AKAMAI 고객 사례

Akamai를 통해 컴플라이언스 포스처를 개선하고 클라우드로 전환한 대규모 헬스케어 시스템

포괄적인 네트워크 가시성

IT 인프라 간 세그멘테이션

신기술의 안전한 도입

고객 요약

대규모 헬스케어 시스템인 이 Akamai 고객은 6000개 이상의 자산과 환자 데이터를 잠재적인 위협으로부터 보호해야 합니다.

비즈니스 도전 과제 및 요구사항

이 기업은 몇 가지 중요한 워크로드 중 몇 가지를 Microsoft Azure로 전환할 계획이었지만 IT 이해 관계자들은 성공적인 클라우드 도입을 가로막는 여러 가지 장애물에 직면해 있었습니다.

이 회사의 현재 환경에는 의료 사물 인터넷 디바이스의 모니터링되지 않는 데이터 센터 접속과 잘 사용되는 BYOD 정책을 사용하는 비교적 평탄한 네트워크를 포함하여 몇 가지 기존 보안 리스크가 있었습니다. 따라서 유출이 발생할 경우 다른 비즈니스 크리티컬 애플리케이션의 환자 및 결제 데이터가 감염될 수 있는 상당한 수준의 측면 확산이 발생할 수 있습니다. 또한 격리 기능이 거의 없기 때문에 감사자에게 컴플라이언스를 입증하려면 보안 로그를 일일이 살펴봐야 하는 수작업이 필요했습니다.

마찬가지로 트래픽 및 애플리케이션 의존성에 대한 가시성이 부족해 Azure로 워크로드를 이전하려는 시도가 힘을 얻지 못하고 있었습니다.

Akamai를 선택한 이유

VLAN 또는 방화벽을 사용하여 기업의 현재 가시성 및 보안 문제를 해결하려면 필요한 네트워크 변경을 실행하기 위해 이미 한계에 다다른 여러 팀 간의 조정과 상당한 노력이 필요했을 것입니다.

따라서 Akamai 팀이 다양한 환경을 세부적으로 매핑하고 온프레미스와 클라우드 전반의 워크로드에 세그멘테이션 정책을 일관되게 적용할 수 있는 소프트웨어 정의 세그멘테이션 접근 방식을 시연할 수 있게 되자, 이해관계자들은 예산을 확보하고 IT 경영진은 구매 결정을 내렸습니다.

Large Healthcare Systen

업계
헬스케어

솔루션
Akamai Guardicore Segmentation

주요 장점
- 무단 측면 이동 방지
- 중요 애플리케이션 보호
- 컴플라이언스 간소화 및 가속화
- 클라우드로의 안전한 전환 지원

Akamai

Akamai Guardicore Segmentation 결과

마이크로세그멘테이션의 간소화 및 가속화

Akamai Guardicore Segmentation은 기반 인프라와 독립적으로 소프트웨어 오버레이 접근 방식을 사용하기 때문에 고객 보안 팀은 세그멘테이션 프로젝트를 독립적으로 가속해 다른 그룹에 미치는 영향을 제한할 수 있었습니다.

이 새로운 플랫폼을 통해 중요한 애플리케이션을 신속하고 엄격하게 제한하여 다운타임이나 애플리케이션 또는 네트워크 변경 없이 데이터 센터에 대한 디바이스 접속을 제한할 수 있었습니다. 실시간 및 과거 데이터에 대한 새로운 가시성을 통해 이제 기업은 모든 규제 자산이 효과적으로 격리되어 있음을 감사자에게 쉽게 증명할 수 있습니다. 현재 이 회사는 단 두 명의 직원으로 데이터 센터 보안을 관리하고 있습니다.

마지막으로 헬스케어 시스템은 애플리케이션 의존성을 매핑하고 필요한 정책을 생성함으로써 클라우드 도입 목표를 성공적으로 달성하고 향후 클라우드로 워크로드를 전환하는 경우에도 보안을 안전하게 유지할 수 있었습니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

> 모든 잠재적 헬스케어 고객에게 [Akamai] 솔루션을 보여 줘야 합니다. 그러면 전체 데이터 센터 트래픽을 단일 뷰에서 볼 수 있고, 하이브리드 클라우드 환경에서 보안 정책을 만들고 적용하기가 얼마나 쉬운지 알 수 있을 겁니다.
>
> – 대규모 헬스케어 시스템의 IT 보안 리더