AKAMAI 솔루션 설명서

하이브리드 클라우드 환경을 위한 세그멘테이션

클라우드 인프라를 세그멘테이션함으로써 공격을 차단하는 솔루션

클라우드로 이동하는 애플리케이션과 워크로드가 증가하면서 보안 및 클라우드 팀은 더 많은 도전과제에 직면하고 있습니다. 그 중 하나가 세그멘테이션 및 제로 트러스트 원칙을 클라우드 환경의 애플리케이션과 워크로드로 확장하는 것입니다. Akamai Guardicore Segmentation을 사용하면 에이전트를 설치하지 않고도 퍼블릭 클라우드 환경의 애플리케이션과 워크로드에 대한 공격표면을 줄이고 공격을 차단할 수 있습니다. 이는 자동 애플리케이션 검색, 클라우드 흐름의 포괄적인 시각화, 정밀한 세그멘테이션 정책, 네트워크 보안 알림을 한 곳에서 모두 제공함으로써 가능합니다.

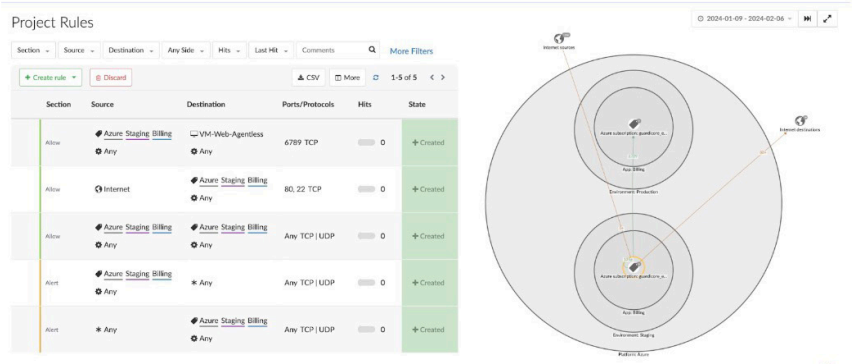
클라우드의 고유한 과제

오늘날 기업들은 중요 시스템을 관리하고 가장 중요한 데이터를 저장하기 위해 클라우드에 대한 의존도를 높이고 있습니다.

IBM의 2023년 데이터 유출 비용 보고서에 따르면, 유출 사고의 82%가 퍼블릭, 프라이빗 또는 두 가지 클라우드 환경 모두에 저장된 데이터와 관련된 것으로 나타났습니다. 공격자는 종종 둘 이상의 클라우드 플랫폼에 접속하는 데 성공했으며, 유출의 39%는 여러 환경에 걸쳐 발생했고 평균보다 높은 475만 달러의 비용이 발생했습니다.

클라우드의 독특하고 동적인 특성으로 인해 클라우드 워크로드는 온프레미스 리소스보다 외부 위협에 더 많이 노출됩니다. 보안팀은 몇 가지 고유한 문제에 직면하고 있습니다.

- **가시성 부족** - 클라우드 공급업체의 가시성은 서로 다른 워크로드 간의 흐름에 대한 원시 로그를 기반으로 합니다. 클라우드 환경 내의 다양한 워크로드와 애플리케이션 간의 관계를 명확하게 이해하지 못하면 효과적인 보안 정책을 만들 수 없습니다.
- **단일 정책의 부재** - 기본적인 클라우드 보안 툴만 사용해 하이브리드 클라우드 환경 전체에 일관된 정책을 만드는 작업은 매우 복잡합니다. 클라우드 인스턴스마다 고유한 오브젝트와 룰이 있고 이에 맞는 고유한 정책이 존재해, 정책이 파편화되기 때문입니다.
- **통합된 거버넌스의 부재** - 클라우드에서 보안이 언제나 우선순위인 것은 아닙니다. 이로 인해 워크로드 가동 시 보안을 반드시 고려하지는 않는 애플리케이션 소유자와 보안팀 간에 갈등이 발생합니다.



자동화된 정책 제안으로 Azure 애플리케이션 링펜싱

기업이 누릴 수 있는 혜택

단일 인터페이스로 클라우드 흐름을 시각화
동적 네트워크 의존성 맵을 사용해 클라우드 워크로드와 애플리케이션이 상호 작용하는 방식을 심층적으로 이해하고 보안 제어를 간편하게 적용합니다.

세그멘테이션 정책을 일관성 있게 적용
보안 사일로를 발생시키는 벤더사별 솔루션을 피하고 하이브리드 클라우드 환경 전반에서 일관성 있게 작동하는 단일 세그멘테이션 솔루션을 배포합니다.

보안 유출 방지
클라우드 환경 내의 모든 변경 사항에 맞게 보안 정책을 조정하고 수동 업데이트 부담을 경감합니다.

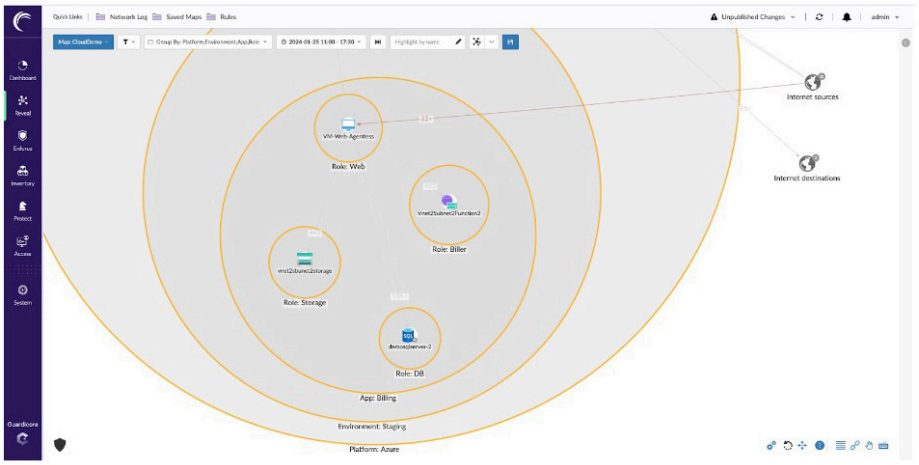
Akamai

클라우드 보안에 대한 위협 방지

Akamai Guardicore Segmentation은 업계 최고의 세그멘테이션 기능을 클라우드 애플리케이션과 워크로드까지 확장합니다. 세그멘테이션을 클라우드 자산으로 확장하면 무단 연결이 자동으로 차단되어 유출이나 랜섬웨어 인시던트로 인한 측면 이동과 피해를 예방할 수 있습니다.

핵심 기능

- 에이전트 없이 포괄적인 클라우드 네이티브 가시성 및 실행 기능을 확보**할 수 있기 때문에 관리자는 실제 네트워크 흐름에 대한 실시간에 가까운 인터랙티브한 맵을 사용해 클라우드 워크로드를 시각화하고, 애플리케이션 의존성을 파악하고, 클라우드 네트워크 보안 거버넌스를 위해 DevOps 및 SecOps 팀을 하나로 모을 수 있습니다.**
- 여러 적용 지점을 활용하는 하이브리드 적용 엔진**을 통해 기업은 네트워크 정책의 의도만 간단히 정의하고 나머지는 Akamai Guardicore Segmentation 정책 엔진이 처리하도록 함으로써 데이터센터 전체에서 어떤 에이전트 기반 및 에이전트리스 적용 지점을 사용할지 동적으로 결정할 수 있습니다.**
- 통합 평판 분석 및 위협 인텔리전스 **방화벽 기능은 유출 발생 시 탐지 시간 및 인시던트 대응 시간을 단축하도록 설계되었습니다.**
- 확장 가능하고 안전한 솔루션**으로 데이터가 클라우드 환경을 벗어나지 않도록 보장하며 솔루션 아키텍처가 클라우드 환경 내에서 자동으로 확장됩니다.**



온프레미스 및 하이브리드 클라우드 환경을 위한 단일 맵

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.