백서

WAF에서 WAAP로 전환: Akamai의 포괄적인 애플리케이션 및 API 보안 솔루션에 대한 접근 방식

목차

서론 **04**

WAF의 기존 정의 **05**

기존 WAF의 문제점 **06**

설계 원칙 - WAF에서 WAAP로 전환 **07**

WAAP에 대한 Akamai의 접근 방식 **10**
- 룰세트를 넘어서 10
- 전송률 제한을 넘어서는 애플리케이션 레이어 DDoS 방어의 최신화 10
- 포괄적인 보안을 위한 단일 솔루션 11

Adaptive Security Engine **12**
- 적응형 위협 탐지 13
- 자동 업데이트 13
- 정확도를 보장하는 테스트 프레임워크 14
- 자동 셀프 튜닝 15
- 설정 및 자동화 유연성 15
  - 실제 환경에서의 검증 16
  - 최신 보안 기능과 통합 16

애플리케이션 보안 및 DDoS 방어 **18**
- Behavioral DDoS Engine: 작동 방식 19
- 애플리케이션 보안 정확도 21
- Client Reputation 점수 22

멀웨어 방어 **23**

애플리케이션 보안 애널리틱스 **24**

API 검색 및 프로파일링 **25**

봇 가시성 및 방어 **27**
App & API Protector에 내재된 봇 가시성 및 방어 27
주요 봇 기능 28

WAF 이상의 기능: Akamai 솔루션의 장점 **29**

위협 인텔리전스 및 탐지 **30**
Akamai 플랫폼 인텔리전스 30
위협 리서치 및 인시던트 대응 31
위협 리서치 31
인시던트 대응 31
신속한 위협 탐지 31
CVE 보안 32

전 세계적으로 분산된 엣지 플랫폼 **33**
안정성과 회복력 33
글로벌 규모 35
성능 35
엣지 플랫폼의 보안 기능 36
매니지드 공격 지원 37
SOCC(Security Operations Command Center) 37

결론 **38**

서론

공격 표면이 점점 더 커지고 다양해지고, 운영상의 제약 조건과 비용이 증가하고, 교묘한 다차원 위협이 지속적으로 증가함에 따라 보안팀은 기존의 웹 애플리케이션 방화벽(WAF)을 넘어서는 가시성을 필요로 합니다. 특히, 효율성을 높이기 위해 더 많은 자동화 툴이 필요하고, 애플리케이션과 애플리케이션 프로그래밍 인터페이스(API) 생태계에서 더 심층적인 보안이 필요합니다. 이러한 보안을 위한 최신 용어는 웹 애플리케이션 및 API 보안(WAAP)입니다. 비즈니스 보안과 고객 안전을 우선시하는 안목 있는 기업은 전체 디지털 자산에 걸쳐 여러 가지 위협에 대한 포괄적인 보안을 요구합니다. 알려진 공격, 알려지지 않은 공격, 제로데이 공격으로부터 애플리케이션을 보호하는 것 외에도 다음과 같은 보안 기능이 포함됩니다.

- 적응형 위협 탐지
- 자동화된 정책 업데이트
- 강력한 DDoS 방어
- API 검색 및 보안
- 봇 가시성 및 방어
- 개발 수명 주기를 위한 간편한 통합

이 백서에서는 기존 WAF 기술, WAF에서 WAAP로의 전환, 그리고 WAAP 솔루션을 발전시키고 있는 지속적인 시장 수요에 대해 설명합니다. 보안 분야의 확고한 리더인 Akamai는 최종 사용자의 온라인 라이프를 지원하고 보호하는 혁신적인 보안 기술에 대한 접근 방식에 집중하고 있습니다.

WAF의 기존 정의

기존 WAF는 최종 사용자와 웹 애플리케이션 사이의 트래픽 흐름의 중간에 위치합니다. WAF는 룰 목록에 정의된 대로 암호화되지 않거나 암호화된 HTTP 트래픽을 검사해 공격이 있는지 확인합니다.

대부분의 WAF는 정상적인 HTTP 트래픽과 섞여 있는 악성 HTTP 요청을 탐지하기 위해 미리 정의된 룰 목록을 사용해 수천 가지의 알려진 잠재적 악용으로부터 보호합니다. 또한, 새로운 공격 기법 또는 기존 공격 기법의 추가적인 변형이 지속적으로 발전하고 있으며 공격자들에 의해 악용되고 있습니다. 이러한 점에서 기존의 WAF는 룰을 지속적으로 업데이트하고 정상적인 트래픽 특성에 맞게 조정해야 합니다. 정상적인 트래픽 특성이 애플리케이션별로 다르며 시간이 지남에 따라 변하기 때문입니다.

최종 사용자들이 더 많은 보안과 성능을 요구함에 따라 WAF는 분산 서비스 거부(DDoS) 방어, API 보안, 봇 방어 기능과 같은 인접 보안 기술과 서비스를 포함하도록 그 범위가 확장되었습니다. 이러한 지속적인 진화에 따라 새로운 정의와 새로운 용어가 필요합니다.

기존 WAF의 문제점

WAF를 사용하는 기업들은 종종 보호되는 애플리케이션과 API에 대한 효과성, 관리 용이성, 영향력 측면에서 WAF가 초기 기대치를 충족하지 못한다고 주장합니다. 수십억 개의 웹 및 API 요청을 검사해 악성 코드를 찾는 과정에서 웹 성능 문제가 자주 발생하기 때문에 WAF는 종종 보안 프로토콜로 인해 기업 내 제약 조건, 성능 저하, 배포 방해의 원인이 되어 왔습니다.

기존 WAF의 가장 중요한 배포 문제는 다음과 같은 것에서 비롯됩니다.

- 부정확한 탐지와 높은 오탐이 알림 피로와 추가적인 리스크를 야기합니다
- WAF가 수동 검토, 튜닝, 유지 관리에 의존합니다
- 세분화된 제어가 부족해 최종 사용자의 경험과 비즈니스 프로세스를 방해하는 무차별적인 거부 정책이 발생합니다
- 구식 위협 인텔리전스로 인해 취약점이 증가합니다
- 제한과 유연성 부족으로 인해 성능과 적용 범위가 감소합니다
- 디지털 확장을 보호하기에는 너무 제한적입니다

기존 WAF는 강력한 보안 툴입니다. 그러나 이로 인해 기업에 운영상의 어려움을 야기하고 여기서 다루게 될 방어되지 않은 리스크를 초래할 수 있습니다.

WAF 기술을 WAAP 솔루션으로 업데이트하려는 기업은 해당 솔루션이 비즈니스 가치와 강력한 보안 보호 기능을 모두 제공하는지 확인해야 합니다. WAF에서 WAAP로 전환하면 보안팀을 비롯해 다른 팀 모두의 비즈니스 요구사항을 충족하는 기능, 효율성, 사용 편의성과 보안 기능이 결합됩니다.

설계 원칙 - WAF에서 WAAP로 전환

기존 WAF 제품은 최종 사용자의 룰 생성에 초점을 맞추고 있기 때문에, 모든 벤더사가 WAF 솔루션을 구축하고 비교적 쉽게 시장에 출시할 수 있습니다. 오픈 소스인 OWASP CRS(Open Worldwide Application Security Project ModSecurity Core Rule Set)를 중심으로 구축된 상용 제품이 널리 보급된 것을 보면 알 수 있습니다.

그러나 공급업체가 다음과 같은 기능을 갖춘 포괄적인 WAAP 솔루션을 설계하는 것은 어렵습니다.

- 새로운 취약점이 등장할 때마다 애플리케이션과 API를 보호하기 위해 인라인으로 배포됩니다
- 최신 애플리케이션 개발 관행을 따라갑니다
- DDoS 방어, 봇 방어, API 보안, 클라이언트 측 웹 애플리케이션 보안의 강력한 레이어를 동등하게 제공합니다

Akamai는 WAAP 솔루션의 설계에 접근할 때, 그것이 '충분히 좋은 수준'을 넘어서는 것이어야 한다고 믿었습니다. App & API Protector는 보안 리스크를 해결하는 동시에 고객사가 주요 비즈니스 목표에 집중할 수 있도록 하기 위해 만들어졌습니다. 설계 시 이상적인 WAAP 솔루션은 다음을 제공해야 한다고 생각했습니다.

효과적인 보안
애플리케이션은 비즈니스의 모든 측면에서 실행됩니다. 악성 공격으로부터 이를 보호하는 것이 기업 보안팀의 기본 목표입니다. 보안팀은 WAAP 솔루션에서 동급 최고의 탐지 기능을 제공하는 WAAP 솔루션을 찾는 데 어려움을 겪고 있습니다. 이상적인 보안 툴은 탐지 효율성이 WAAP 솔루션의 가장 중요한 측면이기 때문에 그것을 우선시하고, 제로데이, 악용, 공통 보안 취약점 및 노출(CVE) 방어에 대한 뛰어난 실적과 인상적인 가용성 기록을 보유해야 합니다.

정확도
보안팀은 리스크를 방어하는 동시에 비즈니스가 빠르게 움직일 수 있도록 하는 적절한 균형을 찾아야 합니다. 이상적인 솔루션은 최종 사용자의 경험과 비즈니스 프로세스를 손상시키지 않으면서 오탐을 줄이는 데 도움이 되는 셀프 튜닝 메커니즘을 갖추고 있어야 합니다.

최신 보안 기능

기업은 새로운 취약점이 발견될 때마다 최신 룰에 따라 보안 기능을 지속적으로(그리고 종종 수동으로) 업데이트해야 합니다. 이를 위해서는 2가지 핵심 능력, 즉 공격 기법 전반에 걸쳐 최신 인텔리전스에 접속할 수 있는 능력과 언제라도 변경될 수 있는 공격에 맞게 방어 전략을 조정할 수 있는 숙련된 보안 리소스가 필요합니다. 이상적인 솔루션은 위협 인텔리전스 커뮤니티의 리더가 되어 자산 보호 전반에 걸쳐 보안 운영을 간소화하는 기능을 제공해야 합니다.

적응성

위협 환경이 빠른 속도로 진화하고 있습니다. AI 기반 공격의 등장이 임박한 상황에서 보안팀은 그 어느 때보다 보안 운영의 효율성을 높여야 합니다. 이상적인 WAAP 솔루션은 최신 자동화, 머신 러닝, 심층적인 글로벌 인텔리전스를 결합해 자동으로 업데이트를 제공하고 클릭 한 번으로 구축되는 사용자 맞춤화된 룰 수정 제안을 제공해야 합니다.

가시성

기존 WAF 솔루션에서는 일반적으로 끊임없이 알림이 발생하며 보안 실무자가 사내 리소스를 활용해 각 알림을 신중하게 분석해야 합니다. 보다 효과적인 WAAP 솔루션은 공격 발생 시점, 발생 장소, 발생 방식 등을 기업에 알려 리소스 부담을 경감함으로써 다중 솔루션 가시성과 공격에 대한 선제적 맥락을 제공해야 합니다.

확장성

수신 트래픽을 처리할 수 있을 만큼 규모가 충분하지 않은 솔루션은 웹 지연 시간을 증가시키는 병목 현상을 쉽게 발생시키고 부하가 걸리면 멈출 가능성이 있습니다. 효과적인 WAAP 접근 방식은 시간이 지남에 따라 변화하는 트래픽 수요와 공격에 맞춰 원활하게 자동으로 확장되며, 중단이나 성능 저하 없이 지속적인 보안을 제공해야 합니다.

협력

효과적인 보안 솔루션은 현재 스택에 통합 가능하고, 프로그래밍이 가능하고, 사용이 간편하고, 원활하게 작동해야 합니다. 이상적인 솔루션은 보안팀과 개발팀 사이에 가교 역할을 합니다.

지원

보안 관련 문제가 발생하면 기업은 적절한 시기에 해결책을 제시하기 위해 필요한 기술과 리소스에 압도당하는 경우가 많습니다. 이상적인 솔루션은 정기적인 매니지드 서비스 옵션과 온디맨드 서비스 옵션을 제공해 진행 중인 공격, 서비스 문제, 직원 교체, 내부 기술 격차 등을 포함한 일반적인 시나리오에 대한 전문 지식과 방어책을 제공할 수 있어야 합니다.

이러한 설계 원칙을 염두에 두고 Akamai가 선도적인 WAAP 솔루션인 App & API Protector를 구축하는 방법을 핵심 기술부터 살펴보겠습니다. Akamai의 솔루션은 여러 보안 제품을 하나로 결합해 애플리케이션 보안, 증폭 DDoS 공격 방어, 자산 전반의 API 보안, 봇 트래픽 제어와 같은 문제를 포괄적으로 해결합니다.

WAAP에 대한 Akamai의 접근 방식

룰세트를 넘어서

시장이 기존 WAF 설계 원칙에서 효과적인 최신 보안 솔루션인 WAAP로 이동함에 따라 효과적인 탐지 및 방어 기술에 여전히 초점이 놓였습니다.

Akamai는 2009년에 세계 최초의 엣지 기반 WAF로 자사의 WAF를 처음 도입했습니다. 당시 보안 벤더사들은 탐지를 위한 기초로 정적 룰 세트를 기반으로 하는 WAF를 제공하고 있었습니다. 당시 Akamai는 Kona Rule Set라는 독자적인 룰 기반 엔진을 구축해 차별화를 꾀했습니다. 이 엔진은 정적 룰이 아닌 유연한 룰을 소수만 사용하며, 공격에 대한 정확도와 가시성을 향상시키기 위해 비정상 점수 모델과 함께 사용되었습니다.

그리고 2017년에 Akamai는 자동화된 공격 그룹을 도입해 Akamai가 관리하는 보안 기능을 통해 기업이 룰을 지속적으로 설정하고 업데이트할 필요가 없도록 했습니다. 자동화된 공격 그룹은 혁신적인 기술로 수천 개의 Akamai 고객 WAF 정책에 빠르게 적용되어 새로운 접근 방식을 활용했습니다.

Akamai는 2021년 App & API Protector를 출시하면서 봇 방어 기능을 포함한 결합된 애플리케이션 및 API 보안을 우선시하는 애플리케이션 보안 접근 방식을 지속적으로 발전시켰습니다. 이 WAAP 솔루션은 기업 및 성장하는 글로벌 비즈니스를 위해 Kona Site Defender WAF를 대체하는 것을 목표로 했습니다. App & API Protector는 Kona Rule Set 기술을 Adaptive Security Engine으로 최신화함으로써 Akamai가 보안 운영에 접근하는 방식을 변화시켰습니다.

전송률 제한을 넘어서는 애플리케이션 레이어 DDoS 방어의 최신화

DDoS와 관련해, 전송률 제한은 효과적이며 검증된 툴입니다. 그러나 정교한 레이어 7 DDoS 공격, 멀티 기법 공격, API 악용이 증가함에 따라 기존 DDoS 방어 시스템은 대응에 어려움을 겪고 있습니다. 고정된 임곗값과 사전 정의된 시그니처에 의존하는 정적 방어는 사후적이며, 특히 공격자들이 악성 트래픽과 정상적인 요청을 혼합하는 경우가 증가함에 따라 오탐이 발생하기 쉽습니다. 따라서 Akamai는 DDoS 방어에 대한 접근 방식을 바꾸고 URL 보호 및 Behavioral DDoS Engine과 같은 새로운 혁신을 도입했습니다.

Behavioral DDoS Engine은 Akamai App & API Protector에 추가된 최첨단 기술로, Adaptive Security Engine의 핵심 기술 중 하나입니다. 이 2가지 엔진이 함께 작동해 오늘날의 위협에 대한 전례 없는 보안 기능을 제공함에 따라 Akamai는 WAAP 분야의 리더가 되었습니다. Akamai는 이러한 듀얼 엔진 접근 방식으로 자동 업데이트, 셀프 튜닝 기능, 맥락 인식 탐지 기능을 제공해 수동 개입이 필요 없는 경험을 제공함으로써 차별화합니다.

포괄적인 보안을 위한 단일 솔루션

오늘날, 서버리스 엣지 컴퓨팅, 마이크로서비스 기반 아키텍처, 단일 페이지 애플리케이션, 애플리케이션 보안을 형성하는 데 사용되는 SaaS/IaaS/PaaS/FaaS 접근 방식을 통해 최신 개발 관행으로 애플리케이션 보안을 재정의하는 변화가 계속되고 있습니다.

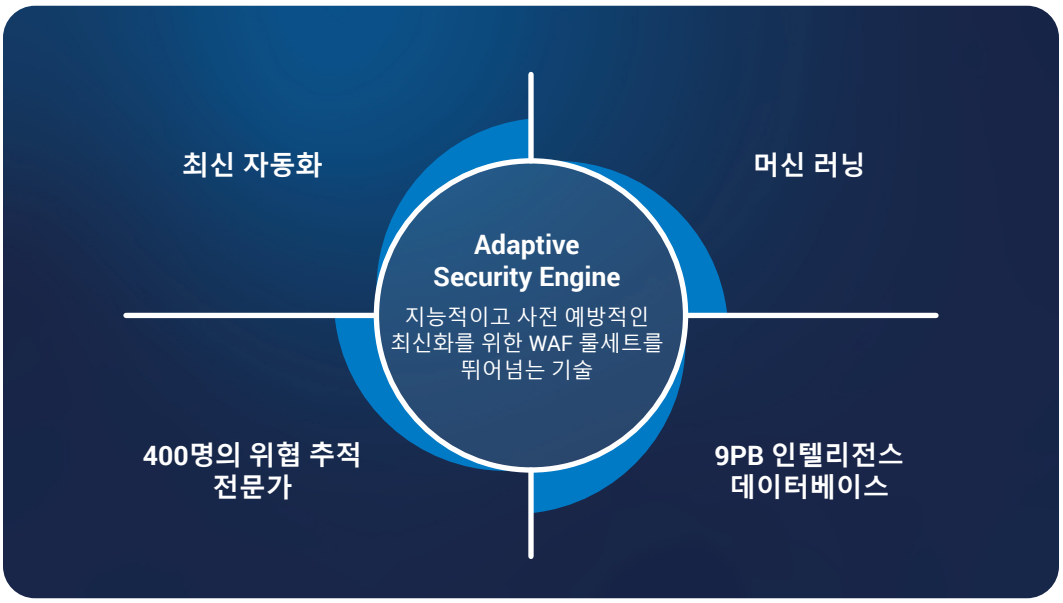
복잡한 IT 환경에서 최신 애플리케이션과 API를 보호하기 위해 Akamai는 보다 적응력 있고, 유연하고, 포괄적인 접근 방식으로 애플리케이션 보안 기술을 재설계했습니다. Akamai의 WAAP 솔루션이 Web Application Protector와 Kona Site Defender에서 App & API Protector로 전환되면서 더 많은 보안 기능과 특화된 툴세트가 통합되었습니다.

App & API Protector는 이제 많은 추가적인 보안 개선 기능을 제공하며, 이 모든 기능은 단일 인터페이스를 통해 표시되고 제어됩니다. Akamai의 WAAP 솔루션은 다음을 결합합니다.

1. Adaptive Security Engine
2. 세분화된 제어를 통한 애플리케이션 보안
3. 최신 레이어 7 DDoS 방어를 포함한 DDoS 방어
4. 검색 및 PII 보안 기능을 포함하는 API 보안
5. 봇 가시성 및 방어 기능
6. 글로벌 규모, 위협 인텔리전스, 회복력을 위한 플랫폼

Adaptive Security Engine

Adaptive Security Engine은 머신 러닝(ML), 실시간 보안 인텔리전스, 사이버 보안 전문가, 최신 자동화의 교차점에서 차세대 보안 기능을 제공합니다. Akamai의 탐지 및 방어 핵심 기술인 Adaptive Security Engine은 전체 웹 애플리케이션과 API 자산을 보호하기 위한 자동 접근 방식을 가능하게 합니다. 이 기술은 또한 WAF에서 WAAP로의 전환이라는 Akamai의 기술 발전에 추가됩니다. 이로 인해 봇 관리자, DDoS 방어, DevOps 통합 등을 포함한 상호 관련된 보안 솔루션이 이 발전에 포함됩니다.



Adaptive Security Engine은 각 고객의 고유한 트래픽과 공격 패턴을 학습하고, 모든 요청의 특성을 실시간으로 분석하고, 그 지식을 사용해 미래의 위협을 차단하고 적응한다는 점에서 독보적인 기술입니다. 동일한 플랫폼 인사이트와 인텔리전스를 사용해 튜닝 권장 사항을 통해 오탐을 줄입니다. 이 셀프 튜닝 기능은 사전 예방적 업데이트로 적응형 위협 보안 기능을 제공함으로써 보안팀 및 개발팀이 쉽게 사용할 수 있도록 합니다.

적응형 위협 탐지

엔진은 플랫폼 인텔리전스와 각 요청의 데이터/메타데이터를 결합하는 다차원 위협 점수 모델을 사용합니다. 이 데이터에 대해서 의사 결정 논리를 통해 실제 공격을 정확하게 탐지하는 조치가 이루어집니다.

정교한 공격자는 접근 방식에 더 많은 시간과 노력을 투자하기 때문에 적응형 탐지는 고도로 표적화되고, 교묘하고, 은밀한 공격을 탐지하는 데 특히 효과적입니다. 공격자가 취약점과 설정 오류를 스캔할 때, Adaptive Security Engine은 공격자의 과거 지문을 더 쉽게 식별할 수 있도록 공격자의 기법에 대한 증거를 수집하고 연관시킵니다.

실제 페이로드와 요청 내에서의 위치 외에도, 각 클라이언트에 대해 다음과 같은 공격 차원을 평가합니다.

- 정찰 또는 공격의 이력(예: 빈도, 규모, 심각도)
- 악성 자동화 및 공격 툴의 징후
- 알려진 공격 트래픽 소스와의 상관관계

또한 Adaptive Security Engine은 다음의 2가지 독점 기술로 강화됩니다. Smart Detect는 입력 내용을 지문으로 토큰화해 매우 정확하게 탐지하고, Smart Sniff는 요청 본문의 올바른 콘텐츠 종류를 탐지해 콘텐츠 조작과 우회를 방지합니다. Akamai 위협 연구원들은 Akamai의 광범위한 인프라와 시스템을 활용해 모든 프로덕션 트래픽에 걸쳐 새로운 탐지 작업을 수동적으로 실행한 다음, ML 모델을 사용해 그 결과를 분석합니다.

자동 업데이트

오늘날 많은 기업은 지속적으로 발전하는 위협을 추적하고, 설정을 업데이트하고, 웹 트래픽에 대한 재검사를 통해 정책을 최적화할 수 있는 리소스나 보안 전문 지식이 부족합니다. 이에 따라 Akamai는 AI/ML 자동 테스트 프레임워크를 사용해 Adaptive Security Engine을 지속적으로 업데이트함으로써 변화하는 위협을 고려하면서 높은 정확도를 유지합니다. 이러한 업데이트는 제로데이 공격이 발표되기 전에 보호하는 경우가 많습니다.

정확도를 보장하는 테스트 프레임워크

WAAP 솔루션 테스트는 간단한 전제를 사용합니다. 바로 다양한 공격 기법을 테스트하고 웹 공격을 차단한다는 것입니다. 그러나 다음 요소를 고려해야 합니다.

- 실제 환경은 테스트 환경보다 복잡하며 종종 오탐과 미탐을 유발합니다.
- 정확도를 염두에 두고 테스트 프레임워크를 설계하려면 추가적인 검증이 필요합니다. 공격 탐지뿐만 아니라 그 과정에서 오탐이나 미탐을 유발하지 않도록 해야 합니다.
- 테스트에는 정상적인 트래픽과 공격 트래픽 등 실제 웹 트래픽을 사용해야 합니다.

Adaptive Security Engine 업데이트는 정상적인 트래픽에 부정적인 영향을 미치지 않도록 다음의 여러 단계로 이루어져 있습니다.

- 모든 탐지는 합성 트래픽을 사용해 실험실에서 테스트함으로써 오탐을 발생시키지 않으면서도 공격을 제대로 포착할 수 있는지 확인합니다.
- 그런 다음, 라이브 프로덕션 트래픽에서 업데이트를 테스트해 샘플이 현재 플랫폼 트래픽에 유효한지 확인합니다. 이 프로세스에는 실제 고객 트래픽에 섀도 모드로 업데이트를 실행하는 것이 포함됩니다. 섀도 모드로 실행하면 테스트 탐지 정확도를 유지하면서 고객 트래픽에는 영향을 주지 않습니다.
- 업데이트가 2단계를 통과하면, ML이 사람이 분석 중 놓쳤을 수 있는 패턴이나 트리거를 식별한 다음, 위협 연구팀이 수동으로 결과를 검토합니다.
- 각 단계에서 이러한 점검을 통과해야만 변경 사항이 다음 단계로 이동해 네트워크의 더 큰 세그멘트에 배포될 수 있습니다. 100% 배포 후, 셀프 튜닝 기능이 고객의 트래픽 패턴에 특정한 나머지 오탐을 제거합니다.

자동 셀프 튜닝

자동 셀프 튜닝 기능은 수동 튜닝의 부담을 덜어 주어, 정책이 오래되어서 발생할 수 있는 문제와 사람의 실수를 방지하고, 거의 손을 대지 않아도 되는 경험을 제공합니다. Adaptive Security Engine은 각 보안 정책의 모든 트리거에 ML, 통계 모델, 휴리스틱을 적용해 실제 공격과 공격으로 잘못 탐지된 최종 사용자 트래픽을 정확하게 구분합니다. 온보딩 과정에서만 적용되는 일반적인 플랫폼 전체 점검이 아니라, 최종 사용자의 설정이나 개입 없이 연중무휴 24시간 지속적으로 수행되는 튜닝 프로세스입니다.

셀프 튜닝은 제약 조건이 없고 간단합니다. 보안 관리자는 사용자 인터페이스를 통해 한 번의 클릭만으로 권장 사항을 쉽게 검토하고 승인할 수 있으며, AppSec API, 명령줄 인터페이스(CLI) 또는 Terraform을 사용해 자동화할 수도 있습니다. 투명성을 높이기 위해, 사전 필터링된 Web Security Analytics 링크를 통해 오탐으로 간주되는 모든 요청을 보여주고, 각 튜닝 권장 사항에 대한 근거를 제공합니다.

설정 및 자동화 유연성

WAAP 솔루션 벤더사가 기존 룰세트 기술을 넘어설 때, 설정과 자동화가 더욱 유연해집니다. Adaptive Security Engine은 다음과 같은 기능을 제공합니다.

- 다양한 애플리케이션 및 그와 관련된 리스크 성향에 따라 다양한 종류의 WAF 업데이트(자동 vs 수동)를 제공합니다
- 공격 그룹별 조치 및 애플리케이션/트래픽 행동이 표준이 아닌 경우 사용자 정의에 필요한 기여 룰을 제어합니다
- IP, 지리적 위치, 헤더, 페이로드 등과 같은 다양한 요청 특성에 대한 단순하고 복잡한 조건을 설정합니다
- Penalty Box를 사용해 자체 애플리케이션에 대한 의심스러운 WAF 공격/스캐닝을 수행하고 탐지된 위협 소스를 사전에 방어합니다
- 디버그 헤더를 수정합니다
- 요청 페이로드 검사 크기 또는 공격 페이로드 로깅 설정을 수정합니다
- 탐지 로직의 변경 사항을 시뮬레이션해 변경 사항을 자신 있게 프로덕션에 적용합니다

실제 환경에서의 검증

평가 모드는 특정 Adaptive Security Engine 버전을 설정하고 업데이트나 새 룰/정책을 테스트할 때 Akamai 고객에게 유연함과 정밀함을 제공합니다. 고객은 새로운 업데이트 또는 변경 사항을 적용하기로 결정하기 전에 그것이 고객의 특정 웹 애플리케이션 환경에 적절하거나 필요한지를 확인할 수 있습니다. 효과적인 보안 최신화를 위해 Akamai는 과거 트래픽을 대상으로 테스트하는 것보다 실시간 트래픽을 대상으로 테스트하는 것이 보안 결과를 개선한다고 생각합니다. 평가 모드는 섀도 룰을 적용하는 것과 유사합니다. 평가 모드에서는 정책이 적용된 것처럼 실시간 결과를 볼 수 있지만 현재 최종 사용자에게 영향을 미치지 않습니다. 기업은 수동/평가 모드를 선택해 오탐과 미탐에 대한 예기치 않은 영향을 최소화할 수 있습니다.

최신 보안 기능과 통합

보안팀 및 DevOps 팀은 CLI, Akamai Terraform 또는 자신의 CI/CD 자동화 파이프라인의 스크립트를 사용해 Akamai API 호출을 통합함으로써 보안을 운영할 수도 있습니다. 설정 및 자동화의 유연성은 강력한 보안이 개발 속도를 절대 저해하지 않도록 보장합니다. 이러한 통합으로 다음이 가능합니다.

- 신속한 온보드 애플리케이션 활성화
- 대규모 애플리케이션 포트폴리오 전반에 걸쳐 보안 정책의 통일된 관리 제공
- 하이브리드 및 멀티클라우드 인프라 전반에 걸쳐 보안 적용의 중앙 집중화
- 최적의 적용 범위를 위해 GitOps 워크플로우에서 DevOps 팀과 보안팀 간의 협업 개선

또한 보안 정보 및 이벤트 관리(SIEM)를 통해 Akamai 플랫폼에서 발생하는 보안 이벤트를 수집할 수 있습니다. 따라서 Akamai의 SIEM 통합 솔루션은 SIEM 이벤트를 Splunk, QRadar와 같은 온프레미스 및 클라우드 기반 SIEM 분석 툴에 전달하는 방법을 제공하므로, Akamai 보안 이벤트를 4가지 기본 단계에 따라 전체 이벤트 및 보안 인프라에 통합할 수 있습니다.

다음과 같은 방법으로 데이터 피드를 보호하고 제어할 수 있습니다.

- **이벤트 필터링**
  보안 설정과 보안 정책을 활용해 실제 위협에 집중할 수 있습니다.
- **데이터 보존**
  수집기는 12시간 동안 데이터를 저장하므로 누락된 이벤트를 캡처할 수 있습니다.
- **SIEM 과부하 방지**
  SIEM 커넥터에서 각 요청에 대해 가져오는 보안 이벤트의 최대 수를 정의할 수 있습니다. 이를 통해 SIEM 애플리케이션의 과부하를 방지할 수 있습니다.
- **가져오기 간격**
  SIEM 커넥터가 보안 이벤트 데이터를 가져오기 위해 SIEM API를 호출하는 빈도를 정의할 수 있습니다.

애플리케이션 보안 및 DDoS 방어

애플리케이션 보안은 오늘날 사이버 보안의 중요한 측면으로, 애플리케이션이 다양한 위협과 취약점에 대해 안정성을 유지할 수 있도록 보장합니다. 그 중요성은 여러 가지 핵심 영역에 있습니다. 애플리케이션 보안은 민감한 데이터가 무단 접속 및 변조로부터 보호되도록 보장하므로 데이터 무결성과 기밀성이 매우 중요합니다. 또한 보안 인시던트로 인한 중단으로부터 애플리케이션을 보호함으로써 일관된 서비스 가용성을 보장하기 때문에 비즈니스 연속성에도 중요한 역할을 합니다. 더불어 애플리케이션 보안은 평판 관리에 필수적이며 기업의 평판을 훼손하고 고객 신뢰를 약화시킬 수 있는 유출을 방지합니다. 마지막으로, 기업이 규제 요구사항을 준수하도록 지원해 법적 및 재정적 처벌을 피할 수 있도록 합니다.

기능적으로, WAAP 솔루션은 웹 애플리케이션과 인터넷 사이의 HTTP 트래픽을 필터링하고 모니터링합니다. 이를 통해 XSS, SQL 인젝션, DDoS와 같은 일반적인 웹 기반 공격으로부터 보안 기능을 수행합니다.

App & API Protector는 리소스를 압도적으로 공격하는 증폭 공격을 막기 위해 설계되었으며, 업계 최고의 DDoS 방어 기능으로 인정받고 있습니다. 솔루션은 다음과 같은 방법으로 DDoS를 방어합니다.

- **엣지 기반 DDoS 방어**
  App & API Protector는 Akamai의 전 세계적으로 분산된 엣지 플랫폼을 활용함으로써 DDoS 공격이 애플리케이션의 오리진에 도달하기 전에 즉시 차단할 수 있습니다. 이러한 엣지 우선 접근 방식은 애플리케이션의 성능에 영향을 미치지 않으면서 최소한의 지연 시간과 최대의 보호를 보장합니다.

- **전송률 제한**
  App & API Protector는 분산된 애플리케이션 레이어 DDoS 공격을 방어하기 위해 적응형 전송률 제한 기능을 포함하고 있습니다. 이러한 제어 기능은 IP, 지리적 위치, IP 평판 제어, 다양한 HTTP 헤더, 일치 조건 등 다양한 기준에 따라 수신 요청의 전송률을 제한하도록 설정할 수 있습니다.

- **지능형 부하 분산을 통한 URL 보호**
  전송률 제한에 대해 다른 접근 방식을 취합니다. URL 보호 기능을 사용하면 오리진 용량에 따라 허용 가능한 요청 속도(최대 RPS)를 기준으로 과도한 요청으로부터 오리진을 보호할 수 있습니다. 특히 연산량이 많은 URL, API 엔드포인트 등을 고도로 분산된 애플리케이션 레이어의 DDoS 공격으로부터 보호하도록 설계되었습니다.

- **Behavioral DDoS Engine**
  App & API Protector에 새로 추가된 Behavioral DDoS Engine은 심층적 방어 전략에 강력한 툴입니다. 트래픽 기준선을 설정하고 규범에 대한 비정상을 탐지하는 데 ML을 사용해 DDoS 이벤트를 관리하고 방어하는 자동 접근 방식을 도입합니다. 이 엔진은 변화하는 트래픽 패턴을 이해함으로써 작동하며, 사용자가 명시적인 임곗값을 설정하지 않고도 시스템이 다양한 비정상에 반응하는 방식을 정의할 수 있도록 해 시스템 관리 및 튜닝이라는 운영상 부담을 줄여 줍니다.

- **자동 업데이트 및 적응형 셀프 튜닝**
  Akamai의 2가지 엔진 전략인 Adaptive Security Engine과 Behavioral DDoS Engine을 사용하는 App & API Protector는 자동 업데이트와 ML 기반 셀프 튜닝을 통해 새로운 위협에 지속적으로 적응함으로써 운영 부담을 줄입니다.

Behavioral DDoS Engine: 작동 방식

Behavioral DDoS Engine의 핵심은 실시간 트래픽을 지속적으로 모니터링해 정상적인 행동에 대한 기준선을 설정하고 공격으로 의심되는 편차를 즉시 탐지하는 최신 ML 모델입니다. 엔진은 발생 국가, TLS 패턴, IP, TLS 지문 등 여러 동적 차원의 트래픽 패턴을 분석해 비정상을 신속하게 탐지하고 조치를 취할 수 있습니다.

Behavioral DDoS Engine의 주요 구성요소는 다음과 같습니다.

- **실시간 행동 모니터링**
  엔진은 트래픽을 지속적으로 분석해 정상적인 활동의 기준선을 설정하고 잠재적인 DDoS 공격을 나타내는 편차를 즉시 탐지합니다.

- **정밀성을 위한 머신 러닝**
  최신 ML 모델이 트래픽 패턴의 미묘한 비정상을 탐지하는 엔진의 능력을 강화해, 정상 사용자를 차단하지 않고도 정확한 방어를 보장합니다.

- **사전 예방적 방어**
  엔진은 Akamai의 글로벌 네트워크 인사이트(하루 1056TB의 트래픽)를 활용해 공격이 비즈니스에 영향을 미치기 전에 예측하고 무력화합니다.

- **다차원 분석**
  IP, 국가, TLS 패턴 등 여러 차원에서 트래픽을 평가해 각 애플리케이션의 요구사항에 맞는 강력한 보안 기능을 제공합니다

탁월한 방어를 위한 최신 아키텍처

Behavioral DDoS Engine은 다음과 같은 몇 가지 중요한 구성요소를 포함하는 정교한 아키텍처를 통해 작동합니다.

- **탐지 엔진**
  동적 차원과 과거 공격 데이터를 사용해 실시간으로 DDoS 공격을 탐지합니다.
- **방어 엔진**
  기준선 생성기와 위협 신호로부터 얻은 인텔리전스를 사용해 자동으로 공격을 차단함으로써 보안팀의 운영 오버헤드를 줄입니다.
- **알림/오탐 감소**
  ML 모델이 관련 없는 데이터를 걸러내어 분석과 방어에 정상 트래픽이 사용되도록 합니다.
- **기준선 생성기**
  2주 동안 정제된 데이터를 처리해 트래픽 프로파일을 지속적으로 개선함으로써 최신 공격 전략에 맞춰 엔진을 업데이트합니다.
- **기준선 검증기**
  이 중요한 구성요소는 AI의 도움을 받아 매달 수백 건의 DDoS 공격을 평가해 솔루션을 미세 튜닝합니다.

보안팀은 자동화된 프레임워크 덕분에 엔진을 통해 수동 개입 없이 방어를 동적으로 조정할 수 있습니다. 솔루션은 봇에 의해 생성된 트래픽이나 DDoS 공격 시도 등 비정상적인 트래픽 활동을 탐지하고 필터링해 애플리케이션을 효과적으로 보호합니다.

애플리케이션 보안 정확도

정확도가 떨어지는 애플리케이션 보안 솔루션(WAF 또는 WAAP)은 매일 증가하는 알림 수를 관리하기 위해 더 많은 내부 리소스를 필요로 합니다. 부정확성은 많은 수의 오탐(악성 요청이 아니지만 악성 요청으로 표시되는 경우)과 미탐(악성 요청이지만 악성 요청으로 표시되지 않는 경우)을 유발할 수 있으며, 이러한 종류의 알림에 대한 리서치와 분석에 귀중한 보안 기술과 시간을 낭비하게 만듭니다.

기업은 종종 알림 피로라는 도전 과제에 직면하지만, 너무 광범위한 제어 또는 과잉/과소 조정 기능 때문에 해결책을 찾지 못하고 있습니다. 이 때문에 기업은 WAF를 오프라인으로 전환하거나, 더 나쁜 경우 알림과 버전 업데이트를 무시하게 됩니다. 이렇게 하면 실수로 정상 사용자를 차단하는 것에 대한 기업의 우려를 많이 줄일 수 있지만, 웹 및 API 공격에 대한 보호는 줄어듭니다. 또한 많은 기업은 정상적인 트래픽에 대한 접속을 균형 있게 조정하고 악성 트래픽을 정확하게 차단할 수 있는 정밀한 제어 기능이 부족합니다.

효과적인 WAAP 솔루션은 포괄적인 WAAP 제어 및 기능 세트를 통해 오탐과 미탐을 모두 줄여 정확도를 높이고 정상 사용자에게 미치는 영향을 최소화하는 장점이 있습니다.

정확도 이해

정확도는 WAF 또는 WAAP가 공격은 차단하면서 정상 사용자를 실수로 차단하지 않는 능력을 측정합니다. 정확도는 다음 4가지 변수를 고려합니다.

- **정탐(TP):** 악성으로 올바르게 식별된 실제 공격
- **오탐(FP):** 악성으로 잘못 식별된 정상적인 요청
- **정미탐(TN):** 애플리케이션으로 전달된 정상적인 요청
- **미탐(FN):** 애플리케이션으로 잘못 전달된 실제 공격

Client Reputation 점수

Client Reputation은 정교한 리스크 분석 엔진을 사용해 사이트에 접속하려는 각 IP 주소에 대한 일련의 '리스크 점수'를 계산합니다. 수신 IP 주소를 분석하고 공격자의 지속성, 표적 애플리케이션의 수, 공격의 심각성, 규모, 업계, 고객의 애플리케이션을 표적으로 한 이전 공격과 같은 다양한 요소를 사용해 해당 IP 주소가 다음과 같은 웹 공격을 수행할 가능성을 나타내는 점수를 결정합니다.

- **DOSATCK**
  봇넷을 사용해 서비스 거부(DoS) 공격을 시작합니다. DoS 공격의 목표는 사이트에 가짜 요청을 너무 많이 보내서 사이트가 엄청나게 느려지거나 심지어 다운되도록 하는 것입니다. 분산 서비스 거부(DDoS) 공격에서 이러한 요청은 수천 개의 위치(일반적으로 멀웨어에 감염된 컴퓨터 또는 휴대전화)에서 발생하므로 특정 IP 주소를 차단하는 것만으로는 공격을 막을 수 없습니다.

- **SCANTL**
  스캐닝 툴은 SQL 인젝션, 교차 사이트 요청 위조(CSRF), 잘못된 리디렉션, 기타 취약점과 같은 잠재적인 보안 리스크를 탐지할 수 있습니다. 소유한 사이트에 대해 웹 스캐닝 툴을 실행하는 것은 좋은 생각입니다. 하지만 공격자가 웹사이트에 대해 스캐닝 툴을 실행하는 것은 좋지 않습니다.

- **WEBATCK**
  SQL 인젝션, 원격 파일 인클루전 또는 크로스 사이트 스크립팅과 같은 기술을 사용해 멀웨어를 설치하거나 사용자 데이터를 훔치는 등의 작업을 수행합니다. 해커는 비밀번호, 신용카드 번호, 주민등록번호, 그리고 사용자 데이터베이스에 저장되어 있을 수 있는 그 밖의 모든 정보를 포함한 사용자의 모든 사용자 데이터를 가져올 수 있습니다.

- **WEBSCRP**
  자동화된 툴을 사용해 웹페이지의 사본을 다운로드한 다음, 해당 페이지의 모든 콘텐츠를 '스크레이핑'(즉, 복사)합니다. 콘텐츠는 불법적이거나 비윤리적인 용도로 재사용될 수 있습니다.

Client Reputation을 사용하면 Akamai Connected Cloud의 누적 위협 인텔리전스를 기반으로 의심스러운 위협 소스로부터 기업을 사전에 보호할 수 있습니다.

멀웨어 방어

공격자는 멀웨어를 일반적인 공격 기법으로 사용합니다. 애플리케이션을 포괄적으로 보호하기 위해 Akamai는 멀웨어로부터 보호하는 솔루션을 제공합니다. 모든 규모의 기업에서 다음과 같은 일반적인 용도를 포함해 내부 및 외부 모두에서 효율성을 위해 파일 업로드를 허용합니다.

- 입사 지원용 이력서
- 고용 계약, 온보딩, 전자 확인, 계좌 자동 이체 설정 등
- 대출, 계좌 설정, 신용 요청을 포함한 신청서
- 자동차, 주택 등에 대한 보험 또는 수리 견적서
- 보험 또는 환자 계좌 설정을 위한 의료 기록
- 이미지를 포함한 고객 제품 또는 경험 리뷰

애플리케이션 내의 멀웨어 방어 기능과 API 보안 기능은 멀웨어 위협이 표적 기업 시스템에 도달하기 전에 엣지에서 멀웨어 위협을 탐지하고 격리합니다. 기업은 애플리케이션과 API에 대한 멀웨어 방어 기능의 장점을 활용해 시간, 예산, 생산성, 내부 데이터 및 고객 데이터를 보호할 수 있습니다.

- **엣지에서 멀웨어를 탐지하고 차단합니다**
  멀웨어가 이미 확산되었을 수 있는 서버에서 스캔하는 리스크를 피할 수 있습니다.
- **복잡성을 피하고 시간을 확보합니다**
  ICAP 및 에이전트 기반 스캐너와 같이 각 시스템에 개별적으로 보안 기능을 설정하는 대신 파일을 한 번만 스캔합니다.
- **성장할 수 있는 보안 체계를 갖춥니다**
  기업은 예방적인 레이어드 접근 방식을 선택함으로써 비즈니스가 성장함에 따라 보안 기능을 확장할 수 있으며, 엣지에서 추가 보안 기능과 오리진에서 다시 스캔할 수 있는 옵션을 제공합니다.
- **애플리케이션에 일관성을 제공합니다**
  기업은 애플리케이션 코드를 설정하거나 변경할 필요가 없습니다. 멀웨어 방어는 Akamai Connected Cloud에서 완전히 호스팅됩니다.

애플리케이션 보안 애널리틱스

App & API Protector에는 (가장 많이 사용되면서) 가장 사랑받는 Akamai 제품인 Web Security Analytics가 포함되어 있습니다. 이 Akamai WAAP 솔루션을 사용하면 Akamai 플랫폼에서 웹 애플리케이션과 API에 대해 발생하는 보안 이벤트를 캡처하고 제공된 보안 애널리틱스 툴에서 시각화할 수 있습니다.

Web Security Analytics는 웹 트래픽과 잠재적 위협에 대한 포괄적인 인사이트를 제공하는 오늘날 사이버 보안의 핵심 구성요소입니다. 트래픽 패턴, 사용자 행동, 보안 이벤트 등 방대한 데이터 포인트를 분석함으로써 웹 애플리케이션의 보안 체계에 대한 상세한 가시성을 제공합니다. 이러한 사전 예방적 접근 방식을 통해 기업은 위협을 보다 효과적으로 탐지하고 대응할 수 있으며 심각한 피해를 입기 전에 리스크를 방어할 수 있습니다. Web Security Analytics는 봇 공격, SQL 인젝션, 크로스 사이트 스크립팅과 같은 악성 활동을 탐지하는 데 도움이 될 뿐만 아니라 웹 애플리케이션의 취약점을 이해하고 해결하는 데도 도움이 됩니다. 또한 보안 정책 및 규제 요건 준수를 보여 주는 보고서를 생성해 컴플라이언스 노력을 지원합니다.

API 검색 및 프로파일링

기업은 API를 사용해 백엔드 데이터와 로직을 노출해 새롭고 혁신적인 제품을 개발함으로써 강력한 웹 및 모바일 경험을 만들 수 있습니다. API는 공격 표면도 확장시킵니다. 기업은 어떤 API 엔드포인트가 환경에 있는지, API의 기능은 무엇인지, 트래픽 프로필은 어떤지 파악해야 합니다. Akamai의 API 검색 및 프로파일링 기능은 이 모든 것과 그 이상의 일들을 자동으로 그리고 지속적으로 수행합니다.

API 검색 기능은 기업의 다양한 사업 부문에서 연결된 새로운 애플리케이션과 API가 있으며 이것이 종종 보호되지 않는다는 사실을 보안팀에 알려줍니다. 이 자동 탐지 기술은 개발팀, 비즈니스 리더, 보안팀의 협업을 유지하기 위한 Akamai의 WAAP 솔루션의 새로운 기능입니다.

Adaptive Security Engine은 응답 콘텐츠 종류, 경로 특성, 트래픽 패턴을 고려한 점수 부여 메커니즘을 기반으로 24시간마다 API를 자동으로 검색합니다. 검색 데이터에는 다음과 같은 세부 정보와 함께 관찰된 API 사양에 대한 정보가 포함됩니다.

- 호스트네임
- 기본 경로
- 리소스 경로
- 매개변수와 데이터 종류
- 방법
- API 포맷

기본 경로와 리소스 경로는 API 트래픽이 있는 특정 호스트네임에서 관찰된 트래픽의 경로 깊이, 자식 수, 형제 항목을 고려하는 알고리즘을 기반으로 결정됩니다. 리소스 경로 내에서 특정 방법에 대해 매개변수가 관찰되면 그것에 표시하고 해당 매개변수의 데이터 종류가 식별됩니다.

API 엔드포인트의 트래픽 프로필에는 API의 목적과 현재 위협 수준에 대한 인사이트를 제공하는 정보가 포함되어 있습니다. 포함된 데이터 포인트 중 일부는 다음과 같습니다.

- API가 처음 발견된 이후의 총 요청 수(지난 24시간 동안 및 시간 경과에 따른 트렌드)
- API가 처음 발견된 날짜와 마지막으로 확인된 날짜
- GET, PUT, POST, DELETE, OPTIONS 등 다양한 방법에 걸친 요청 수
- 2xx, 3xx, 4xx, 5xx 응답을 생성하는 요청의 수
- 사용자 에이전트를 기반으로 한 최종 클라이언트 식별
- 클라이언트 측 및 서버 측 오류를 초래하는 트래픽 비율과 같은 응답 오류
- 알려진 공격자로부터의 히트 수(Akamai 플랫폼에 대한 알려진 공격자로부터의 전체 트래픽의 백분율 포함)를 웹 공격자, 웹 스캐너, 스크레이퍼, DoS 공격자별로 구분

가시성이 없으면 API 보호가 큰 장애물이 될 수 있습니다. 기업은 보이지 않는 것을 어떻게 보호할 수 있을까요? 기업은 Akamai를 사용하여 엔드포인트, 정의, 리소스, 트래픽 특성을 포함해 API를 자동으로 지속적으로 검색하고 프로파일링할 수 있습니다. Akamai는 API를 확인한 후 DoS, 악성 인젝션, 인증정보 도용 공격, API 사양 위반에 대처하기 위한 광범위한 보호 기능을 제공합니다. Akamai의 클라우드 및 오리진에 구애받지 않는 접근 방식은 최종 사용자가 추가적인 설정 없이 전체 애플리케이션 자산에서 API를 쉽게 발견할 수 있도록 해줍니다. 이러한 가시성을 통해 개발자, 애플리케이션 소유자, 보안팀은 새로운 API, 알려지지 않은 API 또는 변화하는 API를 미리 파악하고 보호를 위해 쉽게 등록할 수 있습니다.

봇 가시성 및 방어

봇이 웹사이트 트래픽의 절반 이상을 차지하고 있기 때문에 어떤 봇이 기업의 목표 달성에 도움이 되고 어떤 봇이 기업에 해를 끼치려는 의도를 가지고 있는지 파악하기가 어려울 수 있습니다. 정상 봇은 평가, 대화 또는 추천을 자동화함으로써 기업의 효율성을 향상시킵니다. 악성 봇은 트래픽 경로를 막고 고객 및 운영 경험에 영향을 주어 매출에 영향을 미칠 수 있습니다. App & API Protector 내에서 봇 가시성 및 방어는 정상 봇을 확인하고 통과시키면서 악성 봇을 차단하는 강력한 탐지 기능을 제공합니다. 이를 통해 기업은 다음을 수행할 수 있습니다.

- **봇을 확인하고 그 영향을 이해**
  검색, 사이트 성능 확인, 비즈니스 파트너와의 상호 작용과 같은 작업에 봇이 널리 사용되고 있다는 점을 고려하면 봇 트래픽에 대한 가시성은 오늘날 디지털 비즈니스에 매우 중요합니다.
- **운영 제어 향상**
  악성 봇을 차단하면 효율성을 향상시키고, 비즈니스 리스크 및 재정적 리스크를 줄이고, IT 지출을 더 잘 관리할 수 있습니다.
- **데이터를 기반으로 보다 현명한 의사 결정**
  상세한 애널리틱스 및 리포팅 기능을 활용해 고객 여정, 보안 체계, 리스크 허용 범위, IT 운영에 대한 창의적이고 효과적인 의사 결정을 내릴 수 있습니다.

App & API Protector에 내재된 봇 가시성 및 방어

App & API Protector는 웹 자산의 성능과 보안에 부정적인 영향을 미칠 수 있는 봇 트래픽에 대한 봇 탐지 및 제어를 제공합니다. 시간이 지남에 따라 발생하는 봇 관련 비정상과 위협을 사전에 모니터링할 수 있도록 조기 가시성을 제공합니다.

App & API Protector에서 제공되는 Akamai의 봇 솔루션 사용:

- Akamai에 알려진 1700개 이상의 정의된 봇에 접속
- 실시간 봇 트래픽 가시성 확보
- 맞춤형 봇 정의 생성
- 정상 봇 허용 및 악성 봇 거부
- 봇 가시성 및 트렌드 보고 확인

최신 봇 문제가 있는 사이트의 경우, Akamai는 이커머스 및 디지털 보안을 강화하기 위한 최신 봇 보안 기능을 포함하는 Bot Manager를 제공합니다. Bot Manager는 다음과 같은 공격에 사용되는 것과 같은 지속적이고 공격적인 봇에 대해 보다 세밀한 조치를 제공합니다.

- 크리덴셜 스터핑
- 재고 비축
- 콘텐츠 및 가격 스크레이핑
- 비즈니스 로직 악용

주요 봇 기능

Akamai는 WAAP를 통한 봇 관리에 대한 변화하는 요구사항을 인식하고, 다음과 같은 새로운 기능을 포함하도록 봇 가시성 및 방어 툴을 개선했습니다.

- **브라우저 사칭 탐지**
  고객들이 선호하는 이 Akamai Bot Manager는 동적 점수 산정 모델과 ML을 사용해 브라우저 내 봇 활동을 구별하고 대응하며, App & API Protector에 포함되어 있습니다.
- **조건부 대응 조치**
  이제 고객은 브라우저 내 봇 활동에 대해 더 잘 이해하게 되며, 조건부 조치를 통해 악성 봇에 대해 다른 대응 전략을 적용할 수 있습니다.
- **도전 과제 조치**
  해결되지 못했을 때 콘텐츠에 대한 접속을 차단할 수 있는 틈새형 도전 과제를 비롯해 다양한 도전 과제를 통해 봇을 처리할 수 있습니다.

WAF 이상의 기능: Akamai 솔루션의 장점

WAAP에 대한 Akamai의 접근 방식은 App & API Protector라는 솔루션으로 이어졌습니다. 그러나 WAAP 고객에게 혜택을 제공하는 제품은 이것만이 아닙니다. 가장 분산된 글로벌 플랫폼을 기반으로 구축되고 수백 명의 위협 전문가가 지원하는 Akamai Connected Cloud는 성능, 가용성, 인텔리전스, 전문 지식, 효과적인 보안 결과를 제공합니다.

위협 인텔리전스 및 탐지

강력한 사내 위협 인텔리전스 기능을 갖추면 WAAP 벤더사가 발전하는 위협에 대응하는 능력이 향상됩니다. 그러나 제공되는 인텔리전스의 품질,시의성, 실행 가능성에 따라 애플리케이션 보안 효과에 미치는 영향의 정도가 결정됩니다. Akamai는 Akamai Connected Cloud를 통해 제공되는 데이터를 지속적으로 분석해 위협 환경의 현재 트렌드, 처음 발견되는 새로운 공격 기법, 현재 활동 중인 공격자를 탐지합니다. 그런 다음, Akamai는 해당 인텔리전스를 여러 가지 방법으로 WAAP 솔루션에 통합합니다.

백서 초반부에 소개된 Akamai Adaptive Security Engine은 2가지 계층의 심층 위협 인텔리전스를 결합해 고객사를 위해 최신 보안 기능을 자동으로 관리하는 강력한 독점 엔진을 만듭니다. Adaptive Security Engine은 ML과 자동화된 룰 도입 외에도 Akamai의 글로벌 플랫폼과 대규모 전문 위협 연구팀에서 파악한 위협 인텔리전스를 제공합니다.

Akamai 플랫폼 인텔리전스

Akamai는 세계 최대 규모의 글로벌 플랫폼을 보유하고 있기 때문에 모든 Akamai 고객을 대상으로 한 전 세계의 공격 트래픽을 적시에 분석할 수 있는 메커니즘을 갖추고 있습니다. Akamai의 인텔리전스 데이터베이스에는 매일 평균 1056TB의 공격 데이터가 포함됩니다. Akamai의 웹 트래픽 가시성을 활용해 트래픽이 가장 많고, 가장 빈번하게 공격받는 수천 개의 온라인 비즈니스에 대한 관련성 있는 고품질의 데이터를 확보하면 Akamai의 위협 연구팀이 분석합니다.

- **WAAP 트리거**
  Akamai의 글로벌 WAAP 배포에서 직접 데이터를 수집해 모든 Akamai 보안 고객을 대상으로 하는 실제 공격 이벤트를 포착합니다.

- **CDN 로그**
  WAAP 솔루션을 배포하지 않은 고객을 포함해 모든 Akamai 고객의 이벤트 로그에 대한 오프라인 분석을 통합합니다.

Akamai의 인텔리전스 데이터베이스는 세계에서 가장 큰 데이터 세트 중 하나를 보유하고 있습니다(9PB). 비즈니스와 고객의 보안을 우선시하는 기업을 위해 Akamai의 위협 인텔리전스는 WAAP 솔루션 공급업체를 선도합니다.

위협 리서치 및 인시던트 대응

위협 리서치 및 인시던트 대응 기업은 인간 인텔리전스와 분석을 제공해 WAAP 솔루션의 공격 범위를 보완하고 확대합니다. Akamai는 WAAP 고객을 지원하고 추가적인 보안이 필요할 수 있는 새로운 공격 기법을 탐지하기 위해 다양한 임무를 가진 여러 팀을 고용하고 있습니다.

위협 리서치

Akamai 위협 연구팀은 전체 Akamai 고객 기반에 걸쳐 웹 공격 트렌드에 대한 정기적인 분석을 수행하고, 필요에 따라 개별 고객에 대한 맞춤형 분석도 수행합니다. 또한 핵심 WAF 룰 로직 및 Client Reputation의 생성 및 업데이트를 지원하기 위해 실행 가능한 인텔리전스를 쿼리하는 휴리스틱을 설계하고 구축합니다.

인시던트 대응

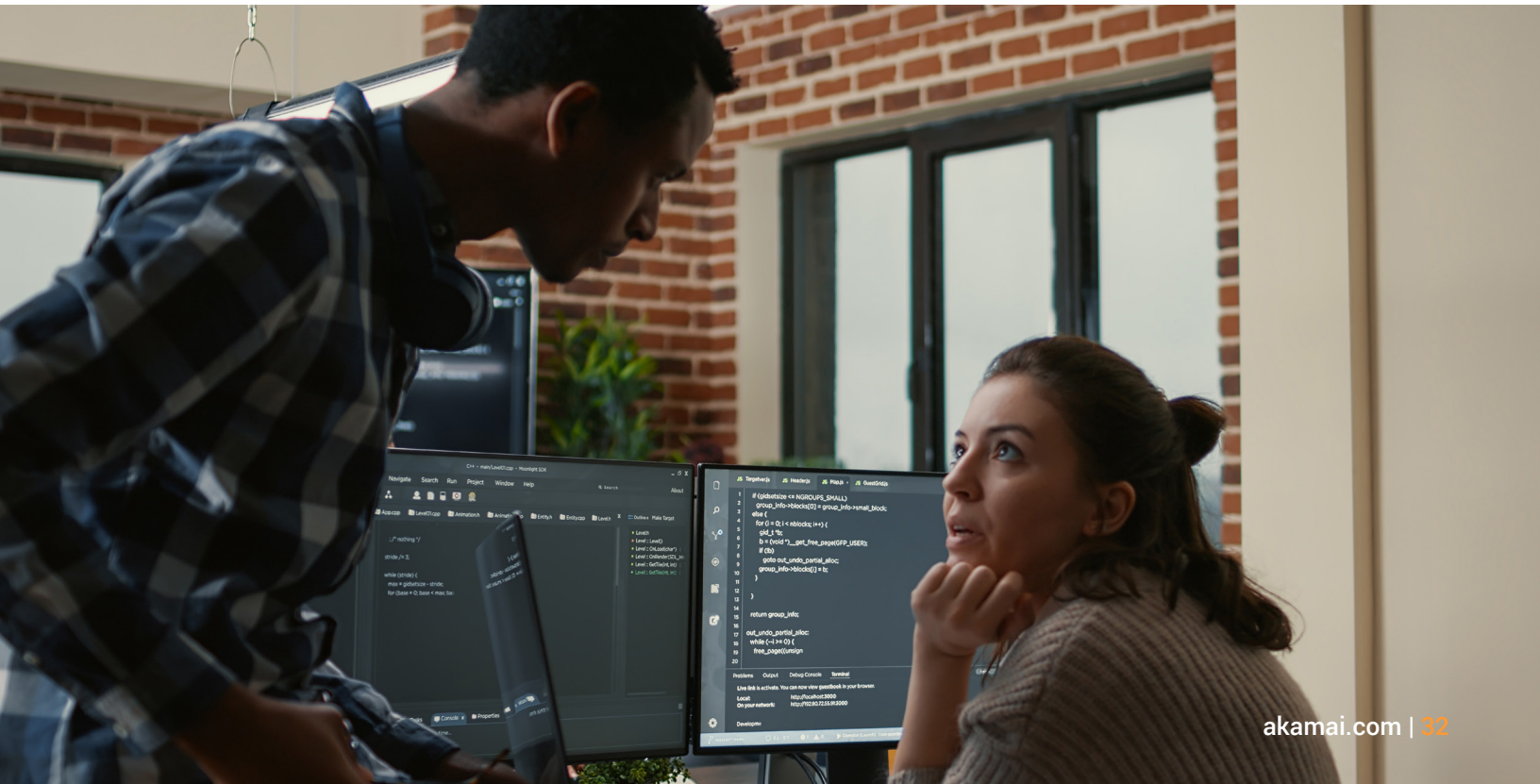
Akamai는 컴퓨터 보안 인시던트 대응팀(CSIRT)과 보안 인텔리전스 대응팀(SIRT)이라는 두 개의 인시던트 대응팀을 운영해 Akamai의 글로벌 보안관제센터(SOC)와 협력하고 개별 고객이 공격을 당했을 때 분석 및 인시던트 대응을 제공합니다. 또한, CSIRT는 자주 공격받는 Akamai 고객을 모니터링해 새로운 공격 기법이나 트렌드의 선행 지표로서 다양한 업계를 대변합니다.

신속한 위협 탐지

Akamai의 새로운 기능 덕분에 새롭게 등장하는 위협과 주요 CVE에 대한 보안 기능을 신속하게 배포할 수 있습니다. 자동 업데이트와 'Akamai가 관리하는' 작업 옵션을 통해 방어 기능을 민첩하게 관리할 수 있습니다.

CVE 보안

Akamai 위협 연구팀은 계속해서 공통 보안 취약점 및 노출(CVE)을 모니터링하고, WAAP 솔루션이 고객 애플리케이션을 보호하고 Akamai CVE 조회 툴을 통해 필요한 확인을 제공하도록 업데이트되도록 합니다. 이 툴은 위협 수준과 Akamai의 현재 보안 기능에 대한 인사이트를 포함해 CVE에 대한 자세한 정보를 제공함으로써 도움이 됩니다. Akamai의 CVE 보안 카탈로그는 가시성을 제공해 Akamai의 보안 기능에 맞춰 보안 작업의 우선순위를 정할 수 있도록 해줍니다. 또한 CVE 데이터베이스를 검색해 취약점에 대한 Akamai의 적극적인 보안 조치를 결정하고 위협 수준을 평가하고 CVE 세부 정보에 접속할 수 있습니다.



전 세계적으로 분산된 엣지 플랫폼

안정성과 회복력

프리미엄 WAAP 솔루션은 대규모 사이버 공격에도 불구하고 고객의 트래픽을 제한하지 않는 광범위하고 강력한 네트워크를 기반으로 구축됩니다. WAAP 공급업체의 글로벌 플랫폼의 검증된 품질, 역량, 실행 능력은 솔루션의 기능과 마찬가지로 중요합니다. WAAP 공급업체가 공격이 활발하게 진행 중인 동안 양질의 트래픽을 제공하지 못하는 경우, 고객은 솔루션에 투자했는지 아니면 툴에만 투자했는지 평가해야 합니다.

Akamai는 고객사에 업계를 선도하는 성능과 보안 기능을 제공하기 위해 최선을 다하고 있습니다. 이 사명은 가장 강력한 기반 위에 서비스를 구축해야만 가능합니다. Akamai Connected Cloud. Akamai는 130개 이상의 국가에 4200개 이상의 엣지 PoP로 구성된 세계에서 가장 분산된 클라우드 플랫폼을 구축했습니다.

Akamai의 고객에는 상위 10대 증권회사 전체, 상위 10대 은행 전체, 상위 10대 비디오 스트리밍 서비스 제공업체 전체, 상위 10대 게임사 전체가 포함됩니다. Akamai의 고객 기반은 대부분의 상위 자동차 회사, 헬스케어 공급업체, 리테일, 통신 사업자부터 상당수의 정부 기관과 군대에 이르기까지 다양합니다.

고객들은 매일 400억 개의 봇, 매일 7억 8000만 건의 애플리케이션 공격, 분기당 1889건의 DDoS 공격으로 인해 네트워크가 다운될 수 있는 상황에서 Akamai의 능력을 믿고 그로부터 보호를 받고 있습니다. Akamai가 성공적으로 보안을 제공할 수 있는 것은 한 고객으로부터 확보한 위협 인텔리전스가 모든 고객에게 혜택을 주고 보안 조치를 적용하기 때문입니다. Akamai의 글로벌 플랫폼 규모는 AI 시대로 진입하는 기업을 보호하는 데 필요한 양과 질 모두를 제공합니다.

글로벌 규모

WAF의 경우, 규모 문제는 초기 및 시간이 지남에 따라 필요한 웹 트래픽의 양을 검사할 수 있는 능력과 그 트래픽을 평가하는 데 필요한 WAF 룰의 수를 중심으로 전개됩니다. 기존의 하드웨어 기반 WAF 솔루션은 어플라이언스 내에서 사용할 수 있는 CPU와 메모리 리소스에 제한을 받기 때문에 확장성이 떨어지는 경우가 많습니다. 또한, 동일한 어플라이언스에서 다른 솔루션과 경쟁해야 할 수도 있습니다.

Akamai의 클라우드 플랫폼에 통합된 WAAP 솔루션을 배포하면 Akamai의 분산된 서버 리소스를 활용해 들어오는 웹 트래픽을 검사함으로써 확장성 문제를 해결할 수 있습니다. 사용자와 공격자는 가장 가까운 Akamai 서버를 통해 보호된 웹사이트에 연결한 다음, 트래픽을 검사해 공격 여부를 확인하고 악성 요청이 탐지되면 차단합니다. 이를 통해 Akamai의 WAAP 솔루션은 웹 애플리케이션 트래픽의 양이 증가할 때(트래픽 급증과 장기적인 증가 모두)뿐 아니라 전 세계의 새로운 사용자 위치에 맞춰 원활하게 확장할 수 있습니다.

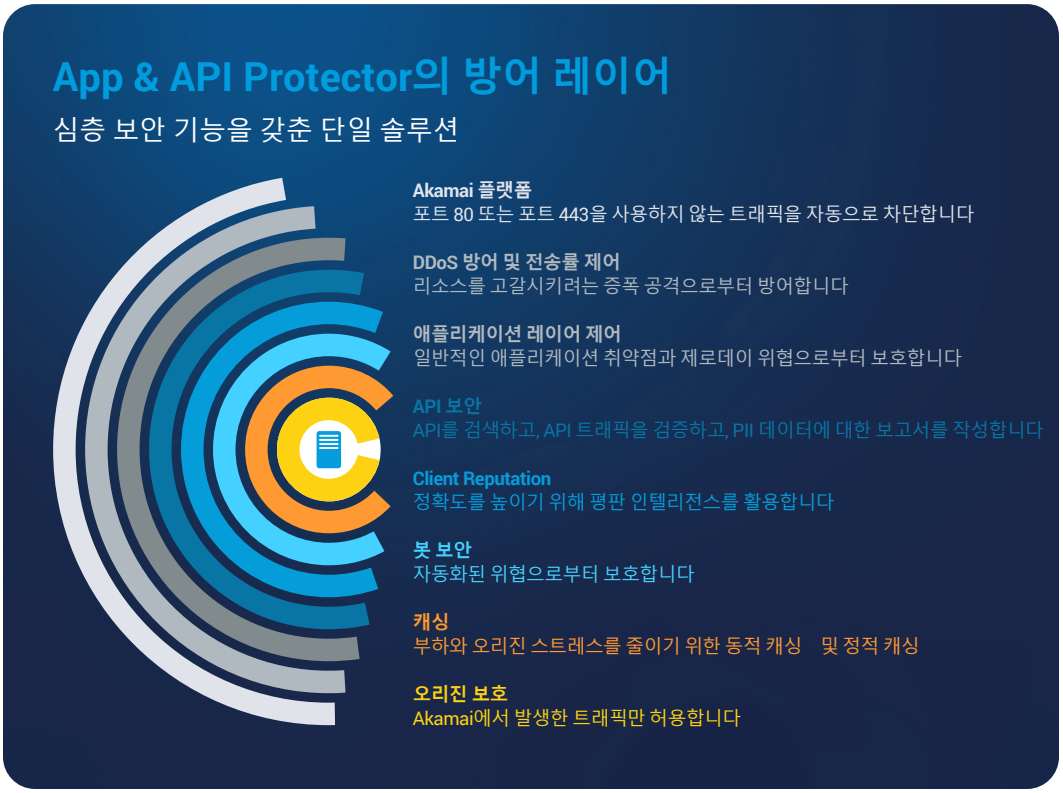
성능

성능 저하는 보안 솔루션, 특히 애플리케이션 앞에 인라인 방식으로 배포된 WAAP 솔루션의 배포를 방해할 수 있습니다. 비즈니스에 중요한 웹사이트의 성능을 저하시키면 생산성 저하, 사용자 경험 저하, 출시 기간 지연, 매출 감소 등의 문제가 발생할 수 있습니다.

Akamai의 클라우드 플랫폼은 전 세계적으로 규모가 크기 때문에 WAAP를 통해 성능 저하 없이 웹 애플리케이션을 보호할 수 있습니다. 전 세계에 분산된 WAAP는 플랫폼에 처음 들어오는 HTTP 트래픽을 검사하고, 플랫폼의 모든 서버에 걸쳐 해당 트래픽을 검사하는 데 필요한 CPU와 메모리 리소스를 분배합니다. 이를 통해 기업 내 제약 조건의 원인이 되고 배포를 방해하는 성능 문제를 제거할 수 있습니다.

엣지 플랫폼의 보안 기능

Akamai의 클라우드 애그노스틱 웹 애플리케이션 보안 솔루션은 플랫폼 전체에서 원활하게 작동해 다양한 애플리케이션 및 API 기반 공격을 방어합니다. 아래 이미지는 위협을 오리진에서 멀리 떨어뜨리는 동시에 정상 사용자의 성능과 접근성을 향상시키는 데 사용되는 Akamai의 계층형 보안 메커니즘과 제어 기능의 풀스택을 보여줍니다.



Akamai App & API Protector에는 다양한 보안 메커니즘과 제어 기능이 자동으로 내장되어 있어 (파란색으로 표시됨) 즉시 포괄적인 방어 기능을 제공할 수 있으며, 다른 Akamai 제품과 서비스가 추가되어 완벽한 레이어 7 보안을 제공합니다

매니지드 공격 지원

Akamai는 지속적인 WAAP 관리 외에도 고객에게 매니지드 공격 지원을 통해 보호 대상 웹사이트에 대한 연중무휴 24시간 모니터링과 탐지된 공격에 대한 매니지드 대응을 제공합니다.

매니지드 공격 지원은 Akamai의 글로벌 SOC 직원을 활용해 보안 인시던트가 발생했을 때 다음과 같은 방법으로 대응합니다.

- WAAP 알림 및 고객 요청에 대응하고 문제에 대한 추가 조사 수행
- 적절한 공격 시그니처를 확인하고 추가 방어 조치 배포
- 고객 애플리케이션 팀과 협력해 배포된 방어 조치의 효과와 정확도를 측정하고, 필요에 따라 방어 조치를 조정
- 인시던트 발생 후 고객 애플리케이션 팀과 함께 전반적인 대응 검토
- 긴급 지원 요청이 게시되도록 인터페이스에 공격 알림 버튼 제공

SOCC(Security Operations Command Center)

Akamai의 SOCC는 10년 이상 전 세계에서 발생한 대규모 공격의 상당수를 방어하는 데 도움을 주어, 끊임없이 진화하는 글로벌 위협 환경으로부터 고객을 보호해 왔습니다.

악성 공격을 모니터링하고 방어하기 위해서는 다음의 4가지 기능이 필요합니다.

- 글로벌 가시성
- 사전 예방적 모니터링 및 알림 경고
- 민첩한 공격 방어
- 숙련된 보안팀의 지속적인 자문 서비스

Akamai SOCC는 세계 최대 규모의 보안 인프라를 운영함으로써 이러한 기능을 제공합니다. 모든 네트워크 트래픽은 실시간으로 인텔리전스를 수집하는 통합 보안 플랫폼을 통해 실행됩니다. 예를 들어, Akamai는 최근 SQL 인젝션 공격의 급격한 증가와 같은 보안 트렌드를 수집했습니다.

이 모든 것이 Akamai 보안팀이 최대한의 효율성과 최소한의 영향으로 고객의 위협을 신속하게 방어하는 데 도움이 됩니다.

결론

네트워크 및 애플리케이션 레이어의 DDoS 공격으로부터 보호하는 것 외에도 새로운 형태의 자동화된 봇과 API 및 클라이언트 측 구성요소를 통한 표적 공격으로 인해 기업은 포괄적인 심층 방어 보안 접근 방식을 통해 모든 웹 애플리케이션, API 엔드포인트, 브라우저, 인프라를 보호해야 합니다. 보안 리더와 실무자들은 다양한 공격 기법을 통해 발생하는 위협을 신속하게 탐지하고 방어할 수 있는 웹 애플리케이션 보안이 필요하며, 최상의 보안 방어를 위해 방화벽을 넘어 인접한 보안 기술로 기존의 보안 기능을 확장해야 합니다.

WAAP에 대한 Akamai의 접근 방식은 최신 보안 체계를 유지하는 데 필요한 모든 보안 기술을 제공하기 때문에 기술의 폭과 효율성 면에서 타의 추종을 불허하는 솔루션 세트를 제공하는 것입니다. Akamai는 최고의 보안 솔루션이 세계에서 가장 크거나 가장 인기 있는 브랜드만을 위한 것이 되어서는 안 된다고 생각합니다. 애플리케이션 및 API 보안을 위한 Akamai의 포트폴리오는 계층화된 포트폴리오를 통해 보안이 최우선인 모든 기업에 효과적인 웹 애플리케이션 보안을 제공합니다.

지속적으로 발전하고 적응하는 보안 솔루션을 통해 심층적이고 광범위한 공격 인텔리전스를 활용하는 Akamai는 글로벌 기업들과 협력해 보안 성과를 최신화하고 지속적으로 개선합니다. Akamai는 기업의 보안팀이 내부 이니셔티브를 추진하는 동시에 기업 시스템에 침입자를 차단할 수 있도록 보안팀에 인텔리전스, 가시성, 자동화, 가이드를 제공해 역량을 강화할 수 있도록 지원합니다. 이것이 바로 온라인 라이프를 지원하는 가장 까다로운 브랜드들이 Akamai에게 보안을 맡기는 이유입니다.

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com, akamai.com/blog를 확인하거나 X, LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2025년 2월 발행.