AKAMAI 제품 설명서

Akamai Guardicore Segmentation

정밀한 가시성과 마이크로세그멘테이션 제어를 통한 측면 이동 차단

기업 IT 인프라는 전통적인 온프레미스 데이터센터에서 클라우드 및 하이브리드 클라우드 아키텍처로 계속 진화하고 있으며 플랫폼과 애플리케이션 배포 모델이 혼합되어 있습니다. 많은 기업들이 이런 디지털 전환을 통해 비즈니스 민첩성을 강화하고, 인프라 비용을 절감하며, 원격 근무를 지원하고 있지만 경계가 분명하게 정의되지 않은 보다 크고 복잡한 공격 표면도 만들어지고 있습니다. 따라서 개별 서버, 가상 머신, 클라우드 인스턴스, 엔드포인트가 노출될 수 있습니다. 랜섬웨어와 제로데이 취약점 등의 위협이 빈번하게 발생하면서 공격자들은 침투하는 방법을 찾으면 부가가치가 높은 표적으로 측면 이동하는 데 점점 능숙해지고 있습니다.

Akamai Guardicore Segmentation은 네트워크 내에 제로 트러스트 원칙을 구현하는 가장 간편하고, 빠르고, 직관적인 방법을 제공합니다. IT 환경 내부의 활동을 시각화하고 정밀한 마이크로세그멘테이션 정책을 구축하며 유출을 신속하게 탐지함으로써 측면 이동을 차단합니다.

기업이 누릴 수 있는 혜택

- 랜섬웨어 차단
- 제로 트러스트 구축
- 컴플라이언스 가속
- 중요한 애플리케이션 보호
- 안전하게 클라우드로 전환
- 원격 근무자 보호
- 엔드포인트 보호
- 내부 방화벽에서 전환

핵심 기능

AI 기반의 정밀한 세그멘테이션

AI 추천, 랜섬웨어와 기타 일반적인 사용 사례를 위한 템플릿, 정확한 워크로드 속성(프로세스, 사용자, 도메인 이름 등)을 사용해 몇 번의 클릭만으로 정책을 실행합니다.

실시간 및 이력 가시성

애플리케이션 의존성을 매핑하고 실시간 또는 이력을 바탕으로 사용자와 프로세스 레벨까지 추적합니다.

광범위한 플랫폼 지원

베어메탈 서버, 가상 머신, 컨테이너, IoT, 클라우드 인스턴스에 걸쳐 최신 및 레거시 운영 체제를 지원합니다.

유연한 자산 레이블링

맞춤형 레이블링 계층 구조로 강력한 컨텍스트를 추가해 가시성과 실행력을 높여주고, 오케스트레이션 툴과 설정 관리 데이터베이스를 통합해 레이블링을 자동화합니다.

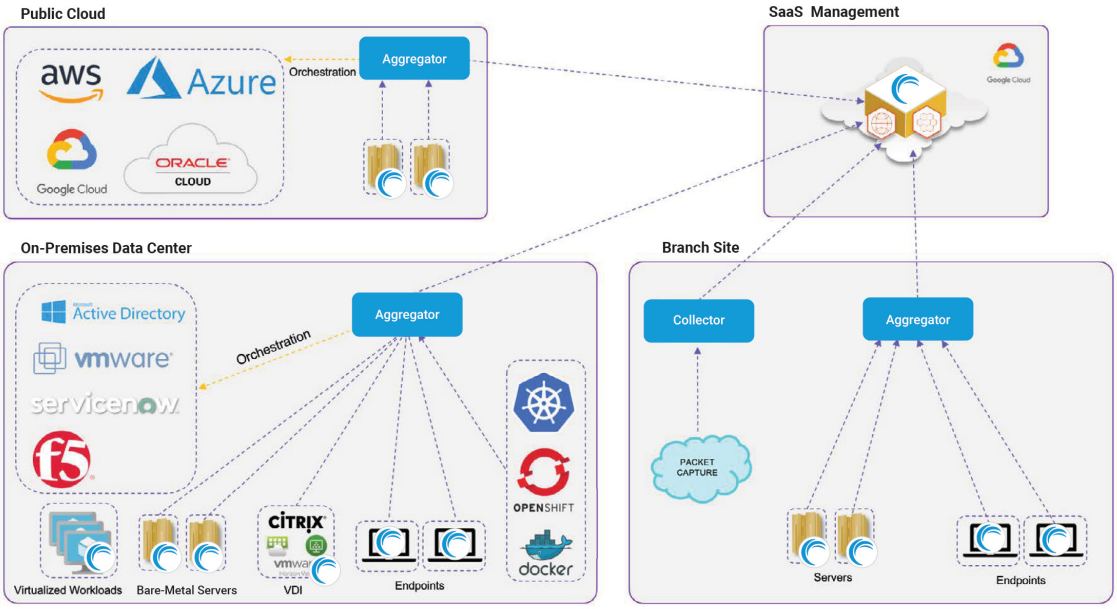
다양한 보안 방법

위협 인텔리전스, 방어, 유출 탐지 기능을 통합하여 인시던트 대응 시간을 단축합니다.

작동 방식

Akamai Guardicore Segmentation은 에이전트 기반 센서, 네트워크 기반 데이터 수집기, 클라우드 공급업체의 가상 프라이빗 클라우드 흐름 로그, 에이전트리스 기능을 구현하는 통합을 통해 기업의 IT 인프라에 대해 상세한 정보를 수집합니다. 오케스트레이션 시스템과 설정 관리 데이터베이스 같은 기존 데이터 소스와 통합되는 유연하고 고도로 자동화된 레이블링 프로세스를 통해 이런 정보에 관련성 있는 컨텍스트를 추가합니다.

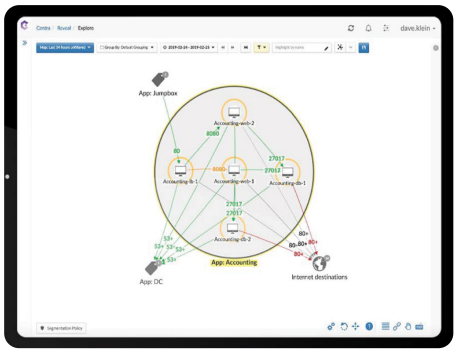
인프라 토폴로지



대부분의 고객은 SaaS 관리를 사용하지만 온프레미스 관리 옵션도 사용할 수 있습니다.

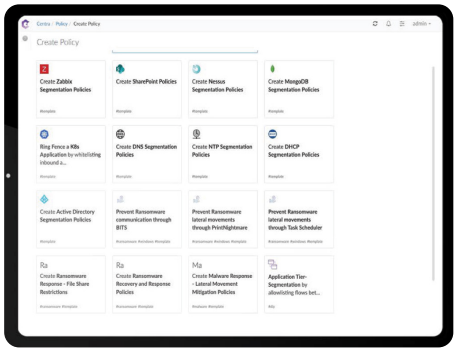
네트워크 맵

전체 IT 인프라에 대한 동적 맵이 생성되므로 보안팀은 실시간 또는 이력을 바탕으로 사용자 및 프로세스 레벨에서 활동을 상세히 파악할 수 있습니다. 이러한 상세 정보에 AI 기반 정책 워크플로우가 결합되어 실제 워크로드 컨텍스트를 기반으로 빠르고 직관적으로 세그멘테이션 정책을 생성할 수 있습니다.



템플릿

미리 구축된 템플릿으로 대부분의 일반적인 사용 사례에 대한 정책을 간편하게 생성할 수 있습니다. 정책이 기본 인프라와 완전히 분리되어 실행되기 때문에 복잡한 네트워크 변경이나 다운타임 없이 보안 정책을 생성하거나 변경할 수 있습니다. 또한 온프레미스 데이터센터나 퍼블릭 클라우드 환경 등 워크로드의 위치와 상관 없이 정책은 워크로드를 따라갑니다. 정교한 위협 헌팅 및 유출 탐지 기능은 물론 Akamai Hunt 매니지드 위협 탐지 서비스가 세그멘테이션 기능을 보완합니다.



포괄적이고 확장이 가능한 보안

모든 환경

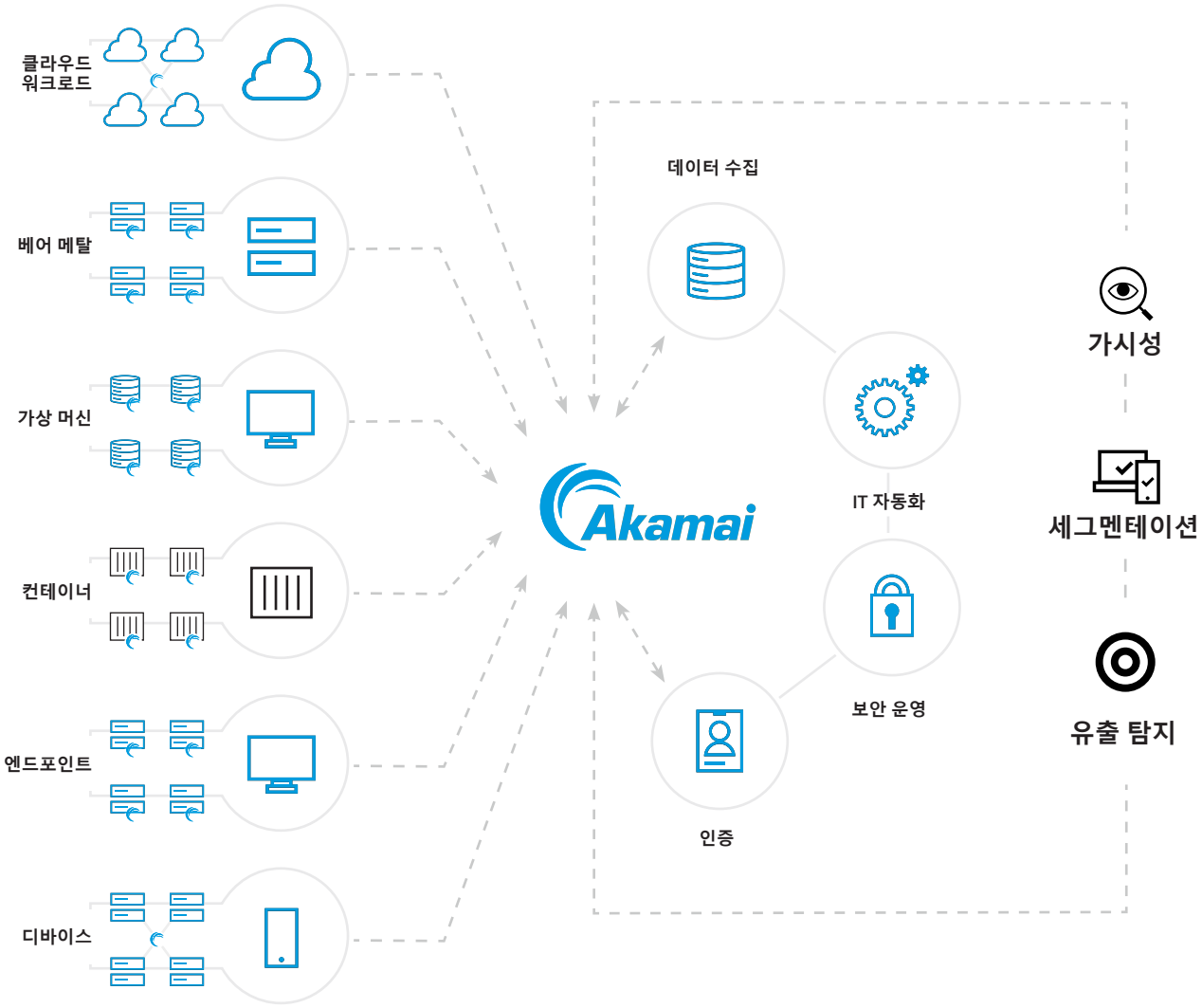
다양한 온프레미스 워크로드, 가상 머신, 레거시 시스템, 컨테이너 및 오케스트레이션, 퍼블릭 및 프라이빗 클라우드 인스턴스, IoT를 통합해 복잡한 IT 환경에서 워크로드를 보호합니다.

보안 간소화

네트워크 시각화, 세그멘테이션, 위협 방어, 유출 탐지 기능, 제로 트러스트 이니셔티브를 위한 정책 실행을 제공하는 하나의 플랫폼으로 보안 관리를 간소화합니다.

확장성 및 성능

가장 중요한 디지털 자산부터 집중적으로 보호하기 시작해 복잡성, 인프라 변경, 성능 병목 현상 없이 기업 전체를 보호합니다.



지원 플랫폼 및 기술

- Akamai Guardicore Segmentation은 기존 인프라와 통합되도록 설계되었습니다.
- 고객의 필요에 따라 OS 지원을 계속 확장하고 있습니다.
- 전체 통합 목록을 보려면 기술 파트너 페이지를 확인하세요.

운영 체제

Linux

Apple

Microsoft

Unix

퍼블릭 클라우드 공급업체

하이퍼바이저

하이퍼비전 오케스트레이션

보안 게이트웨이

컨테이너 오케스트레이션 및 엔진

웹 콘솔용 브라우저

메모리 및 시스템 최소 요구 사항

Management Server
32 GB RAM, 8 vCPUs, 530 GB

Aggregator
4 GB RAM, 4 vCPUs, 30 GB

Deception Server
32 GB RAM, 8 vCPUs, 100 GB

ESC Collector
2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Akamai Guardicore Segmentation에 대한 자세한 내용이 궁금하시거나 개인 맞춤형 제품 데모를 요청하려면 akamai.com/guardicore를 방문하시기 바랍니다.

 | 지원 | 2025년 3월 발행.