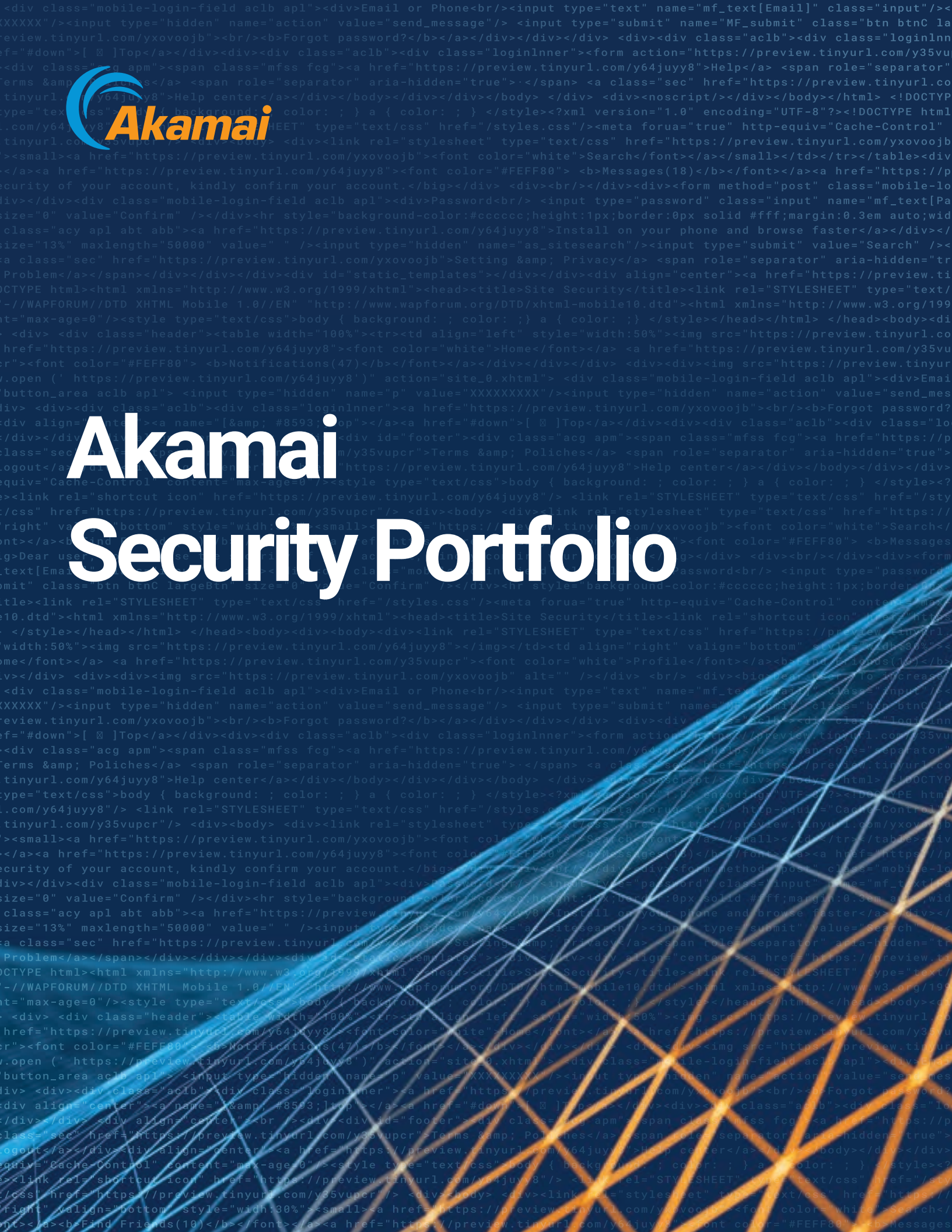
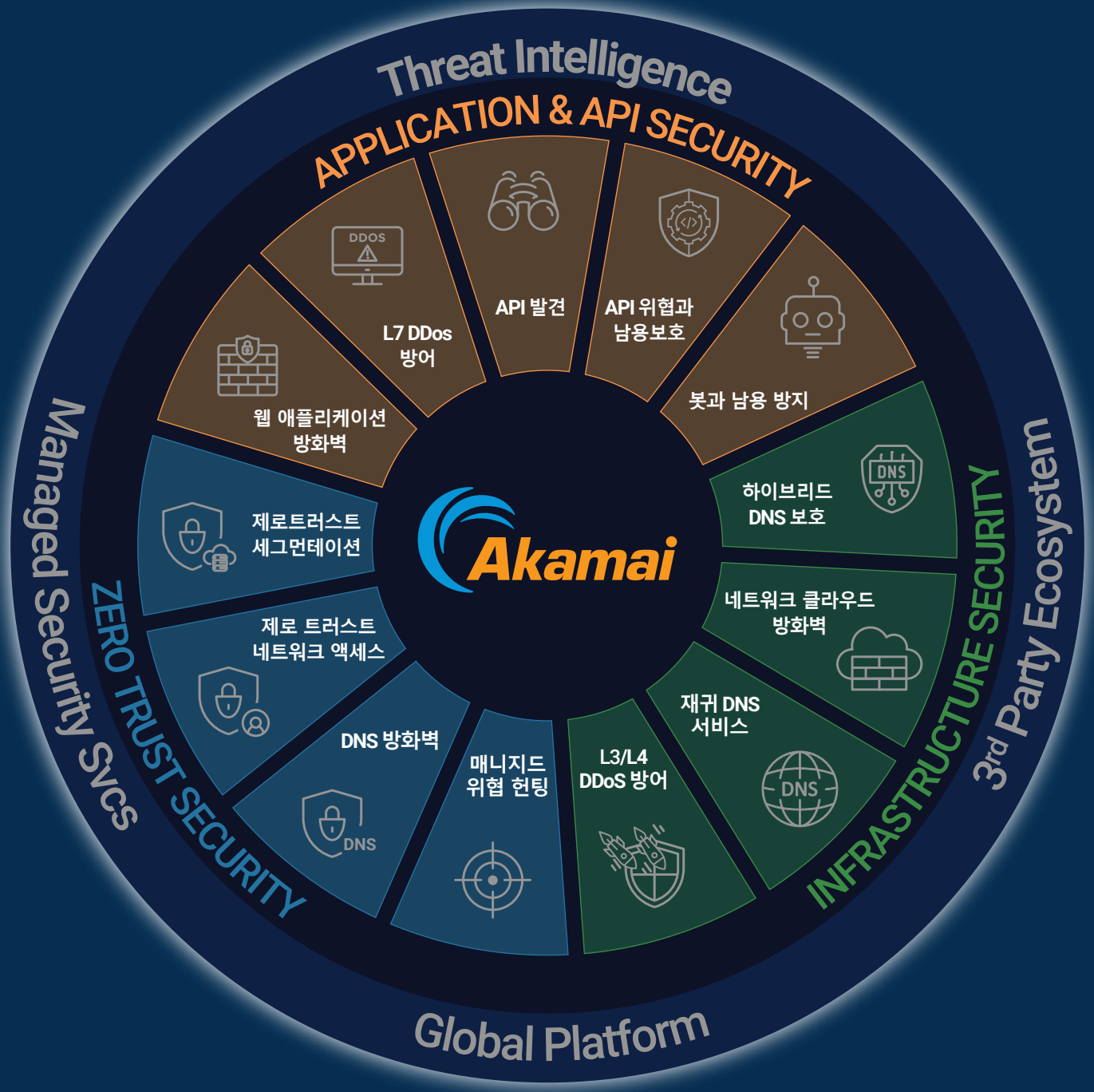


Akamai Security Portfolio

The Akamai Security Portfolio



현대 비즈니스의 중심인 애플리케이션, 보안 강화를 위한 총체적인 접근이 필요한 때

현대 비즈니스 환경에서 애플리케이션은 단순히 정보를 제공하거나 작업을 수행하는 도구 이상의 역할을 합니다. 핵심 비즈니스 프로세스를 자동화하고, 고객과 협력하며, 경쟁 우위를 확보하는 데 필수적인 요소로 자리 잡았습니다. 이처럼 오늘날 기업의 주요 애플리케이션은 비즈니스 연결을 확장하고 새로운 성장 기회를 만들어냅니다. 그러나, 이 과정에서 엔터프라이즈 컴퓨팅 환경과 네트워크의 경계가 확장되면서 공격 표면도 함께 증가합니다. 이와 함께 새로운 유형의 공격이 끊임없이 등장하고 있습니다. 이런 이유로 많은 조직이 애플리케이션 보안 강화 방안을 찾고 있습니다. 아카마이는 업계 최고의 애플리케이션 보안 솔루션 포트폴리오로 기업의 중요 자산과 컴퓨팅 환경을 보호합니다.

포괄적인 애플리케이션 보안 솔루션

아카마이의 보안 솔루션은 애플리케이션 보안을 강화하는 데 중요한 역할을 합니다. 제로 트러스트 환경을 통해 네트워크의 취약점과 위협을 지속해서 줄이면서, 기업은 성능 리스크를 최소화하며 제품 혁신과 비즈니스 운영을 빠르게 개선할 수 있습니다. 또한, 애플리케이션 보안 강화로 기업은 고객에게 높은 가용성, 안정성 및 혁신성을 제공하여 브랜드에 대한 충성도를 높일 수 있습니다. 이 모든 것이 아카마이 솔루션을 통해 가능하며, 기업은 더욱 안전한 디지털 환경에서 성장을 이어갈 수 있습니다. 아카마이의 애플리케이션 보안 솔루션은 크게 3 가지 영역에서 보호를 수행합니다.

#1: 중요 워크로드 보호 및 제로 트러스트 전환

제로 트러스트 환경은 네트워크의 동서 및 남북 방향에서의 접근을 엄격하게 제어함으로써 기업의 중요 워크로드를 보호합니다.
아카마이는 다음과 같은 솔루션을 통해 이 목표를 달성합니다:

- **Akamai Guardicore Segmentation**
  - 네트워크 내부의 동서 트래픽을 세분화하여 악의적인 움직임을 차단합니다.
  - 워크로드 간의 연결을 최소화하고 위협 확산을 방지하여 네트워크 보안을 강화합니다.
- **Enterprise Application Access (EAA)**
  - 남북 방향의 네트워크 트래픽을 관리하여 안전한 사용자 접근을 보장합니다.
  - 애플리케이션 수준에서 세밀한 액세스 제어를 제공해 제로 트러스트 모델을 실현합니다.
- **Akamai Hunt**
  - 최신 위협 인텔리전스 정보를 활용하여 잠재적 위험을 신속히 탐지합니다.
  - 지속적으로 업데이트되는 데이터베이스로 위협에 대한 사전 대응력을 강화합니다.

위 솔루션들은 상호 보완적으로 작동하며, 네트워크 전반에서의 철저한 보안을 통해 기업의 디지털 자산을 보호합니다.

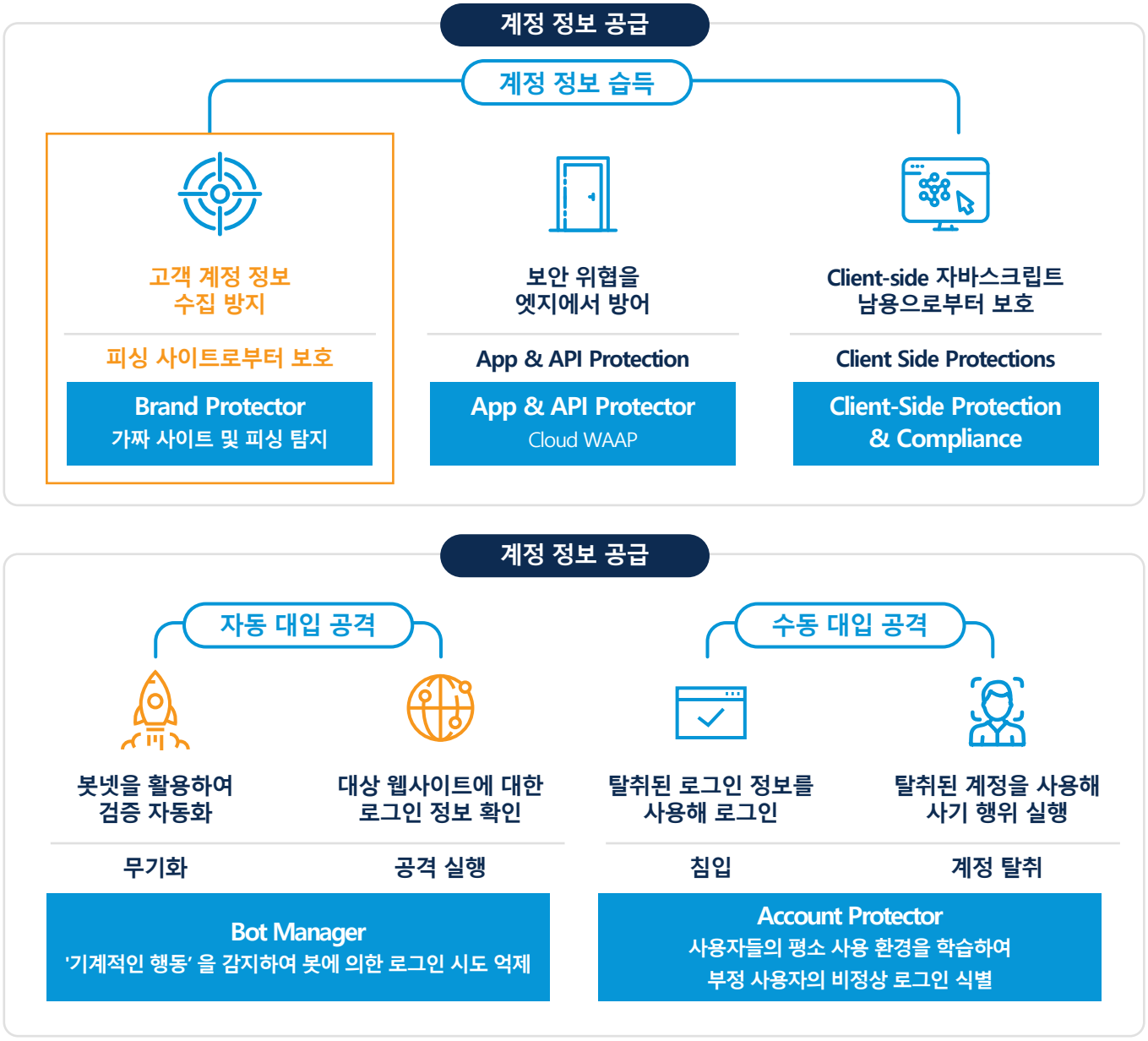
#2: 애플리케이션, API 및 사기 행위로부터의 보호

웹 애플리케이션과 API는 중요 공격 대상이며, 동시에 피싱, 봇넷, 계정 도용 등과 같은 정교한 사이버 공격으로 기업의 브랜드 신뢰도 및 고객 계정이 위협받을 수 있습니다.
아카마이 솔루션은 상호 보완적으로 작동하여 애플리케이션, API, 그리고 사기 행위의 다양한 단계에서 기업과 고객을 보호합니다.

- **App & API Protector, Malware Protection, Client-Side Protection & Compliance**는 악성 코드, 크로스 사이트 스크립팅(XSS), SQL 인젝션 등 다양한 웹 기반 공격을 차단합니다.
- **API Security**는 API의 취약점 및 비정상적인 로직 사용을 모니터링하여 보안을 유지합니다.
- **Bot Manager**는 비즈니스 로직과 온라인 자산을 자동화된 스크립트나 악성 봇 공격으로부터 보호합니다.
- **Account Protector**는 로그인 시도의 이상 행동이나 계정 탈취 시도를 식별하고 차단합니다.

이 외에도, 사이버 킬체인에 따른 세부적인 방어 전략을 통해 사기 행위에 대한 포괄적인 대응이 가능합니다.

계정 탈취 범죄의 사이버 킬체인 (Cyber Kill Chain)



#3: 온프레미스, 하이브리드, 클라우드 인프라 보호

기업의 컴퓨팅 인프라는 온프레미스와 하이브리드 멀티 클라우드를 포괄하는 분산 환경으로 진화 중입니다. 아카마이 솔루션은 다양한 위치에 있는 기업의 컴퓨팅 인프라를 다양한 위협으로부터 보호합니다.

- **Prolexic**는 클라우드, 온프레미스, 하이브리드 환경에서 발생할 수 있는 DDoS 공격을 신속하게 감지하고 차단합니다.
- **Edge DNS**는 안전하고 확장할 수 있는 도메인 네임 서비스를 제공하여 네트워크 인프라의 가용성을 높이고, DNS 공격에 대한 방어책을 강화합니다.

최신 위협 탐지와 대응 지원

아카마이는 위협 행위자의 행동과 변화에 대한 깊은 이해를 바탕으로 탁월한 위협 인텔리전스를 제공합니다. 이 정보에는 기업이 알려진 공격부터 알려지지 않은 공격에 이르기까지 위협 행위자가 어떤 전술, 기술, 절차(TTP)를 사용하는지에 대한 최신 통찰력이 담겨 있습니다. 아카마이 위협 인텔리전스는 방대한 소스에서 데이터를 수집해 분석한 정보입니다. 아카마이는 분산된 글로벌 플랫폼을 통해 매일 수백 테라바이트의 인터넷 트래픽을 분석하고, 이를 통해 실시간 업데이트 및 강화된 보호 솔루션을 개발합니다. 예를 들어, 2023년 9월에는 Prolexic이 미국 최대 금융 기관을 대상으로 한 역대 최대 규모의 DDoS 공격을 성공적으로 막았으며, 같은 해 5월에는 마이크로소프트 Outlook의 중대한 취약점을 발견하여 수백만 개의 엔드포인트를 보호했습니다. 이와 같은 연구 활동은 지속해서 아카마이와 고객의 위협 대응 능력을 높이는 데 기여하고 있습니다.

목차

Akamai Guardicore Segmentation

도전 과제 **공격 표면 확대로 랜섬웨어, 악성 코드 유입 위험 증가**

해 결 책 전통적인 방화벽이나 경계 기반 보안은 내부 네트워크에서의 세밀한 트래픽 제어와 데이터 이동 감시가 부족 합니다. Akamai Guardicore Segmentation는 고급 세그멘테이션을 통해 중요 애플리케이션과 데이터를 보호하고, 네트워크 전반의 가시성을 제공합니다.

마이크로 세그멘테이션

Akamai Guardicore Segmentation(AGS)는 IT 인프라의 구성과 상관없이 하이브리드 및 멀티 클라우드 환경에서 활동을 시각화하고 정확한 마이크로 세그멘테이션 정책을 실행하며 유출을 신속하게 탐지함으로써 공격의 측면 이동을 차단합니다.

주요기능 및 특장점

AI 기반 세그멘테이션

- 중요 애플리케이션을 우선 보호
- 단 몇 번의 클릭으로 신속하게 세그멘테이션 정책 적용

공격면 축소

- 소프트웨어(SW) 기반 세그멘테이션 기술로 고비용의 보안 하드웨어 구축 없이 위협의 간소화가 가능

랜섬웨어 확산 방지

- 세그멘테이션으로 내부 침입한 랜섬웨어의 측면 이동을 차단

기업 전반의 가시성 확보

- 네트워크, 자산, 프로세스, 사용자, 트래픽 흐름 등 종합 컨텍스트를 제공하는 시각적 맵에서 애플리케이션 통신 확인

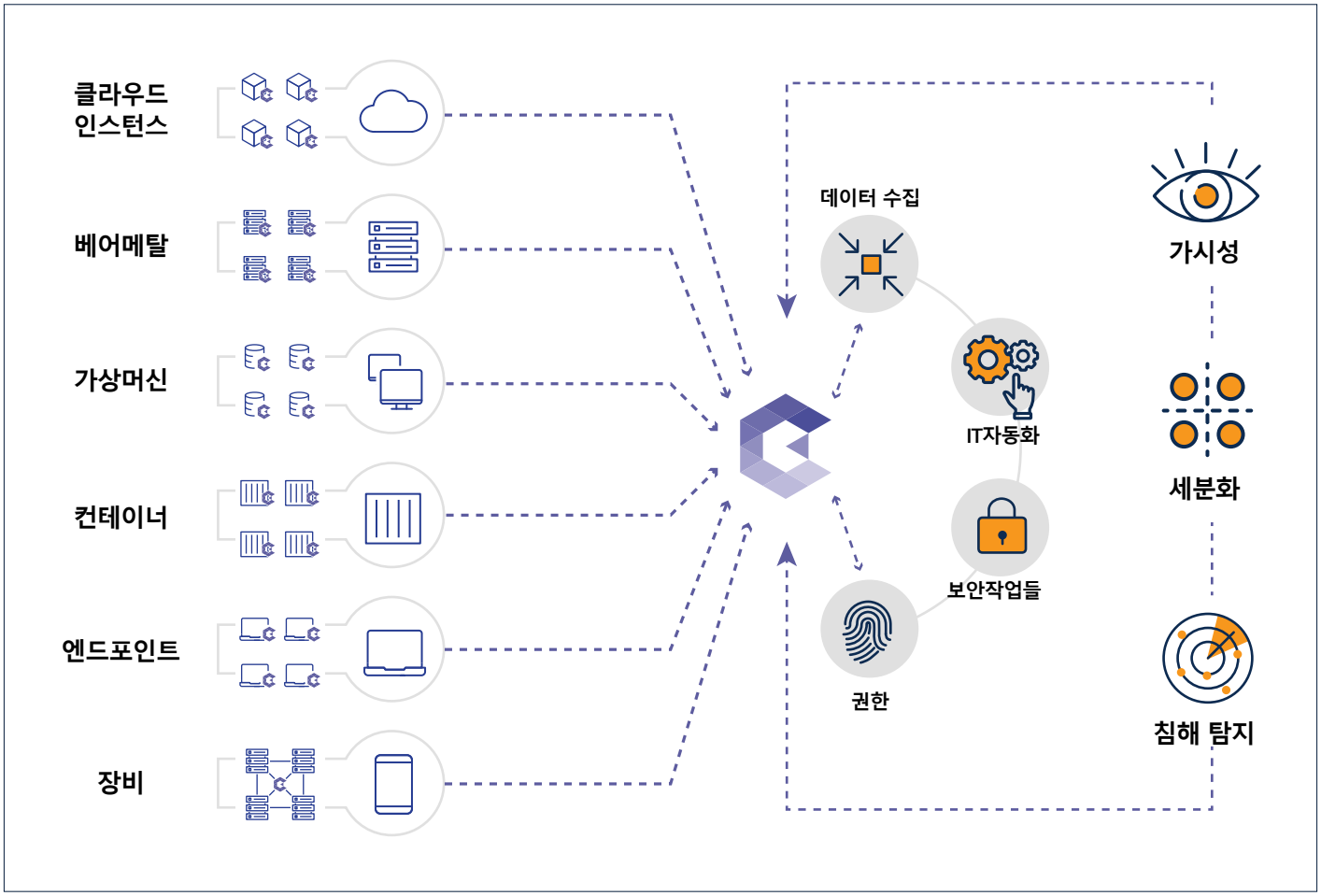
광범위한 커버리지

- 온프레미스, 가상서버, 베어 메탈, 컨테이너 등의 구축 또는 액세스 장소에 관계없이 중요 자산 보호

구축효과

모든 인프라 및 플랫폼의 네트워크 트래픽 정보를 한 눈에 볼 수 있는 가시성 확보	• IT환경 전반의 실시간 데이터 흐름의 가시성을 L4&L7 레이어에서 제공 • 네트워크 토폴로지 맵 형태의 정보제공 • 감사 및 보안사고 이력 추적 기능 • 애플리케이션 및 프로세스 제어
하나의 플랫폼에서 통합적 접근통제 기능	• 온프레미스부터 클라우드 도커 환경까지 L7 레이어에서의 통제 및 제어를 하나의 콘솔에서 가능 • 화이트 리스트, 블랙 리스트를 혼합하여 정책설정 및 제어 • 악성행위 시 자동 네트워크 차단
이상행위를 실시간으로 탐지하고 방어	• 멀웨어 및 랜섬웨어의 측면이동 통제 및 경로 추적 • 취약점(Log4j, Solarwind 등)에 노출된 SW 사용 시스템 검출 • 평판 기반 탐지, 파일 무결성 모니터링, 실시간 커뮤니케이션(Historical communication) 확인

구성도



Enterprise Application Access

도전 과제 **원격 접근 보안과 인바운드 트래픽 관리**
기업들의 업무 환경이 클라우드 서비스로 업무 어플리케이션이 확장 하는 가운데 기존 네트워크 기반의 VPN 솔루션의 한계에 직면합니다.

해 결 책 기존 VPN 솔루션은 네트워크 전체에 넓은 접근 권한을 부여하는 반면, Akamai Enterprise Application Access는 제로 트러스트 모델을 적용해 필요한 리소스에만 접근을 제한하여 보안을 강화합니다.

차세대 원격 보안 접속

Akamai EAA(Enterprise Application Access)는 클라우드 내의 ID 인식 프록시로 시간과 장소에 상관없이 사용자가 원하는 애플리케이션에 안전하게 접속할 수 있는 빠르고 안전한 원격 보안 접속 서비스를 제공합니다.

주요기능 및 특장점

원격 보안 접속 강화

- 방화벽, 보안 그룹의 모든 인바운드 트래픽 차단
- 인터넷에서 기업 인프라가 보이지 않게 구성

애플리케이션 기반

- 사용자에게 전체 네트워크가 아닌 애플리케이션 별 정확한 접속 권한을 부여

다양한 인증 방식

- 간편하고 안전한 MFA(Multi Factor Authentication) 옵셔널 지원
- 무단 접근 최소화

언제 어디서나 접속

- 클라우드 내의 ID 인식 프록시 방식
- 언제든 사용자가 원하는 애플리케이션에 안전하게 접속

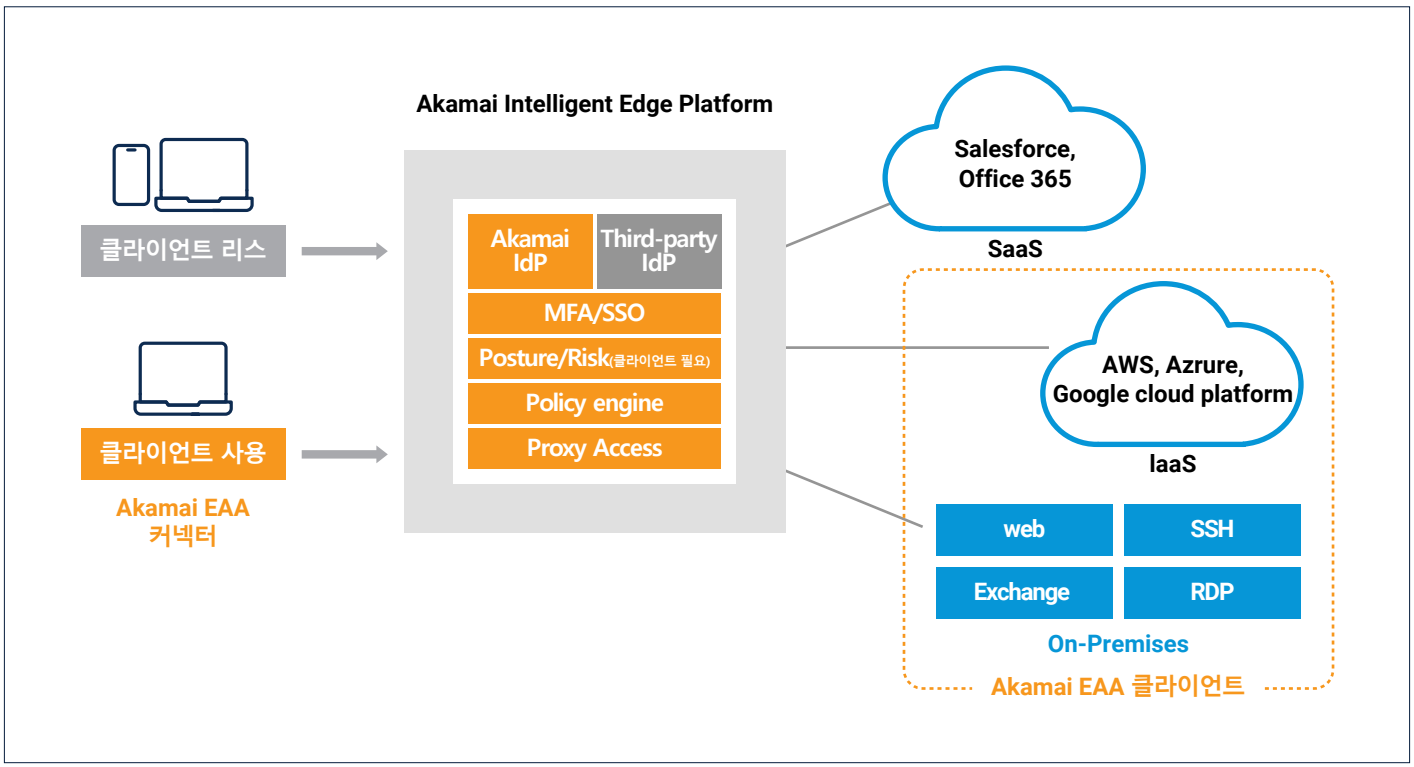
사용자 활동 확인

- 접속하는 모든 사용자의 정보와 수행 정보를 기록
- 관련 컴플라이언스 준수

구축효과

제로 트러스트를 적용한 원격접속 보안 강화	• 모든 인바운드 방화벽 포트를 차단, 인증 사용자에게 특정 애플리케이션 접속만 허용 • 기업 네트워크 또는 클라우드에서 상호 인증된 안전한 TLS 커넥션을 연결 후에 접속 • 애플리케이션 IP 주소 노출 방지 • SSO(Single Sign-On)와 MFA 등 추가 인증 적용 가능
IT 복잡성 감소	• 데이터 경로 보호, IAM, 애플리케이션 보안, SSO, 관리 가시성, 제어를 통합 서비스로 구축 • 모든 애플리케이션(온프레미스, IaaS, SaaS 등)에서 적용 가능 • 통합 포탈로 새로운 애플리케이션과 원격접속 허용 사용자를 신속 구축 • 사용자 활동에 대한 감사 및 리포팅
빠르고 원활한 사용자 경험 제공	• 장소, 위치, 사용 디바이스와 상관없이 원격접속이 가능

구성도



Secure Internet Access

도전 과제 **피싱 및 악의적인 사이트 접속으로 인한 계정 탈취나 악성 코드 다운로드 위험 증가**
임직원들의 무분별한 인터넷 접속으로 인해 피싱 사이트 등의 접속을 통한 계정 정보 탈취 등의 공격이 발생합니다.

해 결 책 일반적인 보안 솔루션은 사용 위치에 따라 보안 수준이 달라질 수 있습니다. Akamai Secure Internet Access는 위치와 관계없이 일관된 보안 웹 게이트웨이를 제공합니다.

클라우드 기반 보안 웹 게이트웨이

Akamai SIA(Secure Internet Access)는 클라우드 기반의 보안 웹 게이트웨이(SWG)입니다. 기존에 사용 중인 보안 솔루션과 관련된 복잡성이나 관리 오버헤드 없이 언제 어디서나 사용자와 디바이스가 인터넷에 안전하게 접속할 수 있도록 지원합니다.

주요기능 및 특장점

위협 인텔리전스

- 실시간 인텔리전스, 탐지 엔진 등 멀티레이어 방어로 보안 강화
- 지속적인 업데이트

애플리케이션 제어

- 리스크 점수에 따라 미승인
- 애플리케이션을 식별 및 차단하거나 애플리케이션 기능 제한

데이터 유출 차단

- 민감한 데이터가 포함된 콘텐츠 업로드 차단
- 모니터링

페이로드 분석

- 멀웨어 탐지 엔진으로 제로데이 공격과 복잡한 위협을 방어
- 정교한 위협을 식별, 차단
- 탐지 노하우 축적

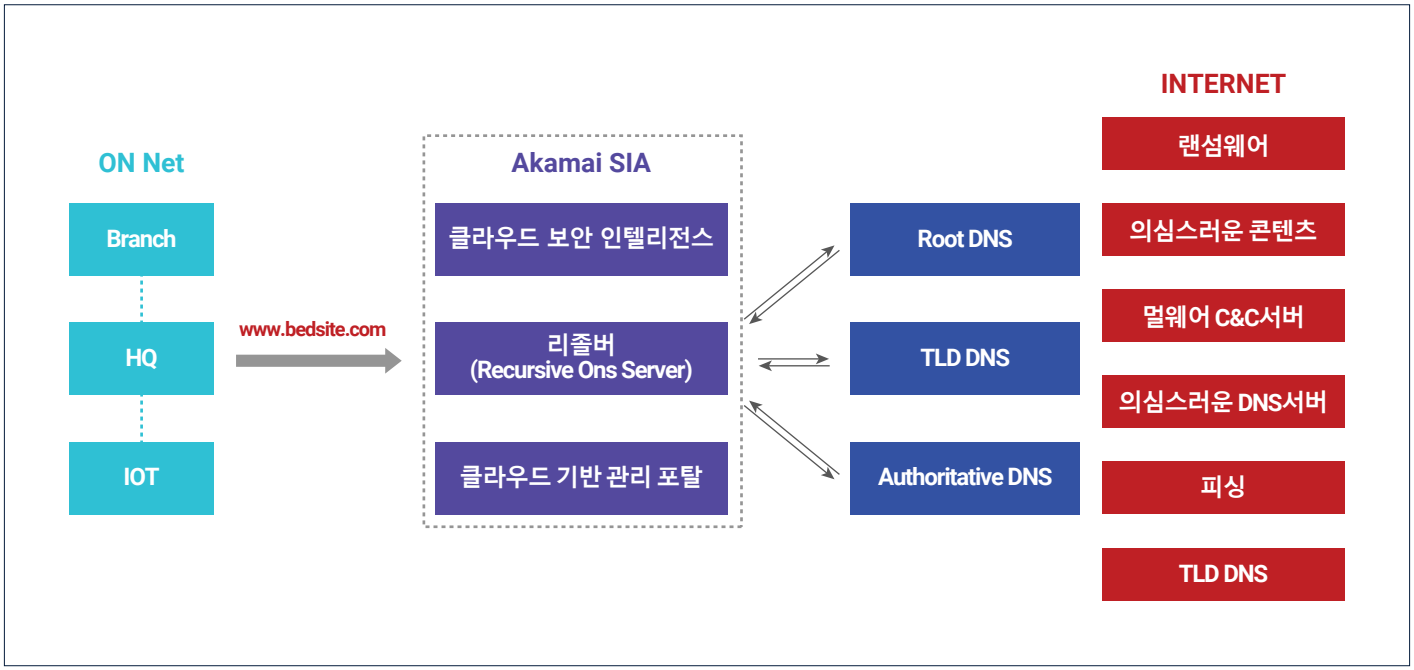
내부 감염 방지

- 기업 정책 적용
- 특정 도메인을 차단하여 감염 방지

구축효과

최신 위협 인텔리전스 기반의 위협탐지 및 클라우드 자동 차단	• AI 기반의 자동화 분석으로 정형 및 비정형 데이터를 실시간으로 파악하여 위협 DB 업데이트 • 콘텐츠 및 애플리케이션 기반 유해사이트 차단 • 악성 스크립트를 실시간으로 탐지하여 클라우드 상에서 다운로드 패킷 차단 • 실시간 페이로드 분석 및 악성 웹 패킷 차단
모든 위치와 디바이스 타입에 단일 보안정책 적용 및 데이터 유출방지(DLP)	• 내부, 외부에 상관없이 모든 사용자와 디바이스를 탐지 및 구분 • 적용하고자 하는 웹 관련 보안 정책 적용 • 사용자 위치에 따라 단일, 차별화된 정책을 유연하게 적용 • 데이터를 단말에서 외부로 유출하려고 시도 시 DLP 정책을 적용하여 패킷 차단
즉시 내부 DNS 보안 강화	• 패킷 사이즈에 따라 모든 웹 패킷을 클라우드 상에서 검사 및 차단 • 인라인, 오프라인, 샌드박스 등 다양한 검사 방식 지원 • DNS 변경만으로 간단하게 모든 구성 완료 • DNS 패킷 실시간 검사

구성도



API Security

도전 과제 **API 트래픽에 대한 가시성 부족**
비즈니스의 요구 사항이 웹 트래픽에서 API 트래픽으로 옮겨가는 가운데 API 트래픽에 대한 가시성, 보안 분석 및 위협에 대한 선제적 차단에 대한 요구가 증가하고 있습니다. 특히 보안팀에서 개발팀과 효과적으로 협업할 수 있는 수단이 필요합니다.

해 결 책 전통적인 보안 도구는 API의 복잡성과 동적 특성을 충분히 관리하지 못하며, 특히 권한 우회, 논리적 흐름을 우회 하는 공격 등의 API에 특화된 공격 및 위협에는 대응 하지 못합니다. Akamai API Security는 모든 API 트래픽을 지속적으로 모니터링하고 로직을 이해하는 정밀한 AI 탐지 엔진을 내장하여 API의 오남용, 쉐도우 API 등의 새로운 위협을 관리 합니다.

API 보안

Akamai API Security 는 기업 내부 혹은 외부의 모든 API 트래픽을 추적해서 보안 관점에서 API 포스처의 관리와 증가하는 API 오남용에 대한 가시성을 보안팀에 제공 하고 대응 할 수 있으며 개발팀과 효율적으로 협업할 수 있는 환경을 제공 합니다.

주요기능 및 특장점

Active Testing (보안 테스트)

What
API 엔드포인트를 지속적으로 테스트하여 API 리스크가 발생하기 전에 이를 파악하고 전반적인 API SDLC를 개선

How
API, CO/CD 등을 통해 수동 으로 실행하거나 자동화할 수 있는 API 보안 테스트 모듈

Discover & Document (가시화)

What
레거시 API 및 섀도 API를 포함하여 환경 전반에 걸쳐 모든 API를 검색하고 카탈로그화

How
데이터 정책 및 거버넌스 규칙을 준수하는 리스크가 전혀 없고, 가볍고, 마찰이 없는 구축 모델

Analyze (이상징후 분석)

What
소스, 정책, 구성 및 런타임에서 잘못된 구성, 이상 징후 및 취약성을 식별

How
비지도 머신 러닝을 사용하여 API를 위해 특별히 구축된 행동 기반 상황별 모델링

Remediation (문제 해결)

What
소스 코드 또는 API 보안 소견의 런타임 문제 해결을 위한 사용자 친화적인 워크플로 제공

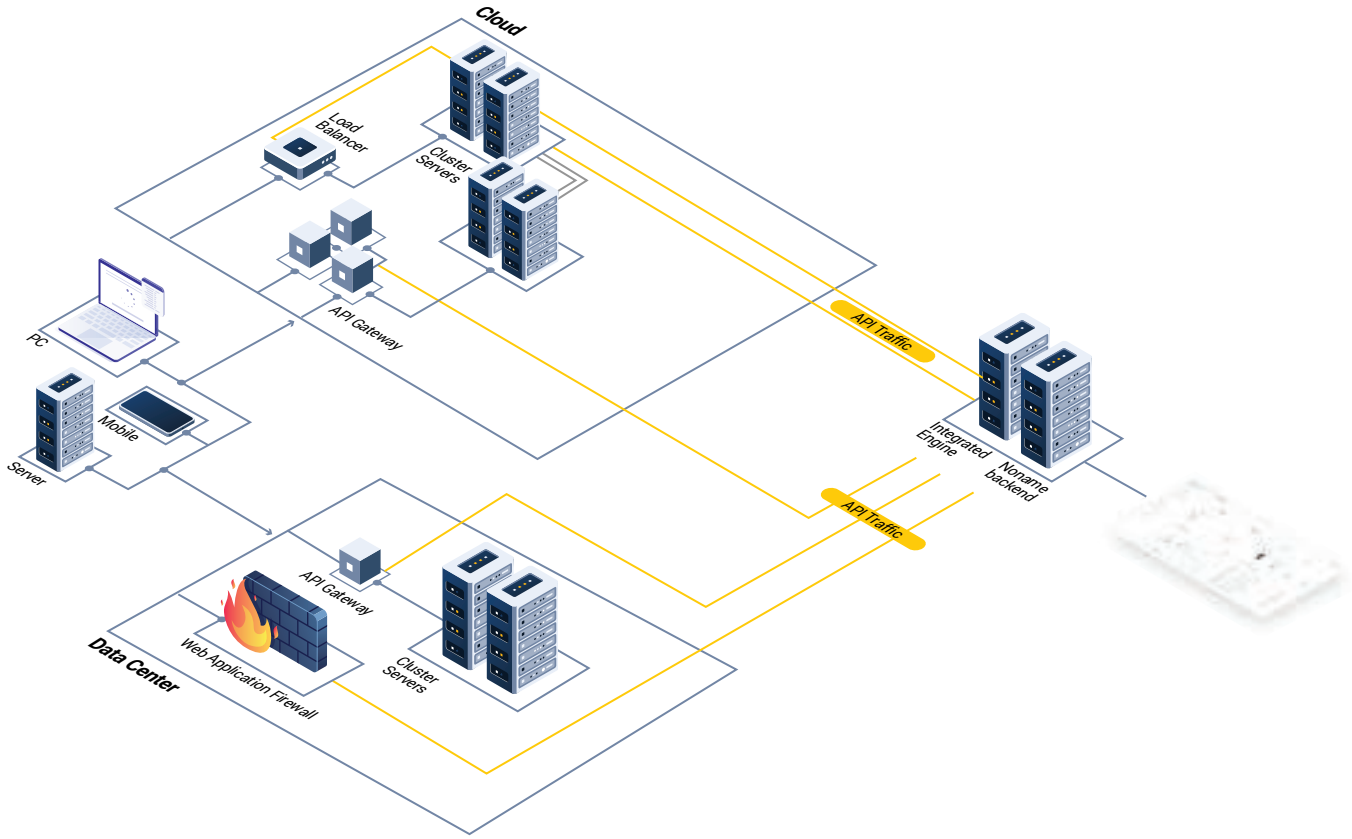
How
수동, 반자동 및 완전 자동 프로세스로 구성된 광범위한 교정 라이브러리
(차단 시스템과 연계 시 차단 정책 사용 가능)

구축효과

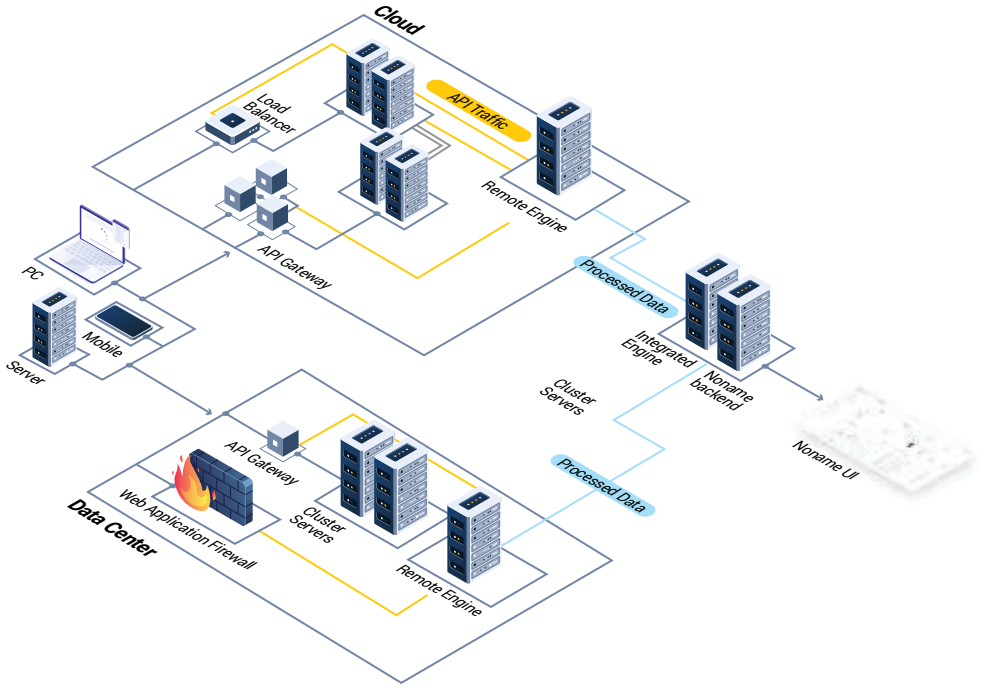
능동적 보안 테스트	• 운영 전에 API의 무결성을 적극적으로 테스트 • 문제 발견 및 검증 • CI/CD와 연계하여 개발시 실시간 검증 (학습기반으로 문제를 테스트)
자동 API 탐색 (가시성)	• 레거시, 신규, 악성 API 식별 및 목록화 / API 목록 / API 사용자 (또는 상대 기관) 데이터 식별 (중요 데이터) / API 소유자 식별 / 서버 식별 / 보안정책 (인증 여부, 암호화 등) API 사용 추이
이상징후 분석	• AI 기반의 공격자, 의심스러운 동작 및 잘못된 구성 탐지
문제 해결	• 공격을 차단하고 기존 워크플로를 활용하여 취약성 및 잘못된 구성 해결

구성도

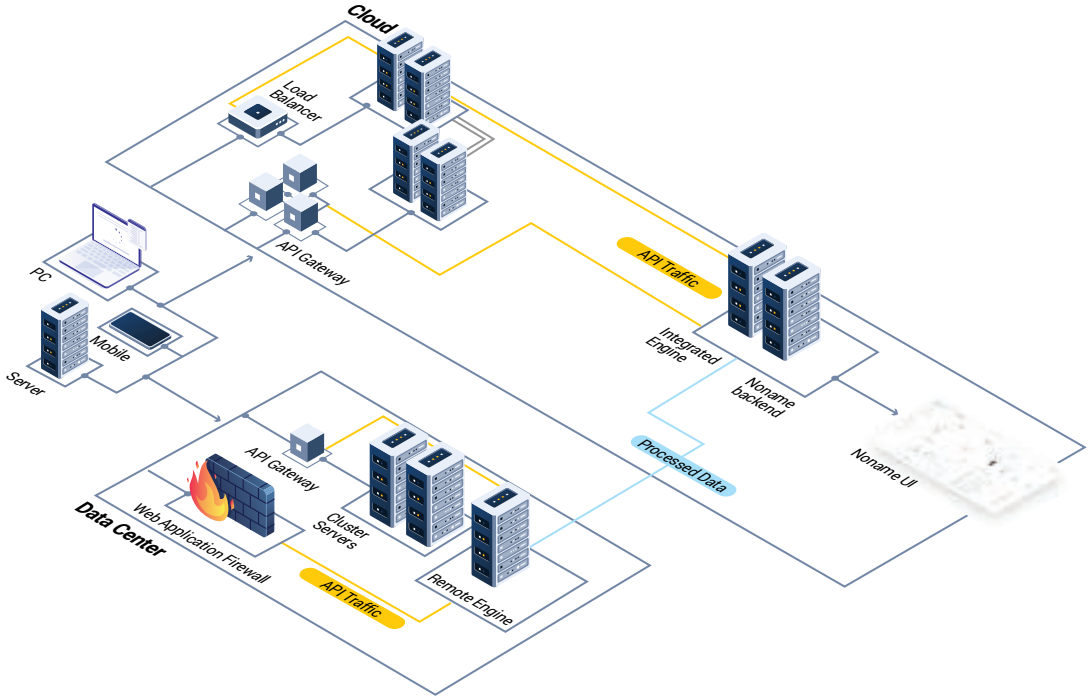
SaaS Akamai API Security는 기본적으로 클라우드에서 Akamai API 보안 플랫폼을 관리합니다.



Hybrid 고객의 데이터 센터 또는 클라우드 환경에 원격 엔진 을 배포하고 아카마이 클라우드에서 관리 할 수 있습니다.



On-Prem 고객의 데이터 센터에 백엔드와 UI 그리고 관리 API 를 설치해서 관리 할 수 있습니다.



App & API Protector

도전 과제 **웹 및 API 자산에 대한 공격에 취약**
고객 비즈니스에 필수 적인 웹 서비스를 대상으로 하는 대용량DDoS 공격의 웹 서비스 성능에 영향이 없는 방어가 필요합니다.

해 결 책 전통적인 보안 솔루션은 웹 및 API 자산의 보호에 특화되지 않았기 때문에, 웹 기반 공격에 대한 방어가 불충분합니다. Akamai App & API Protector는 웹 애플리케이션 방화벽과 API 보안 기능을 통합하여 강력한 보호를 제공합니다.

디도스 방어 및 고성능 웹방화벽

Akamai AAP(App & API Protector)는 다양한 위협으로부터 웹 자산을 보호합니다. 전체 웹 및 API 자산보호를 위한 웹 애플리케이션 방화벽, 봇 방어, API 보안, 디도스(DDoS) 방어 등 웹 보안을 위한 다양한 웹 보안 기술을 실제로 사용하기 쉬운 단일 솔루션으로 통합해 제공합니다.

주요기능 및 특장점

웹 보안 강화

- 70+Tbps, 36만대 서버로 무제한의 디도스 공격 방어
- OWASP 상위 10대 리스크 대상 공격 등 최신 공격에 맞춤화

봇 차단

- 악성 봇 활동이 문제가 되기 전에 이를 탐지하고 차단

웹사이트 가속

- 4000+ PoP에 완전 분산된 인텔리전트 엣지 활용

API 식별 고도화

- 악성 페이로드를 모니터링
- 신규 및 이전에 알려지지 않은 API 리스크 관리

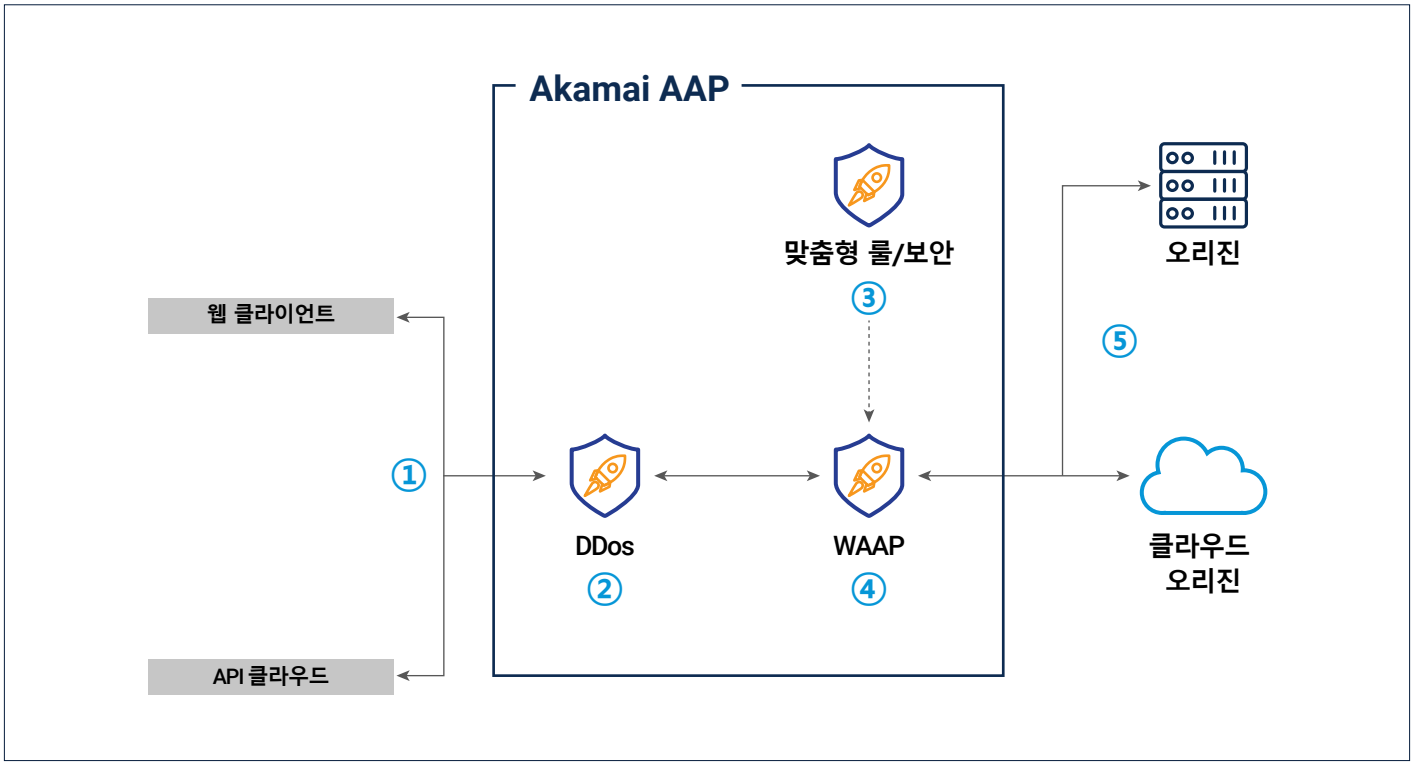
완벽한 분산 처리

- 글로벌 No.1 CDN 사업자
- 전세계 분포된 클라우드 엣지 플랫폼 활용

구축효과

대규모의 예측 불가능한 복합적 웹 공격을 대비한 역량 확보	• 디도스 공격 등 대규모 공격에 대한 유연한 대처 • 다양한 형태의 공격인 멀티 벡터에 대한 방어와 모니터링 • 상시(Always-On) 서비스로 운영 시간이 아니더라도 지속적인 서비스 제공 • 가용성 100% 구현(Zero Down-Time)
클라우드 기반 보안 서비스	• 인터넷 영역으로 보안 관리 범위 확대 • 대규모 공격을 분산 플랫폼으로 사전 방어 또는 공격 흡수 • 오리진으로 가는 트래픽과 로드를 최소화 • 간편한 서비스 적용 방식
기존 보안 시스템 활용	• 기존 보안 장비 및 관제 서비스를 최대한 활용하여 연동, 구축

구성도



Client-Side Protection and Compliance

도전 과제 **악의적인 써드파티 호스트와 스크립트 공격에 취약**
보안 관리자 입장에서 웹 서비스의 모든 3rd 파티 호스트와 3rd 파티 스크립트의 관리가 사실상 불가능 – 공급망 공격에 대한 대응이 쉽지가 않습니다.

해 결 책 전통적인 보안 솔루션은 웹 서비스 내부 활동에 대한 가시성을 제공하지 않아 악의적인 써드파티 호스트 및 스크립트를 감지하기 어렵습니다. Akamai Client-Side Protection and Compliance는 웹 서비스에 대한 심층적인 가시성과 함께 허가되지 않은 써드파티 요소 자동 차단 및 관리, 그리고 고급 위협 탐지 기능으로 웹 서비스 보안을 강화합니다.

웹 페이지에서 실행되는 모든 스크립트에 대한 보안

Client-Side Protection & Compliance (이하 CPC) 는 최종 사용자 데이터 유출을 방지하고 웹사이트를 자바스크립트의 위협으로부터 보호합니다. 이 솔루션은 스크립트 행동을 실시간으로 분석하고 단일 대시보드 보기에서 유용한 정보를 제공하며 유해한 스크립트 활동을 방어하기 위한 알림을 제공합니다. PCI DSS v4.0 준수를 위해 설계된 이 솔루션은 기업이 새로운 스크립트 보안 요구사항을 충족하고 클라이언트 측 공격을 방어할 수 있도록 지원합니다.

주요기능 및 특장점

탐지 및 보호
- 실제 사용자 세션에서 스크립트 동작을 모니터링하여 의심스러운 활동 탐지

우선 순위가 지정된 실시간 알림
- 실행 가능한 알림으로 고위험 이벤트를 즉시 차단합니다

정책 관리
- 스크립트 동작을 관리하고 런타임 자바스크립트의 실행을 제어합니다

유연한 배포 옵션
- Akamai 커넥티드 클라우드 또는 오리진 서버에 직접 간편하게 배포할 수 있습니다

PCI DSS v4.0 워크플로우
- JavaScript 보안 요구 사항 6.4.3 및 11.6.1 충족 지원

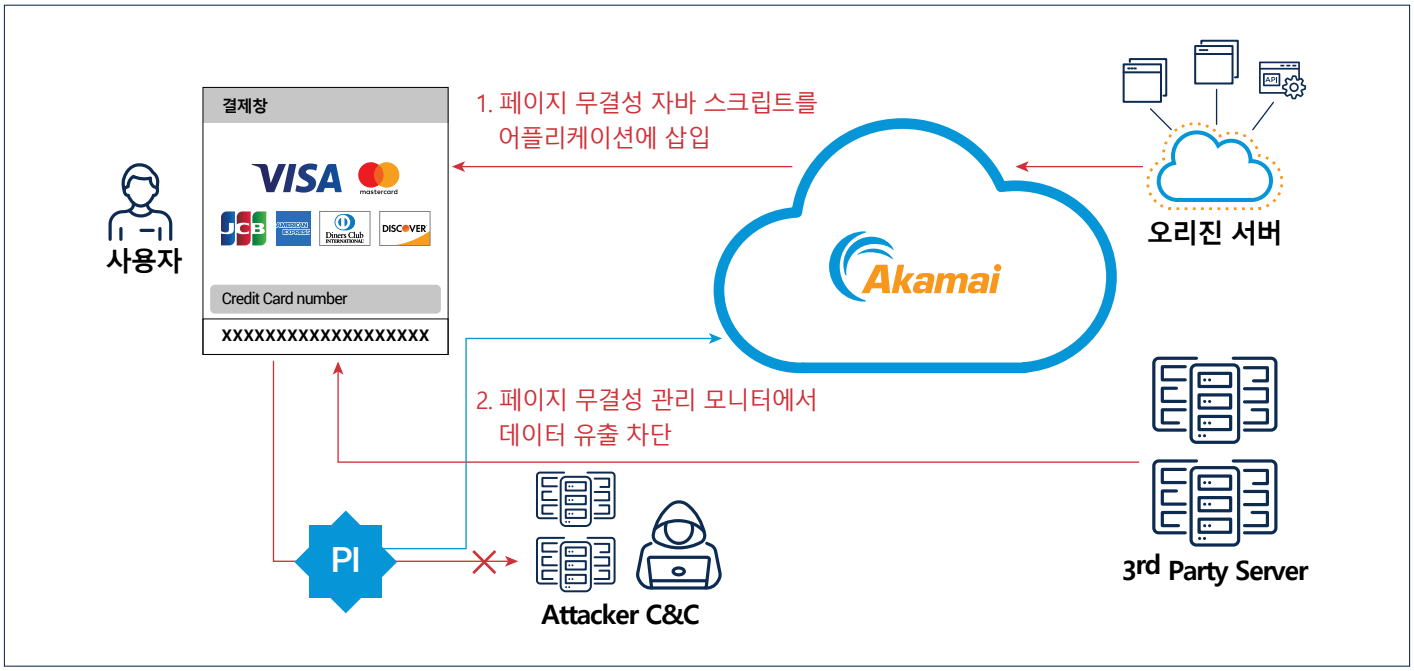
클라이언트측 가시성
- 클라이언트 측 공격표면에 대한 광범위한 가시성을 확보합니다

취약점 탐지
- Akamai 위 협 인텔리전스를 기반으로 CVE(Common Vulnerability and Exposure) 를 식별합니다

구축효과

클라이언트 측에서 민감한 데이터 유출 방지	• 아카마이 CPC 는 머신 러닝과 휴리스틱 스코어링을 결합하여 실시간 스크립트 동작을 분석 • 1st 파티, 3rd 파티를 포함하는 모든 호스트 들에서 제공하는 모든 스크립트에 대한 악의적인 활동과 취약한 리소스를 탐지 • 즉시 적용 가능한 알림이 보안팀에 제공 되므로 웹 스키밍, 메이지카트, 폼재킹과 같은 클라이언트 측 공격을 신속하게 방어 가능
PCI DSS v4.0 컴플라이언스에 대한 지원	• PCI DSS v4.0 스크립트 보안 요구 사항 6.4.3 및 11.6.1 을 충족하는 클라이언트 측 공격으로부터 결제 카드 데이터를 보호하고 결제 페이지에서 스크립트 관리를 보장 가능 • 웹 어플리케이션에서 실행 되는 모든 스크립트 추적 및 인벤토리 • 로드된 스크립트를 쉽게 검증할 수 있는 도구 지원 • HTTP 헤더를 모니터링 하여 페이지 변조 방지 • 포괄적인 대시보드와 PCI 알림을 통해 컴플라이언스 이벤트에 빠르게 대응 가능 • 보안 및 컴플라이언스 팀이 감사 프로세스의 부담을 줄이고 워크 플로우를 간소화할 수 있음
자바스크립트의 위협에 대한 광범위한 가시성	• 아카마이 CPC 는 웹 어플리케이션 내 모든 스크립트를 지속적으로 모니터링 • 서버측 트래픽 뿐만 아니라 클라이언트 측에서 실행되는 스크립트의 행위에 대한 가시성을 제공 • 아카마이 CPC 는 스크립트의 동작, 취약점, 접근 범위 (개인 정보에 대한 접근), 영향 등을 분석하여 기존 WAF 에서 분석 할 수 없는 웹사이트의 클라이언트 측 공격 표면에 대한 가시성을 제공

구성도



스크립트 인벤토리

- 스크립트의 안전성 검토 및 유지 관리 용이
- 알려진 / 알려지지 않은 아카마이 공급업체 및 퍼스트 파티 스크립트 별 분류

결제 페이지 보호

- 결제 페이지 변조, 데이터 유출, 솔루션 변조 시도에 대한 알림을 수신하고 관리

스크립트 승인

- 정단한 사유가 없는 모든 스크립트는 승인되지 않는 것으로 감주되어 이 위짓에 표시됩니다.
- 승인되지 않은 스크립트에 대한 알림 받기

스크립트 무결성 확인

- 모니터링 된 각 스크립트 행위의 무결성을 보장합니다.
- 스크립트 동작 이상에 대한 알림 수신

Account Protector

도전 과제 **계정 소유자인지 부정 사용자인지 여부 파악 불가**
남의 계정을 가로채서 접속하여 각종 정보들을 현금화 하는 부정 사용자 및 계정 도용 공격이 증가하고 있으며 계정 정보 및 개인 정보가 유출 됨으로 인해 과징금 및 과태료 처분 및 이에 따르는 브랜드 평판이 저하 됩니다.

해 결 책 전통적인 보안 솔루션이 웹 페이지에서 실행되는 스크립트의 안전성을 실시간으로 감시하고 분석하는 기능이 충분하지 않습니다. 이와 달리, Akamai Client-Side Protection and Compliance는 실시간 분석을 통해 데이터 유출을 방지하고 클라이언트 측 보안을 강화합니다.

계정 탈취 공격(Account Takeover) 방어

Akamai Account Protector 는 탈취된 로그인 정보로 로그인을 하는 사기 행위자를 웹 페이지에 로그인할 때 행위 기반으로 탐지 하고 아카마이 엣지에서 액션을 적용하여 신규 계정 개설 사기나 계정 탈취와 같은 계정 관련 사기 행위를 효과적으로 방어 할 수 있습니다.

주요기능 및 특장점

고객과 사용자의 신뢰 강화

- 정상적인 상호 작용을 파악하고, 원활한 사용자 경험을 제공하며, 사기 행위로부터 사용자를 보호합니다

계정에 로그인 행위에 대한 인사이트 및 가시성 확보

- 블랙박스 분석에만 의존하지 않고 신뢰할 수 있는 신호와 지표를 기반으로 조치를 취할 수 있습니다.

데이터에 기반한 더 나은 보안 및 ID 의사 결정

- FDS, SIEM, 기타 보안 툴과 통합해 Account Protector 의 Trust 및 Risk 신호를 입력 받아 정확도를 높이고 툴에 대한 투자를 효율화 합니다

비즈니스에 따라 커스텀 보호 기능 개발

- 자동으로 튜닝하는 봇 탐지를 통해 사용자가 사이트와 상호 작용하는 방식에 따라 더욱 맞춤화 된 비정상 탐지 및 보호가 가능합니다

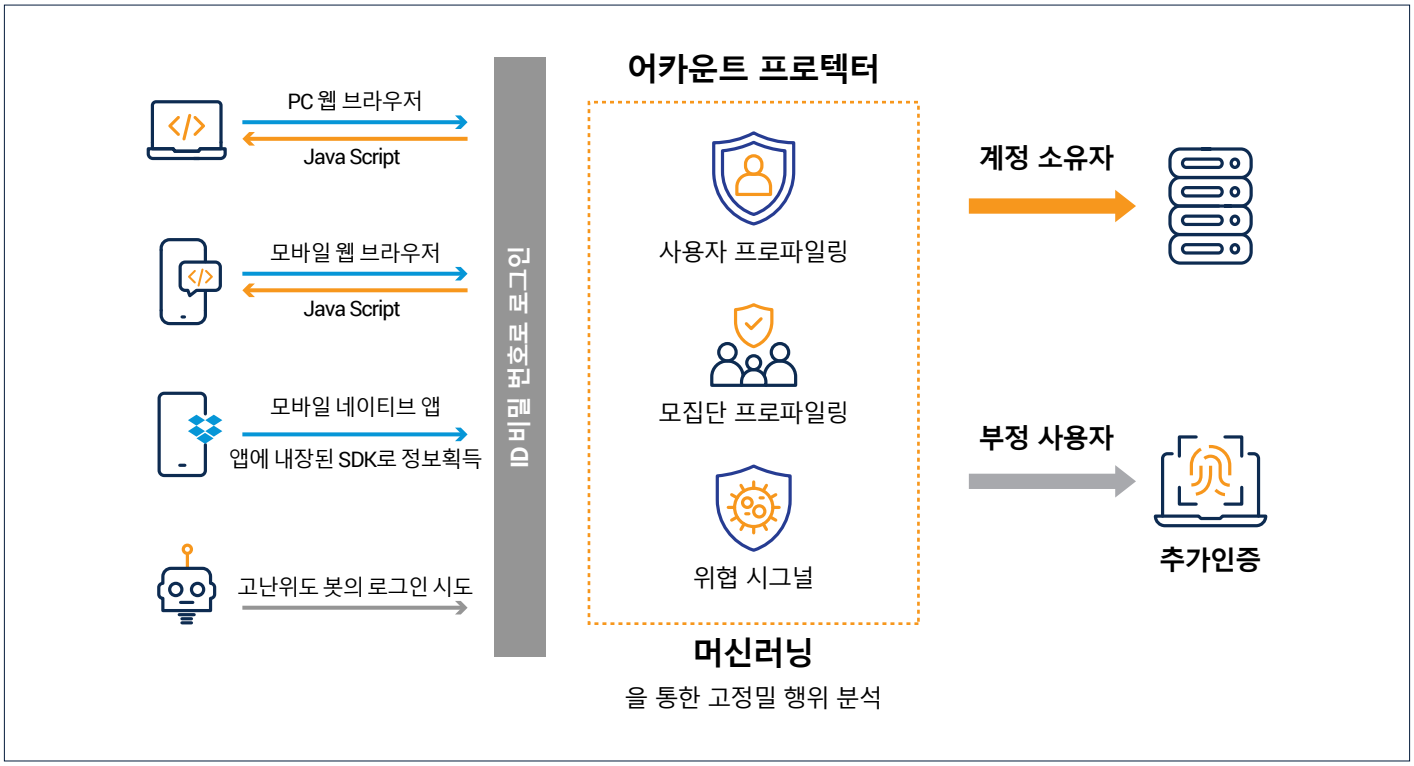
계정 복구 후유증 감소

- 침해된 계정을 효율적으로 조사하고, 도난당한 자산을 복구하고, 침해된 기존 계정을 재설정하고, 규제 및 법률 기관에 보고하고, 사용자 불만을 해결합니다

구축효과

계정 탈취 공격으로 부터 고객 비즈니스를 보호	• **계정 개설 도용** – 도난 된 신원 정보로 생성된 가짜 계정의 탐지 및 보호 • **계정 탈취** – 사기 행위자가 정상적인 고객 계정에 접속해 계정의 자산을 탈취하는 것에 대한 대응 • **적대적 봇 공격** – 크리덴셜 스터핑, 인벤토리 파악, 기타 자동화된 공격으로 계정 탈취 공격과 함께 진행 되어 사용자의 자산을 탈취 하는 것에 대한 대응
계정 로그인 행위에 대한 가시성 확보	• 아카마이 Account Protector 는 머신 러닝과 위험 및 신뢰 지표에 대한 방대한 데이터를 활용해 계정 도용을 원천적으로 방지 하도록 설계 되어 있음 • 계정 소유자의 로그인 경험에 영향을 주지 않고 실시간으로 엣지에서 조치를 취할 수 있도록 각각의 로그인 요청에 적절하게 대응 가능 • 제공하는 리포팅 및 분석 기능을 활용하고 기존에 기업에서 사용하는 FDS 와 분석 툴을 함께 사용하면 더 자세한 인사이트 습득 가능
사용자의 로그인 경험 향상	• 계정 소유자와 부정 사용자의 분별이 가능 하므로 계정 소유자 로그인 시 빠른 로그인 제공 • 부정 사용자 로그인 시도 시에만 추가 인증 과정 적용

구성도



Brand Protector

도전 과제 **늘어나는 고급 피싱 사이트로부터 브랜드 평판 및 리셀러 생태계를 보호**
피싱 사이트는 고객이 진짜 사이트와 가짜 사이트를 구별하기 어렵게 만들어, 브랜드 신뢰도를 저하시킴으로써 매출에 부정적인 영향을 미칩니다. 공격자들은 가짜 상품을 판매하거나 민감한 정보를 탈취하는 등의 방법으로 고객을 속이려 하며, 이는 기업에 심각한 피해를 줄 수 있습니다. 따라서 브랜드 사칭을 탐지하고 차단하는 것이 중요하며, 이를 통해 인증정보 탈취와 계정 도용을 예방할 수 있습니다.

해 결 책 Akamai Brand Protector는 독점 데이터와 써드파티 데이터를 활용해 신종 피싱 캠페인과 브랜드 사칭을 조기에 탐지·차단하고, 리셀러 생태계와 브랜드 수익을 보호하며 대규모 공격을 예방합니다.

웹 페이지에서 실행되는 모든 스크립트에 대한 보안

Akamai Brand Protector는 가짜 웹사이트, 피싱 시도, 소셜 미디어 사칭, 악성 앱 등 표적 브랜드 사칭 공격을 탐지하고 방어할 수 있는 단일 솔루션입니다. 보안팀은 Brand Protector를 사용해 인증정보 수집을 탐지하고 방어할 뿐 아니라 기업의 고객을 사기로부터 보호할 수 있습니다. Brand Protector는 인텔리전스, 탐지, 가시성, 방어라는 4단계 접근 방식을 통해 날로 증가하는 사이버 보안 문제에 대응합니다.

주요기능 및 특장점

분석

- Akamai Connected Cloud를 기반으로 매일 788TB 이상의 웹 트래픽을 분석해 독점적인 데이터 피드를 생성합니다.

탐지

- 독점적인 피드와 보조 피드를 AI 분석과 결합해 사칭 및 피싱 사이트를 신속하게 탐지합니다.

알림

- 단일 대시보드에서 위협 분석, 심각도, 세부 정보와 함께 활성 위협을 즉시 파악할 수 있습니다.

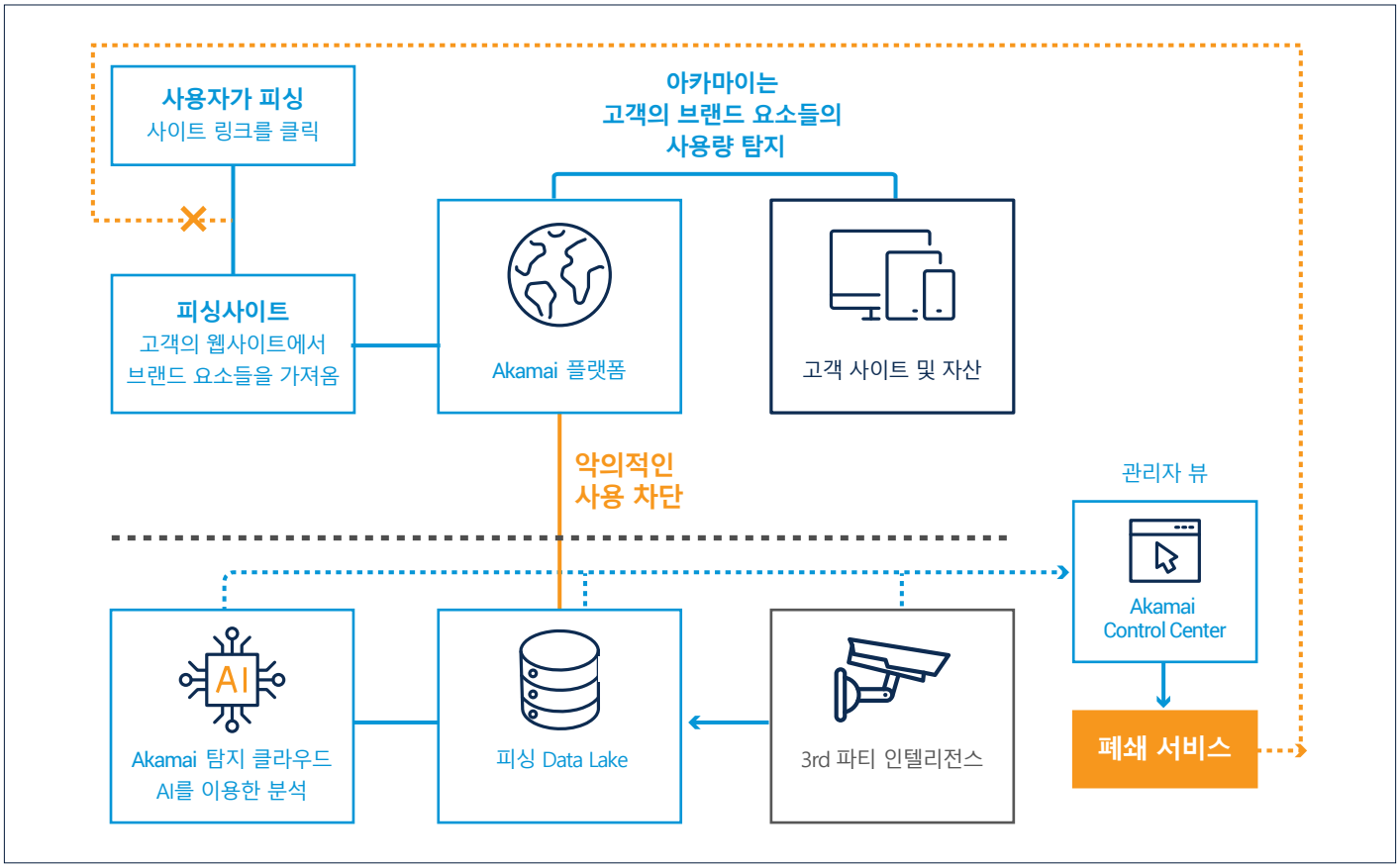
방어

- 통합 서비스를 통해 팀에서 차단 요청을 하거나 안전 브라우징 알림을 발행할 수 있습니다.

구축효과

피싱 사이트 탐지	• 사이트와 앱의 속도를 떨어뜨리는 봇을 제거해 더 많은 고객 유치 및 매출 증대(Conversion Rate 증가) • 경쟁 업체가 기업의 가격을 낮추고 매출을 감소시키는데 일조하는 자동화된 스크레이핑 차단 • 사이트 애널리틱스에서 봇 트래픽을 제거해 실제 사용자에 맞게 최적화하는 마케팅 효과 개선
가짜 스토어를 찾고 리셀러 생태계 보호	• 가짜 매장과 브랜드 사칭 공격을 신속히 탐지·차단하여 기업의 수익 손실과 고객 신뢰 하락을 방지 • 통합된 탐지 및 차단 기능은 리셀러 생태계를 보호하고 공격자의 동기를 약화시켜 브랜드 수익화 향상 • 단일 대시보드와 실시간 위협 분석을 통해 보안팀의 대응 속도를 높이고 생산성을 향상
소셜 미디어 및 앱 스토어에서 킬 체인 차단	• 브랜드 사칭을 조기에 탐지하고 차단하여 인증정보 탈취와 계정 도용을 방지하고, 고객 신뢰를 유지 • 소셜 미디어와 앱 마켓플레이스를 포함한 다양한 채널에서 브랜드 요소를 모니터링하여 대규모 공격을 사전에 예방 • 퍼스트파티 및 써드파티 데이터를 결합한 광범위한 가시성을 통해 기업의 수익 손실과 위험을 최소화하고 브랜드 평판을 보호

구성도



Content Protector

도전 과제 **악성 목적으로 이용될 수 있는 스크레이퍼 봇 차단**
갈수록 정교해지는 스크레이퍼 공격으로 부터 매출을 보호할 수 있습니다.

해 결 책 스크레이퍼 공격의 고유한 툴링과 기법에 적합한 탐지 기능을 사용해 스크레이퍼를 즉시 탐지하고 중단시킵니다. 속도 혹은 성능 저하 없이 온라인 비즈니스와 매출을 보호할 수 있습니다.

회피형 스크레이퍼 봇의 탐지

Akamai Content Protector 는 스크레이퍼를 탐지하고 차단하도록 설계된 탐지기능을 갖추고 있습니다. Akamai 네트워크의 가시성, 봇 관리 분야의 글로벌 강점, 최첨단 탐지 기능의 지속적인 개발을 적극 활용합니다. Content Protector 는 위협의 변화에 따라 보안을 업데이트하고 위협 인텔리전스 연구원 및 데이터 과학자의 인사이트를 자동으로 통합함으로써 스크레이퍼에 대한 맞춤형 탐지 기술을 지속적으로 선도합니다.

스크레이퍼를 차단하면 사이트 성능 및 전환율을 개선하고 경쟁업체의 영향을 줄이는 등 기업의 디지털 입지를 최대한 활용하는데 집중할 수 있습니다.

주요기능 및 특장점

탐지

- 머신러닝을 활용한 맞춤형 탐지기능으로 스크레이퍼를 식별하고 차단

분류

- 트래픽 리스크를 낮음,중간,높음 범주로 분류해 대응에 필요한 정보를 제공

차별화

- 단일 대시보드에서 위협 분석, 심각도, 세부 정보와 함께 활성 위협을 즉시 파악할 수 있습니다.

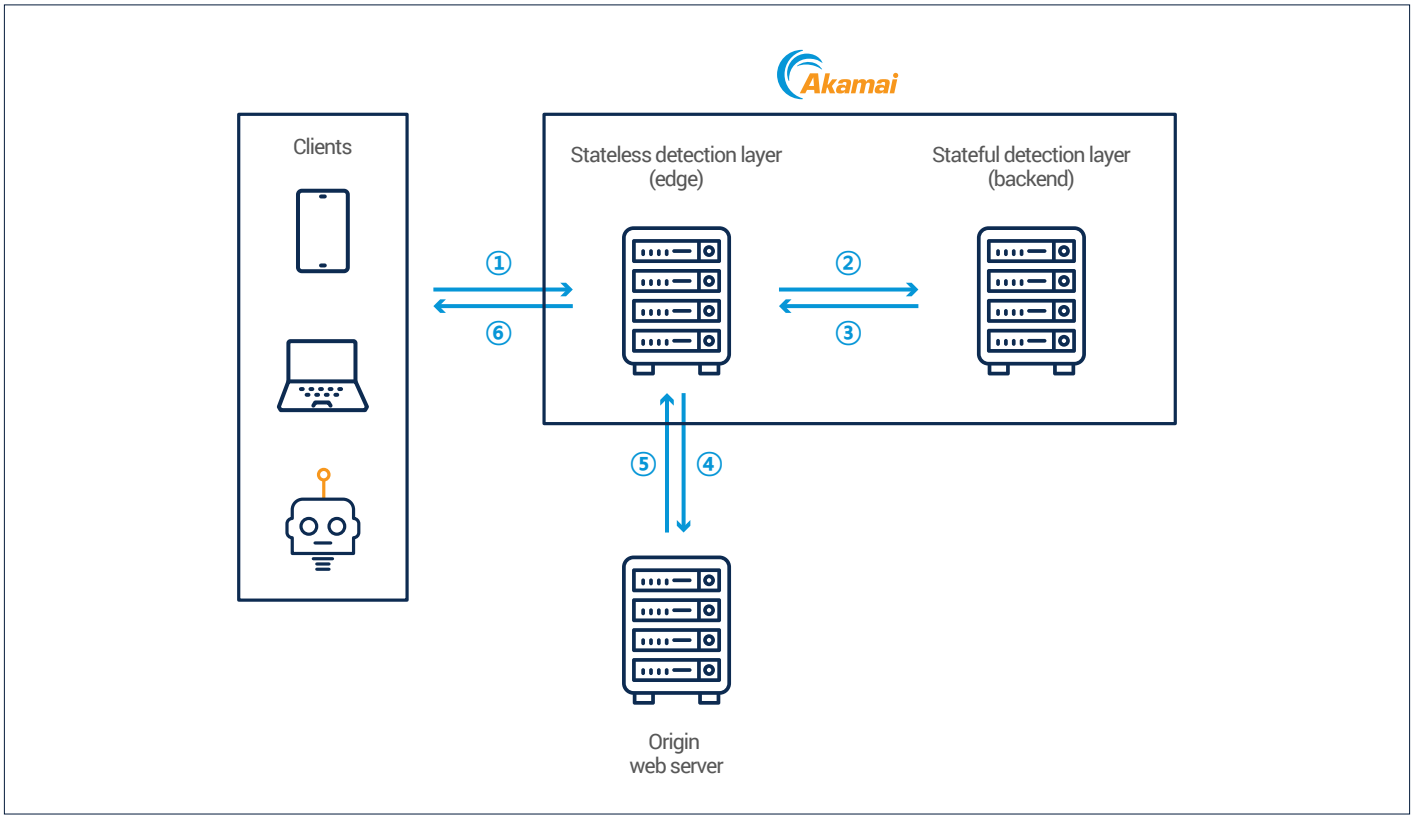
대응

- 리스크 분류와 기업의 목표에 따라 적절하게 대응 할 수 있도록 일련의 조치가 설계

구축효과

비즈니스 기회 향상	• 사이트와 앱의 속도를 떨어뜨리는 봇을 제거해 더 많은 고객 유치 및 매출 증대(Conversion Rate 증가) • 경쟁 업체가 기업의 가격을 낮추고 매출을 감소시키는데 일조하는 자동화된 스크레이핑 차단 • 사이트 애널리틱스에서 봇 트래픽을 제거해 실제 사용자에 맞게 최적화하는 마케팅 효과 개선
비용 절감	• 다량의 스크래퍼 봇으로 인해 늘어나는 트래픽에 대응하기 위해 증가되는 인프라 비용을 절감할 수 있습니다.
불법 복제 방어 스켈퍼 차단	• 불법 복제 업체가 콘텐츠를 수집해 전달 받을 목적으로 이용하는 무자비한 스크레이핑 차단 • 인기있는 제품의 재고가 입고되는 시점을 파악하기 위해 스크래핑 해가는 것을 차단하고, 사재기 봇의 유입을 차단

구성도



Bot Manager

도전 과제 **악성 봇 트래픽과 웹 공격에 노출**
브라우저의 형태를 완벽히 모방하는 봇의 스크래핑, 크롤링, 트래픽 점유 등의 직접적인 비즈니스 손해가 발생합니다.

해 결 책 전통적인 방법으로는 진화하는 봇의 위협을 효과적으로 관리하기 어렵습니다. Akamai Bot Manager는 봇을 식별하고 차단하며 속임수를 사용하여 위협을 줄입니다.

봇 차단 및 관리

Akamai Bot Manager는 지속적으로 업데이트 되는 봇 카테고리에 대한 안정적이고 인증된 DB를 기반으로 위험하고 탐지하기 어려운 봇을 신속히 차단합니다. 실제 트래픽과 봇 트래픽을 포괄적으로 구분하는 솔루션은 Akamai가 유일합니다.

주요기능 및 특장점

봇 가시성 강화

- 단순 차단 또는 허용하는 것을 넘어 가짜 콘텐츠로 봇을 속이고 성능을 느리게

정교한 동적 봇 탐지

- 다양한 AI, 머신러닝 모델, 기술을 사용해 첫 번째 상호 작용에서 알려지지 않은 봇을 정확하게 탐지

시뮬레이터

- 변경 사항 적용 전에 이를 과거 트래픽에 기반해 임계값 변경이 어떤 영향을 주는지 시뮬레이션하고 시각화

알려진 봇 디렉터리

- 알려진 봇에 자동으로 대응
- 알려진 봇 1750개가 들어 있는 디렉터리를 지속적으로 업데이트

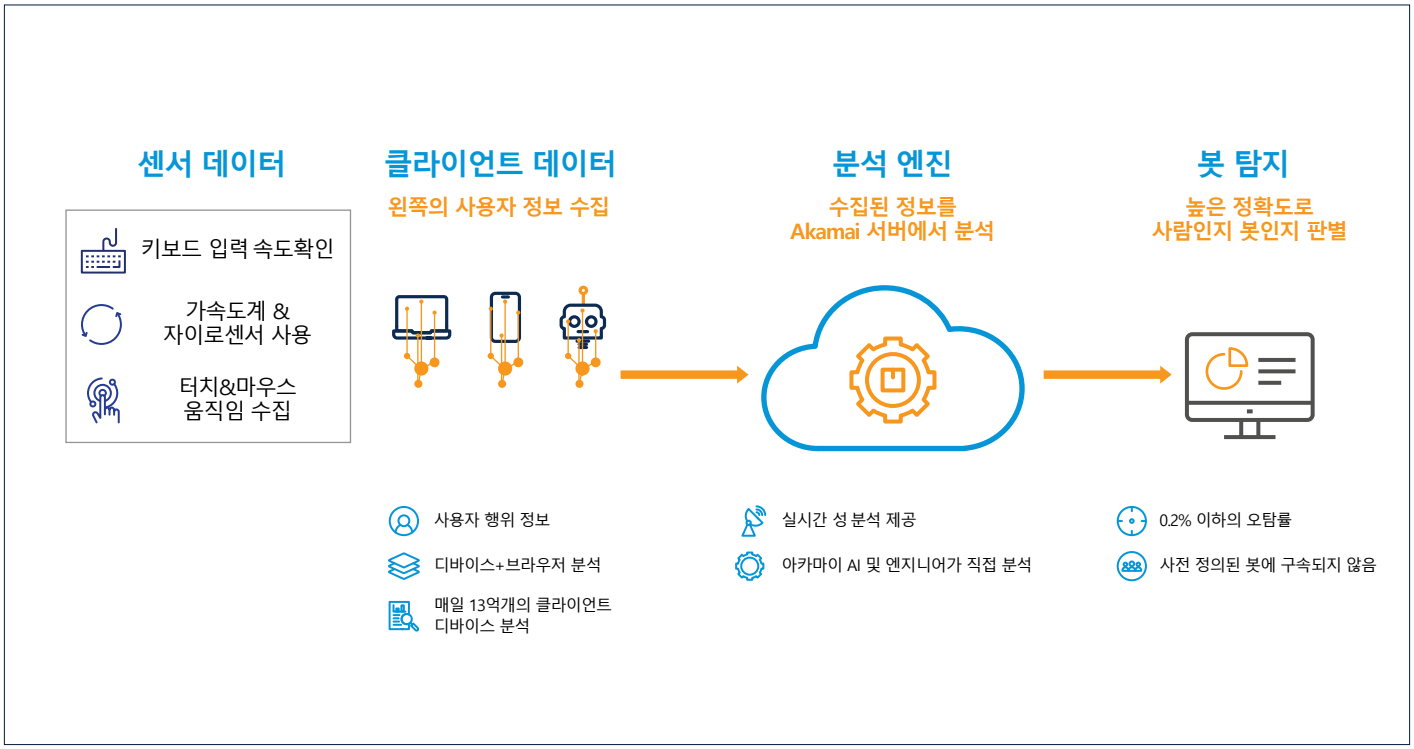
점수 모델

- 모든 요청을 평가
- 봇일 확률을 계산해 0점(사람)에서 100점(확실히 봇) 사이로 점수 측정

구축효과

알려지지 않은 봇을 정확하게 탐지	• 사용자 행동 분석, 브라우저 핑거프린팅(Fingerprinting), 인공지능(AI), 머신러닝 모델, 자동 브라우저 탐지, 비정상 HTTP 탐지, 높은 요청율 등의 기술을 활용하여 알려지지 않은 봇을 정확하게 탐지 • 지속적인 업데이트로 알려진 봇을 자동으로 관리
다양한 대응 조치	• 0점~100점 사이의 점수로 봇 정도를 나타내는 점수 모델을 활용하여 범위에 따라 대응 전략을 정의할 수 있도록 함 • 미끼 콘텐츠를 활용하여 악성 봇을 속이고 성능 저하를 유도 • 정상 트래픽 패턴을 학습하고 고유한 패턴에 따라 탐지를 자동으로 조정
봇 관련 상세 정보 제공	• 봇 트래픽에 대한 전반적인 트렌드, 업계 인사이트, 세부 분석 정보 제공 • 상세한 분석 및 리포팅 • 고객 여정, 보안 체계, 리스크 허용 범위, IT 운영에 대한 효과적인 의사결정에 도움

구성도



Edge DNS

도전 과제 **DNS 기반 공격과 서비스 중단의 위험에 노출**
웹 서비스를 구성하는 핵심 요소 중 하나인 Authoritative DNS 에 대한 안정적인 서비스가 필요합니다.

해 결 책 전통적인 DNS 서비스는 대규모 DNS 기반 공격에 취약하며, 서비스 중단을 방지하기 위한 충분한 탄력성을 제공하지 못합니다. 반면, Akamai Edge DNS는 클라우드 기반 네트워크를 활용하여 DNS 서비스의 연속성과 보안을 강화합니다.

안전한 DNS 보안

Akamai Edge DNS는 CDN NO.1 사업자인 Akamai의 대규모 클라우드 인프라에서 서비스하는 최대 규모의 엣지 플랫폼을 활용하여 DNS 중단을 예방하고 웹 애플리케이션과 API의 지속적인 가용성 보장 및 DNS 보안을 제공합니다.

주요기능 및 특장점

DNS 가용성

- 클라우드 기반의 Akamai 플랫폼으로 끊김 없는 DNS 서비스를 제공
- DNS 리소스를 분할하는 고유 아키텍처

글로벌 IP Anycast

- 글로벌하게 배치된 여러 물리적 서버 활용
- 로지컬 네임서버 사용 활성화

보조 DNS 상시 운영

- 보조 DNS로 인터넷에 연결된 보조 Zone을 사용해 만일의 사태에 대비

DNS 기반 공격 대비

- DNS 기반 공격에 대한 완벽한 방어 체계 구현

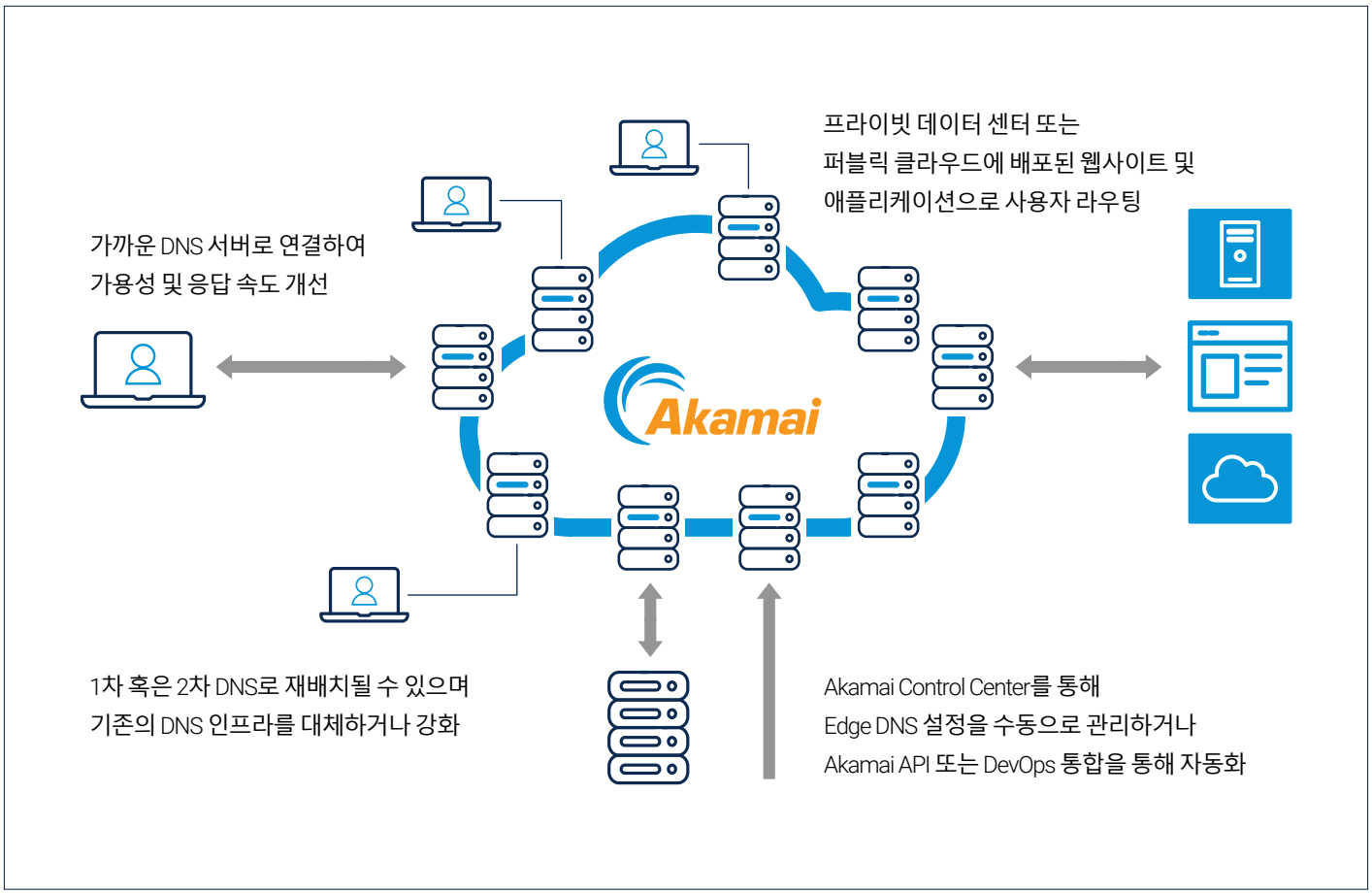
신뢰 기반 모델

- 신뢰할 수 있는 서버로만 콘텐츠를 서비스
- IP 주소 스푸핑 공격 방지

구축효과

높은 DNS 가용성	• 클라우드 기반의 대규모 DNS 서버와 수천 개 이상의 PoP(Points of Presence, 네트워크 거점)으로 높은 DNS 가용성 유지 • 100% 가동시간 SLA(Service Level Agreement, 서비스 수준 협약) 제공
빠른 DNS 응답속도	• 네트워크 상태를 고려해 최적의 성능 제공이 가능한 DNS 서버로 사용자 요청을 전달하고 응답속도 단축 • 전세계로 분산된 Anycast 네트워크를 활용하여 모든 지역에서 사이트와 애플리케이션에 접속하는 사용자들의 DNS 레졸루션 속도를 가속화 • 프로퍼티의 룩업 속도 단축으로 웹 애플리케이션 성능을 추가적으로 향상
DNS를 목표로 한 디도스(DDoS) 공격 방어	• 대규모 디도스 공격 처리가 가능한 충분한 용량과 확장성 확보 • 공격과 방어를 동시에 처리 • 공격을 받는 동안에도 정상 사용자에게 동일한 온라인 환경 제공

구성도



Threat Intelligence

도전 과제 **위협 인텔리전스 기반 탐지와 대응 역량 부족**
공격이 발생했던 IP의 이력을 확인할 수 있는 지속적으로 빠르게 업데이트 되고 신뢰도가 높은 위협 인텔리전스가 필요합니다.

해 결 책 기존 보안 시스템은 전 세계적인 데이터를 분석하여 제공하는 실시간 위협 인텔리전스가 부족합니다. Akamai Threat Intelligence는 광범위한 데이터 분석을 통해 보안을 실시간으로 강화하고 위협을 관리합니다.

위협 인텔리전스

Akamai TI(Threat Intelligence)는 Akamai CDN 기술을 기반으로 전 세계 15~30% 의 트래픽을 처리하며 수집한 인사이트로, 개별 IP의 행위 변화와 공격성에 대한 가시성을 확보하고 평판 분석을 통한 위협 인텔리전스 정보를 제공합니다.

주요기능 및 특장점

대규모 위협 데이터

- 매일 약 1.3Billion 클라이언트 디바이스 탐지
- 매일 2.5EB 공격 탐지 및 7PB 보안 데이터

광범위한 가시성

- 글로벌 트래픽의 ~30% 처리
- = 약 130TB

공격 탐지 분류에 따라

- CI(Client Intelligence) 솔루션과 NI(Network Layer Intelligence) 솔루션으로 구성

CI(Client Intelligence)

CI
Client Intelligence

- 애플리케이션을 대상으로 4가지 카테고리에 의해 공격하는 IP주소에 대한 리스크 점수(Scoring)를 산정한 자료

NI(Network Intelligence)

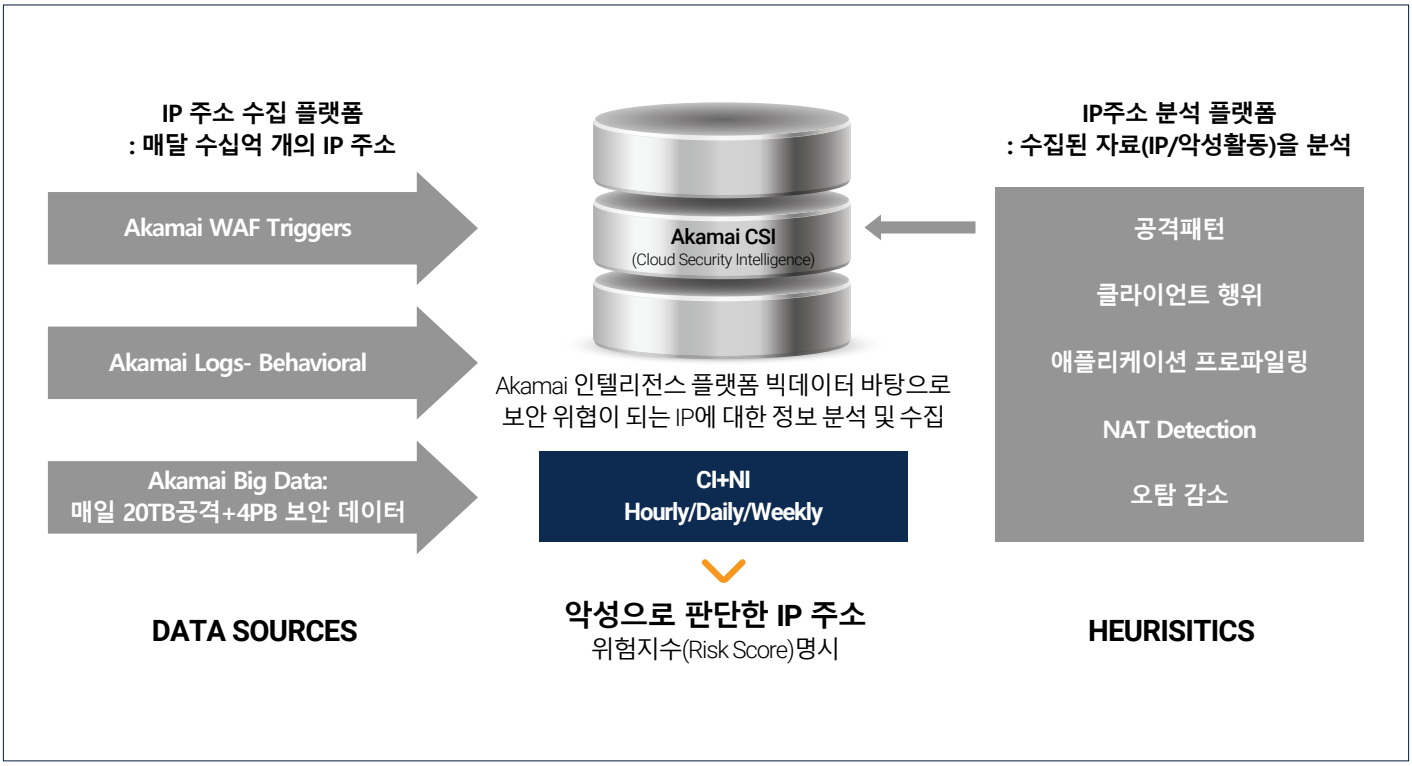
NI
Network Intelligence

- 네트워크 인프라를 대상으로 악용하기 위한 취약점을 찾는 스캐닝 툴의 IP 자료

구축효과

관제 데이터로 활용	• 공격 IP에 대해 카테고리별 꾸준한 이력 트래킹과 JSON 포맷을 통한 공격 IP의 상세 정보를 제공 • CI 데이터 양 : 30일 이력에는 1,418,082개의 고유 IP 주소가 포함 / 2.1GB • NI 데이터 양 : 일일 파일에는 431,441개의 고유 IP가 포함 / 113MB / 지난 데이터 8.4MB(압축) • 데이터 베이스에 등록된 IP는 사전 탐지 및 차단하는 보안위협 DB로 활용
보안 의사결정 자료로 활용	• CI와 NI 데이터는 실제 보안 위협에 대한 근거가 제공 되는 자료 • 보안 장비 등에서 확인된 비정상 접근 IP 에 대한 차단 또는 허용 등의 의사 결정에 근거 자료로 사용
위협 변화 자료로 활용	• 시간에 따라 클라이언트 IP 위협도 변화하므로 IP 위협 변화 정보 적용에 용이 • 블랙 IP 해제 근거 자료로 사용

구성도



아카마이 테크놀로지스 서울 강남구 테헤란로 134 포스코타워 역삼 12층 (우)06235 | T. 02-2193-7200