Akamai

백서

방화벽 재검토

소프트웨어 기반 세그멘테이션이 필요한 흥미로운 경제 사례

핵심 요약

네트워크 및 보안팀이 내부 네트워크 세그멘테이션을 위해 아직도 레거시 방화벽에 의존하는 이유는 무엇일까요? 정책으로 보호되는 애플리케이션과 세그먼트가 증가하면서 물리적 방화벽 어플라이언스는 오늘날 더 많아진 동적 하이브리드 클라우드 환경의 보안 과제를 해결하기에 너무 복잡하고 유연성이 떨어지며 비효율적이라는 점이 드러났습니다. 게다가 팀에서 가능한 것보다 훨씬 더 비용이 많이 듭니다. 방화벽과 하드웨어의 엄청난 초반 비용은 제쳐두고 프로젝트 관리, 인력, 유지 관리에 드는 상당한 고가의 다운스트림 비용과 긴 구축 시간으로 인해 자산이 장기간 노출되는 실질적인 리스크가 뒤따릅니다. 오늘날 기업이 민첩한 DevOps, 신속한 애플리케이션 배포 및 클라우드의 이점을 활용하려면 세그멘테이션을 통해 중요한 자산을 안전하게 보호하는 더 나은 방법이 필요합니다. 소프트웨어 기반 세그먼테이션이 해답이 될 수 있습니다. 이 백서에서도 설명하겠지만, 소프트웨어 기반 세그먼테이션은 보다 쉽고 빠르며 효율적입니다. 또한 기존의 세그멘테이션 방법보다 훨씬 더 낮은 총소유비용으로 최적의 보안을 제공합니다.

서론

오늘날 세 가지 요소가 수렴하며 네트워크와 개별 자산을 세그멘테이션하는 보다 정밀한 수단을 요구하고 있습니다. 첫 번째는 민첩한 DevOps 및 기타 빠른 전송 모델은 프로덕션 환경으로의 빠른 애플리케이션 배포를 중요하게 생각합니다. 이 때문에 보다 정확한 정책을 사용해 보다 안전한 영역을 만들어야 합니다. 두 번째는 기업이 클라우드로 전환하고 하이브리드 IT 인프라를 도입함에 따라 애플리케이션이 서로 다른 여러 환경 사이에서 전환되기도 하면서 이로 인해 네트워크 전체에서 세그먼트 간 트래픽이 증가했습니다. 세 번째는 민첩한 개발로 인해 애플리케이션이 급속히 늘어나자 해커가 표적으로 삼을 수 있는 공격표면이 늘어났습니다.

세그멘테이션을 위한 방화벽: 과거의 빛바랜 영광

이러한 상황에서 세그멘테이션을 위해 VLAN 및 방화벽에만 의존하는 방식은 더는 지속 가능하지 않습니다. 기술적인 측면에서만 봤을 때 애플리케이션 개발에 보조를 맞추는 방식으로 여러 VLAN과 방화벽 설치를 설정하는 작업은 복잡하고 번거롭습니다. 또한 노동 집약적 작업이어서 많은 팀원이 우선순위가 높은 보안 프로젝트에서 이탈할 수 있습니다. 배포 시간은 또 다른 문제이며 자산 노출 장기화와 취약점이라는 리스크를 유발합니다. 무엇보다 추가 트래픽을 지원하기 위한 방화벽과 새 하드웨어의 초반 비용뿐 아니라 설치의 지속적인 관리, 수정 및 유지 관리에서 발생하는 관련 비용 때문에 구축 비용도 매우 많이 듭니다.

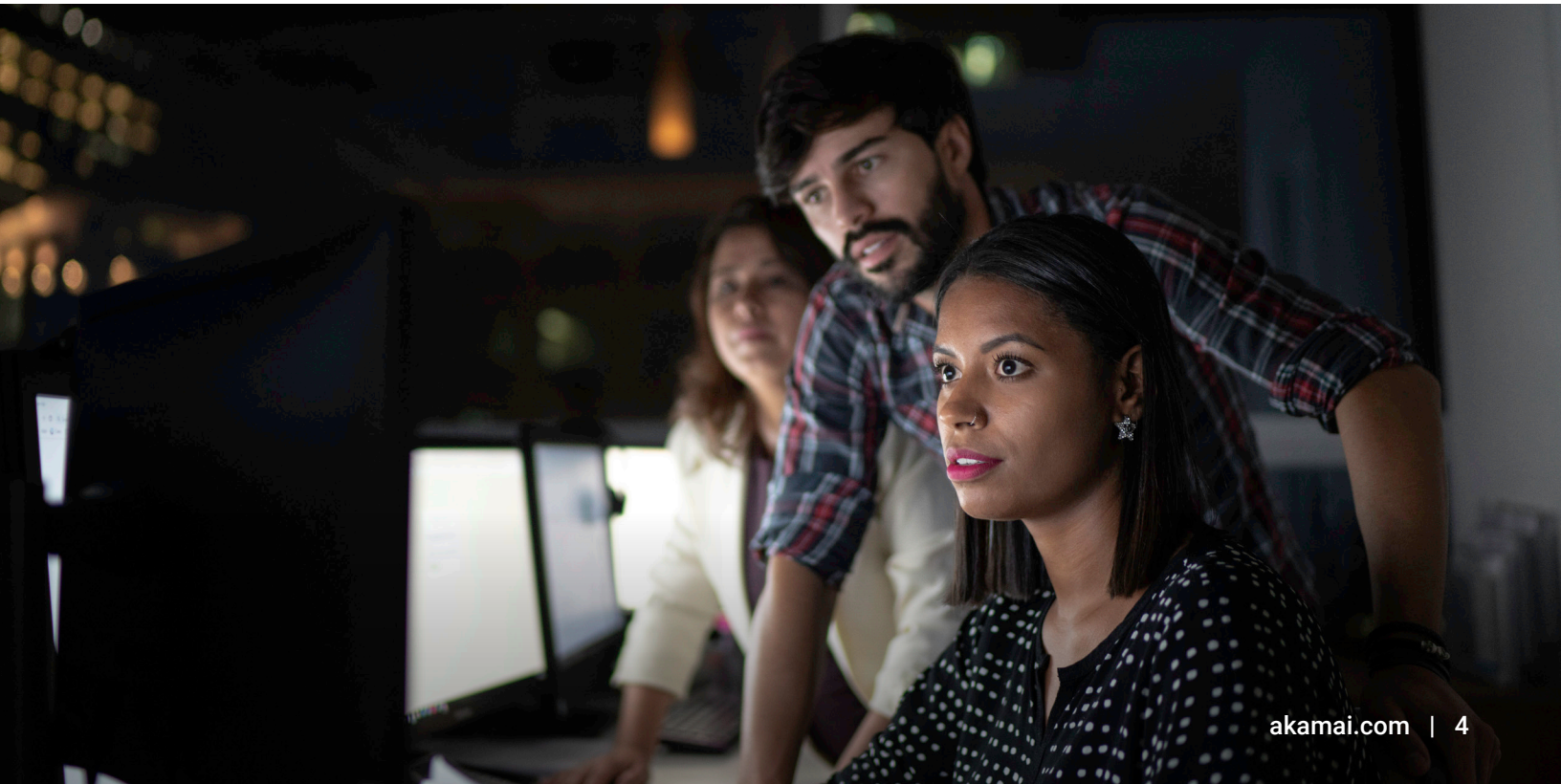
한마디로 기존의 네트워크 세그멘테이션 접근 방식으로는 한계에 직면했습니다. 특히 기업이 동적 클라우드 및 하이브리드 환경을 활용하려는 경우 보안을 위해 내부 방화벽에 의존하는 방식으로는 민첩성, 정책 생성 및 적용 속도, 운영 환경을 안전하게 확장하는 역량이 제한됩니다. 레거시 방화벽의 대안으로 간소화되고 비용이 적게 들며 궁극적으로 보다 효과적인 최신 세그멘테이션 방식이 그 어느 때보다도 절실합니다. 소프트웨어 기반 세그멘테이션의 시대가 온 것입니다.

레거시 방화벽의 대안으로 간소화되고 비용이 적게 들며 보다 효과적인 최신 세그멘테이션 방식이 그 어느 때보다도 절실합니다.

고충 - 많은 비용이 소요되는 방화벽 관리 작업

소프트웨어 기반 세그멘테이션의 이점을 자세히 살펴보기 전에 현재 상황과 비교해보는 것이 좋습니다. 기업이 성장함에 따라 애플리케이션 수와 관련 데이터 트래픽 양도 증가하면서 추가 네트워크 세그먼트와 보다 복잡한 보안 정책에 대한 수요가 증가하고 있습니다. 방화벽으로 보호되는 VLAN에 의존하는 경우 세그먼트 간 트래픽이 이동하는 모든 스위치 트렁크 포트에 새로 배포된 VLAN을 각각 추가해야 합니다. 그리고 이 모든 새 VLAN에 대해 IP 서브네트워크도 생성해야 합니다. 방화벽에 대한 하위 인터페이스도 만들어야 합니다. 그런 다음, 방화벽 정책을 만들어야 합니다. 보통 이러한 모든 변경에는 승인 및 유지 관리 기간이 필요하고 가동 중단 가능성도 있으므로 네트워크 중단 리스크가 증가합니다.

VLAN과 방화벽을 추가하려면 각각 스위칭, 라우팅, 방화벽 구축, ESXi 서버 및 보안 정책 생성을 담당하는 5개 팀이나 참여하는 번거로운 다단계 프로세스를 거쳐야 합니다. 결국 이 모든 작업이 구축 시간을 늘리고 기업을 장기간 리스크에 노출시키며 소프트웨어 및 하드웨어 비용과 인건비를 증가시킵니다. 또한 엔지니어의 관점에서 봤을 때 이 작업은 리스크가 높고 보상이 적습니다. 즉, 드는 노력에 비해 보상이 적어 다른 우선순위가 높은 리스크 관리 활동에서 시간과 리소스를 이탈하게 만듭니다. 안타깝게도 방화벽 VLAN 환경 내에서 변경 관리 프로세스에서 자동화에 적합한 단계는 매우 적습니다.



해결책 - 소프트웨어 기반의 간단한 3단계 세그멘테이션

레거시 경계 방화벽 기술은 정밀한 내부 세그멘테이션의 보다 정밀하면서도 대역폭을 제한하는 요구에 적합하지 않습니다. 최근 몇 년 사이에 소프트웨어 기반 세그멘테이션은 오늘날의 동적 환경에서 보다 긴밀하게 연결된 네트워크 세그먼트에 대한 수요를 충족시키기 위한 실용적이면서 빠르고 효과적이며 저렴한 대안으로 부상했습니다. 소프트웨어 기반 세그멘테이션 구축의 핵심은 기존 네트워크 방화벽 어플라이언스보다 훨씬 더 민첩하고 관리하기 쉬운 '분산 방화벽'의 개념입니다.

> 소프트웨어 기반 세그멘테이션은 기존 방화벽에 비해 배포 속도가 **10배, 심지어 20배까지 더 빠르며** 필요한 인원도 적고 가동 중단이나 장애도 거의 발생하지 않습니다.

소프트웨어 기반 세그멘테이션 솔루션의 대표적인 예로, Akamai Guardicore Segmentation이 있습니다. 오래 걸리고 복잡한 고가의 VLAN 방화벽 구축 프로세스와 비교했을 때, Akamai의 소프트웨어 기반 세그멘테이션 솔루션은 3단계로 충분합니다.

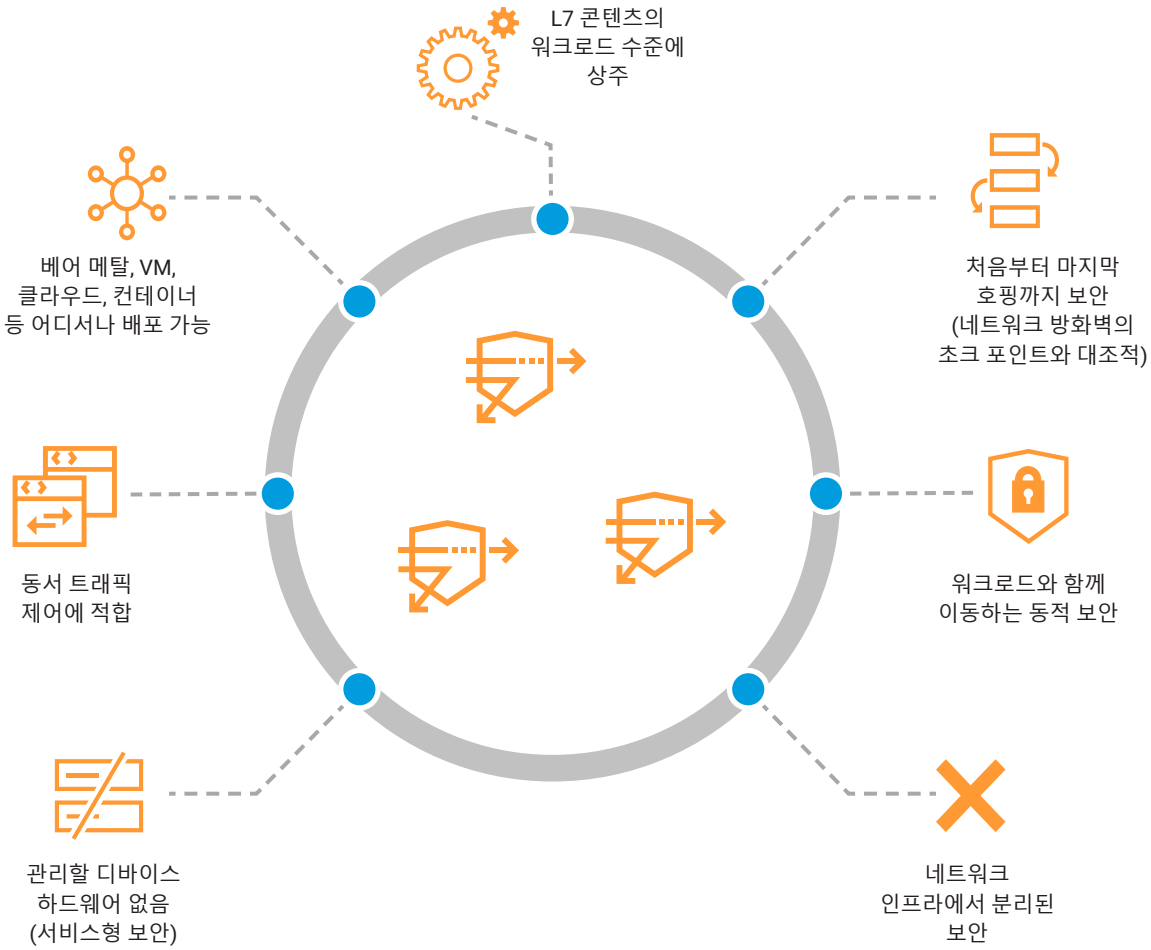
1. **자산 식별 및 레이블링:** 기존 방화벽 구축 프로세스 중에 발생하는 주요 장애 요소는 보안이 필요한 자산에 대한 가시성이 부족하다는 점입니다. Akamai Guardicore Segmentation에는 운영자가 기업 인프라 전체에서 실행되는 모든 애플리케이션과 의존성을 식별하고 레이블링할 수 있게 지원하는 시각화 기능이 포함되어 있습니다.

2. **레이블별 시각화 및 그룹화:** 그러면 운영자는 맥락에 맞는 가시성을 바탕으로 해당 레이블에 따라 애플리케이션을 논리적 그룹으로 구성하고 애플리케이션 사이에서 의존성을 매핑할 수 있습니다. Akamai의 레이블링 프로세스는 매우 유연해서 이미 익숙한 용어를 사용해 기업의 비즈니스 맥락에 따라 애플리케이션을 그룹화할 수 있습니다.

3. **정책 생성:** 그러면 운영자는 관찰된 실제 흐름에 따라 어떤 애플리케이션이 서로 통신할 수 있는지 결정하는 정밀한 보안 정책을 생성할 수 있습니다. 일반적인 사용 사례용으로 사전 구축된 정책 템플릿을 사용하면 프로세스가 더욱 간소화됩니다. 이제 애플리케이션 및 워크플로우는 환경에서 어디에 있든 효과적으로 세그멘테이션됩니다.

소프트웨어 기반 세그멘테이션은 기존 방화벽에 비해 구축 속도가 10배, 심지어 20배까지 더 빠르며 필요한 인원도 적고 가동 중단이나 장애도 거의 발생하지 않습니다. 또한 시각화 및 세그멘테이션 프로세스를 시작한 후에는 레이블을 기반으로 네트워크를 쉽게 분할하거나 다른 정책을 추가하고 프로세스를 자동화하며 보안 인시던트를 해결하고 비즈니스 또는 규정 요구사항에 따라 신속하게 변경할 수 있습니다.

분산 방화벽의 장점



사례 연구: 세그멘테이션으로 85%의 비용을 절감한 대형 식품 가공업체

미국의 주요 돼지고기 가공업체 중 한 곳은 두 곳에 배포된 45개의 애플리케이션에 대해 애플리케이션당 평균 5대의 서버로 애플리케이션을 세그멘테이션해야 했습니다. 이 회사의 목표는 서비스 중단을 최소화하면서 플랫 네트워크를 없애고 가능한 한 빨리 정책을 수립하는 것이었습니다.

회사는 여러 대안을 검토한 후 Akamai의 소프트웨어 기반 세그멘테이션 솔루션을 선택했습니다. 구축 속도와 간소함 때문에 Akamai의 솔루션을 선택했지만, 주요 방화벽 공급업체를 통해 VLAN을 보호하는 방식에 비해 3년 동안 90만 달러(85%) 이상의 비용 절감 효과를 보여주는 분석이 결정적인 요인이 되었습니다. 예를 들면 다음과 같습니다.

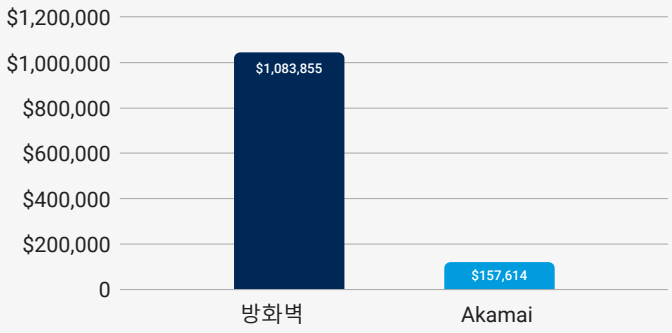
- Akamai Guardicore Segmentation의 라이선스 비용은 VLAN 방화벽 구축에 드는 하드웨어 비용보다 55% 더 저렴합니다.
- 인건비 측면에서 주당 2천 달러를 가정할 때 Akamai가 기간이 훨씬 긴 VLAN 프로젝트보다 93% 더 저렴합니다.

또한 Akamai는 불과 6주 만에 45개의 애플리케이션을 중단 없이 안전하게 보호함으로써 고객의 빠른 정책 구축 요구도 충족했습니다.

방화벽 총소유비용(TCO)*
$1,083,855

Akamai 총소유비용(TCO)*
$157,614
-$926,241

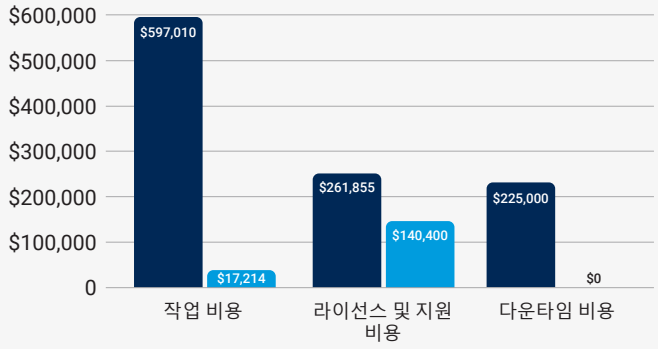
* 3년간 비용



Akamai 작업 비용*
$17,214
-$579,796

Akamai 라이선스 및 지원 비용*
$140,400
-$121,455

Akamai 가동 중단 비용*
$0
-$255,000



종합적 의미

소프트웨어 기반 세그멘테이션은 기존 방화벽 방식에 비해 세 가지 주요 이점을 제공합니다.

보다 효과적인 리스크 감소: 매우 정밀한 수준에서 애플리케이션을 빠르게 세그멘테이션함으로써 소프트웨어 기반 세그멘테이션은 공격표면을 크게 줄일 수 있습니다. 네트워크 자산에 접속하려는 모든 사용자, 디바이스 또는 애플리케이션에 대해 엄격한 인증을 요구하는 제로 트러스트 원칙을 활용하는 소프트웨어 기반 세그멘테이션은 데이터 센터 또는 네트워크 환경 내에서 위협의 측면 이동을 방지합니다. 더 나아가 데이터 유출 영향을 방어하며 공격자가 경계 방어를 뚫었다 하더라도 어떠한 프로세스에도 침투할 수 없게 합니다. 또한 기업은 중요하고 민감한 애플리케이션을 일반 네트워크 트래픽으로부터 별도로 격리해야 하는 규정을 보다 빠르게 준수할 수 있습니다.

빠른 속도로 최적의 보안 체계 구축: 즉, 소프트웨어 기반 세그멘테이션을 보안팀이 민첩한 DevOps 애플리케이션 배포 속도를 따라잡고 프로덕션 환경의 모든 애플리케이션을 적절히 보호함으로써 보다 안전하고 신속하게 비즈니스를 운영할 수 있습니다. 또한 세그멘테이션 프로젝트에서 기술 또는 인적 리소스가 묶이는 기간도 줄어든다는 점을 의미합니다. 대신 팀은 다른 중요한 이니셔티브에 시간을 집중할 수 있습니다.

상당한 총소유비용 절감: 이는 실제 수익에 해당하며, 비즈니스 관점에서 가장 중요한 이점일 수도 있습니다. 소프트웨어 기반 세그멘테이션은 방화벽 어플라이언스 및 추가 하드웨어 구매와 비교했을 때 훨씬 적은 소프트웨어 솔루션의 자본 지출(CapEx)을 지원할 수 있습니다. 또한 시간이 지남에 따라 지속적인 유지 관리 및 관리에 필요한 인력 및 리소스가 줄어들어 운영 비용(OpEx)이 크게 낮아집니다.

이 수치만으로도 10개 애플리케이션 세그먼트에 대한 소프트웨어 기반 세그멘테이션과 방화벽 솔루션을 나란히 비교했을 때 Akamai의 접근 방식은 잠재적으로 85%의 총 비용 절감 효과를 달성했으며, 이는 약 1백만 달러에 해당합니다.

물론 배포 첫 주부터 수치상으로 상당한 절감 효과를 기대할 수 있지만, 총소유비용(TCO)은 초기 구매 가격이나 지속적인 사후 정산 비용보다 더 많은 의미를 내포합니다. 소프트웨어 기반 세그먼테이션의 경우 전체 가격표를 쉽게 파악하지 못할 수도 있지만 가동 중단 시간과 서비스 장애를 사실상 거의 없앰으로써 상당한 비용 절감 효과를 제공합니다. 또한 기업은 데이터 유출로 인한 재정적 손실과 규정 미준수로 인한 벌금을 피할 수 있습니다. 유출로 인한 평판 훼손 및 비즈니스 손실 리스크도 크게 줄어듭니다. IT팀과 리소스를 방화벽 변경 관리에서 보다 생산적인 프로젝트로 재배치할 수 있습니다. 이러한 모든 비용 요소는 소프트웨어 기반 세그멘테이션 솔루션을 선택하는 기업에 보다 낮은 TCO와 강력한 수익의 이점을 제공합니다.

사례 연구: 컴플라이언스 제재에 직면한 대형 글로벌 은행의 Akamai Guardicore Segmentation 채택

플랫 네트워크의 보안 리스크가 드러난 감사 결과에 따라, 보다 엄격한 세그멘테이션을 요구하는 새로운 규정 단체에 대처해야 했던 유럽의 한 주요 금융 기관은 VLAN과 방화벽 룰을 사용해 세그멘테이션 프로젝트를 시작했습니다. 그러나 프로젝트가 상당히 길어지면서 여러 관계자와 팀을 투입해야 했고 이로 인해 프로덕션 가동 중단이 발생했을 뿐 아니라 정책의 모호성이 드러났습니다. 그 결과, 은행은 감당하기 어려운 높은 구축 비용 외에도 규정 미준수에 대한 벌금을 지불해야 했습니다.

IT 팀은 신속하게 대체 솔루션을 모색했고, Akamai가 회사의 보안 운영에 제공할 수 있는 자동화 수준에 감명을 받았습니다. 은행은 여러 지역 및 IT 인프라 종류에 걸쳐 Akamai Guardicore Segmentation을 배포했습니다. 프로젝트는 3개월도 채 걸리지 않았습니다. 기존의 세그멘테이션 방법보다 10배나 빠른 속도였습니다. 은행은 보안 체계를 업그레이드했을 뿐 아니라 1만 개 이상의 자산에 대한 컴플라이언스 요구사항도 이행했습니다. 신속한 배포로 리스크 완화 속도가 가속되었고 이와 함께 비용 및 내부 리소스도 대폭 절감되었습니다.

대형 글로벌 은행

프로젝트 목표:

Dev/Prod/UAT 분리

프로젝트 범위:

1. 프로덕션 환경과 비프로덕션 환경 간 트래픽 제한
2. 애플리케이션 링펜싱 준비

레거시 세그멘테이션

- 매우 느린 진행 속도
- 감사 실패, 벌금 및 프로덕션 오류
- 애플리케이션 가동 중단으로 프로덕션 중단

시간: 방화벽/VLAN 사용 시 2년

Akamai의 이점

- 1만 개의 규정 미준수 자산 세그멘테이션
- 가동 중단 없는 애플리케이션
- 10배 빠른 구축 속도
- DevOps를 통한 수동 작업 감소

시간: 6개월
인력: 아키텍트 3명

결론: 모든 장점

방화벽은 더 이상 효과적이지 않습니다. 네트워크 경계 보안에는 확실히 적합합니다. 그러나 오늘날 동적 환경에서는 경계가 다소 무정형 상태가 되어가고 있습니다. 기업은 보안과 민첩성 간의 필수적인 균형을 이루기 위해서는 L4 네트워크 수준뿐 아니라 L7 애플리케이션 수준, 특히 개별 프로세스 수준에서 디지털 자산을 보호할 수 있어야 합니다. 방화벽은 이러한 목적에 부적합하며, 실제로 발전의 장애물이 되었습니다. 방화벽을 사용해 정밀한 세그멘테이션을 하려고 하면 인력, 기술, 재무 등에서 낭비되는 리소스가 너무 많습니다.

방화벽과 비교했을 때 소프트웨어 기반 세그멘테이션은 기존 접근 방식에 비해 훨씬 낮은 총소유비용(TCO)으로 보안 리스크와 전반적인 가치 실현 시간을 크게 줄이는 것으로 나타났습니다. 즉, ROI를 더 빠르게 달성할 수 있습니다. 미래의 일이 아닙니다. 소프트웨어 기반 세그멘테이션은 지금 이용 가능하며, 현재 광범위한 부문의 기업이 이러한 이점을 누리고 있습니다.

IT 진화에 대한 연구

기술의 역사는 지속적인 개선, 간소화, 비용 절감을 위한 노력으로 이루어졌습니다. 세그멘테이션도 예외가 아닙니다.

20년 만에 플로피 디스크에서 플래시 드라이브로, NAS(Network Attached Storage)를 거쳐 클라우드 스토리지로 진화한 스토리지를 떠올려 보세요. 컴퓨팅 런타임은 서버에서 가상 머신으로, 클라우드 컴퓨팅에서 컨테이너로, 그리고 궁극적으로는 서버리스 컴퓨팅으로 진화했습니다. 모든 사례에서 주요 동인은 비용 절감과 유연성 향상이었습니다. 물론 기술의 빠른 발전으로 가능했습니다.

물리적 방화벽 어플라이언스에서 네트워크에서 추상화된 소프트웨어 기반 분산 방화벽으로 세그멘테이션이 진화한 것도 이와 비슷합니다. 기본적인 동인은 같습니다. 즉, 비용 절감과 유연성 향상(즉, 배포 속도 향상)과 동시에 제로 트러스트를 지원하는 보다 정밀한 접근 방식으로 보안 정책의 효율성을 지속적으로 개선하기 위함입니다.

네트워크팀 및 보안팀은 다른 기술 분야에서와 마찬가지로 세그멘테이션을 통한 새로운 보안 모델을 도입해야 할 때입니다. 세그멘테이션을 위한 물리적 방화벽은 플로피 디스크와 같이 사양길에 접어들었습니다.

Akamai 솔루션이 실제로 어떤지 알고 싶으신가요?
오늘 데모 요청하기: akamai.com/guardicore