AKAMAI 솔루션 설명서

다양한 유출 탐지 방법 집중 조명: 데이터 센터 유출 탐지를 위해 세그멘테이션 정책 사용

데이터 센터 유출 시도가 수그러들 조짐이 전혀 보이지 않는 가운데, 이제 보안팀은 애플리케이션이 서로 통신하고 미션 크리티컬 기능을 수행하는 데이터 센터의 핵심에 더 많은 관심을 기울여야 할 때입니다. 여러 가상화 환경에 데이터 센터 자산을 배포하는 기업이 늘어남에 따라 경계 방어는 더 이상 적합하지 않습니다. 보안 관리자에게는 이미 경계 방어 유출에 성공한 공격으로부터 내부 동서 트래픽을 보호할 수 있는 효율적인 수단이 필요합니다.

한계에 직면한 방화벽

전통적으로 방화벽은 데이터 센터 내부와 외부의 통신을 보호하는 데 사용되어 왔습니다. 그러나 데이터 센터의 핵심에 방화벽을 배치할 경우 문제가 될 수 있습니다. 대규모 동서 트래픽을 감당할 수 없어서 결국 성능 병목 현상이 발생하게 됩니다. 서버 수준에서 방화벽을 배치하면 호스트에서 많은 양의 컴퓨팅 리소스가 소모되며, 이 방식은 이미 많은 부담을 안겨주고 있습니다. 또한 데이터 센터의 서로 다른 종류와 브랜드의 운영 체제를 포괄하기 위해 여러 솔루션을 배포해야 하기 때문에 관리가 어렵습니다.

최근까지 L7 프로세스 수준에서 보안 정책을 구축하는 작업도 어려운 과제였습니다. IT가 사용자 환경에서 통신하는 모든 애플리케이션과 프로세스를 파악해야만 했기 때문입니다. 또한 애플리케이션과 데이터 센터 내에서 프로세스가 함께 작동하는 방식에 대한 종합적 이해가 필요합니다. 이러한 인사이트가 없으면 프로세스 수준 보안 정책을 구축할 때 리스크가 따를 수 있으며, 침투 가능성도 높아질 수밖에 없습니다.

데이터 센터의 중요 자산을 보호하는 동시에 유출 탐지 및 대응을 개선하려면 보안팀에 다음과 같은 수단이 필요합니다.

- 데이터 센터에서 실행되는 모든 애플리케이션과 프로세스를 실시간으로 시각화
- 중요한 프로세스를 방해하지 않고 정밀한 보안 정책 구축
- 유출을 나타낼 수 있는 무단 통신 탐지

공격이 최선의 방어: Akamai Guardicore Segmentation을 통한 정책 기반 탐지

정책 기반 탐지는 보안팀이 위협을 보다 신속하게 탐지, 확인 및 격리해 피해를 방지하고 손실을 최소화하도록 지원합니다. 이러한 정밀한 보안 제어는 침입자가 애플리케이션 또는 프로세스에 악의적으로 접속하지 못하도록 하는 동시에 침입자의 존재를 관리자에게 경고하는 두 가지 역할을 수행합니다.

Akamai Guardicore Segmentation의 세그멘테이션 정책 기능은 보안 실무자가 다음과 같은 작업을 수행할 수 있도록 지원합니다.

- 데이터 센터 내 모든 애플리케이션 및 활동에 대한 포괄적인 시각적 맵을 생성해 모든 워크로드에 대한 가시성 확보 및 애플리케이션 레이어 통신 완벽하게 파악

다양한 탐지 방법으로 보다 빠른 유출 탐지

동적 디셉션

리디렉션 아키텍처 및 동적으로 생성된 라이브 환경은 데이터 센터 성능을 떨어뜨리지 않으면서 공격자를 유인해 공격 방법을 탐지함

정책 기반 탐지

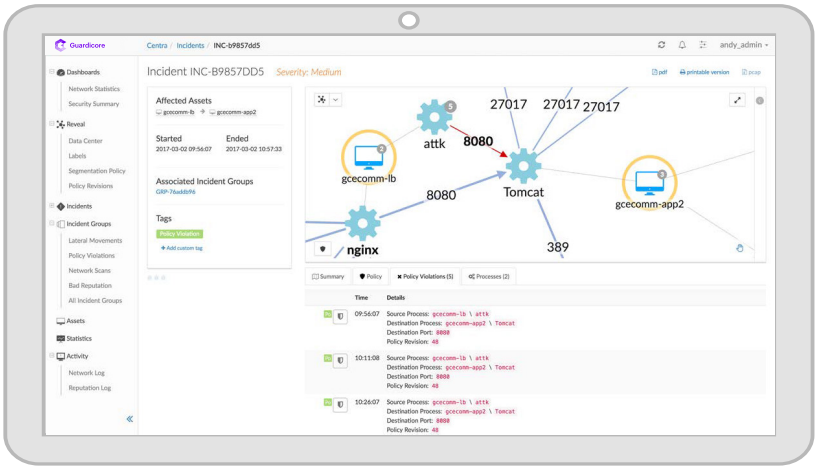
레이어 4 네트워크 및 레이어 7 프로세스 수준의 보안 정책을 통해 무단 통신 및 규정 미준수 트래픽을 즉시 식별할 수 있음

평판 분석

트래픽 흐름 내에서 의심스러운 도메인 이름, IP 주소 및 파일 해시를 탐지해 포괄적인 유출 탐지를 지원함

- 애플리케이션을 그룹으로 필터링 및 구성하고 공통 보안 정책 수립을 목표로 레이블링(예: 특정 워크플로우 또는 비즈니스 기능과 관련된 모든 애플리케이션)
- 애플리케이션 간 허가된 통신을 규제하는 룰 정의 및 생성
- 이러한 룰을 테스트하고 세분화해 정상적인 허가된 트래픽을 방해하지 않도록 함

모든 규정 미준수 트래픽, 무단 통신 또는 기타 정책 위반은 침입자의 존재를 나타내는 알림을 자동으로 트리거합니다. 그러면 위협을 확인하고 격리하기 위한 조사 프로세스가 시작됩니다.



Akamai Guardicore Segmentation은 두 개의 허용된 호스트 사이에서 승인된 포트로 통신을 시도하는 무단 프로세스와 관련된 세그멘테이션 정책 위반을 인식하고 이를 알림으로써 잠재적인 유출을 탐지합니다.

다양한 탐지 방법으로 공격 방어

정책 기반 탐지는 Akamai 솔루션이 실시간 유출 탐지 및 대응을 개선하기 위해 사용하는 여러 방법 중 하나입니다. 다음은 함께 사용해 서로 보완하는 방법입니다.

- **동적 디셉션**: 실제 데이터 센터 서버, IP 주소, 운영 체제 및 서비스를 미끼로 위장해 첫 번째 징후에서 의심스러운 활동을 적극적으로 찾아 유인하고 위협 확인 및 조사를 위해 격리 공간으로 리디렉션함
- **평판 분석**: Akamai의 위협 센서 및 인텔리전스 피드로 구성된 글로벌 네트워크를 활용해 위협과 관련된 부정적인 프로세스 및 의심스러운 IP 주소, 도메인 이름 또는 파일 해시를 식별함

이와 같은 세 가지 방법을 동시에 배포하면 강력한 보안 네트워크를 형성해 데이터 센터의 모든 실시간 유출을 탐지하고 방어하며 심층적 조사를 위해 격리할 수 있습니다.

Akamai Guardicore Segmentation의 포괄적인 유출 탐지 기능에 대해서는 akamai.com/guardicore를 참조하세요.