비교 가이드

Akamai Guardicore Segmentation vs 기존 마이크로세그멘테이션 솔루션

탁월한 가시성

고객의 환경을 이해하려면 워크로드 간 통신에 대한 가시성을 확보해야 합니다. 효과적인 가시성이란 특정 시점에 각각의 워크로드가 어떤 맥락에서 무엇을 하고 있는지 확인하는 것을 의미합니다. 자산과 룰에 대한 그룹화 및 필터링 기능 역시 정책을 빠르게 효과적으로 구축하는 데 필수적인 요소입니다.

Akamai

전체 환경을 간편하게 시각화

Akamai Guardicore Segmentation의 에이전트는 최신 및 레거시 운영 체제에서 실행되는 호스트 기반의 방화벽입니다. MacOS 엔드포인트를 포함, Windows 및 Linux 운영 체제의 네트워크 흐름에 대해 개별 프로세스 및 서비스 수준까지 완전한 가시성을 제공합니다.

탁월한 컨텍스트

가시성을 높이려면 적절한 컨텍스트와 세부 정보를 확보하는 것이 중요합니다. Akamai 솔루션은 플로우 데이터 외에도 프로세스 정보, 파일, 패치 수준 등 중요한 컨텍스트 정보를 수집합니다.

레이블 종류 또는 개수에 제한 없음

Akamai는 보유할 수 있는 레이블의 개수나 종류에 제한을 두지 않기 때문에 사용 사례를 유연하게 추가할 수 있습니다. 이를 통해 설정 관리 데이터베이스(CMDB) 및 기타 데이터 소스에서 기존 레이블을 변환해야 하는 수고를 덜 수 있습니다.

AI 기반 레이블링

신뢰할 수 있는 CMDB가 없을 경우 AI 기반 애플리케이션 탐지 및 레이블링으로 애플리케이션을 식별하고 자동으로 올바른 레이블을 지정할 수 있습니다.

기존의 마이크로세그멘테이션

레거시에 대한 부분적인 가시성

Windows 2002 이전의 Microsoft Windows 시스템에는 광학 장치가 없습니다. 기존의 마이크로세그멘테이션 솔루션 에이전트는 2002년 이후 시스템에서만 사용 가능한 Windows 방화벽에 의존하기 때문입니다. Linux 시스템의 마이크로세그멘테이션 에이전트는 L4 가시성만 지원합니다.

최소한의 컨텍스트

프로세스 및 파일과 같은 중요한 컨텍스트 세부 정보 없이 흐름 및 머신에 대한 정보만 수집합니다. 따라서 애플리케이션 의존성을 파악하는 데 더 많은 노력과 시간이 소요됩니다.

유연성이 떨어지는 레이블링

기존의 솔루션은 미리 정의된 고정식 레이블링 계층 구조를 갖고 있기 때문에, 환경 요구사항 및 비즈니스 요구사항에 정해진 수량만 사용해 애플리케이션 레이블을 지정할 수 있습니다.

CMDB가 없을 때 벌어지는 답답한 상황

기업에 신뢰할 수 있는 CMDB가 없는 경우 수동 레이블링 및 사전 설정된 레이블 계층 구조를 사용하면 레이블링 프로세스가 매우 복잡해집니다.

Akamai

업계 최고의 커버리지

우수한 마이크로세그먼트멘테이션 솔루션의 핵심 요소 중 하나는 레거시와 최신, Windows나 Linux, 온프레미스나 가상 환경, 컨테이너 등 배포 혹은 접속 위치에 관계없이 중요한 자산을 보호하는 기능입니다.

Akamai

Windows 및 Linux에 대한 완벽한 지원

Akamai Guardicore Segmentation 에이전트는 기존 및 새로운 모든 Windows 및 Linux 운영 체제에서 지원됩니다. Akamai 솔루션은 기본 인프라에 의존하지 않기 때문입니다.

컨테이너에 대한 포괄적인 지원

정책 적용에 컨테이너 네트워크 인터페이스(CNI) 제어를 활용하면서 컨테이너화된 환경의 가시성을 완벽하게 확보할 수 있습니다.

기존의 마이크로세그멘테이션

Windows 및 Linux에 대한 제한적인 지원

Windows 환경의 Windows 방화벽과 Linux 환경의 iptables에 따라 정책 적용이 달라집니다. 일부 레거시 Windows OS에 대한 보호가 제한적이거나 존재하지 않으며, Linux 환경에서는 L7 프로세스 수준의 룰이 없습니다.

컨테이너에 대한 제한적인 지원

정책 적용이 컨테이너 환경에서 확장되지 못하는 복잡한 정책 계산과 iptables에 의존하기 때문에 지연 시간 및 가동 중단이 발생합니다.

간편하고 신속한 정책 구축

좋은 정책 엔진을 사용하면 정책 언어 제한을 적용하지 않고 가능한 최소한의 룰을 통해 의도를 표현할 수 있습니다. 또한 자동화 및 마법사를 제공해 정책 관리 작업을 최소화해 줍니다.

Akamai

허용 및 거부

Akamai는 허용 목록과 거부 목록 룰, 그리고 이런 룰의 모든 조합을 지원합니다. 따라서 보안팀과 IR 팀은 모든 보안 시나리오에 발 빠르게 대응할 수 있으며, 정상적인 흐름을 일일이 허용 목록에 추가하지 않아도 됩니다.

다양한 사용 사례에 대한 정책 템플릿

랜섬웨어 방어, 애플리케이션 링펜싱, 환경 세그멘테이션 등 일반적인 시나리오에 즉시 사용 가능한 템플릿과 정책 구축 워크플로우를 제공합니다. 이러한 템플릿은 시간을 절약하고 인적 오류를 줄이는 데 도움을 줍니다.

다양한 정책 기준

정책 기준은 소스, 대상, 포트, 프로토콜, 프로세스, 서비스(일반적으로 랜섬웨어에서 사용되는 작업 스케줄러 등), 사용자, 정규화된 도메인 이름(FQDN)을 포함합니다.

기존의 마이크로세그멘테이션

허용 목록 작성 시 거부 룰에 대한 지원이 제한적

허용 목록 모델은 안전하지만 시간이 많이 소요됩니다. 허용 목록 모델을 고수하는 기존의 세그멘테이션 솔루션은 빠르게 차단해야 하는 알려진 위협에 자동으로 대응하지 못합니다.

한정된 템플릿 세트

세그멘테이션 템플릿은 주로 Microsoft 환경에서 지원됩니다. 링펜싱, 랜섬웨어 방어, 복구와 같은 일반적인 세그멘테이션 사용 사례에 대한 템플릿을 지원하지 않습니다.

제한된 기준

Linux OS에 대한 L7 프로세스 수준의 정책이 없으며 개별 Microsoft Windows 서비스를 기반으로 정책을 구축할 수도 없습니다.

보안을 최우선으로

랜섬웨어처럼 복잡한 보안 위협에 대처하려면 보안에 대한 포괄적인 접근 방식이 필요합니다. 국립표준기술연구원(NIST) 및 백악관은 모두 세그멘테이션을 기본적인 대응 방식으로 규정하고 있지만, 기업의 보안을 유지하려면 보안 및 유출 탐지에 대한 통합적인 접근 방식이 필요합니다.

Akamai	기존의 마이크로세그멘테이션
랜섬웨어 차단 및 방어 Akamai Guardicore Segmentation은 예방, 방어, 차단에 이르기까지 공격 킬체인의 모든 단계에서 즉시 사용 가능한 템플릿을 제공합니다.	**랜섬웨어 템플릿 없음** 기존 솔루션은 즉시 사용 가능한 템플릿을 사용해 랜섬웨어 공격을 차단하는 기능에 한계가 있습니다.
위협 탐지 및 컴플라이언스를 위한 엔드포인트 쿼리 Akamai의 Osquery 기반 툴인 Insight를 사용하면 서버와 엔드포인트를 실시간으로 쿼리해 컴플라이언스를 달성하고 멀웨어를 탐지할 수 있습니다.	**실시간 탐지 기능 없음** 기존 솔루션은 데이터 센터의 실시간 악성 활동을 탐지할 수 없습니다.
디셉션 기능 Akamai Guardicore Segmentation 에이전트는 특허받은 기술을 기반으로 차단되거나 실패한 세션을 동적 디셉션 엔진으로 리디렉션해 추가 분석 및 격리를 실행합니다.	**격리 기능 없음** 기존 솔루션에는 알려진 감염 지표(IOC)로 머신을 탐지 또는 격리하는 기능과 디셉션 기능이 없습니다.
매니지드 위협 탐지 팀 Akamai는보안 팀의 역량을 확대하고 기업이 최신 위협보다 한발 앞서 나갈 수 있도록 매니지드 위협 탐지 서비스를 제공합니다.	**위협 탐색 서비스 없음** 기존 벤더사는 자사 솔루션에 기반한 위협 탐지 서비스를 제공할 수 없기 때문에 랜섬웨어와 멀웨어가 증가하는 상황에서 경쟁력을 가질 수 없습니다.
위협 인텔리전스 방화벽 Akamai Guardicore Segmentation은 알려진 악성 행동을 방지하기 위해 자동 방화벽 룰을 사용해 악성 IP, 파일, 해시를 차단합니다.	**위협 피드 없음** 기존 솔루션은 유사한 기능이 없기 때문에 알려진 악성 IP 및 URL에 대한 접속을 차단할 수 없습니다.

운영 또는 성능 및 지연 시간

세그멘테이션 프로젝트가 성공하려면 짧은 지연 시간이 매우 중요합니다. 즉, 지연 시간을 늘리지 않고 더 많은 룰, 자산별 레이블, 기타 정책 오브젝트로 정책을 확장할 수 있어야 합니다.

Akamai

지연 시간에 최적화된 엔진

Akamai의 세그멘테이션 엔진은 대규모 시나리오에 맞게 구축되었습니다. 최적화된 필터링 메커니즘으로 완성되어 지연 시간이 정책 크기의 영향을 상대적으로 덜 받습니다.

기존의 마이크로세그멘테이션

룰이 많을수록 지연시간 증가

룰의 양과 크기가 커질수록 에이전트로 인해 지연시간이 길어집니다. Linux iptables는 엔터프라이즈 규모의 동서 트래픽에 맞게 확장되도록 구축되지 않았습니다. 따라서 정책 크기에 따라 지연 시간이 크게 증가할 수 있습니다.

Akamai Guardicore Segmentation에 대한 자세한 내용이 궁금하시거나 개인 맞춤형 제품 데모를 요청하려면 akamai.com/guardicore을 방문하시기 바랍니다.