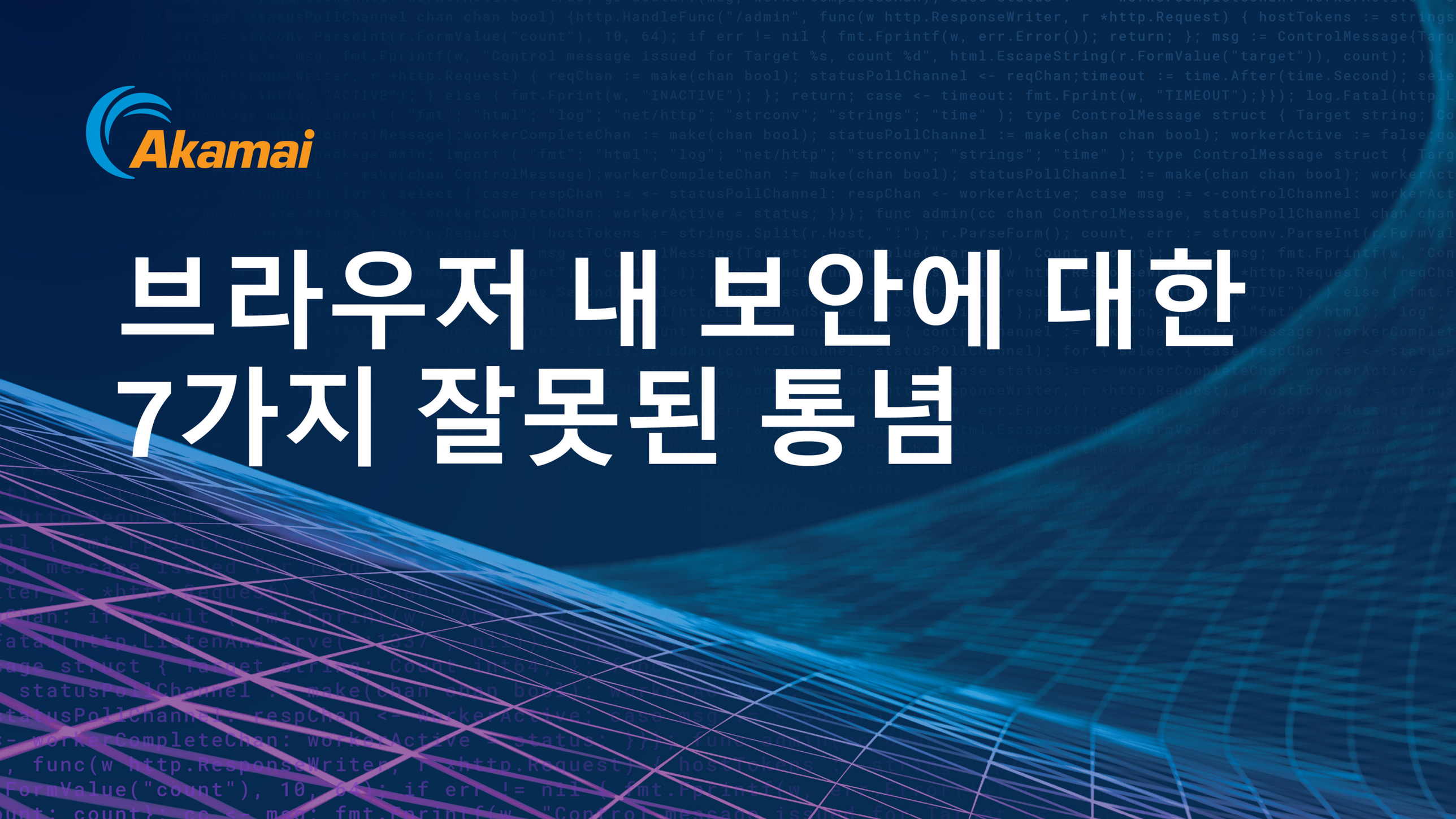

Akamai
브라우저 내 보안에 대한
7가지 잘못된 통념

인터넷상에서 다양하고 복잡한 사이버 공격에 웹 기반 애플리케이션과 자산이 노출되는 건 잘 알려진 사실입니다. 기업은 서버 측 공격으로부터 미션 크리티컬 애플리케이션을 보호하는 데 상당한 중점을 두고 있지만, 브라우저 내에서 또는 웹페이지 내에서 클라이언트 측 위협이 초래할 수 있는 피해를 과소평가하고 있는 기업이 많습니다. 이러한 사각 지대로 인해 웹사이트는 사기, 민감한 데이터 유출, 고객 신뢰도 저하로 이어질 수 있는 위험한 클라이언트 측 취약점에 노출됩니다.

브라우저 내 보호에 대한 몇 가지 일반적인 오해를 분석해 실제로 문제가 되는 위태로운 사항을 명확하게 살펴보겠습니다.

잘못된 통념 1

CSP(콘텐츠 보안 정책)는 가장 효과적인 클라이언트 측 방어다

콘텐츠 보안 정책은 웹사이트 운영자가 브라우저 내에서 실행할 수 있는 자산(스크립트 포함)의 종류를 세부적으로 제어할 수 있는 보안 표준입니다. 콘텐츠 보안 정책 응답 헤더는 실행 가능한 코드의 정상적이고 안전한 출처로 간주되는 승인된 도메인 목록을 유지 관리하는 데 사용됩니다. 이는 자바스크립트 위협을 차단하는 방어의 중요한 요소일 수 있지만, 유지 관리에 수많은 리소스가 사용됩니다. 그리고 대부분의 클라이언트 측 공격은 신뢰할 수 있는 소스를 활용하는 과정에서 발생합니다. 따라서 신뢰할 수 있는 스크립트라 하더라도, 사이트에서 실행 중인 모든 스크립트의 행동을 파악하는 것이 중요합니다. Akamai Page Integrity Manager는 행동 기술을 활용해 웹페이지의 모든 스크립트 실행 행동을 모니터링함으로써 스크립트의 동작 및 다른 스크립트와의 관계에 대한 인텔리전스를 수집합니다. 그런 다음 이 데이터를 휴리스틱, 리스크 평가, 인공 지능 등을 비롯한 멀티레이어 탐지 접근 방식과 함께 사용해 의심스러운 활동을 즉시 탐지합니다.

오늘날 웹사이트 중

94%는

하나 이상의 써드파티 스크립트를 사용하고 있습니다

출처: Third Parties, 2021년 11월

잘못된 통념 2

WAF는 웹 스키밍 공격으로부터 기업을 보호한다

WAF(Web Application Firewall)는 트래픽을 모니터링 및 필터링하고, 웹 애플리케이션으로 들어오는 악성 트래픽 또는 앱에서 나가는 무단 데이터를 차단해 일반적인 공격으로부터 웹 애플리케이션을 보호하는 보안 솔루션입니다. WAF는 서버와 최종 사용자 간의 연결을 보호하는 데 중점을 두지만, 브라우저 수준에서 웹 애플리케이션을 보호하도록 설계되지는 않았습니다. 웹 스키밍 공격은 악성 코드 실행을 통해 최종 사용자의 브라우저 내에서 일어나므로, WAF는 이를 탐지하거나 방어할 수 없습니다.

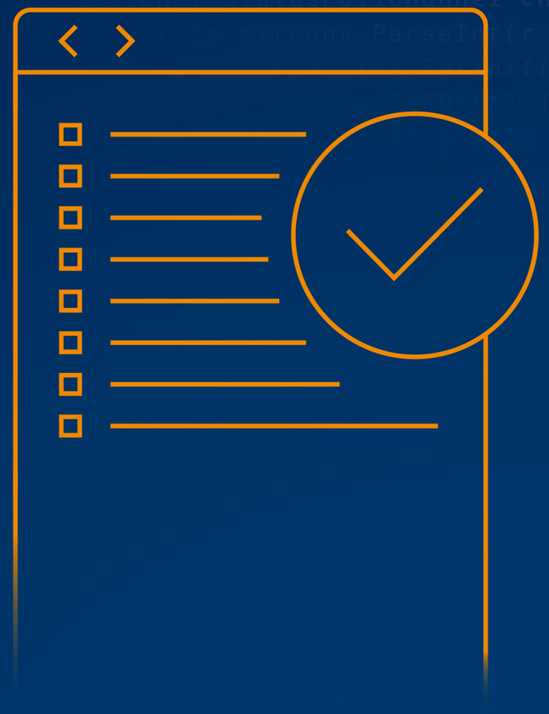
잘못된 통념 3

요새 Magecart 공격은 예전만큼 자주 발생하지 않는다

Magecart 공격은 그 어느 때보다도 활발히 성행 중이지만, 탐지하기가 더 어려워지고 있습니다. 최근 Akamai 위협 연구팀은 Google Tag Manager 같은 유명한 써드파티 벤더사를 가장하거나, Base64 인코딩을 사용해 악성 코드를 위장하는 등의 정교한 기술을 사용해 여러 이커머스 사이트를 표적으로 하는 글로벌 Magecart 캠페인을 적발했습니다. 이 캠페인은 공격자가 보안 조치를 우회하고, 웹 스키밍 공격을 실행하는 방법을 한층 더 교묘하게 터득해 끝까지 발각되지 않고 숨어 있으려 하는 술래잡기 같은 공격 수법입니다. Akamai Page Integrity Manager는 다른 스크립트와 상호 작용하는 방식을 포함해 스크립트의 모든 행동을 모니터링함으로써 의심스러운 활동을 밝혀내고, 최신 공격도 신속하게 방어합니다. 자세한 내용은 최신 블로그 게시물에서 확인하시기 바랍니다.

잘못된 통념 4

PCI DSS v4.0에 대한 새로운 스크립트 요구사항을 준수할 때까지 기다려도 된다



2018년에 PCI DSS의 이전 버전인 v3.2.1이 릴리스된 이래로 발생한 결제 카드 데이터에 대한 위협 증가 및 중대한 시장 변화에 대응하기 위해 2022년 3월에 PCI DSS의 최신 버전(v4.0)이 출시되었습니다. 새로운 요구사항 6.4.3 및 11.6이 적용됨에 따라, 결제 카드를 온라인으로 처리하는 기업은 이제 사이트에서 어떤 스크립트가 실행되는지, 해당 스크립트가 언제 변경되는지, 각 스크립트가 언제 실행 중단되는지 알아야 브라우저 내 스크립트 공격을 방어할 수 있습니다. PCI DSS v4.0은 2025년까지 발효되지 않지만, 민감한 결제 카드 데이터가 웹사이트의 결제 페이지에서 스키밍되고 유출되지 않도록 보호하려면 더 이상 미룰 시간이 없습니다. Akamai Page Integrity Manager는 PCI 컴플라이언스의 가속을 지원합니다.

잘못된 통념 5

고객 탈취는 온라인 리테일 기업의 중대한 도전 과제가 아니다

고객 탈취란 클라이언트 측에 설치된 브라우저 확장 프로그램 또는 플러그인으로 인해 발생하는 원치 않는 악성 브라우저 활동을 설명하는 데 사용되는 용어입니다. 이러한 원치 않는 활동에는 제휴사 사기, 경쟁 사이트 또는 악성 사이트로의 무단 리디렉션, 의도하지 않은 할인, 방문자가 구매를 완료하지 못하게 막는 방해 광고 주입 등이 포함될 수 있습니다. 기업은 자사 웹사이트의 총 사이트 방문자 중 15%~24%가 고객 탈취 기법으로 인해 작업이 중단되는 피해를 받고 있는 것으로 추정합니다.

이는 어떤 결과를 초래할 수 있을까요? 구매 전환율 감소, 브랜드 충성도 하락, 수백만 달러의 잠재적 매출 손실로 이어집니다. Akamai Audience Hijacking Protector를 통해 사용자는 일반적인 브라우저 확장 프로그램이 사이트 세션에 어떤 영향을 미치는지, 그리고 확장 프로그램 운영자가 악의적인 활동을 어떻게 전개할지 파악할 수 있습니다. 이 솔루션은 개별 확장 프로그램 수준에서 활동을 차단하거나 허용하는 세분화된 정책 설정을 사용함으로써, 사이트와의 상호 작용을 허용할 확장 프로그램의 종류를 결정할 수 있습니다.

기업은 자사 웹사이트의 총 사이트 방문자 중

15%~24%가

고객 탈취 기법으로 인해 작업이 중단되는 피해를 받고 있는 것으로 추정합니다

출처: 온라인 리테일 기업의 고객 탈취에 대한 인식, Retail Dive, 2023년 2월

잘못된 통념 6

디지털 경험 플랫폼은 브라우저 내 활동 및 브라우저 확장 프로그램의 영향에 대한 가시성을 제공할 수 있다

디지털 경험 플랫폼은 콘텐츠 기반 경험을 최적화하고 제공하기 위해 함께 작동하는 기술입니다. 이러한 플랫폼을 통해 제공되는 최신 애널리틱스는 사이트 세션의 기업 측에서 일어나는 사항에 대한 인사이트만 전달하며, 최종 사용자와 관련된 인사이트는 제공하지 않습니다. 이는 기업이 사이트 방문자가 기업 사이트와 상호 작용하는 방식과 행동은 추적할 수 있지만, 브라우저가 최종 사용자와 상호 작용하는 방식은 볼 수가 없다는 걸 뜻합니다. 브라우저 확장 프로그램과 원치 않는 브라우저 활동이 기업의 사이트 세션에 어떤 영향을 미치는지 파악하면 전체 고객 여정을 포괄적으로 파악할 수 있고, 쇼핑 이탈률의 원인을 더 정확히 규명할 수 있습니다.

잘못된 통념 7

쿠폰 및 가격 비교 확장 프로그램은 비즈니스에 악영향을 미치지 않는다

이 문제는 해결하기 까다로운 일이란 걸 충분히 이해합니다. 괜찮은 가격에 좋은 물건을 구입할 기회를 마다하는 사람은 없으며 Honey, Rakuten, Amazon Assistant 같은 확장 프로그램은 온라인 리테일 기업의 전환율을 높이는 데에도 도움이 됩니다. 그러나 이러한 확장 프로그램은 안 좋은 이면을 지닐 수 있습니다. 예를 들어, 어떤 쿠폰 확장 프로그램은 의도한 고객이 아닌 고객의 결제 페이지에 특별 할인 코드를 자동으로 삽입해 대량 할인을 발생시킵니다. 또는 Amazon Assistant는 경쟁사에서 더 낮은 가격으로 우리 회사의 상품 또는 서비스를 제공하는 광고를 우리 회사 사이트에 자동으로 삽입합니다. 이러한 확장 프로그램은 상당한 잠재적 매출 손실로 이어질 수 있고, 가장 충성도 높은 고객을 잃을 수 있습니다. Akamai Audience Hijacking Protector는 전 세계에서 가장 널리 사용되는 다양한 브라우저 확장 프로그램을 지원하며, Akamai의 고급 대시보드는 개별 확장 프로그램 수준에서 인사이트를 제공합니다. 따라서 사용자는 비즈니스에 실제로 도움이 되는 확장 프로그램과 허용할 가치가 없는 확장 프로그램을 분석할 수 있습니다.

Akamai 고객사의 글로벌 사이트 트래픽 전체를 보았을 때, 블랙 프라이데이와 사이버 먼데이 사이에 쿠폰 및 가격 비교 확장 프로그램의 영향을 받은 사이트 세션 수는

25%

증가했습니다

출처: Akamai 위협 연구팀, 2022

Akamai의 서비스

클라이언트 측 공격의 영향을 받을 리스크는 명백히 가속하고 있으며, 이러한 리스크를 줄이기 위해서는 브라우저 내 행동과 원치 않는 활동에 대한 가시성을 확보하는 것이 매우 중요합니다. Akamai의 Page Integrity Manager는 취약한 리소스를 식별하고, 의심스러운 행동을 탐지하고, 악성 활동을 차단함으로써 웹 스키밍, 폼재킹, Magecart 공격과 같은 자바스크립트 위협으로부터 웹사이트를 보호합니다. 그리고 원치 않는 브라우저 내 행동을 차단하기 위해 Audience Hijacking Protector는 상세 분석과 방어 옵션을 통해 디지털 커머스 사이트에서 발생하는 브라우저 활동에 대해 실시간 가시성을 제공합니다

Akamai의 애플리케이션및 API 방어와 브라우저 내 보호 솔루션이 어떤 방식으로 클라이언트 측 보안 체계를 개선할 수 있는지 알아보세요.