AKAMAI 솔루션 설명서

글로벌 확장성으로 효과적인 보안을 위한 인텔리전스 제공

확장성, 가시성, 인텔리전스

AI 툴을 구동하는 복잡한 알고리즘부터 기업의 CRM 시스템에 저장된 중요한 데이터에 이르기까지, 시스템에 투입되는 정확한 데이터의 양과 결과물의 품질 사이에는 부인할 수 없는 상관관계가 있습니다. 사이버 보안에서는 이러한 양질의 데이터를 수집하는 것이 특히 중요해졌습니다. 다행히 Akamai의 플랫폼은 고객에게 효과적이고 시장을 선도하는 보안 솔루션을 제공하는 데 반드시 필요한 탁월한 확장성을 제공합니다. Akamai의 확장성을 통해 글로벌 활동에 대한 귀중한 가시성을 확보하고 데이터를 유용한 인텔리전스로 전환해 점점 복잡해지는 위협으로부터 기업을 보호할 수 있습니다.

글로벌 도달 범위 및 배포

Akamai의 플랫폼은 전 세계 2000개 지역에 걸쳐 있으며, 다른 공급업체보다 10배에서 100배 더 넓은 커버리지를 제공합니다. 이 광범위한 네트워크는 기업 및 고객과의 근접성을 보장해 비즈니스 성능과 가용성을 향상시킵니다. 또한 DDoS(Distributed Denial of Service)와 같은 증폭 공격에 직면했을 때, 이런 확장성은 강력한 방어 메커니즘으로 작용합니다. 플랫폼은 트래픽을 여러 위치로 분산할 수 있어 공격의 영향을 방어하고, 지연을 줄이고, 운영을 유지합니다. 플랫폼의 여러 장점은 단순한 보안을 넘어, 수조 개의 경로 조합과 지능적인 트래픽 라우팅을 제공함으로써 사용자 경험을 향상시키는 수준으로 확장됩니다.

전례 없는 데이터 인사이트

Akamai는 최근 하루 평균 788TB의 퍼스트파티 데이터를 분석했습니다. 이 방대한 데이터 세트와 고급 휴리스틱 및 머신 러닝 모델 덕분에 Akamai는 여러 애널리스트 기관이 선정한 글로벌 트래픽 패턴 분석, 이벤트 추적, 위협 탐지 분야의 리더로 자리매김할 수 있었습니다. 이런 확장성에서 비롯된 실시간 인텔리전스는 보안 서비스 및 제품을 강화합니다. 기업들은 CVE와 글로벌 위협으로부터 스스로를 보호하기 위해 끊임없이 노력하고 있습니다. 이런 가운데 Akamai 고객들은 Akamai가 빠르고 정확한 자동 적응형 방어 기능을 제공하기 위해 머신 러닝으로 지속적으로 업데이트 및 분석하는 9PB 규모의 인텔리전스 데이터베이스를 믿고 활용할 수 있습니다.

DDoS 공격에 대한 강력한 방어

DDoS 공격과 같이 리소스 과부하를 목표로 하는 시나리오에서는 플랫폼의 규모가 운영 유지에 중요한 역할을 합니다. 공격이 전년 대비 45% 증가한 상황에서 Akamai의 규모와 분포는 매우 중요한 의미가 있습니다. 한 위치가 포위 공격을 받으면 트래픽을 인근의 다른 위치로 라우팅해 공격의 효과를 차단할 수 있습니다. 최근 Akamai 플랫폼은 최대 공격 규모가 900GB인 대규모 공격을 견디고 방어하는 능력을 보여주었습니다. Akamai는 레이어 3, 레이어 4, 레이어 7, DNS에서 증폭 공격을 방어해 DDoS 문제를 해결합니다.

Akamai Connected Cloud

클라우드 컴퓨팅, 보안, 콘텐츠 전송을 위한 세계에서 가장 대규모로 분산된 플랫폼

4,100+
엣지 네트워크 거점

1,200+
네트워크

130+
국가

750+
도시

SSD 기반
하드웨어

가용성을 보장하고 리스크를 줄이는 플랫폼 구성요소

DNS 기반의 장점

독점 DNS 네트워크를 포함한 DNS 기반의 아키텍처는 Akamai 플랫폼의 기본적인 구성요소입니다. Akamai 네트워크는 DNS를 인터넷의 관문으로 인식하며 성능에 우선순위를 두고 탁월한 사용자 경험을 제공합니다. DNS 네트워크의 이중화는 100% 가용성 SLA로 뒷받침되는 중단 없는 서비스를 보장합니다.

간소화된 트래픽 관리

Akamai 플랫폼의 기반인 콘텐츠 전송 네트워크는 포트 80 및 포트 443 트래픽만 허용합니다. 이와 같은 즉각적인 조치로 인터넷의 노이즈를 최소화해 공격표면을 크게 줄입니다. 기업은 엣지에서 불필요한 트래픽을 차단함으로써 리스크를 방어하고 해당 트래픽을 지원하는 데 필요한 리소스를 제거해 전반적인 효율성을 향상시킬 수 있습니다.

다양한 보안 솔루션 포트폴리오 지원

Akamai 플랫폼의 규모는 방대하고 균일한 데이터 세트를 생성해 포괄적인 보안 솔루션 포트폴리오에 머신 러닝 기반의 권장 사항을 제공합니다. 이러한 정보를 단일 인터페이스로 제공해 기업이 보안 운영을 간소화하고 리소스를 확보하며 전반적인 사이버 보안 체계를 개선하도록 지원합니다.

결론

Akamai는 플랫폼의 규모 덕분에 25년 이상 신뢰할 수 있는 리더로 자리매김했습니다. 독보적인 규모와 가시성, 최첨단 인텔리전스를 겸비해 기업이 복잡한 위협 환경을 자신 있게 헤쳐나갈 수 있도록 지원합니다. CISO는 보안에 대한 Akamai의 포괄적인 접근 방식을 도입함으로써 업계에서 독보적인 효율성, 안정성, 인텔리전스로 기업을 보호할 수 있습니다.

Akamai 플랫폼의 특별한 성능을 경험하고 싶으신가요?

Akamai의 보안 솔루션은 플랫폼의 고유한 장점을 활용해 기업과 고객을 보호합니다. 고객의 요구사항이 확장되고 변화함에 따라 Akamai는 포트폴리오에 요구사항 변화에 부합하는 솔루션을 도입했습니다. 고객은 다양한 솔루션을 시도, 추가, 변경할 수 있으며 어떤 솔루션이든 단일 플랫폼 포털을 통해 접속하고 하나의 계약으로 처리하며 전담 팀의 지원을 동일하게 받을 수 있습니다.

> Akamai를 사용하면 백그라운드에서 조용하고 효과적으로 보안이 실행됩니다.
>
> **– British Council 운영 및 커머셜 매니저**

Akamai App & API Protector

DDoS, 봇, 애플리케이션 레이어, API 공격 방어

Akamai Bot Manager

정교한 악성 봇은 탐지 및 방어하지만 정상 봇은 허용하도록 설계된 고급 봇 관리 기능

Akamai Account Protector

계정 탈취, 계정 개설 남용, 크리덴셜 스터핑 탐지 및 방어

Akamai Brand Protector

피싱 및 가짜 웹사이트를 포함한 브랜드 사칭 공격 탐지 및 방어

Akamai Client-Side Protection & Compliance

PCI 컴플라이언스 지원 및 자바스크립트 공격으로부터 웹사이트 보호

Akamai Edge DNS

외부 권한 DNS 서비스를 통해 DNS 인프라 강화

Akamai Prolexic

DDoS 공격으로부터 인프라 보호

Akamai API Security

실시간 분석으로 API 활동을 발견, 모니터링, 감사해 위협 및 악용에 대응

> 모든 WAF에서 탐지는 매우 중요합니다. Akamai는 복잡한 환경에서도 탐지가 효과적으로 이뤄지도록 지원합니다.
>
> **– Panasonic 유럽 비즈니스 지원 수석 IT 컨설턴트**

자세한 내용은 애플리케이션 및 API 보안 페이지를 참조하시기 바랍니다.