Akamai 고객 사례

하루 동안 4000건의 사이버 공격을 방어한 미국 헬스케어 기업

네트워크 엔지니어가 사이버 리스크를 줄이기 위해 마이크로세그멘테이션을 통한 스마트한 정책과 레이어 7 가시성을 활용

랜섬웨어 차단 | 심층적인 가시성 확보 | 정책 개선

필수적인 헬스케어 서비스와 환자 연결

점점 더 정교해지는 사이버 공격에 대비하면서 환자의 생명에 직접적인 영향을 미치는 네트워크를 보호하기 위해 노력한다고 상상해 보세요. 이것은 한 중견 헬스케어 기업이 직면한 현실이었습니다. 이 기업의 네트워크 엔지니어링 팀은 점점 더 커지는 랜섬웨어 위협에 직면해 있었고 보다 높은 수준의 가시성이 필요했는데 기업의 보안 체계를 강화하기 위해 Akamai Guardicore Segmentation을 선택했습니다.

제로 트러스트 아키텍처 확장

이 기업은 HIPAA와 SOC 2 컴플라이언스 요구사항을 충족하면서 제로 트러스트 원칙을 통해 IT 환경을 강화한다는 대담한 비전을 가지고 있었습니다. 리스크 부담이 컸기 때문에 네트워크 엔지니어링 팀은 다음과 같은 내용을 목표로 삼았습니다.

- 보안 인시던트가 발생하는 동안에도 중요한 애플리케이션을 온라인 상태로 유지
- 랜섬웨어의 확산을 억제해 랜섬웨어 공격의 영향 줄이기
- 기존의 방화벽을 훨씬 뛰어넘는 세부적인 네트워크 가시성 확보

이 기업은 기존 IT 인프라를 제거하거나 교체할 필요가 없는, 비용 효율적이고 확장 가능한 마이크로세그멘테이션 솔루션이 필요했습니다. 또한, 소규모 팀이 관리할 수 있을 만큼 간단하고, 기업과 함께 성장할 수 있을 만큼 확장 가능해야 했습니다.

한 네트워크 엔지니어는 "랜섬웨어는 헬스케어 분야를 표적으로 삼습니다. 랜섬웨어 위협은 더 빨리 격리하고 제거할수록 좋습니다."라고 설명했습니다.

Healthcare Company

위치

미국

업계

헬스케어 및 생명과학

솔루션

Akamai Guardicore Segmentation

Akamai

적합한 마이크로세그멘테이션 솔루션 찾기

컨테이너 방식의 접근 방식을 신속하게 배제한 후, 기업에서는 마이크로세그멘테이션 솔루션을 평가했습니다. 네트워크 엔지니어는 "차세대 방화벽에서 볼 수 있는 기능, 즉 애플리케이션 레이어에서의 가시성을 원했습니다."라고 설명했습니다.

많은 솔루션을 평가한 후, 이 기업은 Akamai Guardicore Segmentation을 발견했습니다. Akamai 엔지니어들의 직접적인 지원과 함께 데모를 긍정적으로 진행한 후 계약을 체결했습니다. 이 솔루션은 다음을 포함한 모든 조건을 충족했습니다.

- **심층적인 가시성:** 레이어 7 검사 및 전체 네트워크 인사이트
- **배포 용이성:** 하드웨어를 추가할 필요 없는 소프트웨어 기반 에이전트
- **안정성:** 핵심 네트워크에 단일 장애 지점 없음
- **유연성:** 다양한 운영 체제 지원

IT 인프라 및 정보 보안 부사장에 따르면, Akamai Guardicore Segmentation은 인력이 부족한 팀에 큰 이점을 제공합니다. "배포를 시작한 직후, 가시성과 제어 측면에서 장점을 확인했습니다."

IT 인프라 관리자는 "여러 개의 동서 방화벽을 구매하고 관리할 필요가 없어 막대한 비용을 절감할 수 있고, 방화벽으로는 불가능한 수준의 가시성을 확보할 수 있습니다."라고 덧붙였습니다.

랜섬웨어의 확산 차단

곧바로 인상적인 결과를 얻을 수 있었습니다. 네트워크 엔지니어링팀은 앱을 보다 효과적으로 링펜싱하고 Akamai Guardicore Segmentation의 즉시 사용 가능한 랜섬웨어 차단 정책을 사용해 첫날 4000건의 사이버 공격을 무력화했습니다. Akamai Guardicore Segmentation은 기업의 특정 요구사항에 맞게 정책을 맞춤화하기도 했습니다.

네트워크 엔지니어는 "중간 정책의 경우, 다운타임을 발생시키지 않고 인시던트를 표시하기 위해 알림 모드를 사용했습니다. 방해 없이 정책을 개선할 수 있는 좋은 방법입니다."라고 말했습니다.

> "Akamai Guardicore Segmentation은 랜섬웨어 문제를 해결하는 것 이상의 역할을 했으며, 사이버 보안에 대한 접근 방식을 강화했습니다.
>
> - 네트워크 엔지니어

> “제로 트러스트라는 ‘산’을 오르는 것은 매우 어렵습니다. Akamai Guardicore Segmentation 덕분에 비용과 복잡성 문제를 줄이면서 빠르게 그 산을 오를 수 있었습니다.”
>
> **- IT 인프라 및 정보 보안 부사장**

탁월한 레이어 7 인사이트 확보

IT 인프라 관리자에 따르면, Akamai Guardicore Segmentation은 다양한 애플리케이션 간의 트래픽 흐름에 대한 귀중한 가시성을 제공합니다. 이를 통해 네트워크 엔지니어링팀은 엄청난 양의 데이터를 확보할 수 있었습니다. 이제 레이어 4 로그를 넘어 사용자 ID, 명령줄 입력, 심지어 서비스 상관관계에 이르기까지 세분화된 세부 정보를 검사할 수 있습니다.

네트워크 엔지니어는 “네트워크 팀은 트래픽 흐름을 조사해 문제를 해결하고, 보안팀에 인시던트를 완전히 조사하는 데 필요한 정보를 제공할 수 있습니다.” 라고 말했습니다.

이러한 가시성은 예기치 않은 정책 위반이 발생했을 때 유용하게 사용되었습니다. 신입 직원이 가정용 라우터로 보호되는 LAN 포트 대신 PC를 통신사의 CPE(Customer Premises Equipment)에 직접 연결했습니다. CPE가 PC에 공용 IP를 할당하여 인터넷의 공개 스캔에 취약해졌기 때문에 엄격하게 금지되었습니다.

기업의 네트워크 엔지니어는 “Akamai Guardicore Segmentation이 즉시 문제를 탐지해 PC를 격리하고 상황이 악화되기 전에 문제를 해결할 수 있었습니다. 또한, 이를 계기로 향후 이러한 종류의 인시던트가 발생하지 않도록 하는 정책을 만들게 되었습니다.”라고 설명했습니다.

더 스마트한 레이블링, 더 나은 정책

직관적인 레이블링과 정책 생성 덕분에 네트워크 엔지니어링 팀은 트래픽을 쉽게 매핑하고 보안 룰을 적용할 수 있었습니다. 네트워크 엔지니어는 “환경에 가장 적합한 것을 결정할 수 있었습니다. 그 기능은 예상했던 것보다 훨씬 더 인상적이었고, 효율적으로 정책을 만드는 데 도움이 되었습니다.” 라고 말했습니다.

예를 들어, 프린트 서버에 대한 접속을 제한해 신뢰할 수 있는 영역만 허용했습니다. 따라서 기업의 전반적인 보안 체계를 신속히 개선할 수 있었습니다. 엔지니어는 “덕분에 어렵지 않은 문제를 바로 해결할 수 있었습니다.”라고 말했습니다.

신뢰를 심어주는 가시성

예상치 못한 장점이 한 가지 있었습니다. 바로 내부 트래픽 흐름과 애플리케이션 행동에 대한 명확한 시각입니다. 새로운 가시성으로 애플리케이션 소유자와의 협업을 개선하고 유지 관리 기간을 간소화할 수 있습니다. 예를 들어, 트래픽 차단 여부를 애플리케이션 소유자에게 보여줄 수 있습니다.

네트워크 엔지니어는 "과거에는 문제 해결과 미래에 대한 대비가 문제였습니다. 이제 전환 과정에서 트래픽이 기존 서버에서 새 서버로 이동하는 시기를 확실하게 확인할 수 있습니다. 이를 통해 기존 시스템을 확실하게 폐기할 수 있었습니다."라고 말했습니다.

기업의 IT 인프라 및 정보 보안 부사장은 "Akamai Guardicore Segmentation은 이미 영향을 미치고 있으며, 보안 관행에 필수적인 제품이 되었습니다. 기업 전체로 배포 범위를 확대할 수 있기를 기대합니다."라고 말했습니다.