AKAMAI 고객 사례

# Akamai Guardicore Segmentation을 통해 보안 제어를 표준화하고 시간을 절약한 상장 제조 기업

제조 기업에 필요한 안전한 글로벌 솔루션

포괄적인 네트워크 가시성

IT 인프라 간 세그멘테이션

랜섬웨어 위협에 대한 대응

## 고객사

이 선도적인 제조 기업은 NYSE에 상장되었으며, 글로벌 시장에서 서비스를 제공하고 있습니다.

## 도전 과제

### 글로벌 기업 보호

IT 보안 그룹은 전 세계의 수많은 사이트를 담당하고 있으며, 그 중 대부분은 사무실과 제조 시설이 혼합된 환경입니다. 강력한 보안 체계를 구축하기 위해 IT 보안 팀은 기업 전반의 보안 제어를 표준화하고 분산된 여러 지역에서 일관된 보호 기능을 제공해야 했습니다.

세그멘테이션 프로젝트를 맡고 있는 인프라 아키텍처는 "우리는 개방형 플랫 네트워크에서 세그먼트 아키텍처의 모범 사례로 전환하고 싶었습니다."라고 설명했습니다.

많은 기업과 마찬가지로 이 제조 기업도 처음에는 방화벽에 눈을 돌렸습니다.

그러나 네트워크에서 인프라 기반 룰 및 워크스테이션 수준의 변경과 업그레이드를 관리하는 데 많은 시간이 걸렸습니다. 단일 사이트에서도 마찬가지였습니다. 가시성이 향상되긴 했지만 특정 영역에만 국한되어 네트워크 활동 및 자산 간 의존성을 중앙에서 완벽하게 파악하기 어려웠습니다.

### 무단 측면 이동 방지

방화벽이 대략적인 세그멘테이션 제어를 제공하긴 하지만, 이 기능으로는 보안 팀의 또 다른 주요 사안인 관리되지 않는 P2P(Peer-to-Peer) 통신을 해결하지 못했습니다. 따라서 특정 영역까지 보호와 가시성을 확장하는 기능이 필요했습니다. 이 문제를 해결하지 않으면 기업은 PTH(Pass-the-Hash) 공격, 랜섬웨어 및 엔드포인트 간 측면 이동에 의존하는 기타 위협에 취약해질 가능성이 있었습니다.

Manufacturing Company

**위치**
미국

**업계**
제조

**솔루션**
Akamai Guardicore Segmentation

**주요 장점**
- 측면 이동을 통한 멀웨어 확산 방어
- 정밀한 가시성 제공
- 세그멘테이션으로 엔드포인트 보안
- 신속한 인시던트 대응

Akamai

## 솔루션 선택

여러 차례에 걸쳐 방화벽 제어 시스템을 힘겹게 구축한 후, Akamai Guardicore Segmentation에 대해 알게 된 이들은 차세대 세그멘테이션의 이점과 가능성에 대한 내부 논의를 시작했습니다.

보안 팀은 여러 대안을 평가하기 위해 회사가 구축하는 모든 새로운 솔루션을 종합적으로 조사해야 했습니다. 철저한 심사 과정을 거친 팀은 결국 Akamai Guardicore Segmentation을 선택하게 되었습니다. 인프라 아키텍트는 이렇게 말했습니다. "클라이언트의 단일 에이전트만을 통해 트래픽 모니터링, 유연한 레이블링, 풍부한 애플리케이션 수준 가시성을 갖춘 완전한 솔루션을 제공하는 기업은 [Akamai]가 유일했습니다."

> 머신에 단일 에이전트를 배포해 측면 이동으로 인한 엔드포인트 공격 문제를 해결했습니다.
>
> 제조 기업 인프라 아키텍처

## Akamai Guardicore Segmentation

회사는 프로젝트의 첫 번째 단계에서 약 2천 대의 워크스테이션에 Akamai Guardicore Segmentation을 배포했습니다. IT 보안 팀은 솔루션을 구축하자마자 바로 네트워크와 통신 흐름에 대한 새로운 수준의 가시성을 경험했습니다.

### 새로운 인사이트 및 세그멘테이션 활용

인프라 아키텍트는 이렇게 덧붙였습니다. "[Akamai] 트래픽 맵으로 가시성이 1000% 개선되었고 PC 간 통신에 대한 가시성도 확보했습니다."

회사는 개별 컴퓨터의 활동을 드릴다운하는 동시에 전체 애플리케이션 수준의 활동을 파악하는 기능으로 정보에 입각해 보다 나은 보안 결정을 내릴 수 있게 되었습니다. 예를 들어 일부 사용자가 회사 노트북에 가정용 프린터 애플리케이션을 설치했습니다. 그런데 이러한 애플리케이션 중 다수가 회사 네트워크에서 지원되는 디바이스를 지속적으로 스캔하는 것으로 밝혀졌습니다. 보안 팀은 Akamai의 가시성에서 얻은 새로운 인사이트를 바탕으로 이러한 스캔을 차단할 수 있었습니다.

### Akamai Hunt: Akamai Guardicore Segmentation을 활용한 위협 탐지

네트워크 활동에 대한 새로운 이해는 외부 공격자를 저지하는 데에도 큰 도움이 되었습니다. 예를 들어 플랫폼을 배포한 직후 Akamai Hunt 서비스는 GoldenSpy로 알려진 멀웨어의 특성을 갖고 있는 파일과 자산의 통신을 탐지했습니다. Hunt 팀은 탐지된 위협을 회사 IT 보안 팀에 알렸습니다. 또한 고객에게 감염 범위 분석, 잠재적 리스크(GoldenSpy에 대한 MITRE의 정보와 조사 일치), 포렌식(Insight 활용), 내부 조사 및 방어를 위한 권장 사항을 제공했습니다. 이후 회사는 Akamai 정책 제어를 사용해 감염된 시스템을 격리하고 멀웨어가 새로운 머신으로 측면 이동하는 것을 차단했습니다.

### 표준화 및 시간 절약

이제 이 회사는 중앙 글로벌 워크스테이션 정책을 포함해 여러 정책을 중앙에서 생성 및 관리할 수 있으며, 사용 사례에 필요한 경우 일회성 예외를 생성할 수 있는 유연성도 갖추었습니다. 이를 통해 Akamai 에이전트가 배포된 모든 곳에서 일관성 있게 정책을 적용하고 설정 실수 및 지연 리스크를 줄일 수 있습니다.

또한 기업의 정책 수립 시간도 크게 단축되었습니다. 예를 들어, 새 플랫폼을 사용하기 전에는 방화벽 제어를 변경하는 데 수일의 기간이 소요되었습니다. IT 보안 팀은 Akamai의 새로운 정책 템플릿을 초기 가이드로 사용해 가장 복잡한 사용 사례도 1시간 이내에 보안 제어를 생성하고 단 몇 초 만에 전체 설치 기반에 적용할 수 있습니다.

## Akamai와 함께하는 미래

프로젝트는 초기에 엔드포인트 세그멘테이션 및 접속에 대한 보안 제어의 표준화에 초점을 맞추었지만, Akamai를 통해 추가적인 사용 사례도 처리할 계획입니다. 관계자들은 기업의 ERP 시스템과 같은 서버 및 중요한 애플리케이션을 포함하도록 보호 기능을 확장하는 방안을 논의 중입니다.

앞으로의 계획에 무엇을 포함하든, 원래 프로젝트는 이미 제조업체의 성공 사례로 인정받았으며 기업 워크스테이션의 공격표면 및 리스크를 크게 줄였습니다. 이제 보안 팀은 엔드포인트 간 측면 이동 공격에 대한 기업의 보안 체계를 더욱 신뢰할 수 있게 되었습니다. 프로젝트 리더는 이렇게 말했습니다. "머신에서 에이전트 하나만으로 문제를 영구적으로 해결했고, 30초 안에 정책이 없는 워크스테이션에서 완전한 보안 제어 구현으로 전환할 수 있습니다."

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

> [Akamai] 트래픽 맵으로 가시성이 1000% 개선되었고 PC 간 통신에 대한 가시성도 확보했습니다.
>
> 제조 기업 인프라 아키텍처