Akamai

백서

2023년 세그멘테이션 현황

배포 장애물을 극복하는 혁신적인 과정

목차

서론

IT 보안 부서의 업무는 언제나 쉽지 않았습니다. 그러나 이제는 더욱 교묘해진 공격자들이 다양한 기술을 결합해 더 큰 위협을 더욱 빈번하게 일으키면서 보안팀이 그 어느 때보다 큰 압박을 받고 있습니다. 기업은 온라인 활동 없이 비즈니스를 운영할 수 없지만, 단 한 번의 보안 유출만으로 평판과 매출에 회복할 수 없을 정도의 막대한 피해가 발생할 수 있습니다.

이 보고서의 조사 결과에서 알 수 있듯이 공격의 영향력은 더 커지고 있으며, 보안 리더는 전반적인 성능이나 혁신을 희생하지 않고 적합한 솔루션을 선택해 전체 환경을 안전하게 유지해야 하는 압박을 받고 있습니다.

우리는 2021년 이후 이 보고서의 조사 결과를 업데이트하면서 세그멘테이션이 올바른 선택인지 그리고 그것이 효과적인지에 대해 알아보고자 했습니다. 1200명의 응답자들은 세그멘테이션이 자산을 보호하는 데 효과적이라는 데 압도적으로 동의했지만, 중요한 비즈니스 애플리케이션과 자산을 중심으로 세그멘테이션을 배포하는 데 있어 전반적인 진행 상황은 예상보다 더뎠습니다. 모든 지역에 걸쳐 가장 큰 장애물은 세그멘테이션 배포를 위한 전문 지식이 부족하다는 것이었으며, 이는 특히 IT 환경이 점점 더 복잡해지는 상황에서 성능에 지장을 줄 수 있는 프로젝트를 시작하는 것을 주저할 수 있음을 시사합니다.

하지만 다행히 인내심은 효과가 있습니다. 대부분의 중요 자산을 세그멘테이션한 기업들은 세그멘테이션이 방어에 혁신적인 효과를 발휘해, 하나의 자산만 세그멘테이션한 기업보다 11시간 더 빠르게 랜섬웨어를 방어하고 차단할 수 있었습니다. 이 11시간의 차이가 팀, 고객, 브랜드 평판, 매출에 미치는 영향을 상상해 보세요.

랜섬웨어 공격과 공격의 영향력 모두 지속적으로 증가

지난 2년간 랜섬웨어 공격 건수(성공 및 실패)는 2021년 평균 43건에서 2023년 86건으로 두 배 증가했습니다. 약 90개의 랜섬웨어 그룹의 유출 사이트에서 수집한 데이터를 보면 2022년 1분기와 2023년 1분기 사이에 공격 건수 증가율이 더 높은 것을 알 수 있습니다. 2023년 8월 발표된 멈추지 않는 랜섬웨어: 진화하는 악용 기술과 활발한 제로데이 공격에 따르면, 제로데이 및 원데이 취약점의 사용으로 인해 전 세계적으로 랜섬웨어 피해자가 총 143% 증가했습니다.

미국 기업들은 여전히 가장 많은 랜섬웨어 위협에 직면하고 있습니다(그림 1). 미국의 IT 보안팀과 의사 결정권자들은 지난 12개월 동안 평균 115건의 랜섬웨어 공격을 받았다고 보고했으며, 이는 조사 대상 국가 중 가장 큰 수치입니다.

지난 12개월간 국가별 평균 랜섬웨어 공격 건수

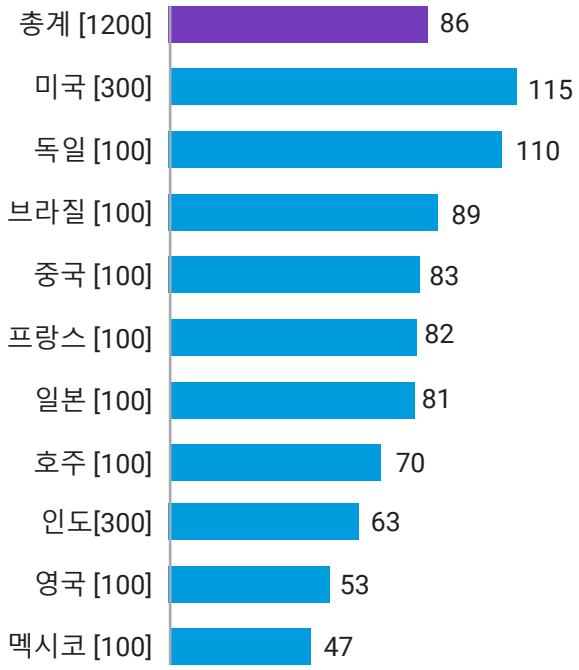

그림 1: 지난 12개월 동안 귀사는 공격의 성공 여부와 무관하게 얼마나 많은 랜섬웨어 공격을 받으셨나요? [1200], 지난 12개월 동안의 평균 공격 건수만 국가별로 구분해 표시했습니다.

미국이 2개 이상의 미션 크리티컬 비즈니스 영역에 세그멘테이션을 구축한 비율이 가장 낮은 국가 중 하나라는 점을 고려하면(그림 2), 랜섬웨어 공격 건수 1위와 세그멘테이션 배포 비율의 낮은 순위가 연관이 있을 수도 있습니다.

물론 미국에서 랜섬웨어 공격 건수가 많은 것은 2023년 러시아 사이버 범죄 그룹이 연방 기관을 대상으로 일으킨 사건과 같은 주요 유출 사고가 언론에 크게 보도되었고 미국에서 IoT 디바이스가 증가(2위 중국보다 20억 개 더 많음)하는 등 여러 이유가 있는 것으로 보입니다. R4IoT(Ransomware for IoT)는 IP 카메라와 같이 취약한 IoT 디바이스를 악용해 초기 발판을 마련한 다음, IT 네트워크에서 측면으로 이동하고 취약한 보안 관행을 악용해 미션 크리티컬 프로세스를 인질로 잡습니다.

2021년 대비 2023년에는 전 세계적으로 랜섬웨어 공격이 더 빈번하게 발생했을 뿐만 아니라 그 영향력도 더욱 커진 것으로 보이며(그림 3) 응답자들은 네트워크 다운타임, 데이터 손실, 평판 손상 등이 증가해 보안팀의 부담이 크게 증가하고 있다고 답했습니다. 이러한 압박은 전략 측면에도 영향을 미칩니다. 랜섬웨어뿐만 아니라 끊임없이 변화하는 공격표면에 대응하기 위해 사이버 보안 전략이나 정책을 지속적으로 업데이트하는 기업의 수가 2021년 5%에서 2023년 13%로 증가했습니다. 여기에 분산된 인력과 애플리케이션, 클라우드로 전환되는 데이터의 두 가지 요소도 일상적인 보안 전략에 영향을 미칩니다.

국가별로 자산 및 영역을 2개 이상 세그멘테이션한 응답자 수

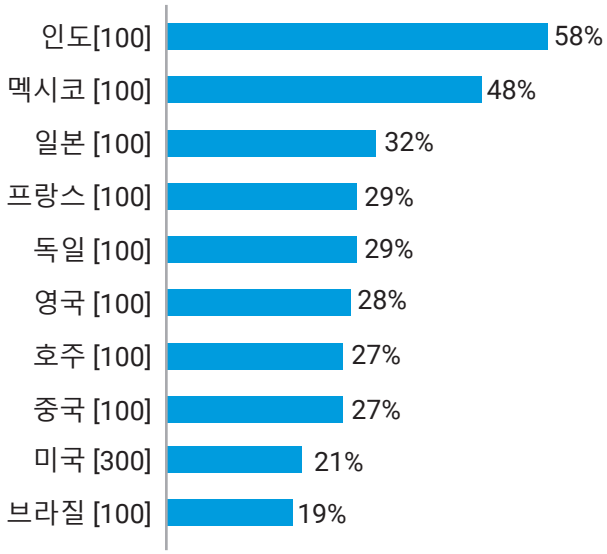

그림 2: (해당하는 경우) 귀사에서는 다음과 같은 IT 보안 조치로 각각 어떤 자산을 보호하고 있습니까? [1200], 세그멘테이션 보안 조치에 대한 응답만 표시하고 주요 자산을 보호하기 위해 세그멘테이션을 사용하는 비율을 국가별로 나눈 값입니다.

랜섬웨어 및 사이버 공격의 영향

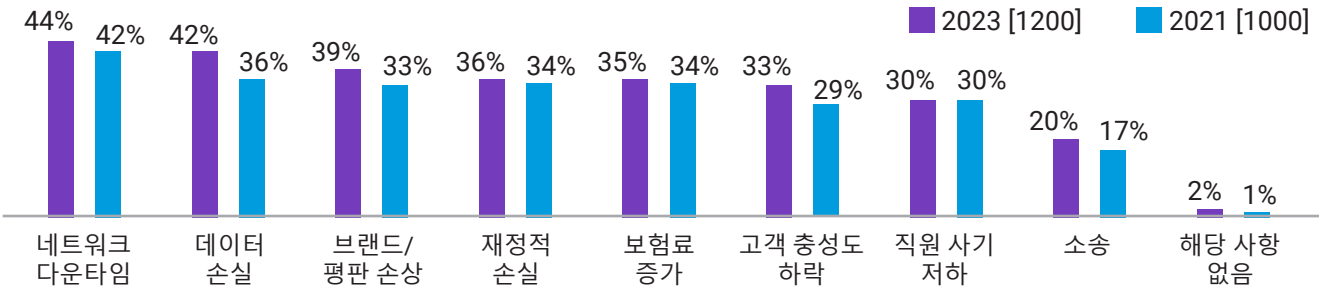

그림 3: 귀사에서는 이전에 랜섬웨어나 기타 사이버 공격을 탐지한 적이 있습니까? 만약 있다면 이것이 기업에 어떤 영향을 미쳤습니까? [차트의 기본 크기], 모든 답변 옵션이 표시되지 않음, 과거 데이터로 구분.

지역별 핵심 내용

사이버 공격자들은 미주 지역을 공격 대상으로 삼을 가능성이 높습니다. 지난 12개월 동안 평균 96건의 랜섬웨어 공격이 발생한 미주 지역에서 가장 많은 랜섬웨어 공격이 발생했으며, EMEA는 83건, APAC는 75건이었습니다.

세그멘테이션과 마이크로세그멘테이션은 EMEA보다 APAC과 미주 지역에서 더 중요한 조치로 인식되고 있습니다. APAC(62%)과 미주지역(60%)의 IT 보안팀과 의사결정권자는 네트워크 세그멘테이션이 기업의 보안을 유지하는 데 매우 중요하다고 응답한 비율이 EMEA(53%)에 비해 높았습니다.

미주 지역 응답자들은 마이크로세그멘테이션이 최우선 과제라고 답한 비율(41%)이 APAC(35%)이나 EMEA(23%)에 비해 더 높았습니다.

EMEA 지역에서는 세그멘테이션을 전혀 구축하지 않았다는 응답이 더 많았습니다. 비즈니스 크리티컬 자산을 전혀 세그멘테이션하지 않았다고 응답한 비율은 EMEA(10%)가 APAC(4%)이나 미주(1%)보다 훨씬 높았습니다.

배포 속도가 가장 느린 지역, 즉 세그멘테이션된 영역이 없는 곳은 영국(23%)으로 나타났으며, 레거시 장비가 주요 장애물(46%)로 보고되었습니다.

세그멘테이션이 가장 많이 이뤄지고 있는 지역은 APAC입니다. APAC의 기업은 EMEA(29%)나 미주(26%)에 비해 두 개 이상의 비즈니스 크리티컬 자산을 세그멘테이션(36%)한 비율이 더 높았습니다.

모든 지역의 기업이 어려움을 겪고 있습니다. 미주 지역 응답자의 97%는 네트워크를 세그멘테이션하는 데 문제를 겪고 있다고 답했습니다. EMEA(94%)와 APAC (97%)에서도 비슷한 비율의 응답자가 같은 문제를 겪고 있다고 답했습니다.

EMEA와 APAC의 응답자들은 모두 기술(38%) 및 전문 지식 부족(43%)을 세그멘테이션의 가장 큰 장애물로 꼽았습니다. 미주 지역의 경우, 가장 큰 장애물은 성능 병목현상 증가(41%)였습니다.

미주 지역에서는 자사의 제로 트러스트 보안 프레임워크가 성숙하다고 평가하는 기업이 더 많았습니다. 미주 지역 응답자들은 제로 트러스트 배포가 완전히 완료되고 정의되었다고 답한 비율(49%)이 APAC(35%)이나 EMEA(33%)보다 높았습니다.

제로 트러스트의 중요한 부분으로 널리 인식되고 있는 세그멘테이션

응답자들은 세그멘테이션이 기업의 보안을 유지하는 데 중요하며, 특히 멀웨어 대응에 중요하다는 데 동의했습니다. 업계 전반적으로는 응답자의 93%가 세그멘테이션이 치명적인 공격을 막는 데 중요하다고 답했으며, 제조 및 생산 분야의 경우 이 비율은 99%로 증가했습니다. 이는 이들 업계가 공급망에서 여러 써드파티에 크게 의존하고 있어, 중단이 발생하면 비즈니스에 막대한 연쇄적인 영향을 미칠 수 있기 때문일 수 있습니다.

세그멘테이션은 제로 트러스트 프레임워크에도 크게 기여합니다. 세그멘테이션 프로젝트를 시작한 이유에 대해 세 번째로 많은 응답자가 제로 트러스트를 발전시키기 위해서라고 답했습니다. 세그멘테이션을 구축한 거의 모든 기업이 제로 트러스트 보안 프레임워크를 배포 중이거나 이미 배포한 적이 있지만(99%), 5명 중 2명(40%)만이 제로 트러스트 프레임워크가 완전히 정의되고 완성되었다고 답했습니다.

전 세계적으로 응답자의 대다수는 현 상황에서 한 걸음 더 나아가 애플리케이션 워크로드를 세밀한 수준에서 보호하는 마이크로세그멘테이션을 구축하고자 합니다. 89%는 마이크로세그멘테이션이 적어도 높은 우선순위라고 답했으며, 34%는 마이크로세그멘테이션을 최우선 순위로 꼽았습니다. IT 보안팀과 의사 결정권자의 97%는 해당 업계에서 적어도 소수의 기업들이 마이크로세그멘테이션을 도입하고 있다고 답했습니다. 공공 부문(의료 제외)의 경우 이 수치는 80%로 떨어졌는데, 이는 예산 부족과 레거시 인프라가 마이크로세그멘테이션의 워크로드 수준 보안을 배포하는 데 더 큰 장애물로 작용하기 때문일 수 있습니다.

마이크로세그멘테이션

적어도 업계의 소수 기업이 마이크로세그멘테이션을 도입하고 있다고 답한 IT 보안팀과 의사결정권자의 비율

그러나 공공 부문은 마이크로세그멘테이션과 같은 고급 보안 기술을 구축함으로써 큰 장점을 누릴 수 있습니다. 공공 부문의 시스템은 상호 작용이 이루어지도록 설계되어 있지 않기 때문에 상호 운용성이 부족하며 이로 인해 인간 오류의 가능성과 사이버 공격이 성공할 가능성이 모두 높습니다.

세그멘테이션 수준에서는 공공 부문 응답자의 15%가 세그멘테이션의 중요성을 인식하고 있음에도 불구하고 세그멘테이션이 이뤄지지 않고 있다고 답했습니다. 이는 부문별 가장 낮은 배포 수준이고, 가장 큰 장애물은 컴플라이언스 요구사항(52%)이었습니다.

세그멘테이션의 효과, 마이크로세그멘테이션으로 더 커집니다.

세그멘테이션은 성능과 보안을 강화하기 위해 네트워크를 더 작은 세그먼트로 나누는 아키텍처 접근 방식입니다.

마이크로세그멘테이션은 네트워크를 개별 워크로드 수준에서 세그먼트로 분할하기 때문에 각각의 세그먼트에 따라 보안 제어와 서비스 전송을 정의할 수 있습니다.

배포에 시간이 걸리더라도 인내심을 갖고 지속하면 혁신적인 결과에 도달

세그멘테이션이 공격을 차단하는 핵심 요소라는 데 폭넓게 동의하고 있음에도 불구하고 세그멘테이션 배포가 예상보다 더디게 진행되고 있다는 것이 냉혹한 현실입니다. 2023년에는 30%의 기업만이 두 개 이상의 중요한 비즈니스 영역에 세그멘테이션을 적용했으며(2021년 25%), 44%는 네트워크 세그멘테이션 프로젝트를 시작한 지 2년이 넘었다고 답해 세그멘테이션에 대한 노력이 지지부진한 것으로 나타났습니다.

응답자들이 직면한 가장 큰 장애물은 세그멘테이션에 대한 기술 및 전문 지식 부족(39%), 성능 병목 현상 증가(39%), 컴플라이언스 요구사항(38%, 그림 4)이었으며, 이는 배포가 느린 이유를 가장 명확하게 보여줍니다. 설문조사에 참여한 거의 모든 기업이 부문, 업계, 국가에 관계없이 동일한 장애물을 언급했지만 그 정도는 조금씩 달랐습니다. 세그멘테이션 프로젝트 지연의 가장 큰 원인은 기술 및 전문 지식 부족이지만, 사이버 보안 분야는 전반적으로 인력이 부족하며 이 분야의 변화가 매우 빠르게 일어나고 있기 때문에 기술 격차가 존재할 수밖에 없다는 점에 주목할 필요가 있습니다.

변화의 속도는 느리지만 세그멘테이션 비율은 전체적으로 조금씩 증가하고 있습니다. 비즈니스 크리티컬 애플리케이션/데이터를 세그멘테이션한 기업의 비율은 2021년부터 2023년까지 12%, 세그멘테이션된 서버의 비율은 8% 증가했습니다.

네트워크 세그멘테이션 과정에서 직면하는 장애물

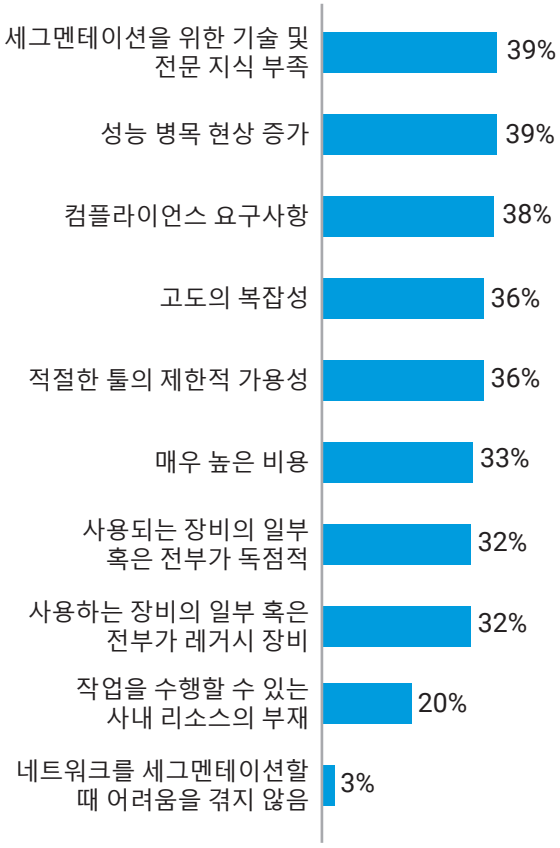

그림 4: 네트워크를 세그멘테이션할 때 어떤 문제를 겪었거나 혹은 겪을 것으로 예상하십니까? [1187], 네트워크를 세그멘테이션한 적이 있는 응답자에게만 표시되며 모든 답변 옵션이 표시되지는 않습니다.

핵심 내용: 리스크를 대폭 감소시키는 6가지 중요 비즈니스 영역의 세그멘테이션

더 많은 자산을 보호하고 세그멘테이션하면 기업의 보안이 즉시 강화됩니다. 보안팀은 공격을 더 효과적으로 식별하고 훨씬 더 효과적으로 대응할 수 있습니다. 미숙하거나 잘못 정의된 세그멘테이션 전략을 실행하면 기업의 리스크가 증가하지만, 올바른 전략을 세운다면 장애물을 극복하고 세그멘테이션을 구축할 만한 충분한 가치가 있습니다.

연구 결과에 따르면 세그멘테이션을 통해 보안 유출이 발생한 후 복구가 11시간 더 빠르게 이루어지는 것으로 나타났습니다. 계산하기: 6가지 미션 크리티컬 영역에 세그멘테이션을 구축한 기업의 경우 랜섬웨어 공격을 완전히 차단하는 데 평균 4시간이 걸렸고, 하나의 자산에만 세그멘테이션을 구축한 기업의 경우 15시간이 걸렸습니다.

마찬가지로 세그멘테이션을 통해 측면 이동을 제한하면 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 11시간이 보안팀과 비용 및 브랜드 손상을 통제하는 데 얼마나 큰 차이를 가져올지 생각해 보세요.

공격 차단

4시간

랜섬웨어 공격을 완전히 차단하는 데 걸리는 평균 시간(6개의 비즈니스 자산을 모두 세그멘테이션한 경우)

하나의 자산만 세그멘테이션한 경우: **15시간**

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 보다 진보된 정밀한 종류의 세그멘테이션을 가능하게 할 뿐만 아니라 구축도 더 간편하게 만들어줍니다.

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 자체 드라이버를 사용하기 때문에, 베어메탈 서버부터 멀티클라우드 배포, Windows Server 2003과 같은 레거시 기술부터 최신 IoT/OT 디바이스와 컨테이너화된 기술에 이르는 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

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

성능 병목 현상은 세그멘테이션 솔루션으로 인한 시스템의 기술적 부담으로 인해 발생하는 것이 아니라, 비즈니스 영역을 수동으로 세그멘테이션한 후 문제가 발생하면 해당 영역을 수동으로 해결해야 하는 인력 병목으로 인해 발생합니다. Akamai는 수동 세그멘테이션의 필요성을 줄이고 최고 수준의 기술 지원과 전문 서비스를 제공함으로써 이러한 문제와 배포의 가장 큰 장애물인 전문 지식의 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 기반의 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 총 비용이 100만 달러 이상 소요될 것으로 예상되는 정밀 세그멘테이션 프로젝트를 엔지니어 한 명이 단 6주 만에 완료해 전체 프로젝트 비용을 85% 절감함으로써 정교한 세그멘테이션이 병목 현상 없이 빠르고 쉽게 배포될 수 있음을 입증했습니다.

컴플라이언스가 간편해지는 이유

많은 고객이 PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR 등 다양한 국내 및 국제 컴플라이언스 의무를 준수하고 이를 입증하기 위해 솔루션을 배포합니다. 이러한 컴플라이언스 의무에 따라 일반적으로 범위 내 데이터를 사용자 환경의 다른 시스템과 분리해야 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. 실시간에 가까운 기록 보기가 가능한 시각적 맵을 사용해 권한 없는 사용자와 머신이 범위 내 데이터에 접속하지 못하고 있음을 물리적으로 보여줌으로써 이러한 의무를 준수하고 있음을 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 방식으로 세그멘테이션을 구축하면 위협이 측면으로 이동하는 것을 제한하고 유출이 발생하는 동안 더 빠르게 대응할 수 있습니다. 또한 유출이 발생한 후에도 복구 작업을 완료하는 데 걸리는 시간을 단축할 수 있습니다.

세그멘테이션 배포의 일반적인 과제를 극복하도록 설계된 솔루션을 선택하고 여정을 진행하는 동안 적절한 전문가와 협력하면 가장 좋은 조건에서 보안 체계를 혁신할 수 있습니다. 또한, 더 많은 비즈니스 영역을 세그멘테이션할수록 현재의 리스크를 줄이고 미래의 위협 기법에 대한 1차 방어를 보장함으로써 제로 트러스트 아키텍처를 더욱 발전시킬 수 있습니다.

Akamai 설문조사 그룹

Akamai는 10개국 1200명의 IT 및 보안 의사결정권자를 대상으로 인터뷰를 실시해 세그멘테이션의 역할을 중심으로 기업이 환경을 보호하는 측면에서 이룩한 발전을 측정했습니다.

응답자들은 IT 보안 접근 방식, 세그멘테이션 전략, 2023년에 기업이 직면한 위협과 관련된 질문을 받았습니다. 해당 조사 결과는 2021년 이후 보안 전략이 어떻게 변화했는지, 그리고 아직 개선해야 할 부분이 무엇인지에 대한 인사이트를 제공합니다.

설문조사는 미국, 멕시코, 브라질, 영국, 프랑스, 독일, 중국, 인도, 일본, 호주의 보안 담당자와 의사 결정권자를 대상으로 진행되었습니다. 이들은 1000명 이상의 직원을 보유한 다양한 업계와 부문의 기업에서 근무하고 있습니다.

참고: 이 샘플은 2021년과 약간 다릅니다. 샘플 규모 - 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 Segmentation에 대해 자세히 알아보기

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 시스템, 데이터를 보호합니다. Akamai 플랫폼의 글로벌 위협에 대한 가시성은 제로 트러스트 구축, 앱 및 API 보안, 인프라 보안 등의 보안 체계를 조정하고 발전시키기 때문에 기업은 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 방문하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 10월 발행.

VansonBourne

Vanson Bourne은 기술 분야의 독립적인 시장 리서치 전문 기관입니다. 견고하고 신뢰할 수 있는 연구 기반 분석에 대한 명성은 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.