Akamai 솔루션 설명서

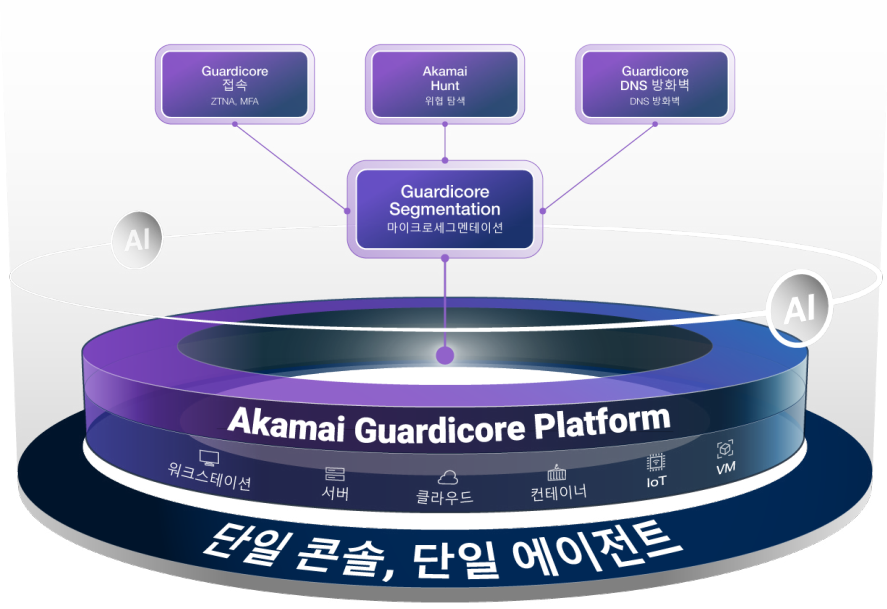
Akamai Guardicore Platform: 제로 트러스트 보안

대부분의 기업에서 제로 트러스트를 구축하는 것은 매우 복잡하고 비용이 많이 드는 과정이며, 온프레미스와 클라우드의 자산과 원격 또는 사무실 인력을 보호해야 하는 경우 부담이 더욱 가중될 수 있습니다. 이것이 바로 Akamai Guardicore Platform이 하나의 콘솔과 에이전트로 제로 트러스트의 모든 기능을 효율적으로 처리하도록 설계된 이유입니다.

사이버 위협이 점점 더 정교해지고 규제 요건이 계속 강화됨에 따라, 기업은 운영 효율성을 유지하면서 네트워크를 보호해야 하는 큰 부담에 직면했습니다. Akamai Guardicore Platform은 강력한 제로 트러스트 보안 모델을 효과적으로 구축하는 데 필요한 툴과 기능을 제공함으로써 이러한 문제를 해결할 수 있는 포괄적인 제로 트러스트 솔루션을 제공합니다.

Akamai Guardicore Platform은 동급 최고의 마이크로세그멘테이션, ZTNA(Zero Trust Network Access), DNS 방화벽, 위협 탐색을 하나의 플랫폼으로 결합해 제로 트러스트 프로젝트를 지원합니다. 이러한 구성요소를 함께 활용하면 제로 트러스트 구축을 위한 노력을 간소화해 공격표면을 크게 줄이고 기업 전체의 보안 체계를 강화할 수 있습니다.

Akamai Guardicore Platform



마이크로세그멘테이션

Akamai Guardicore Platform의 핵심 구성요소 중 하나는 마이크로세그멘테이션입니다. 네트워크 보안은 전통적으로 네트워크 외부의 경계를 보호하는 데 중점을 둔 경계 기반 방어에 의존해 왔습니다. 그러나 사이버 위협이 진화하면서 경계 방어만으로는 더 이상 정교한 공격을 방어하기에 충분하지 않다는 것이 점점 더 분명해지고 있습니다.

장점

통합 인프라
성능에 미치는 영향을 최소화하면서 신속하게 배포하고 손쉽게 확장하세요.

광범위하고 풍부한 가시성
네트워크 자산 및 통신에 대한 포괄적인 인사이트를 확보하세요.

통합 정책 엔진
단일 UI로 다양한 환경 전반에 대한 정책 적용을 간소화하세요.

모듈식 유연성
비즈니스 요구사항에 맞는 모듈식 구성요소를 활용하세요.

완벽한 적용 범위
온프레미스와 클라우드에 있는 모든 자산과 가정 및 사무실의 사용자를 보호하세요.

동급 최고의 솔루션
업계 최고의 마이크로세그멘테이션과 ZTNA를 결합해 보안 체계를 강화하세요.

Akamai

마이크로세그멘테이션은 네트워크를 보다 작고 관리하기 쉬운 세그먼트로 나누고 최소 권한 원칙에 따라 각 세그먼트에 보안 정책을 적용하는 새로운 접근 방식을 취합니다. 세분화된 보안 접근 방식은 하나의 세그먼트가 감염되더라도 나머지 네트워크는 보안이 유지됩니다. 온프레미스 데이터센터, 클라우드 인스턴스, 레거시 OS, IoT 디바이스, 쿠버네티스 클러스터 등을 모두 보호하는 Akamai Guardicore Segmentation을 사용하면 콘솔을 변경할 필요 없이 모든 자산을 보호할 수 있습니다.

ZTNA(Zero Trust Network Access)

Akamai Guardicore Platform은 마이크로세그멘테이션 외에 ZTNA(Zero Trust Network Access) 기능도 제공합니다. ZTNA는 제로 트러스트를 가정하는 보안 모델로, 기업 네트워크 내부에 있더라도 기본적으로 어떤 사용자나 디바이스도 신뢰하지 않습니다. 대신 ID, 디바이스 체계, 기타 상황적 요인에 대한 엄격한 검증을 기반으로 리소스에 대한 접속 권한을 부여합니다. 이러한 접근 방식은 무단 접속의 리스크를 최소화하고 기업이 데이터 유출 및 내부자 위협을 방지하는 데 도움을 줍니다.

DNS 방화벽

Akamai Guardicore Platform의 또 다른 핵심 구성요소는 DNS 방화벽입니다. DNS(Domain Name System)는 사람이 읽을 수 있는 도메인 이름을 IP 주소로 변환하는 인터넷의 기본 구성요소입니다. 그러나 수많은 멀웨어 변종이 명령 및 제어 서버와 통신하거나 데이터를 유출하는 데 DNS를 이용하기 때문에 사이버 공격의 일반적인 표적이 되기도 합니다. 기업은 DNS 방화벽을 배포함으로써 악성 DNS 쿼리를 차단하고 멀웨어가 악성 도메인과 통신하는 것을 방지해 데이터 유출과 기타 사이버 위협의 리스크를 줄일 수 있습니다.

위협 탐색

마지막으로 Akamai Guardicore Platform에는 보안 위협이 본격적인 인시던트로 확대되기 전에 선제적으로 식별하고 방어할 수 있는 적응형 세그멘테이션 서비스가 포함되어 있습니다. 위협 탐색은 네트워크 내에서 비정상적인 행동이나 IOC(Indicator Of Compromise)와 같은 감염 징후를 능동적으로 검색합니다. 기업은 위협 탐색 툴과 기술을 활용함으로써 사이버 공격자보다 한 발 앞서 대응하고 소중한 자산을 위험으로부터 보호할 수 있습니다.

Akamai Guardicore Platform은 핵심적인 기능 외에도 시중의 다른 보안 솔루션과 차별화되는 몇 가지 주요 장점을 제공합니다. 이 플랫폼은 에이전트 부하와 콘솔 피로를 최소화하는 경량의 통합 인프라를 제공해 기업이 보안 스택을 보다 효율적으로 배포하고 관리할 수 있도록 지원합니다. 또한 네트워크 자산과 통신에 대한 광범위하고 풍부한 가시성을 제공해 보안 전문가가 네트워크 환경에 대한 포괄적인 인사이트를 확보하고 위협에 빠르고 효과적으로 대응할 수 있도록 지원합니다.

> Gartner®, Quick Answer: What Is Zero Trust Networking? 보고서(Andrew Lerner, John Watts, 2023년 9월 13일)에서 'Gartner는 ZTN(Zero Trust Networking) 체계로의 전환을 위해 마이크로세그멘테이션 및 ZTNA를 구축할 것을 제안했습니다.'*

자세한 내용은 **Akamai 제로 트러스트 보안**을 참조하시기 바랍니다.