Akamai

e-Book

세그멘테이션 현황

배포 장애물을 극복하는 혁신적인 과정

이커머스 부문

목차

서론

IT 보안팀, 특히 이커머스 기업을 방어하는 팀의 업무는 결코 쉽지 않습니다. 전통적으로 빠듯한 예산과 제한된 보안 리소스로 인해 기업 보안팀은 적은 자원으로 많은 일을 해야 했습니다. 하지만 이제 점점 복잡해지는 인프라 관리와 더불어 강한 동기를 가진 정교한 공격자들이 등장하면서 보안팀은 그 어느 때보다 더 큰 부담을 안고 리스크를 방어해야 합니다. 이커머스 기업은 운영상 성능 좋은 온라인 환경에 의존하기 때문에 랜섬웨어 공격과 같은 유출이 한 번 발생하면 브랜드 평판과 매출에 회복할 수 없을 정도의 막대한 피해를 입을 수 있습니다. 대량 암호화로 인해 중요한 서버와 시스템을 사용할 수 없게 되어 온라인 운영, 주문 처리 또는 프로덕션 라인이 중단되고 데이터 유출을 통한 이중 갈취가 발생할 경우 그 피해를 상상해 보세요.

이커머스 부문 세그멘테이션 현황 보고서의 조사 결과에서 알 수 있듯이, 이러한 공격은 더 큰 영향을 미치고 있으며, 리더들이 성능 저하나 운영 오버헤드 없이 중요한 데이터를 안전하게 보호하는 데 도움이 되는 올바른 툴과 솔루션을 선택해야 할 필요성은 커지고 있습니다. 이 보고서는 이커머스 업계가 전체 설문 조사 응답자 중 랜섬웨어 공격을 가장 많이 받는 업계이며 랜섬웨어 공격을 최대한 빨리 예방, 탐지, 대응해 피해를 최소화하는 것이 시급하다는 점을 강조합니다.

이커머스 부문 기업의 응답자(미국, LATAM, EMEA, APAC 등 모든 지역 대표)들은 IT 자산을 보호하는 데 있어 세그멘테이션의 효과에 대해서는 압도적으로 동의했지만, 중요한 비즈니스 애플리케이션, 서버, 시스템을 중심으로 세그멘테이션을 구축하는 진행 속도는 전반적으로 예상보다 느렸습니다. 이커머스 기업의 주요 장애물은 세그멘테이션을 효과적으로 배포할 수 있는 전문 지식의 부족과 부담스러운 데이터 컴플라이언스 요구사항입니다. 이는 각 팀이 업계에 필요한 인재를 채용하거나 유지하는 데 어려움을 겪고 있을 뿐 아니라 법규 준수를 위해 귀중한 시간을 소비해 이미 부족한 리소스를 더욱 소모하고 있다는 것을 보여줍니다.

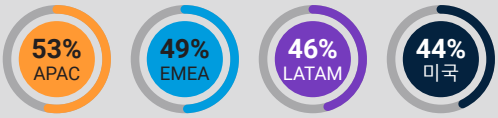
하지만 다행히 인내심을 갖고 올바른 솔루션을 선택하면 성과를 거둘 수 있습니다. 6개의 주요 영역에 걸쳐 대부분의 중요 자산을 성공적으로 세그멘테이션한 기업의 경우, 세그멘테이션이 방어 역량에 혁신적인 효과를 발휘해 하나의 자산만 세그멘테이션한 기업보다 11시간 더 빠르게 랜섬웨어를 방어하고 차단할 수 있었습니다. 이 11시간의 차이가 인시던트에 대응하는 인력 뿐만 아니라 고객과 브랜드 평판에 얼마나 큰 영향을 끼칠지 상상해 보세요.

세그멘테이션은 전반적으로 느리게 진행되었지만, 인내심을 가지고 꾸준히 노력한 기업들은 리스크를 크게 줄였습니다.

세그멘테이션보다 더 효과적인 마이크로세그멘테이션

세그멘테이션은 보안을 개선하고 플랫 네트워크와 관련된 리스크를 줄이기 위해 네트워크를 더 작은 세그먼트로 나누는 아키텍처 접근 방식입니다. 또한, 이커머스 중심 기업이 PCI 컴플라이언스 달성 및 유지의 범위, 비용, 어려움을 줄이는 데에도 사용되었습니다.

마이크로세그멘테이션은 네트워크를 개별 워크로드 또는 프로세스 수준(레이어 7)까지 논리적으로 별개의 보안 세그먼트로 분할하는 소프트웨어 정의 보안 기술입니다. 그러면 레이어 4 제어만 제공하는 기존의 세그멘테이션 방법인 VLAN, ACL, 내부 방화벽과 비교해 고유한 세그먼트별로 보안 제어 및 서비스 제공을 더 정밀한 수준에서 정의할 수 있습니다. 이커머스 응답자의 94%가 기존 방식보다 소프트웨어 기반 세그멘테이션 솔루션을 선호하는 이유도 바로 이 때문입니다.



네트워크 세그멘테이션이 기업의 보안을 유지하는 데 매우 중요하다고 응답한 비율은 APAC의 보안 의사 결정권자가 EMEA, LATAM, 미국보다 높았습니다. LATAM 지역의 보안 의사 결정권자가 마이크로세그멘테이션이 최우선 순위라고 응답한 비율(42%)은 APAC(35%), 미국(34%), EMEA(26%)에 비해 높았습니다.

가장 많은 공격을 받는 이커머스 업계, 랜섬웨어 공격은 계속 증가

지난 12개월 동안 이커머스 기업에서 발생한 랜섬웨어 공격 건수(성공, 실패 모두 포함)는 평균 167건입니다. 이는 평균 랜섬웨어 공격 건수에서 이커머스 업계가 1위를 차지했을 뿐만 아니라, 2위(건설 업계 평균 89건)의 약 2배에 달하는 수치입니다.

사이버 공격자들은 미국 내 이커머스 기업을 표적으로 삼을 가능성이 더 높습니다. 미국의 랜섬웨어 공격 건수는 지난 12개월 동안 평균 312건으로 모든 지역 중 가장 높았으며, APAC 119건, EMEA 91건, LATAM 68건과 비교했을 때 가장 높은 수치를 기록했습니다(그림 1).

지난 12개월 동안 이커머스 기업에서 발생한 랜섬웨어 공격의 지역별 평균 건수

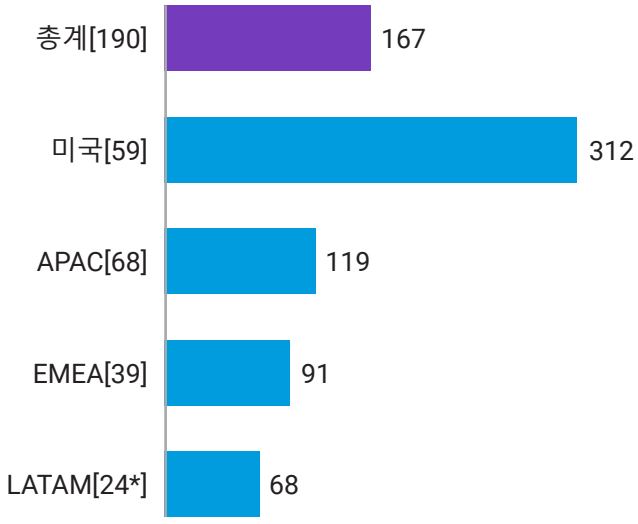


그림 1: 지난 12개월 동안 공격의 성공 여부와 무관하게 얼마나 많은 랜섬웨어 공격을 받으셨나요? 이 차트는 지난 12개월 동안의 평균 공격 건수를 지역별로 구분해 이커머스 부문 데이터만 보여줍니다.

* 주의 - 30개 미만의 낮은 기본 규모

미국 외 지역의 평균이 낮다고 할 수는 없지만, 미국을 겨냥한 공격 건수에 비하면 매우 적은 수치입니다. 세계 최대의 경제 대국인 미국은 랜섬웨어 조직의 가장 많은 표적이 되는 국가이며, 공격자들은 다른 영어권 및 서구 국가를 자주 표적으로 삼습니다. 지정학적 동기도 가장 큰 타격을 받는 국가와 부문에 영향을 미칩니다. 이커머스 기업은 전통적으로 금융 서비스 등 다른 업계에 비해 보안 성숙도가 낮아 더 쉬운 공격 표적이 됩니다. 공격자는 특히 공휴일, 축제, 스포츠 이벤트, 신학기 또는 기타 쇼핑 성수기와 같은 중요한 매출 창출 기간에 랜섬웨어 공격이 성공하면 운영 중단으로 인한 대가를 받게 될 가능성이 높아진다고 생각하기 때문에 기업의 부담이 가중될 수 있습니다.

이커머스 기업이 랜섬웨어 공격의 표적이 되는 경우가 많음에도 불구하고 세그멘테이션 구축 수준은 실망스러운 수준입니다. 이커머스 기업의 11%만 두 개 이상의 영역을 세그멘테이션했으며, 이는 모든 지역에서 대체로 일관된 수치입니다. 이는 이러한 기업 중 상당수가 문제와 공격이 발생했을 때 이를 처리하는 데 필요한 리소스에 한계가 있을 수 있음을 나타냅니다.

이커머스 부문의 랜섬웨어 공격은 비즈니스에 막대하고 즉각적인 영향을 미칠 수 있으며(그림 2), 응답자들은 금전적 손실과 평판 손상을 지적하며 이커머스 기업의 보안팀이 큰 부담을 안고 있다고 답했습니다. 또한, 보험료가 증가했다고 답한 응답자의 비율도 증가했습니다. 이는 재고 또는 창고 보관과 관련된 물류 문제와 관련된 리스크 외에도 개인 및 쇼핑 습관에 대한 개인 데이터를 보유하고 있는 이커머스 기업이 감당할 수 있는 리스크의 수준을 보여줍니다.

영향은 지역마다 다를 수 있습니다. APAC 응답자들은 특히 금전적 손실을 강조하는 비율이 절반 이상(51%)으로 전체 평균인 42%에 비해 높았습니다. 반면, 미국 응답자들은 네트워크 다운타임을 가장 많이 언급했는데, 전체 평균 39%에 비해 절반에 가까운 응답자(49%)가 다운타임을 언급했습니다. EU 응답자들은 직원 사기 저하를 영향이라고 답한 비율이 41%로, 전체 36%에 비해 더 높았습니다.

이러한 압박은 전략 측면에도 영향을 미칩니다. 랜섬웨어뿐 아니라 끊임없이 변화하는 공격 표면에 대응하기 위해 사이버 보안 전략이나 정책을 지속적으로 업데이트하는 이커머스 기업의 수가 2021년 3%에서 2023년 13%로 증가했습니다. 워크로드가 클라우드로 전환됨에 따라 인프라의 복잡성이 증가하는 것은 매일 보안 전략과 보안팀에 영향을 미치는 리스크 요소 중 일부에 불과합니다.

랜섬웨어/사이버 공격이 이커머스 기업에 미치는 영향

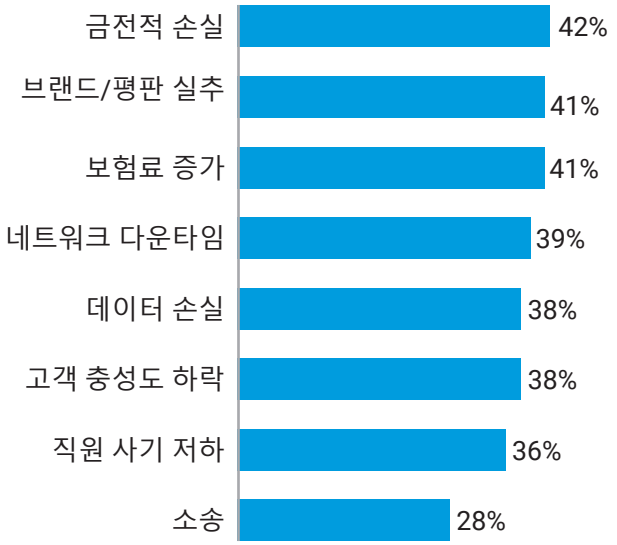


그림 2: 이전에 랜섬웨어나 기타 사이버 공격을 탐지한 적이 있나요? 만약 있다면 이것이 기업에 어떤 영향을 미쳤나요? 차트에는 모든 답변 옵션이 표시되지 않고 이커머스 부문 데이터만 표시됩니다.

제로 트러스트의 중요한 부분으로 널리 인식되고 있는 세그멘테이션

응답자들은 세그멘테이션이 기업의 보안을 유지하는 데 중요하며, 특히 멀웨어 대응에 중요하다는 데 동의했습니다.

거의 절반(48%)이 세그멘테이션이 매우 중요하다고 답했으며, 89%는 세그멘테이션이 피해를 주는 공격을 방어할 때 매우 중요하다고 생각한다고 답했습니다.

또한, 세그멘테이션은 제로 트러스트 보안 프레임워크의 초석으로 인정받고 있으며, 이커머스 기업에 좋은 소식은 이 분야에서 이미 진전이 이루어졌다는 것입니다. 모든 기업이 제로 트러스트 보안 프레임워크를 배포 중이거나 이미 배포한 적이 있다고 응답했지만(100%), 5곳 중 2곳(42%)만이 제로 트러스트 프레임워크가 완전히 완성되고 정의되어 성숙 단계에 접어들었다고 답했습니다. 따라서 이커머스 기업은 세그멘테이션을 통해 제로 트러스트 여정을 발전시켜 나갈 수 있습니다. 데이터에 따르면, 미국의 기업들은 제로 트러스트 보안 프레임워크 배포에 있어 훨씬 더 성숙한 것으로 나타났습니다. 제로 트러스트 배포가 완전히 완료되고 정의되었다고 응답한 비율(63%)이 LATAM(46%), APAC(32%), EMEA(23%)에 비해 훨씬 더 높았습니다.

네트워크 세그멘테이션 프로젝트를 시작한 이유는 지역별로 크게 달랐으며, 사이버 보안에 대한 정부의 관심이 41%로 가장 높았습니다. LATAM과 EU 내 국가 모두 세그멘테이션 이니셔티브를 추진하게 된 가장 큰 동기로 유명한 제로데이 취약점을 꼽았습니다(각각 44%, 42%). 그러나 EU의 응답자들은 모범 사례이기 때문에 프로젝트를 시작했다고 답한 비율이 훨씬 더 높았습니다(전체 22%에 비해 41%로 높음). 반면 미국과 APJ 응답자들은 자국 정부가 사이버 보안에 중점을 두고 있기 때문에 프로젝트를 시작했다는 응답이 더 높았습니다(전체 35%에 비해 각각 41%와 39%로 높음). 또한, APJ 응답자들은 중요 애플리케이션을 클라우드로 이전하는 것이 프로젝트를 시작하게 된 이유라고 답한 비율이 더 높았습니다(전체 32%에 비해 39%로 높음).

이커머스 기업의 응답자 대다수는 한 걸음 더 나아가 애플리케이션 워크로드를 정밀한 수준으로 보호하는 마이크로세그멘테이션을 구축하고자 합니다. 92%는 마이크로세그멘테이션이 적어도 높은 우선 순위라고 답했으며, 34%는 마이크로세그멘테이션을 최우선 순위로 꼽았습니다. 게다가, 이 분야의 모든(100%) IT 및 보안 의사 결정권자는 마이크로세그멘테이션이 적어도 소수의 업계에서 도입되었다고 답해, 현재까지 진전이 제한적이긴 하지만 최소한 모두가 폭넓게 인식하고 있는 솔루션임을 강조했습니다.

응답자들은 기업의 IT 환경 전반에 대한 가시성을 확보하는 것이 필요하다고 답했습니다. 리스크를 줄이기 위해 네트워크 통신, 자산 위치 등에 대해 '훨씬 더 많은' 가시성(63%)이 필요하다는 응답이 LATAM에서 가장 많았고, 다음으로 APAC(56%), 미국(46%), EMEA(44%)가 뒤를 이었습니다.

배포에 시간이 걸리더라도 인내심을 갖고 지속하면 혁신적인 결과에 도달

안타까운 현실은 세그멘테이션이 IT 자산을 보호해 공격을 차단하는 핵심이라는 점에 광범위하게 동의하고 있음에도 불구하고, 세그멘테이션 배포가 예상보다 느리게 진행되고 있다는 점입니다.

이커머스 기업 중 11%만 두 개 이상의 중요 비즈니스 영역을 세그멘테이션했으며, 48%는 2년여 전에 네트워크 세그멘테이션 프로젝트를 시작한 것으로 나타나 노력이 지지부진한 것으로 나타났습니다.

미션 크리티컬 영역

- 중요 애플리케이션
- 퍼블릭 애플리케이션
- 도메인 컨트롤러
- 엔드포인트
- 서버
- 비즈니스 크리티컬 자산/데이터

응답자들이 마주하는 가장 큰 장애물은 세그멘테이션에 대한 기술/전문성 부족(40%), 컴플라이언스 요구사항(40%), 성능 병목 현상 증가(38%) 등 모두 기존의 세그멘테이션 방법과 관련이 있는 것으로, 배포가 느린 이유를 가장 명확하게 보여줍니다. 리소스 또는 전문 지식의 부족이 세그멘테이션 프로젝트 지연의 가장 큰 원인이지만, 사이버 보안 전반에 걸쳐 인력이 부족하고 이 분야의 변화가 매우 빠르게 진행됨에 따라 기술 격차가 존재할 수밖에 없다는 점에 주목할 필요가 있습니다.

모든 지역의 이커머스 기업이 어려움을 겪고 있습니다. 미국과 LATAM 응답자의 100%가 네트워크를 세그멘테이션할 때 문제가 발생한다고 답했습니다. APAC(99%)과 EMEA(97%)에서도 거의 같은 비율의 응답자가 같은 문제를 겪고 있다고 답했습니다.

그러나 지역별로 분류하면(그림 3) 가장 많이 직면하는 장애물에 차이가 있습니다. 이는 특정 문제(예: 기술 부족, 컴플라이언스)가 글로벌 이슈보다 지역적 이슈에 의해 더 많이, 또는 더 크게 영향을 받을 수 있음을 보여줍니다.

EMEA 및 LATAM의 응답자들은 모두 기술/전문성 부족(둘 다 54%)을 가장 큰 세그멘테이션 관련 도전 과제로 꼽았습니다. 미국에서는 성능 병목 현상 증가(44%)를 가장 큰 도전 과제로 꼽았으며, APAC에서는 컴플라이언스 요구사항(43%)이 가장 큰 문제라고 답했습니다.

	가장 많이 경험한 문제	두 번째와 세 번째로 가장 많이 경험한 문제	
미국[59]	성능 병목 현상 증가(44%)	컴플라이언스 요구사항, 적절한 툴의 가용성 제한(둘 다 41%)	
LATAM[24*]	세그멘테이션을 위한 기술, 전문성 부족(54%)	매우 복잡함(46%)	사용 장비의 일부 또는 전부가 독점 장비, 사용 장비의 일부 또는 전부가 레거시 장비(둘 다 38%)
EMEA[39]	세그멘테이션을 위한 기술, 전문성 부족(54%)	적절한 툴의 가용성 제한(41%)	컴플라이언스 요구사항, 사용되는 장비의 일부 또는 전부가 레거시 장비, 매우 높은 가격(모두 36%)
APAC[67]	컴플라이언스 요구사항(43%)	적절한 툴의 가용성 제한, 사용되는 장비의 일부 또는 전부가 독점 장비, 성능 병목현상 증가(모두 37%)	

그림 3: 네트워크를 세그멘테이션할 때 어떤 문제를 겪었거나 혹은 겪을 것으로 예상하시나요? 차트는 네트워크를 세그멘테이션해 본 적이 있는 응답자 중 지역별, 이커머스 부문 데이터에 한해 상위 3개 답변을 보여줍니다.

* 주의 - 30개 미만의 낮은 기본 규모

핵심 내용: 6가지 중요한 비즈니스 영역을 세그멘테이션해 리스크를 크게 줄인 기업

이커머스 환경 전반에서 더 많은 자산을 보호하고 세그멘테이션하면 기업의 보안이 즉시 강화됩니다. 올바른 솔루션을 사용하면 보안팀은 공격을 더 빨리 식별할 수 있으므로 인시던트에 대한 MTTD(Mean Time To Detect)와 MTTR(Mean Time To Respond)을 개선할 수 있습니다. 그러나 일반적으로 레거시 세그멘테이션 기술을 사용해 자산을 제대로 세그멘테이션하지 않으면 보안 공백과 사각지대가 발생해 기업이 더 취약하거나 사후 대응에 취약한 위치에 놓일 수 있습니다. 하지만 소프트웨어 정의 접근 방식을 통해 세그멘테이션을 올바르게 구축한 기업은 공격 표면을 더 잘 관리해 더 효율적이고 비용 효과적인 방식으로 중요 자산을 보호할 수 있습니다.

연구 결과에 따르면, 보안 유출이 발생한 후 세그멘테이션을 통한 복구는 11시간 더 빠릅니다.
계산해 봅시다. 6개의 미션 크리티컬 영역에 세그멘테이션을 구축한 이커머스 기업의 경우, 랜섬웨어 공격을 완전히 차단하는 데 평균 3시간이 걸립니다. 단 하나의 자산에 대해서만 세그멘테이션을 구축한 경우에는 14시간이 걸립니다.

마찬가지로, 세그멘테이션을 사용하면 측면 이동을 포함해 11시간이 단축됩니다.
6가지 미션 크리티컬 영역 모두에 세그멘테이션을 구축한 기업의 경우, 랜섬웨어 공격의 측면 이동을 크게 제한하는 데 평균 3시간이 걸립니다. 하나의 자산에만 세그멘테이션을 구축한 기업의 경우 평균 14시간이 소요됩니다.

두 시나리오에서 모두 11시간 동안 보안팀에 미치는 영향, 브랜드 이미지 타격 및 비용을 고려해 보세요.

공격 차단

3시간

랜섬웨어 공격을 완전히 차단하는 데 걸리는 평균 시간 - 6개의 비즈니스 자산을 모두 세그멘테이션한 경우. 하나의 자산만 세그멘테이션한 경우: **14시간**

이동 제한

3시간

랜섬웨어 공격의 측면 이동을 크게 제한하는 데 평균적으로 걸리는 시간 - 6개의 비즈니스 자산을 모두 세그멘테이션한 기업의 경우. 하나의 자산만 세그멘테이션한 경우: **14시간**

소프트웨어 기반의 마이크로세그멘테이션 솔루션이 문제 해결을 지원하는 방법

마이크로세그멘테이션은 더 발전된 정밀한 종류의 세그멘테이션을 가능하게 할 뿐 아니라 구축도 더 간편하게 만듭니다.

Akamai Guardicore Segmentation과 같은 소프트웨어 기반 솔루션은 네트워크를 물리적으로 변경할 필요 없이 신속하게 배포할 수 있습니다. 새로운 세그먼트를 재구축하거나 서버와 디바이스의 물리적인 위치를 걱정할 필요가 없습니다. 따라서 방화벽이나 VLAN과 같은 인프라 기반 접근 방식보다 훨씬 빠르고 쉽게 솔루션을 배포할 수 있습니다. 또한, 이 솔루션은 정책 적용을 위해 기본 운영 체제에 의존하지 않기 때문에 베어메탈 서버부터 멀티클라우드 배포, Windows Server 2003 및 Windows XP와 같은 레거시 기술부터 최신 POS 시스템, IoT/OT 디바이스, 심지어 컨테이너화된 기술에 이르기까지 모든 머신과 운영 체제에서 원활하게 작동합니다. 즉, 하나의 인터페이스로 하나의 솔루션만 관리하면 물리적 위치에 관계없이 전체 환경에서 다양한 운영 체제 및 디바이스의 연결을 시각화하고 제어할 수 있습니다.

배포가 쉬운 이유

Akamai Guardicore Segmentation은 먼저 사용자 환경에서 이루어지는 모든 연결에 대한 인터랙티브 시각 정보를 생성하며, 이는 배포의 주요 장애물을 극복하는 데 중요한 구성요소입니다. 또한, Akamai는 성능 병목과 컴플라이언스 요구사항을 해결할 수 있는 적극적인 방법을 솔루션에 구축했습니다.

성능 병목 현상은 세그멘테이션 솔루션으로 인한 시스템의 기술적 부담으로 인해 발생하는 것이 아니라 인력 병목 현상으로 인해 발생합니다. 비즈니스 영역을 수동으로 세그멘테이션한 다음에 문제가 발생하면 해당 영역의 문제를 수동으로 해결해야 하는 데 쓰는 시간과 노력은 상당할 수 있습니다. Akamai는 최고 수준의 기술 지원 및 전문 서비스와 함께 수동 세그멘테이션에 소요되는 시간을 줄임으로써 이러한 문제와 배포의 가장 큰 장애물인 전문성 부족 문제를 해결하기 위해 노력합니다. Akamai 세그멘테이션 전문가는 배포 프로세스 전반에서 고객과 협력해 고객의 고유한 IT 환경에서 세그멘테이션 목표를 달성할 수 있도록 지원합니다.

솔루션을 통해 배포에 대한 지원도 제공합니다. 일반적인 사용 사례에 대한 AI 기반 레이블링 및 정책 권장 사항과 즉시 사용 가능한 정책 템플릿을 통해 시간과 클릭 수를 절약하고, 워크플로우를 간소화하고, 전체 정책 수립 시간을 단축하고, 인적 오류로 인한 잘못된 설정을 방지할 수 있습니다. 한 고객의 경우, 2년이 걸리고 총비용이 100만 달러 이상 소요될 것으로 예상되는 정밀 세그멘테이션 프로젝트를 엔지니어 한 명이 단 6주 만에 완료해 전체 프로젝트 비용을 85% 절감함으로써 정밀한 세그멘테이션이 병목 현상 없이 빠르고 쉽게 배포될 수 있음을 입증했습니다.

세그멘테이션을 통해 컴플라이언스를 간소화하는 방법

많은 고객이 PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR 등 다양한 국가 및 국제 컴플라이언스 의무를 준수하고 이를 입증하기 위해 솔루션을 배포합니다. 이러한 컴플라이언스 의무에 따라 일반적으로 PCI DSS의 CDE(Cardholder Data Environment)와 같은 범위 내 데이터를 기업 환경의 다른 시스템과 분리해 보호해야 합니다. 방화벽과 VLAN을 사용하면 이 작업이 불가능할 수 있지만, 소프트웨어 기반 솔루션을 사용하면 범위 내 데이터 전용 세그먼트를 생성하고 해당 데이터에 접속할 수 있는 항목과 접속할 수 없는 항목에 대한 통신 룰을 적용할 수 있습니다. 거의 실시간 및 기록 보기 기능이 있는 시각적 맵을 사용하면 권한이 없는 사용자, 시스템, 머신이 범위 내 데이터에 접속하지 않고 있음을 물리적으로 보여줌으로써 컴플라이언스 준수를 증명할 수 있습니다.

적합한 솔루션과 지원을 기반으로 보안 체계 혁신

세그멘테이션을 구축하는 작업은 상상 이상으로 어려울 수 있습니다. 하지만 이 보고서에서 알 수 있듯이 세그멘테이션을 효과적으로 구축한 기업은 사이버 리스크를 크게 줄일 수 있습니다. 적절한 세그멘테이션을 적용하면 측면 이동을 제한하고 공격이 진행되는 동안 인시던트 대응 담당자가 더 빠르게 대응할 수 있습니다. 또한, 유출이 발생한 후에도 복구 작업을 완료하는 데 걸리는 시간을 단축할 수 있습니다.

기존의 세그멘테이션 배포와 관련된 일반적인 문제를 극복하도록 설계된 소프트웨어 정의 솔루션을 선택하고, 그 여정을 탐색할 때 제공되는 전문가와 협력하면 보안 체계를 혁신할 수 있는 최적의 위치에 포지셔닝할 수 있습니다. 또한, 더 많은 비즈니스 영역을 세그멘테이션할수록 현재의 리스크를 줄임으로써 제로 트러스트 아키텍처를 더욱 발전시킬 수 있습니다.

Akamai 설문 조사 그룹

이 보고서에서는 이커머스 부문에 종사하는 190명(미국 59명, EMEA 39명, APAC 68명, LATAM 24명)의 응답 내용을 분석했습니다.

전체 연구를 위해 10개국에서 1200명의 IT 및 보안 의사 결정권자를 인터뷰해 세그멘테이션의 역할에 중점을 두고 기업의 환경 보안에 대한 진전 상황을 평가했습니다.

질문은 IT 보안 접근 방식, 세그멘테이션 전략, 2023년에 기업이 직면할 위협과 관련된 것이었습니다. 여기서 얻은 인사이트와 조사 결과를 통해 2021년 이후 보안 전략이 어떻게 변화했는지 그리고 여전히 개선이 필요한 부분이 무엇인지 자세히 알아볼 수 있습니다.

설문 조사에는 미국, 인도, 멕시코, 브라질, 영국, 프랑스, 독일, 중국, 일본, 호주 등 전 세계의 응답자가 참여했습니다. 응답자는 1000명 이상의 직원을 보유한 기업과 다양한 업계 및 부문에 속해 있었습니다.

참고: 이 샘플은 2021년과 약간 다릅니다. 샘플 크기: 2023년: 1200명 완료, 2021년: 1000명 완료. 2023년에는 호주, 일본, 중국의 응답자들도 인터뷰에 참여했습니다. 분야는 2021년과 약간 달랐습니다. 2023년에는 특히 디지털 커머스 부문에 초점을 맞췄습니다.

Akamai Guardicore Segmentation 자세히 알아보기

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관한 자세한 정보는 akamai.com과 akamai.com/blog에서 확인하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 5월 발행.

Vanson Bourne은 기술 분야의 독립적인 시장 리서치 전문 기관입니다. 견고하고 신뢰할 수 있는 연구 기반 분석에 대한 평판은 엄격한 연구 원칙과 모든 비즈니스 부문 및 모든 주요 시장에서 기술 및 비즈니스 기능 전반의 고위 의사 결정권자로부터 의견을 구하는 능력에 바탕을 두고 있습니다. 자세한 정보는 www.vansonbourne.com에서 확인하시기 바랍니다.