Akamai

마이크로세그멘테이션에 대한 7가지 잘못된 통념 해결

규모를 확장하는 상황에서 뭔가를 작게 만드는 기술을 추구한다는 게 언뜻 모순 같아 보일 수도 있지만, 여기엔 최신 마이크로세그멘테이션 솔루션에 대한 여러 오인들이 있습니다.

네트워크 다운타임이 발생하거나 소프트웨어 정의 배포를 운영하기가 어려울 것 같다는 생각이 드시나요? 다시 한번 생각해 보세요. 지금부터 세분화의 중요성에 대해 살펴보겠습니다.

잘못된 통념 1

현재 보유한 EDR 솔루션으로 랜섬웨어 공격을 막기에 충분하다

EDR(Endpoint Detection and Response)과 세그멘테이션은 둘 다 랜섬웨어 공격을 해결하지만, 킬체인의 여러 단계에서 서로 다른 방식으로 처리합니다. EDR 솔루션은 모니터링 중인 디바이스 또는 엔드포인트에서 작동 중이거나 실행 중인 랜섬웨어의 존재를 탐지하는 것을 목표로 합니다. EDR은 랜섬웨어를 탐지하면, 프로세스를 중단시키고, 디바이스를 격리하고, 발생한 모든 암호화를 롤백할 수 있습니다. EDR과 세그멘테이션은 상호 보완적입니다. EDR이 랜섬웨어를 탐지하지 못할 경우, 세그멘테이션 솔루션은 네트워크를 분산된 버킷으로 분할해 공격이 측면(동서) 방향으로 이동하는 것을 제한합니다. 랜섬웨어의 경우 공격자가 성공하려면 측면 이동이 이루어져야 합니다. 세그멘테이션을 적용하면 엔드포인트를 넘어서 이동하던 공격이 끝내 장애물에 막히게 되므로, 초기 감염이 폭발하는 영역을 제한할 수 있습니다. EDR과 세그멘테이션의 차이점을 자세히 알아보세요.

1시간 42분

이는 공격자가 초기 거점을 마련한 후 네트워크 내에서 측면 이동을 개시하는 데 걸린 평균 시간입니다

(Microsoft Digital Defense 보고서 2022)

잘못된 통념 2

이미 세그멘테이션을 적용하고 있다

세그멘테이션은 새로 등장한 개념이 아니며 훨씬 더 정교해졌습니다. 수십 년간 기업에서는 VLAN, 내부 방화벽, ACL, 보안 그룹을 조각조각 이어 붙이는 방식을 이용해 업무 환경을 세그멘테이션해 왔습니다. 그러나 이런 기존의 방법은 최신 하이브리드와 멀티클라우드 인프라의 복잡한 요구사항을 충족시킬 수 있는 수준으로 발전하지 못했으며, 충분하지 못한 세그멘테이션으로 인해 방어 격차와 사각지대를 만들고 있습니다.

예를 들자면 레거시 방화벽은 워크플로우 의존성을 매핑하거나 평가하지 않기 때문에 애플리케이션, 워크로드 또는 사용자에 대한 세그멘테이션을 식별하기가 어렵습니다. 따라서 기업은 광범위한 세그멘테이션 정책을 구축해야 하는 상황에 놓이지만, 이런 정책은 범위가 넓어 지나치게 허용적이며, 위험하고 잘못된 구성으로 이어지는 일이 비일비재하기에 문제 해결이 어렵고 번거롭습니다.

마이크로세그멘테이션을 통해 기업은 기존의 세그멘테이션 툴로 가능했던 수준을 훨씬 뛰어넘어 레이어 7까지 세그멘테이션하고 적용할 수 있습니다.

200만 달러

3년 내의 방화벽 업그레이드 절감 비용

(Forrester TEI)

잘못된 통념 3

마이크로세그멘테이션은 운영이 너무 까다롭다

최신 마이크로세그멘테이션은 이제 기업에서 본격적으로 활용할 수 있을 정도로 확실히 준비되었습니다.

Akamai Guardicore Segmentation을 활용하면 데이터 센터와 클라우드에서 컨테이너 기반 자산에 이르는 모든 환경에서 세그멘테이션, 가시성, 정책 생성, 적용을 지원하는 단일 소프트웨어 기반 솔루션을 사용해 운영 효율성을 극대화할 수 있습니다. Akamai Guardicore Segmentation을 배포하면 전체 IT 인프라에 대한 동적 비주얼 맵이 생성되어 보안팀이 실시간이나 시간 경과에 따라 개별 프로세스 수준까지 활동을 확인할 수 있게 됩니다.

애플리케이션 행동에 대한 이러한 세부적인 인사이트를 활용하면 직관적인 시각적 인터페이스를 통해 세분화된 마이크로세그멘테이션 정책을 신속하게 생성할 수 있습니다. 글로벌 거부(deny) 룰, 주요 애플리케이션 링펜싱, 대규모 환경을 즉시 세그멘테이션할 수 있는 기능을 통해 신속히 가치를 실현하고 리스크가 감소됩니다.

레거시 세그멘테이션 방법을 사용하면 가시성 부족으로 인해 어디서부터 시작해야 할지 알기가 어렵습니다.

↑95%

SecOps 생산성 증가

(Forrester TEI)

잘못된 통념 4

마이크로세그멘테이션은 애플리케이션과 네트워크 다운타임을 초래한다

기존의 세그멘테이션 접근 방식을 사용하면 애플리케이션이 서브넷 또는 VLAN 간에 이동하는 경우가 많기 때문에 다운타임이 발생하고 비즈니스 연속성이 중단됩니다. 네트워크 엔지니어와 방화벽 관리자는 예약된 가동 중단 시간, 변경 사항 제어 또는 유지 관리 기간에 대한 계획을 세워야 하기 때문에 새로운 서비스 또는 애플리케이션 업데이트를 배포하는 시간이 길어집니다. 게다가 이러한 지연이 발생하면 자산 노출과 취약점으로 인해 리스크가 높아질 수 있습니다.

이와 달리 소프트웨어 정의 세그멘테이션은 기반 인프라와 운영 체제에서 보안을 분리하므로, 네트워크나 애플리케이션에 손대지 않고도 독립적으로 세그멘테이션을 수행할 수 있습니다. 이벤트가 발생할 경우, 영향을 받은 머신을 완전히 격리하는 대신 공격 기법만 차단하므로 비즈니스에 미치는 부정적인 영향이 제한됩니다.

마이크로세그멘테이션은 다운타임 리스크 없이 라이브 프로덕션 환경에서 정책을 테스트할 수 있도록 경고 모드로 배포할 수도 있습니다. 핵심 내용: 최신 세그멘테이션 솔루션은 보안 개선과 비즈니스 민첩성 중 하나만 선택해야 하는 문제로 여겨선 안 됩니다.

잘못된 통념 5

마이크로세그멘테이션은 IoT 또는 OT 환경을 지원하지 못한다

호스트 기반 보안 소프트웨어를 실행하지 못하는 IoT와 OT 디바이스에 제로 트러스트 정책을 적용할 수 있다는 걸 알고 계셨나요?

Akamai의 에이전트리스 세그멘테이션 기능은 에이전트를 실행할 수 없는 디바이스 간의 방어 격차를 해소해 에어갭(air-gap) 엔드포인트 같은 가시성 사각 지대를 없앱니다.

이러한 확장된 커버리지는 수많은 IoT 디바이스와 레거시 OT 시스템이 네트워크에 연결되어 있고 취약점을 지닌 헬스케어, 리테일, 제조업 환경에서 특히 중요합니다. 에이전트리스 세그멘테이션을 네트워크 인프라에 통합하면 새로운 디바이스 자동 검색, 핑거프린팅, 정책 적용을 실현해 리스크를 방어하는 동시에 제로 트러스트를 향한 전사적 여정을 더욱 빠르게 진행할 수 있습니다.

잘못된 통념 6

마이크로세그멘테이션 에이전트는 지연 시간이 너무 길다

마이크로세그멘테이션에 대한 가장 큰 오해 중 하나는 지연 시간이 증가한다는 겁니다.

그러나 실제로는 모든 트래픽이 특정 방화벽 초크 포인트를 통과하게 하는 대신 분산 소프트웨어 기반의 세그멘테이션 정책을 사용하면 네트워크 병목 현상이 사라집니다. Akamai Guardicore 에이전트는 Linux, Unix, Windows OS, MacOS에서 작동하도록 고도로 최적화되어 있으며, 많은 리소스를 사용하지 않게끔 설계되었습니다.

그리고 이 에이전트는 인라인 방식이 아니므로, 지연 시간을 증가시킬 수 있는 심층 패킷 검사를 수행하지 않습니다.

그 대신 Akamai Guardicore 에이전트는 패킷 헤더에서 최소한의 정보를 가져와 고객 환경을 충분히 파악합니다. 속도와 성능을 높일 방법을 찾고 있다면 그 모든 걸 해결할 수 있습니다.

잘못된 통념 7

마이크로세그멘테이션을 실현하려면 하늘의 별 따기보다 어렵다는 풀타임 직원 고용이 필요하다

CISO는 '적은 리소스로 더 많은 일을 처리'해야 한다는 압박을 느끼고 있으므로, 보안 솔루션은 가뜩이나 부족한 내부 리소스를 추가로 사용하지 않으면서 보안팀 직원의 부담을 덜어주어야 합니다.

방화벽과 VLAN 관리 같은 기존의 세그멘테이션 방법은 스위칭, 라우팅, 방화벽 구축, 보안 정책 생성을 별도로 담당하는 여러 팀이 관련된 번거로운 다단계 프로세스가 필요합니다. 레거시 방화벽을 구축하려면 평균 14~22주가 소요될 수 있습니다. 이 모든 기간이 프로젝트 일정에 추가되므로 기업은 상당한 인건비와 운영 관리비를 부담하게 됩니다.

이와 반대로 Akamai의 소프트웨어 정의 솔루션은 배포 소요 기간이 평균 2주이며, 필요한 정규직 직원 수는 한 명에 불과합니다. 그리고 Akamai의 관리형 위협 사냥 서비스인 Akamai Hunt를 추가하면 작업 환경에 새로운 공격, 측면 이동, 비정상적인 공격 행동이 나타나는지 모니터링함으로써 시간과 리소스를 절약할 수 있습니다.

요즘 사이버 보안 전문가를 채용하기란 매우 힘든 일이며 이러한 인재를 지속적으로 보유하는 건 더욱 어렵습니다. 이제 기업에 해로운 방향이 아닌, 이로운 방향으로 방어 체계를 구축할 때입니다.

주요 통계

106%

12개월 이내에 최대 106%의 ROI 실현 입증

(Forrester TEI)

Akamai의 서비스

Akamai Guardicore Segmentation은 가장 간단하고, 빠르고, 직관적으로 제로 트러스트 원칙을 적용하는 방법을 제공하는 소프트웨어 기반의 마이크로세그멘테이션 솔루션입니다. 따라서 정밀한 세그멘테이션 정책, IT 환경 내 활동에 대한 시각 자료, 네트워크 보안 알림을 통해 네트워크의 악의적인 측면 이동을 방지할 수 있습니다. Akamai Guardicore Segmentation은 데이터 센터, 멀티클라우드 환경, 엔드포인트에서 작동합니다. 인프라 세그멘테이션 접근 방식보다 배포 속도가 더 빠르며 네트워크에 대한 우수한 가시성과 제어 기능을 제공합니다.

Akamai Guardicore Segmentation이 어떤 방식으로 정밀한 보안, 심층적인 가시성, 대규모 보안 정책의 일관된 적용을 실현해 민감한 데이터를 지속적으로 보호하는지 살펴보세요.