Akamai

백서

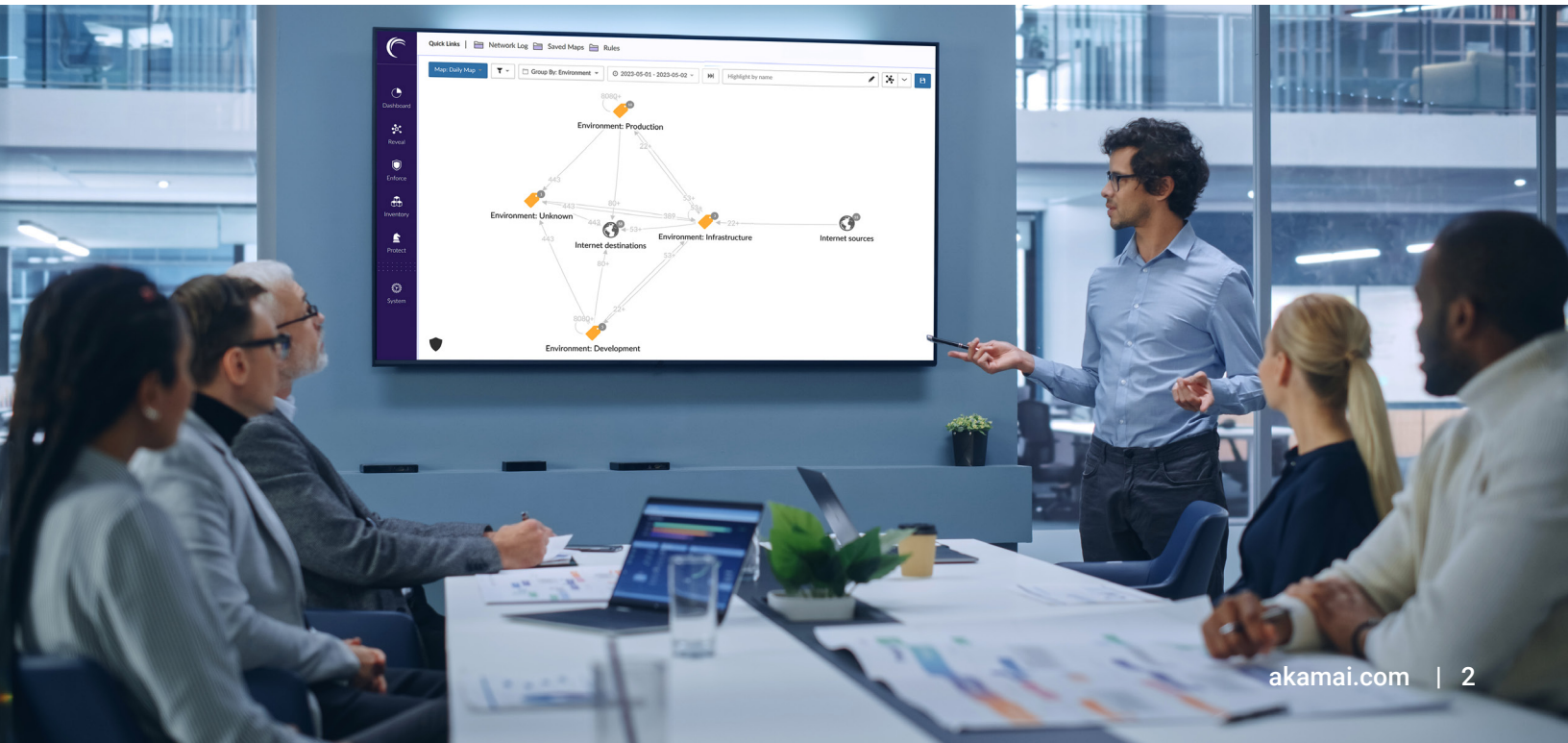
데이터센터운영자를 위한소프트웨어정의 세그멘테이션

멀티 테넌트 데이터 센터 운영자에게 컴퓨팅 환경의 세그멘테이션은 운영 모델의 기본이라 할만큼 중요합니다. 첫째, 데이터 센터 운영자는 클라이언트 환경에서 자체 인프라를 분리하고 특정 리소스를 공유하는 동시에 다른 리소스에 대한 접속은 차단해야 합니다. 둘째, 우발적이든 무해하든 상관없이 클라이언트 환경 간의 '교차 감염'을 방지해야 합니다. 여기에는 공격에 성공한 유출 또는 멀웨어 감염이 하나의 클라이언트 환경에서 다른 클라이언트 환경으로 확산되는 것을 방지하는 것도 포함됩니다. 마지막으로, 이들이 소유하고 있는 운영 애플리케이션 내에서 잠재적인 유출 영향을 제한하려면 적절한 수준의 분리가 필요합니다. 데이터 센터 공급업체의 운영 네트워크를 심층적으로 살펴보면, 세그멘테이션이 효율적으로 구축될 경우 보안 체계를 크게 개선하고 비용을 절감할 수 있는 세 가지 시나리오가 있습니다.

1. **운영 네트워크 분리**: DCIM, BMS 등의 네트워크를 기업 네트워크(요금 청구를 포함한 공급업체의 내부 시스템) 및 고객 네트워크와 분리

2. **운영 네트워크 내부에서 측면 이동 리스크 감소**: 제대로 세그멘테이션되지 않을 경우 리스크에 노출되고 패치가 어려운 시스템이 많은 운영 네트워크 내부에서 측면 이동의 위험 감소

3. **고객이 이용하는 네트워크 간에 효율적이고 안전한 연결 구축**: 사용자 지정 포털이 있는 DMZ와 같이 운영 네트워크(예: 전원 상태 판독) 및 기업 네트워크(요금 청구 정보 판독)에서 데이터에 안전하게 접속해야 하는 네트워크



오늘날 이러한 작업은 매우 복잡하고 구축 속도가 느리며 비효율적인 네트워킹 구조, VLAN, 중간 네트워크 등을 통해 처리됩니다. 복잡한 네트워크 설정에 의존하지 않고 소프트웨어 정의 솔루션을 구축하면 비용을 크게 절감할 수 있으며 연결에 보다 엄격하고 강력한 제어 기능을 적용할 수 있습니다.

고객은 또한 온프레미스에 호스팅된 애플리케이션에서 강력한 수준의 세그멘테이션을 구축하고 유지 관리하는 데 어려움을 겪고 있습니다. 이러한 경우 데이터 센터 운영자는 내부 세그멘테이션 전문 지식, 툴 및 운영 모델을 활용해 고객에게 매니지드 서비스를 제공하고 세그멘테이션 관행을 중심으로 매우 매력적인 매출 흐름을 창출할 수 있습니다. 운영자는 더 나아가 올바른 방법론, 툴, 프로세스를 사용해 보안 정책을 고객 사업장으로 확장함으로써 호스팅되지 않은 애플리케이션에 대한 접속 권한 및 가시성을 확보하고, 이를 통해 호스팅된 데이터 센터로 안전하고 빠르게 전환해 핵심 비즈니스에 기여할 수 있습니다.

Equifax: 최악의 시나리오

보안이 취약하거나 효율성이 낮거나 세그멘테이션이 이루어지지 않은 환경에서 벌어질 수 있는 '최악의 상황' 중 하나로 2017년의 Equifax 유출 사건을 들 수 있습니다. 이 유출 사건으로 인해 1억 4천3백만의 미국인에 대한 매우 민감한 개인 정보가 위험에 노출되었습니다. 미국 GAO(Government Accountability Office)의 조사에 따르면, 공격자는 최초에 Apache Struts 웹 프레임워크에서 CVE 2017-5638로 알려진 취약점을 악용해 거대 신용 조사 기관의 고객 분쟁 해결 포털에 침입했습니다. 내부로 침입한 후 무려 76일간 회사 시스템에 체류하며 자유롭게 이동했습니다. GAO 보고서는 이와 같은 자유로운 측면 이동이 가능했던 이유로 세그멘테이션의 부족을 꼽았으며, 이로 인해 데이터베이스에 쉽게 접속하면서 공격표면이 거의 무제한 노출되었다고 분석했습니다.

문제는 이러한 세그멘테이션을 어떻게 하면 가장 효과적이고 효율적이며 경제적으로 달성할 것인가입니다. 지금까지 운영자들은 기존의 방화벽이나 VLAN에 의존해 멀티 테넌트 또는 멀티 유저 아키텍처 내에서 환경을 분리해 왔습니다. 그러나 이러한 보안 조치를 구축하고 유지하는 작업은 보통 매우 복잡하고 수동적이며 시간과 비용이 많이 소요됩니다. 게다가 이러한 보안 기술은 기밀성을 보장하지 않기 때문에 공격표면이 상당히 노출될 수 있습니다. 경계 방어를 위해 설계된 솔루션의 효율성은 특히 데이터 센터 내에서 문제가 됩니다. 데이터 센터의 환경은 대부분 다양한 가상 머신, 하이퍼바이저, 컨테이너, 클라우드 구성요소를 포함하고 있으며 워크로드 크기가 동적으로 자동 조절되기 때문입니다. 또 다른 중요한 점은 VLAN을 사용해 세그멘테이션하는 경우 애플리케이션을 중단해야 하는데, 이는 주요 운영 제어에 큰 걸림돌이 될 수 있습니다.

이 모든 것이 공유 환경의 운영자가 마이크로세그멘테이션을 포함한 최신 소프트웨어 정의 세그멘테이션 기술에 주목하는 이유입니다. 마이크로세그멘테이션 기술의 발전으로 모든 종류의 기업이 기술을 활용할 수 있게 되었고, 이는 아마도 제로 트러스트 보안 모델을 달성하기 위한 최적의 기술일 것입니다. 마이크로세그멘테이션은 올바른 툴과 약간의 신중한 계획이 뒷받침된다면 앞서 언급한 방법보다 더 빠르고 쉽게 구축할 수 있으며 유지 관리도 더 쉽습니다. 실제로 최근 테스트에서 마이크로세그멘테이션은 기존 방화벽에 비해 최대 30배 더 빨리 배포할 수 있다는 사실이 입증되었습니다. 또 하나의 중요한 이점은 다음과 같습니다. 소프트웨어 정의 세그멘테이션은 네트워킹 변경이나 애플리케이션 가동 중단이 필요하지 않습니다. 이러한 시간 절약 효과와 효율성이 배포 라이프사이클 전반의 비용을 크게 절감해 줍니다.

기존 접근 방식의 위험

소프트웨어 정의 세그멘테이션 또는 마이크로세그멘테이션의 이점을 이해하려면 온프레미스와 클라우드 모두에서 사용되는 표준 기술의 단점과 한계를 비교하며 살펴보는 것이 좋습니다. 여기에는 물리적 방화벽이나 가상화된 방화벽, VLAN과 같은 네트워크 설정의 조합이 포함될 수 있습니다. 일반적으로 이 방법은 리소스 및 노동 집약적입니다. 보안 정책을 생성하는 과정도 꽤 번거롭습니다. 수동으로 추가하고 수정해야 하기 때문에 취약점 리스크가 증가하고 지속적인 운영 효율성을 저해할 수 있습니다.

특히 내부 방화벽은 구입 비용이 높고 설정이 복잡합니다. 또한 정상적인 트래픽 흐름을 방해해 패턴을 변경하고 시스템 성능을 저하시킬 수 있는 소위 '헤어핀'과 같은 우회 경로를 생성합니다. 업계에서는 방화벽이 데이터 센터 내 세그멘테이션을 위해 설계되지 않았다는 점을 깨닫기 시작했고, 공급업체들도 방화벽이 데이터 센터에 적합하지 않다는 사실을 곧 인정하게 될 것입니다.

가동 중인 기존 프로덕션 환경에 세그멘테이션을 도입할 때 가장 어려운 과제 중 하나는, 기존 방식의 경우 애플리케이션의 가동 중단이 필요하다는 것입니다. 가동 중단에는 많은 비용이 소모됩니다. 특정 기간에만 가능할 뿐만 아니라, 아예 불가능할 때도 많습니다.

또 다른 문제는 내부 세그멘테이션을 구축할 때 동서 애플리케이션 의존성에 대한 충분한 정보가 필요하다는 점입니다. 이러한 인사이트를 확보하고 있는 기업은 거의 없습니다. 애플리케이션 의존성을 간단히 매핑할 수 없다면, 개선이 필요한 기존 환경을 분리하는 작업이 매우 어렵고 위험해질 것입니다.

소프트웨어 정의 세그멘테이션이 더 효과적인 이유

운영 효율성, 더 강력한 보안 체계: 소프트웨어 정의 세그멘테이션은 기존 기술의 비효율성을 극복하고, 특히 다중 사용자 환경의 보안을 강화합니다. 이름에서 알 수 있듯이 소프트웨어 정의 세그멘테이션은 네트워크 세그멘테이션의 개념을 가져와 인프라 변경 없이 세그멘테이션을 구축합니다. 이 과정에서 하이브리드 데이터 센터 내 상주 위치와는 상관없이 개별 애플리케이션 또는 논리적으로 그룹화된 애플리케이션을 중심으로 보안 정책을 수립합니다. 이러한 정책은 서로 통신할 수 있는 애플리케이션과 통신할 수 없는 애플리케이션을 지정함으로써 진정한 제로 트러스트 모델을 지원합니다.

수동 변경이나 가동 중단 없음: 소프트웨어 정의 세그멘테이션은 네트워크를 변경하거나 VLAN을 생성할 필요가 없기 때문에 운영 비용이 크게 절감됩니다. 또한 새 VLAN으로 전환하므로 애플리케이션 가동 중단이나 변경이 필요하지 않습니다. 이것은 중요한 이점입니다. 마이크로세그멘테이션은 가동 중단이 불가능하거나 매우 높은 비용이 드는 많은 애플리케이션에 중요한 보안 조치를 구축할 수 있는 유일한 방법이기도 합니다.

광범위한 가시성: 이와 더불어 동서 트래픽 세그멘테이션 문제를 해결하도록 설계된 고급 소프트웨어 정의 세그멘테이션 솔루션은 세그먼트 경계 및 애플리케이션 의존성을 파악하는 데 유용한 통합 가시성 툴을 제공합니다. 이를 통해 프로세스의 효율성을 높이고 정책 생성 시 운영 오류를 방지할 수 있습니다.

정책 및 제어 자동화: 소프트웨어 정의 세그멘테이션을 구축하면 동적으로 정책을 적용할 수 있으므로 워크로드가 감소하거나 증가할 때 적절한 정책이 자동으로 적용됩니다. 수동으로 이동하거나 추가 또는 변경할 필요가 없으므로 상당한 리소스가 절약됩니다.

모든 인프라 지원: 소프트웨어 정의 세그멘테이션의 주요 이점은 인프라로부터 독립적이라는 점입니다. 동일한 툴이 베어 메탈, 가상화, PaaS, 클라우드, 컨테이너 등에서 가시성과 세그멘테이션을 지원하므로, 단일 워크플로우로 단일 창에서 모든 정보를 확인할 수 있습니다. 따라서 기본 인프라로 무엇을 선택하든 제약 없이 보안 표준을 달성할 수 있는 운영상의 자유가 크게 강화됩니다.

매출 증대, 보다 긴밀한 관계 구축: 가장 중요한 점은 데이터 센터 운영자에게 중요한 기회를 제공한다는 것입니다. 운영자는 내부 세그멘테이션을 관리하고 제공하며 교육, 툴, 프로세스를 활용해 호스팅된 애플리케이션뿐만 아니라 고객 온프레미스나 클라우드에 있는 애플리케이션의 세그멘테이션을 관리함으로써 고객에게 절실히 필요한 매니지드 서비스를 제공할 수 있습니다. 이 모두가 하나의 툴, 단일 창 안에서 가능합니다. 이로 인해 추가적인 매출 기회가 생기고 운영자에 대한 의존성이 강화되어 보다 장기적인 관계를 구축하고 수익을 높일 수 있습니다.

Akamai를 선택하는 이유

이러한 이점을 실현하려면 소프트웨어 정의 세그멘테이션 솔루션이 여러 가지 필수 기준을 충족해야 합니다. 또한 컴퓨팅 환경에서 실행되는 모든 애플리케이션에 대한 프로세스 수준의 심층적인 가시성과 애플리케이션 간 모든 데이터 흐름을 매핑할 수 있는 기능을 제공해야 합니다. 정책 생성을 위해 자산에 적절하게 레이블을 지정하고, 워크로드 크기가 자동으로 조정될 때 레이블도 자동으로 수정할 수 있는 유연성도 효율적인 배포 및 관리의 핵심입니다. 또한 플랫폼과 인프라에 구애받지 않는 솔루션이 필요합니다. 정책은 각각의 애플리케이션을 따르고 여러 환경에서 일관된 성능을 유지할 수 있어야 합니다. 마지막으로 정책 생성, 관리 및 적용을 위해 자동화되고 간소화된 운영 모델을 지원하는 솔루션이 필요합니다.

이 모든 기준을 충족하는 솔루션은 오직 Akamai Guardicore Segmentation뿐입니다. 소프트웨어 정의 세그멘테이션은 Akamai의 핵심 역량입니다. Akamai 솔루션은 베어 메탈, 가상 머신, 퍼블릭 클라우드, 컨테이너 또는 IoT 디바이스 등 환경의 모든 자산과 이들 자산의 의존성에 대한 매우 뛰어난 시각 정보를 제공합니다. 이러한 심층적인 가시성을 바탕으로 애플리케이션의 마이크로세그먼트에 대한 보안 정책을 식별, 그룹화 및 생성하는 프로세스를 크게 가속할 수 있습니다.

자세한 내용은 akamai.com/guardicore에서 확인하실 수 있습니다.