탐지 및 인시던트 대응

Akamai를 통해 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 다양한 유출 탐지 방법을 제공합니다.

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

AWS 보안 강화 및 그 이상을 지원하기 위한 통합 솔루션

퍼블릭 클라우드의 이점을 얻는다는 것은 기업이 온프레미스에서 이용하던 보안, 가시성 또는 제어 기능에 만족해야 함을 의미하지 않습니다. Akamai를 통해 전체 인프라에서 AWS 자산 및 리소스에 대한 가시성을 완벽하게 확보할 수 있습니다. 이 기본 맵을 사용하면 정책을 원활하게 생성할 수 있으며 수동 지원 없이도 세분화된 제어를 제공할 수 있도록 기존 보안 조치를 개선합니다. 유출 탐지 및 인시던트 대응의 보완은 AWS 클라우드와 그 이상에 대한 모든 기반을 포괄하는 하나의 엔드 투 엔드 보안 솔루션을 제공합니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

Akamai 보안 소개

Akamai 보안은 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com 및 akamai.com/blog를 확인하거나 X(기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 11월 발행.