AKAMAI 제품 설명서

IoT 및 OT를 위한 세그멘테이션

제로 트러스트 세그멘테이션 기능을 모든 커넥티드 디바이스로 확장하기

많은 기업이 성장을 촉진하고, 효율성을 높이고, 고객에게 보다 효과적인 서비스를 제공하기 위해 사물 인터넷(IoT) 디바이스 및 운영 기술(OT)의 사용을 확대하고 있습니다. 이러한 기술은 상당한 비즈니스 가치를 창출할 수 있지만, 보안팀이 방어해야 하는 중요한 새로운 공격 기법이기도 합니다. IoT 디바이스는 특히 하드웨어 및 소프트웨어 취약점에 취약하고, 많은 레거시 OT 시스템은 커넥티드 세상의 보안 요구 사항을 염두에 두고 설계되지 않았습니다. Akamai Guardicore Segmentation은 제로 트러스트 보안을 이러한 디바이스로 확장함으로써 공격자가 디바이스를 악용해 더 광범위한 기업 IT 인프라에 접속할 수 있는 리스크를 줄여줍니다.

기업이 누릴 수 있는 혜택

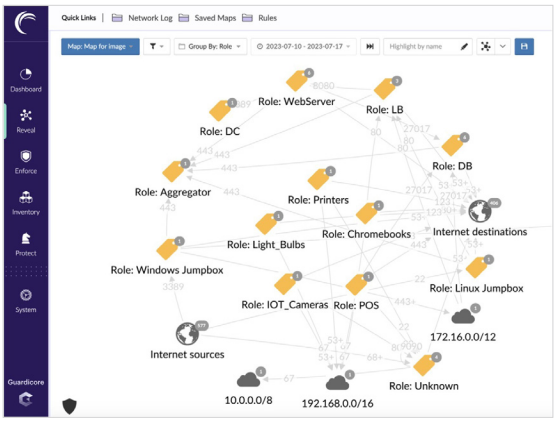
- 모든 커넥티드 디바이스 검색, 핑거프린팅, 분류
- 특수 IoT 및 OT 시스템을 포함해 단일 인터페이스에서 제로 트러스트 세그멘테이션 정책 구축
- 에이전트 기반 및 에이전트리스 정책 실행을 결합해 전체 적용 범위 보장

새로운 커넥티드 디바이스를 지속적으로 검색

IoT 및 OT 디바이스의 배포는 엔드포인트 및 기타 기존 엔터프라이즈 디바이스와는 큰 차이를 보입니다. 특히 IoT 및 OT 디바이스는 훨씬 더 많은 수량이 배포되며, 진화하는 운영 요구사항에 따라 디바이스 설치 공간이 동적으로 변경됩니다. Akamai Guardicore Segmentation은 모든 커넥티드 IoT 및 OT 디바이스를 지속적으로 모니터링하고 검색합니다. 이를 통해 승인되지 않은 디바이스는 통신을 차단하고 승인된 디바이스는 인벤토리화해 보호합니다.

모든 커넥티드 디바이스 식별 및 분류

Akamai Guardicore Segmentation에는 디바이스 핑거프린팅이 통합되어 있습니다. Akamai의 정교한 접근 방식은 쉽게 스푸핑되는 디바이스 식별자를 뛰어넘어 네트워크 행동 및 기타 신호를 분석해 모든 네트워크 커넥티드 디바이스에 대한 신뢰할 수 있는 핑거프린트를 개발합니다. 디바이스가 식별되면 확장 가능한 추상적인 보안 정책을 만드는 데 사용할 수 있는 카테고리로 그룹화됩니다.



모든 엔터프라이즈 자산을 함께 시각화

Akamai Guardicore Segmentation을 통해 검색 및 분류된 IoT 및 OT 디바이스는 고도로 상호 작용하는 단일 시각적 인터페이스인 Akamai의 Guardicore Reveal 맵에 기존의 엔터프라이즈 엔드포인트 및 애플리케이션 워크로드와 함께 표시됩니다. 이를 통해 보안팀은 모든 종류의 커넥티드 디바이스가 서로 상호 작용하는 방식을 쉽게 파악하고 호스트 기반 및 에이전트리스 적용 기술을 결합한 효과적인 제로 트러스트 세그멘테이션 전략을 개발할 수 있습니다.

모든 디바이스에 정밀한 세그멘테이션 정책 적용

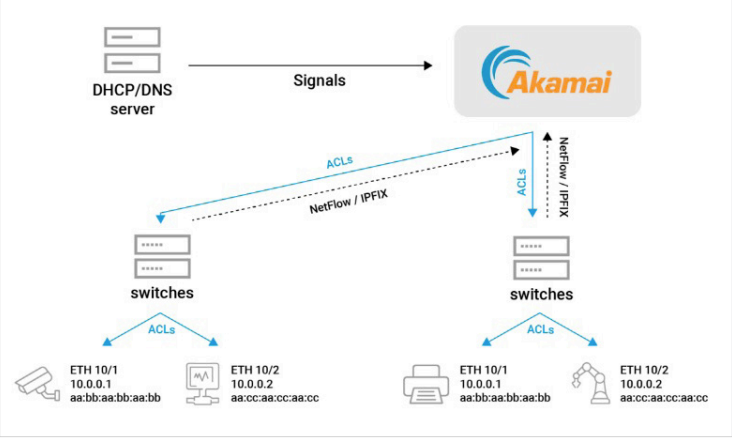
Akamai Guardicore Segmentation은 호스트 기반 보안 소프트웨어를 실행할 수 없는 IoT 디바이스 및 OT 시스템을 위해 특별히 설계된 네트워크 기반 세그멘테이션을 제공함으로써 제로 트러스트 정책 적용을 원활하게 확장합니다. 이를 통해 OT 디바이스와 IoT 디바이스는 물론 기타 네트워크 리소스 간의 통신을 제어하고 제한할 수 있습니다. 또한 보안 경계를 설정하면서 IT 관리 시스템, 전용 업데이트 서버, 로깅 서버에 필요한 연결은 허용할 수 있습니다.

디바이스 로밍 시 가시성 및 제어 유지

Akamai Guardicore Segmentation 아키텍처는 디바이스가 새로운 네트워크 위치로 로밍되는 경우에도 인식과 가시성을 유지합니다. 이를 통해 필요한 위치 기반 조정을 포함해 적절한 제로 트러스트 세그멘테이션 정책이 항상 적용되도록 보장합니다.

작동 방식

네트워크 디바이스에서 생성되는 트래픽은 모든 디바이스를 식별하고 분류하는 데 사용되는 신호(예: DHCP, DNS, Netflow, TCP 등)를 제공하고, 이 신호는 Akamai Guardicore Segmentation에서 사용됩니다. 그런 다음 통합 인터페이스를 통해 세그멘테이션 정책을 생성할 수 있습니다. IoT 및 OT 디바이스, 호스트 기반 에이전트를 실행할 수 없는 기타 디바이스의 경우 네트워크 수준에서 접속 제어 룰을 자동으로 구축해 세그멘테이션 정책을 시행합니다.



제로 트러스트를 IoT 및 OT로 확장하는 방법에 대해 자세히 알아보려면 Akamai 웹사이트를 방문하세요