Akamai

보고서

웹 애플리케이션 보안 간소화

웹 애플리케이션 공격

마이크로서비스 기반의 아키텍처 도입이 증가하면서 최신 웹 애플리케이션은 복잡해지고 있습니다. 사실상 모든 온라인 상호작용이 API에 크게 의존하게 되면서 이런 복잡성이 가중되고, 이는 해커들의 새로운 진입지점이 될 수 있습니다. 알려진 웹 취약점은 계속 존재하며 새로운 세대의 각 코더들이 애플리케이션에 다시 사용합니다. 오늘날의 공격자들은 봇, 분산 서비스 거부(DDoS), 멀티벡터 공격을 통해 웹 애플리케이션, API, 심지어 클라이언트 측 취약점을 공격하며 발전해 왔습니다.

허점을 노리는 기회주의적인 공격이 가장 일반적인 웹 공격 종류인데 이런 공격은 아무 기업이나 무작정 공격하는 것이 아니라 확실한 취약점을 발견한 다음에 공격을 시작한다는 특징이 있습니다. 스캐너는 자동 봇을 이용해 웹사이트를 무작위로 스캐닝하면서 수천 가지의 취약점 중 하나를 발견해 냅니다. 취약점을 발견한 뒤 공격자는 데이터베이스에서 기밀 정보를 유출시키고 웹 서버에 악성 파일을 로딩하며 해당 사이트에서 감당할 수 없는 막대한 양의 트래픽을 집중적으로 전송합니다.

웹 공격으로 인한 리스크

리스크 허용 범위가 낮은 기업은 내부(시스템, 공급망, 운영 등)와 외부(파트너, 고객, 관리 기관 등)의 신뢰 체인을 구축하기 위해 가장 우수한 보안 역량을 필요로 합니다. 특히 마이크로서비스 애플리케이션의 여러 부분 사이의 간소한 내부 흐름에서 주요 비즈니스 간 트랜잭션에 이르기까지 API는 다양한 시스템과 파트너 생태계를 연결하고 디지털 및 옴니채널 고객 경험을 가능하게 하는 디지털 글루(glue)로서의 역할을 하기 때문에 보안을 유지하는 데 특히 중요합니다.

안타깝게도 사이버 범죄자들이 피해를 극대화하기 위해 만든 웹 공격 기법은 거의 무한대에 가깝습니다. 해커들의 공격이 성공해 데이터가 유출되거나 DDoS 공격으로 인해 사이트에 접속이 불가능한 경우 이러한 신뢰가 깨질 수 있으며 고객 충성도 하락, 규제 관련 벌금, 소송, 브랜드 평판 저하 등 상당한 손해가 발생할 수 있습니다.

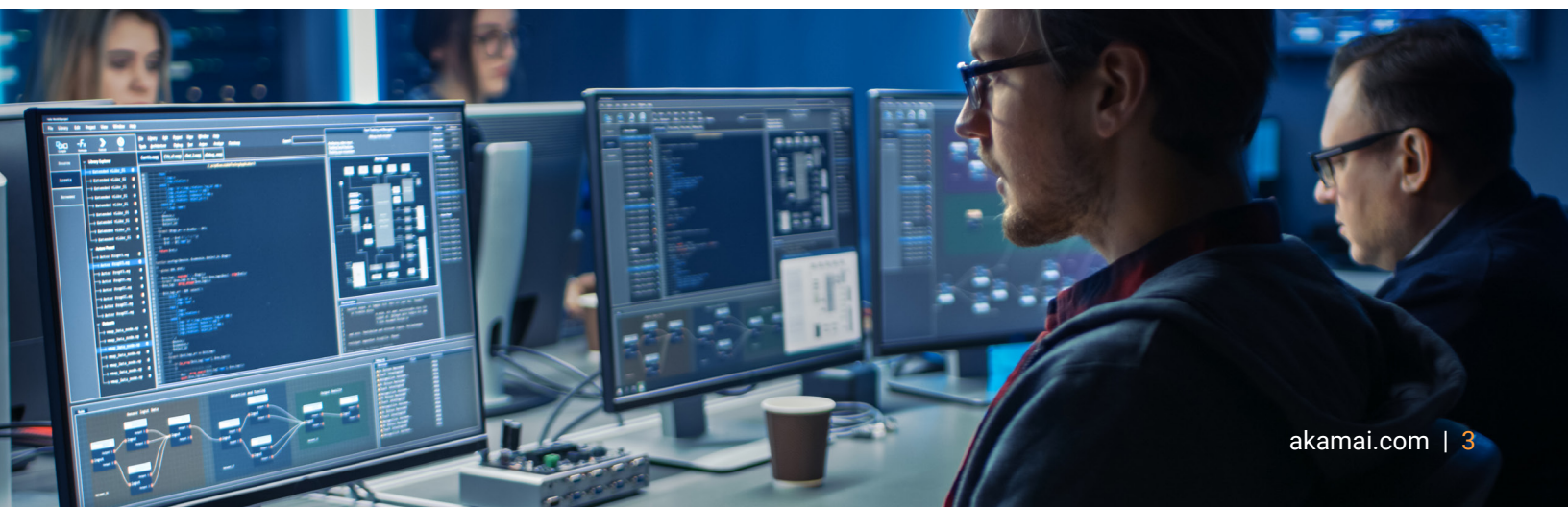
웹 애플리케이션 보안을 둘러싼 도전 과제

클라우드 기반 웹 애플리케이션 및 API 보안(WAAP) 솔루션은 다양한 형태의 웹 애플리케이션, DDoS, API 기반 공격을 방어하도록 설계되었습니다. 하지만 방화벽의 주요 문제 중 하나는 애플리케이션이 변경되고, 위협이 심화되고, 업데이트가 가능해지는 상황에 따라 룰을 지속적으로 분석하고 조정해야 한다는 것입니다. 숙련된 보안 전문가를 확보하는 것은 여전히 어려운 일이며, 숙련된 인력은 2년마다 직무를 옮기는 경우가 많습니다. 이는 시간이 많이 소요되는 수동 프로세스로서 숙련된 운영자가 필요한데 기업 대부분은 이직률, 학습 라이프사이클, 전문 기술 통합 아키텍처로 인해 확장하기 어렵습니다.

알림 피로가 실제 공격과 오탐률을 정확하게 구분하는 능력을 크게 저하시키는 상황에서 오래된 보안 정책은 좌절감의 원인이 될 수 있습니다. 룰을 효과적으로 조정하지 못하는 보안 팀은 적절한 보안을 제공하지 못할 수 있으며 정상 사용자에게 영향을 주고 비즈니스를 저해할 수 있다는 두려움 때문에 리스크 증가를 알면서 받아들이기도 합니다.

왜 Akamai WAAP일까요?

Akamai App & API Protector는 다양한 네트워크와 애플리케이션 레이어 위협으로부터 애플리케이션과 API를 규모에 따라 간편하게 보호하도록 설계된 클라우드 기반 WAAP 솔루션으로서 봇 가시성과 방어 기능을 모두 제공합니다. Akamai의 셀프 서비스 온보딩 마법사는 사전 지식의 필요성을 줄여주며, 빠르고 손쉽게 자산을 보호할 수 있는 가이드와 인사이트를 제공합니다. 자동화된 설정 프로세스는 보안 트리거를 분석하고 애플리케이션의 행동을 학습해 보안 기능을 셀프 튜닝하기 때문에 리소스를 더 많이 절약할 수 있습니다. App & API Protector는 기업 내 마찰, 운영 부담, 배포 장애의 원인이 되는 오늘날의 많은 방화벽 문제를 제거합니다.



세계에서 가장 분산된 플랫폼에 적용되며 Akamai에서 완벽하게 관리하는 자동화된 보안 기능을 통해 애플리케이션 보안 및 API 보안에 대한 완벽한 접근 방식을 취할 수 있습니다. SQL 인젝션(SQLi), 크로스 사이트 스크립팅, 로컬 파일 인클루전 등 웹 공격에 대한 자동 보안 기능을 통해 유지 관리가 거의 필요 없는 광범위한 서비스를 제공합니다. 또한, 머신 러닝과 휴리스틱을 적용해 일반적인 네트워크 전체 점검이 아닌 정책 단위로 트래픽 전반에 걸쳐 오탐률 패턴 식별을 강화해 가장 관련성이 높고 실행 가능한 결과를 도출할 수 있습니다.

내부 보안 및 개발 전략을 수립하는 데 도움이 되는 위협 수준과 Akamai의 현재 보안 기능에 대한 인사이트를 포함한 CVE별 상세 정보를 제공하는 CVE 조회 툴로 보안 상태를 검증할 수 있습니다. 또한 코드, API, CLI, Terraform, 통합 작업 등 Akamai의 사전 구축된 SecDevOps 통합 작업을 통해 내부적으로 조율을 개선하고 출시 기간을 단축할 수 있습니다.

탄력적인 보안 기능으로 수준 향상

그렇다면 Akamai App & API Protector은 어떻게 간편함과 정확성을 모두 제공할까요? 먼저, App & API Protector의 핵심 기술인 Akamai Adaptive Security Engine은 고객별 고유한 트래픽 및 공격 패턴을 학습하고, 모든 요청의 특성을 실시간으로 분석하고, 해당 지식을 활용해 향후 위협을 차단하고 적응한다는 점에서 독보적인 기술입니다. 이 기술은 모든 비정상적이거나 의심스러운 데이터 포인트를 고려하고 각 요청에 위협 점수를 할당해 보안 운영을 쉽게 만듭니다. 위협 점수가 높을수록 보안 수준이 더 강력해지며 탐지된 위협 수준에 맞게 동적으로 보안 기능을 수정해 오탐률을 매우 낮게 유지하면서 가장 교묘한 공격도 식별할 수 있습니다.

애플리케이션 공격에는 일반적으로 일종의 정찰 과정이 수반되지만, 공격자들이 취약점을 스캔함에 따라 Akamai는 공격 기법 및 전략에 대한 증거를 구축합니다. 이를 통해 빠른 속도로 공격자를 식별할 수 있을 뿐 아니라 공격자가 다시 공격할 경우 특정 트래픽에 대한 과거 핑거프린트를 남길 수 있습니다. 공격자가 더 자주 시도할수록 보안 수준을 더 강화할 수 있습니다.

Akamai의 인사이트

7.8억 건 이상
일일 웹 애플리케이션 공격 알림 수

260억 건 이상
봇 요청 수

932TB 이상
일일 데이터 분석량

크라우드소싱 위협 인텔리전스

10대 리테일 기업 중 9곳, 10대 은행 전체, 10대 헬스케어 기업 중 9곳, 6개 미군 조직 등 인터넷에서 가장 많은 공격을 받는 웹사이트 중 상당수가 Akamai 고객사이며 그 외에도 많은 고객사를 두고 있습니다. Akamai는 매일 7억 8000만 건 이상의 웹 애플리케이션 공격과 260억 건의 봇 요청에 대한 가시성을 확보합니다. 수백 명의 Akamai 위협 전문 연구원과 데이터 과학자가 매일 932TB가 넘는 새로운 데이터를 쿼리해 위협을 파악합니다. 이러한 수준의 글로벌 인사이트와 고급 머신 러닝, AI, 인적 분석이 결합되어 일반적인 공격부터 고도로 정교화된 공격까지 선제적이고 예측적으로 차단할 수 있습니다.

Akamai는 10년 넘게 애플리케이션 공격을 방어해 왔으며, 고객을 보호하고 인프라 가용성을 유지하면서 최대 규모의 공격을 막아낸 경험을 보유하고 있습니다. Akamai는 최신 위협을 지속적으로 조사하고 보고하고 있으며, 공격이 진화되고, 공격 규모가 커지고, 공격 방법도 정교해짐에 따라 악성 공격자들보다 한발 앞서 나가기 위해 자체 솔루션을 혁신하고 조정하고 있습니다. 그리고 App & API Protector는 Akamai 플랫폼을 기반으로 설계되었기 때문에 웹사이트, 애플리케이션, API의 성능을 극대화할 수 있는 기능이 이미 구축되어 있습니다.

무료 체험을 통해 웹 애플리케이션 및 API 보안 요구사항을 검토하고 Akamai App & API Protector의 장점을 직접 확인하세요.

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter) LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 6월 발행.