AKAMAI 솔루션 설명서

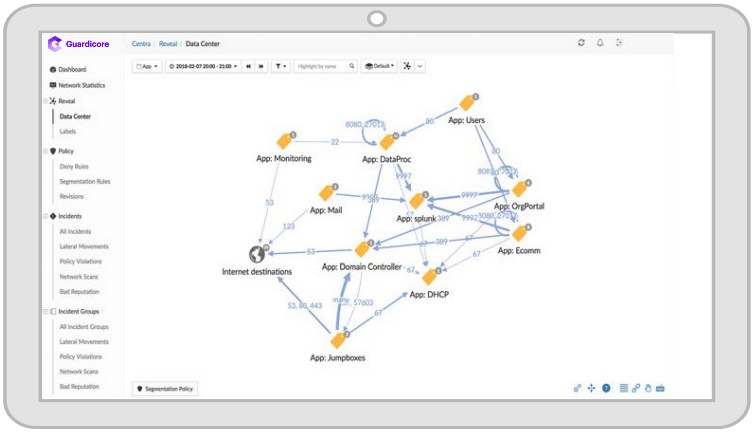
Akamai Guardicore Segmentation을 통해 하이브리드 환경에서 신속한 마이크로세그멘테이션

마이크로세그멘테이션을 구축하는 길이 마냥 순조롭지만은 않습니다. IT 환경에서 애플리케이션 흐름을 파악하고 이해하며 제어하기 시작하는 순간부터 많은 우여곡절을 겪게 됩니다. 그러나 길을 탐색하는 올바른 접근 방식을 알지 못하면 여정을 이어갈 때 여러 가지 어려움을 겪을 수 있습니다. 네트워크 사각지대가 애플리케이션, 워크로드 및 기본 프로세스의 충분한 검색 및 통신 매핑을 방해하는 경우도 종종 있습니다. 엄격한 정책 엔진이 광범위한 의사 결정을 강제로 적용할 수 있으며, 이로 인해 애플리케이션이 손상될 리스크가 있습니다. 운영 체제 사이에서 정책 표현이 일관되지 않으면 위험한 보안 격차가 발생할 수도 있습니다. 마지막으로 정책 위반 데이터를 데이터 유출 탐지 툴로 통합하는 복잡하면서도 때로는 수동적인 작업으로 인해 인시던트 조사 및 응답이 느려질 수 있습니다. Akamai Guardicore Segmentation은 마이크로세그멘테이션의 구축 과정을 성공적으로 탐색할 수 있도록 3단계 지원을 제공합니다.

1단계: 파악

애플리케이션 자동 검색 및 흐름 시각화

Akamai Guardicore Segmentation은 최고의 가시성을 갖추고 있어 어디에 있든 모든 애플리케이션, 워크로드 및 통신 흐름을 프로세스 수준의 컨텍스트에서 자동으로 검색하고 시각화합니다. 온프레미스, 클라우드, 여러 클라우드 등에 걸쳐 있는 자산에 대해 동일한 보기를 제공합니다. 오케스트레이션 메타데이터의 자동 가져오기와 결합된 이 시각화 기능을 통해 보안팀은 모든 자산과 애플리케이션을 쉽고 빠르게 레이블링하고 그룹화함으로써 정책 개발을 간소화할 수 있습니다.



어디에 있든 중요한 애플리케이션 보안

모든 플랫폼 지원

Akamai Guardicore Segmentation은 온프레미스, 클라우드, 여러 클라우드 등 여러 인프라 전반에 걸쳐 자산을 시각화하고 보안 정책을 적용할 수 있습니다.

신속한 정책 수립

자동화된 룰 제안, 유연한 정책 엔진 및 직관적인 사용자 인터페이스 모두 정책을 생성하고 적용하는 데 소요되는 시간을 줄이는 데 도움이 됩니다.

통합된 유출 탐지 및 대응

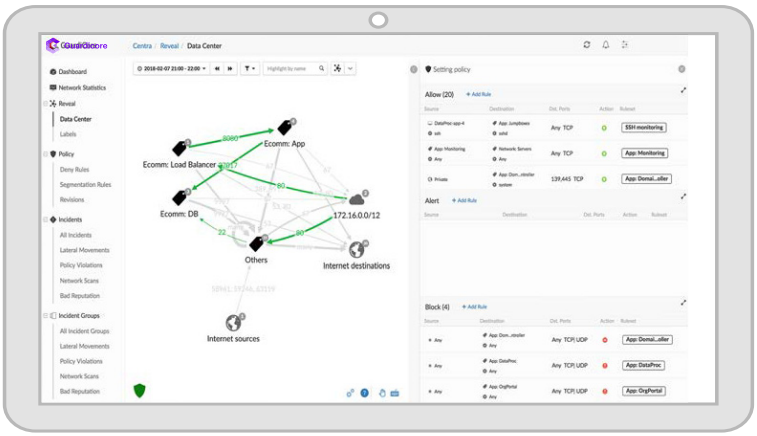
정책 위반을 시각화하고 활성 위협에 신속하게 대응함으로써 가장 중요한 자산이 어디에 있든 보호할 수 있습니다.

Akamai

2단계: 구축

정책의 빠른 고안, 테스트 및 배포

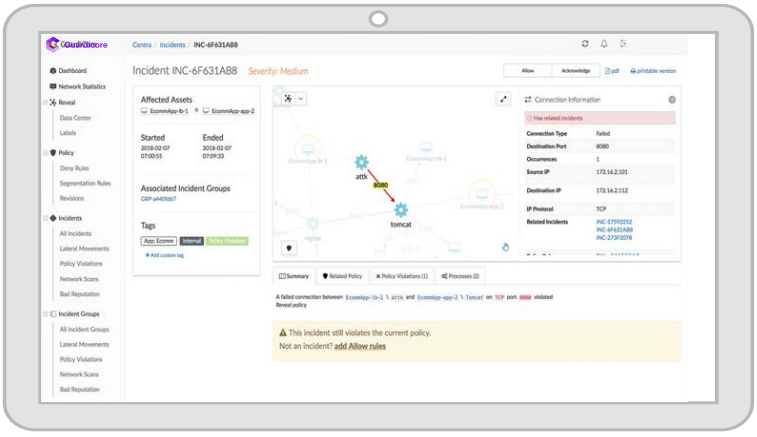
Akamai Guardicore Segmentation은 마이크로세그멘테이션 정책의 개발 및 관리를 간소화합니다. 파악 단계의 맵에서 통신 흐름을 한 번 클릭하면 과거 관측 결과를 기반으로 자동화된 룰 제안이 생성되므로 강력한 정책을 신속하게 구축할 수 있습니다. 직관적인 워크플로우와 유연한 정책 엔진은 지속적인 정책 세분화를 지원하고 비용이 많이 드는 오류를 줄여줍니다.



3단계: 적용

모든 환경에서 보안 강화

Akamai Guardicore Segmentation은 시스템 전반에 걸쳐 네트워크 및 프로세스 수준에서 통신 정책을 적용하는 기능을 통해 운영 체제의 적용 제한에 관계없이 보안을 유지합니다. 또한 통합 유출 탐지 및 대응 기능을 사용해 실제 유출 상황에서 정책 위반을 확인할 수 있으므로 공격 방법을 신속하게 파악하고 문제를 해결할 수 있습니다.



자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

 | 지원 | 2023년 06월 발행