AKAMAI 제품 설명서

Akamai Guardicore Access
통합 ZTNA 및 마이크로세그멘테이션

가시성 및 제어를 위한 단일 콘솔로 제로 트러스트 간소화 및 가속

기업은 랜섬웨어를 차단하고 컴플라이언스 요구사항을 충족하며 하이브리드 인력 및 클라우드 인프라를 보호하기 위해 제로 트러스트 보안을 빠르게 도입하고 있습니다. ZTNA(Zero Trust Network Access) 및 마이크로세그멘테이션은 제로 트러스트 아키텍처로 전환하는 기업에게 가장 중요한 두 가지 솔루션입니다. 모두 공격 표면을 줄이고 유출을 차단하며 사용자 경험을 강화해 접속 제어를 개선하는 데 도움이 됩니다.

통합의 힘

세그멘테이션과 ZTNA를 결합하는 Akamai Guardicore Access는 단일 에이전트에서 배포되고 단일 콘솔로 관리됩니다. 이 혁신적인 접근 방식은 사용자부터 워크로드까지(남북), 엔드포인트에서 엔드포인트 또는 워크로드까지(동서) 포괄적인 가시성을 보장하기 때문에 ID 기반 애플리케이션 접속 제어 및 엔드포인트 세그멘테이션을 한 번에 수행하도록 지원합니다. 이러한 기술을 결합함으로써 기업은 네트워크 방어 체계를 강화하고 리스크를 방어하며 규제를 준수하는 보안 환경을 조성하는 강력한 보안 프레임워크를 활용할 수 있습니다.

Akamai Guardicore Platform은 업계 최고의 마이크로세그멘테이션 및 ZTNA를 결합해 보안 팀이 랜섬웨어를 차단하고 컴플라이언스 규제를 준수하며 하이브리드 인력과 클라우드 인프라를 모두 보호하도록 지원하는 최초의 보안 플랫폼입니다.

기업은 처음부터 모든 유형의 자산과 인프라에서 단일 콘솔을 사용하는 단일 에이전트로 모든 곳에서 하이브리드 인력에 대한 접속을 손쉽게 관리하면서 세그멘테이션을 구축해 공격 표면을 최소화할 수 있습니다.

핵심 기능

엔드투엔드 가시성

엔드투엔드 가시성을 통해 네트워크를 완벽하게 파악하면 맵과 로그 모두에 관련 네트워크 정보를 표시하고 최종 사용자의 접속 패턴에 대한 인사이트를 제공할 수 있습니다. 세그멘테이션 및 ZTNA를 단일 제품으로 결합하는 경우에만 가능합니다. 엔드포인트에서 워크로드, 프로세스 수준까지의 연결 경로를 확인하세요. 실시간에 가까운 과거 가시성을 통해 포렌식 분석을 더 쉽게 진행하고 보다 빠르게 방어할 수 있습니다.

기업이 누릴 수 있는 혜택

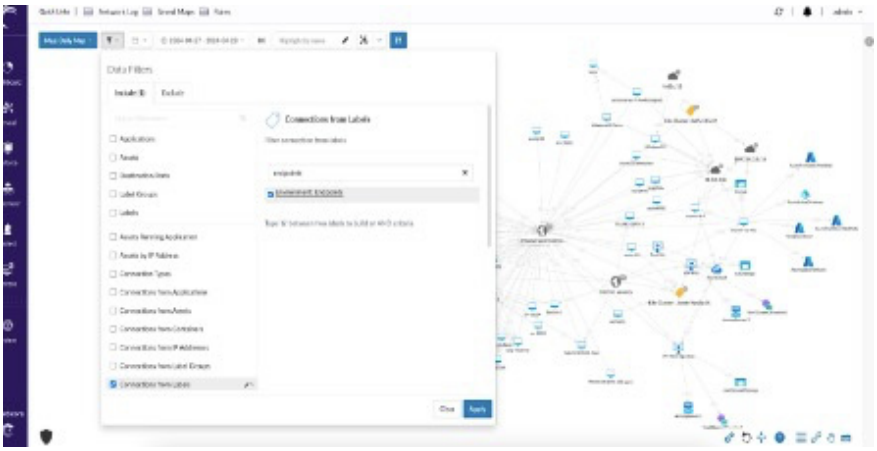
단일 콘솔, 단일 에이전트
단일 콘솔을 사용하는 단일 에이전트를 통해 모든 곳에서 하이브리드 인력의 접속을 손쉽게 관리하는 동시에 공격 표면을 최소화하기 위한 세그멘테이션 구축

넓은 보호 범위
모든 곳에서 접속 제어를 적용하고 사무실 및 원격 인력 보안

정책 통합
구문이나 콘솔을 변경할 필요 없이 동서 트래픽과 남북 접속에 대한 정책을 적용해 가장 간단하고 효과적인 방법으로 제로 트러스트 구축

애플리케이션 검색

접속 권한이 필요한 애플리케이션을 빠르게 식별해 정책 소요 시간을 단축합니다. 프라이빗 애플리케이션을 간편하게 검색하고 사용자 접속 및 빈도를 비롯한 사용 패턴에 대한 귀중한 인사이트를 제공합니다.



접속이 필요한 애플리케이션을 간편하게 검색

접속 및 세그멘테이션 정책 동기화

접속 제어 및 세그멘테이션 룰을 자동으로 동기화해 팀 간 의존성을 줄이고 인적 오류를 방지합니다.

주요 사용 사례

포괄적인 랜섬웨어 보안: ID 기반 및 머신 간 정책을 통해 랜섬웨어 및 기타 멀웨어 공격의 가능성과 영향을 줄입니다. 정밀한 접속 제어를 적용하는 동시에 엔드포인트가 최소 권한에 기반해 리소스에 접속하도록 보장합니다.

- 고부가가치 자산 보호: 사용자가 보안 접속 제어를 기반으로 중요한 자산에 접속하고 직접 VPN 트래픽 차단
- 권한 있는 사용자 제한: 악용 가능한 관리 포트에 대한 VPN 트래픽을 차단해 관리자에게 보안 접속 제공

인력 배분: 엄격한 접속 제어를 적용해 각 디바이스를 필요한 리소스에만 연결할 수 있도록 보장함으로써 장소에 상관없이 업무를 지원합니다. 그러면 공격 표면이 최소화되고 네트워크 내부 측면 이동이 줄어듭니다.

컴플라이언스: 기업의 엔드포인트에서 관련 업계 표준 및 규정을 준수하도록 엔드포인트 세그멘테이션 정책을 구축함으로써 규정 미준수 불이익 리스크를 줄이고 전반적인 보안 체계를 강화합니다.

써드파티 접속: 전용 Akamai 포털을 통해 에이전트 접속을 라우팅 및 인증함으로써 계약자와 파트너가 에이전트를 설치하지 않고 특정 애플리케이션에 연결할 수 있도록 지원합니다.

자세한 내용은 Akamai 제로 트러스트 보안에서 확인하세요