Akamai

웹 애플리케이션 방화벽에 대한 5가지 잘못된 통념 해결

미션 크리티컬 비즈니스를 온라인으로 운영하는 기업의 경우, WAF(웹 애플리케이션 방화벽)는 악성 트래픽을 차단하는 동시에 정상적인 트래픽이 통과할 수 있도록 하는 1차 방어선 역할을 해야 합니다. WAF는 수년간 사용해 온 기술이지만, WAF의 초기 개념은 최근 크게 달라진 사용 사례 대비 너무 단순합니다. 이로 인해 많은 비즈니스 리더와 보안 전문가들은 오래된 인식과 통념을 계속 고수하고 있습니다.

이런 잘못된 통념으로 인해 기업은 이미 스택에 있는 WAF의 능력을 과소평가하고 충분히 활용하지 못할 수 있습니다. 결과적으로, 공격자가 침투할 경로가 생기고 운영 리스크가 증가하게 됩니다. 포괄적인 디지털 보안을 갖춘 WAF 기술에 대한 필요성은 계속 높아지고 있습니다. 보안 체계를 개선하고 최신 WAF 기술의 보안 기능을 활용하려면 우선 가장 일반적인 오해를 해소해야 합니다.

2023년 3분기 99억 3천억 건이 발생한 웹 애플리케이션 공격

2023년 3분기의 일일 공격 건수는 약 3억 2700만 건으로 최고치를 기록

출처: Akamai 위협 연구팀

잘못된 통념 1

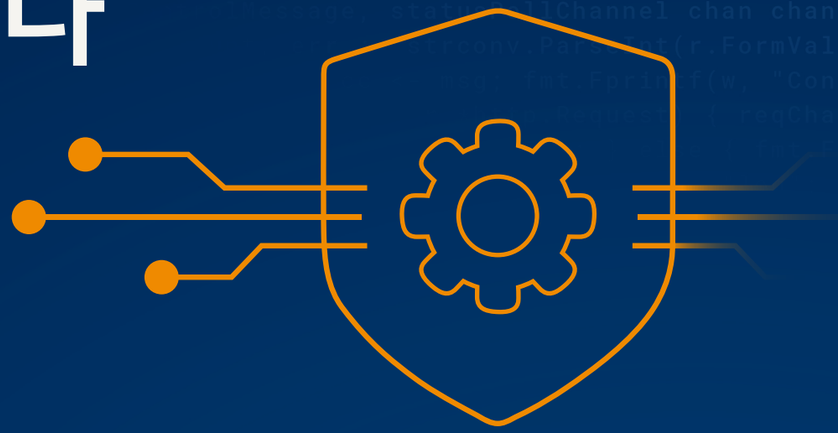
WAF를 효과적으로 유지하려면 지속적인 수동 업데이트가 필요하다

최신 업데이트가 최신 보안 기능을 제공하는 건 사실이지만, 이를 둘러싼 몇 가지 통념은 정확히 바로잡아야 할 필요가 있습니다. 오늘날 많은 기업은 WAF 룰을 지속적으로 업데이트하고 튜닝할 수 있는 리소스나 보안 전문 지식이 부족합니다. 자동화된 적응형 업데이트는 시간을 절약하고 사용 편의성이 높을 뿐만 아니라 리스크를 절감하는 비즈니스 효과가 있습니다. 수동 업데이트를 선택한 기업을 살펴보면 77% 이상이 룰세트 업데이트에서 5개 이상의 버전이 뒤처진 것으로 나타났습니다. Akamai 솔루션은 WAF 업데이트를 지속적으로 자동 푸시함으로써 기업의 시간과 리소스 투자를 절약하고 불필요한 리스크를 줄여줍니다.

잘못된 통념 2

WAF는 트래픽 게이트에 불과하다

레거시 WAF는 사용자와 웹 애플리케이션 간의 트래픽 중간에 위치하며, 정의된 룰 목록을 기준으로 HTTP 트래픽을 검사합니다. Akamai는 기존 WAF를 뛰어넘는 수준으로 빠르고 치열하게 솔루션을 혁신했습니다. 결과적으로 DDoS 방어, API 보안, 봇 방어, 멀웨어 탐지, 민감한 데이터 검색, 성능 가속 등 더 많은 기능과 보안 기능을 제공할 수 있게 되었습니다. App & API Protector가 출시되면서, 이제 WAF 보안 솔루션은 Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager, API Acceleration 등 고객이 가장 선호하는 기술이 포함된 번들로 제공됩니다. Akamai의 WAF 솔루션은 여러 기능이 하나로 통합된 기술로 보안 전문가에게 전사적인 보안을 위한 완벽한 가시성과 제어 기능을 제공합니다.



잘못된 통념 3

WAF가 알림 피로도를 높인다

일선 보안팀 직원에게 물어보면, WAF 방어 체계에서 생성된 엄청난 양의 알림과 트리거를 조사해야 하는 문제로 인해 보안팀이 많은 긴장과 압박에 시달리고 있다는 것을 직접 들을 수 있습니다. Akamai는 이 문제를 해결하기 위해 Akamai의 WAF 솔루션을 뒷받침하는 핵심 기술인 적응형 보안 엔진을 개발했습니다. 적응형 보안 엔진을 사용하면 머신 러닝, 실시간 보안 인텔리전스, 고도의 자동화, 400여 명의 Akamai 위협 연구원이 제공하는 인사이트를 조합해 최신 보안 기능을 사용할 수 있습니다. 전체 웹 애플리케이션과 API 자산을 보호하도록 설계된 적응형 보안 엔진은 각 고객별 트래픽과 공격 패턴을 학습하고, 모든 요청의 특성을 실시간으로 분석하고, 이러한 지식을 활용해 미래의 위협을 차단 및 대응합니다. 적응형 보안 엔진을 이용하면 보안팀 직원은 알림 피로를 방지하는 동시에 귀중한 시간을 절약하고 애플리케이션과 API를 보호하는 데 드는 노력을 줄일 수 있습니다.

오탐률을 낮추는
적응형 보안 엔진의
튜닝 권장 사항

5배

잘못된 통념 4

맞춤형 WAF 룰이 많을수록 보안이 강화된다

룰이 많을수록 설정, 테스트, 분석도 더 늘어납니다. 룰이 많을수록 반드시 보안이 개선되는 건 아니지만, 룰이 적다고 보안이 개선되는 것도 아닙니다. 룰이 많을수록 보안이 강화된다고 생각하는 보안 전문가라면 걱정하지 않으셔도 됩니다. Akamai의 WAF는 무제한 사용자 맞춤 룰이 함께 제공되며, 룰 개수가 아무리 많더라도 선제적인 적응형 룰 업데이트가 제공됩니다. 자동 업데이트 및 자동 셀프 튜닝을 통해 전체 디지털 자산의 대규모 WAF 설정을 효율적이고 효과적으로 검증할 수 있습니다. 새로운 룰을 추가하고 싶으신가요? 평가 모드를 사용하면 신규 및 수정된 룰이 라이브 트래픽에 미치는 영향을 평가해 고객 포털 대시보드에서 실시간 영향을 확인할 수 있습니다. 이러한 섀도(shadow) 모드 방식의 테스트는 새로운 룰 배포 시 해당 룰이 보안 기능을 예상대로 실행하도록 보장합니다.

잘못된 통념 5

WAF는 개발자에게 방해만 된다

개발자는 오늘날 기업에서 고객이 인정하는 가치를 창출합니다. 보안 문제가 발생하면 혁신이 느려지고, 출시 주기가 지연되며, 가치 실현 속도가 느려집니다. 그러나 이와 동시에, 테스트를 거치지 않은 릴리스는 비즈니스 운영을 중단시키는 심각한 보안 결과를 초래할 수 있습니다. Akamai는 보안 전문가와 개발자를 지원합니다. 애플리케이션과 API 등을 보호하는 WAF 방어가 DevSecOps 문화를 실현해 속도, 민첩성, 협업을 촉진할 수 있다고 생각합니다. Akamai의 모든 WAF 기능을 개방형 AppSec API 또는 Terraform을 통해 관리할 수 있는 이유도 바로 여기에 있습니다. 이를 사용하면 애플리케이션 및 API의 온보딩은 물론, 보안 설정 관리도 자동화할 수 있습니다. 도움이 필요한 경우 Akamai TechDocs를 참고하면 개발자를 위해 특별히 설계된 직관적이고 인터랙티브한 최신 기능을 사용할 수 있습니다.

Akamai의 서비스

공격표면이 빠르게 증가하고 위협이 지속적으로 진화하고 있으며 공격자들의 범행 동기가 분명한 상황에서 보안팀은 기존의 WAF 방어 체계를 뛰어넘는 가시성이 필요합니다. Akamai App & API Protector는 웹 애플리케이션 방화벽, 봇 차단, API 보안, DDoS 방어 등 다양한 보안 기술을 통합한 하나의 솔루션입니다. App & API Protector를 사용하면 보안 기능이 지속적으로 자동 업데이트되며, 클릭 한 번으로 맞춤형 정책 권장사항을 구현할 수 있습니다. App & API Protector의 핵심 기술인 적응형 보안 엔진은 머신 러닝, 실시간 보안 인텔리전스, 고급 자동화, 위협 연구자 400여 명의 인사이트를 바탕으로 최신 보안 기능을 제공합니다.

무료 체험을 시작하거나, Akamai 솔루션이 어떤 방식으로 기업의 가장 중요한 웹 기반 자산을 보호해 리스크와 운영 문제를 줄이는지 확인하세요.

| 2024년 01월 발행