AKAMAI 제품 설명서

Client-Side Protection & Compliance

클라이언트측 자바스크립트 취약점으로부터 보호하고 컴플라이언스 간소화

자바스크립트는 최신 웹 애플리케이션에 필수적인 툴입니다. 퍼스트파티 및 써드파티 자바스크립트의 사용은 사용자 경험 최적화부터 기능 및 성능 향상에 이르기까지 시간이 지남에 따라 기하급수적으로 증가했습니다. 자바스크립트 사용에는 여러 가지 이점이 있지만, 자바스크립트의 디지털 공급망은 악성 코드 삽입을 통해 브라우저 내에서 결제 카드 데이터 등 최종 사용자의 민감한 정보를 탈취하려는 클라이언트 측 공격에 웹 사이트를 취약하게 만들 수도 있습니다.

이러한 공격은 서버측 가시성이 부족하고 기존의 보안 조치를 우회하기 때문에 기업이 쉽게 피해를 입을 수 있으며, 결과적으로 고객 신뢰도 하락, 막대한 규제 벌금, 컴플라이언스 처벌, 브랜드 평판 하락 등의 피해를 입게 됩니다.

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance는 최종 사용자 데이터 유출을 방지하고 웹 사이트를 자바스크립트의 위협으로부터 보호합니다. 악성 스크립트 동작을 탐지하고 보안 팀이 유해한 활동을 실시간으로 방어할 수 있게 실행 가능한 알림을 제공하도록 설계되었습니다.

특별히 설계된 PCI DSS v4.0 컴플라이언스 기능을 갖춘 Client-Side Protection & Compliance는 기업이 새로운 스크립트 보안 요구 사항을 충족하고 클라이언트측 공격으로부터 결제 카드 데이터를 보호할 수 있도록 지원합니다. 결제 페이지의 스크립트 인벤토리를 손쉽게 관리하고, 단일 종합 대시보드를 통해 감사 프로세스를 간소화하고, 전용 PCI 알림을 수신해 컴플라이언스 관련 이벤트에 신속하게 대응할 수 있습니다.

핵심 기능

클라이언트 측에서 민감한 데이터 유출 방지

사이버 범죄자들은 최종 사용자의 민감한 정보를 노리고 있습니다. 악성 공격자는 자바스크립트 공급망의 취약점을 악용해 웹 사이트에 코드를 삽입하고, 민감한 정보를 훔쳐 부정 사용을 위해 유출할 수 있습니다. Client-Side Protection & Compliance는 머신 러닝과 휴리스틱 스코어링을 결합해 스크립트 동작을 실시간으로 분석하고 악성 활동과 취약한 리소스를 탐지합니다. 보안 팀에 즉각적으로 실행 가능한 알림을 제공해 웹 스키밍, Magecart, 폼재킹 등 클라이언트 측 공격을 신속하게 방어할 수 있습니다.

기업이 누릴 수 있는 혜택

탐지 및 보호
실제 사용자 세션에서 스크립트 동작을 모니터링해 의심스러운 활동을 탐지합니다

PCI DSS v4.0 워크플로우
자바스크립트 보안 요구 사항 6.4.3 및 11.6.1 충족을 지원합니다

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

클라이언트측 가시성
클라이언트 측 공격표면에 대한 광범위한 가시성을 확보합니다

정책 관리
스크립트 동작을 관리하고 런타임 자바스크립트의 실행을 통제합니다

취약점 탐지
Akamai 위협 인텔리전스를 기반으로 CVE(Common Vulnerability and Exposure)를 식별합니다

유연한 배포 옵션
Akamai Connected Cloud를 통하거나 오리진 서버에 직접 간편하게 배포할 수 있습니다

Akamai

전용 PCI DSS v4.0 컴플라이언스 지원

PCI DSS v4.0 스크립트 보안 요구 사항 6.4.3 및 11.6.1에 따라 기업이 클라이언트 측 공격으로부터 결제 카드 데이터를 보호하고 결제 페이지에서 스크립트 관리를 보장해야 할 필요성이 높아졌습니다. Client-Side Protection & Compliance는 결제 페이지의 모든 스크립트를 추적하고 인벤토리를 생성해 스크립트의 무결성과 권한을 보장합니다. 사전 정의된 정당성과 자동화된 룰을 제공해 로드된 모든 스크립트를 쉽게 정당화할 수 있습니다. 또한 HTTP 헤더의 변경 사항과 결제 페이지 보호 기능을 모니터링해 페이지 변조를 방어합니다. 기업은 포괄적인 대시보드와 전용 PCI 알림을 통해 컴플라이언스 관련 이벤트에 신속하게 대응하고 브라우저 내에서 결제 카드 데이터를 보호할 수 있습니다. 보안 및 컴플라이언스 팀은 이러한 기능을 통해 PCI 감사 프로세스의 부담을 줄이고 워크플로우를 빠르게 간소화할 수 있습니다.

자바스크립트의 위협에 대한 광범위한 가시성

웹 애플리케이션 방화벽과 같은 기존의 웹 애플리케이션 보안 솔루션은 서버 측 트래픽만 모니터링하고 클라이언트 측에서 실행되는 활동에 대한 가시성은 제공하지 못합니다. 이러한 위협으로부터 보호하기 위한 콘텐츠 보안 정책 등의 표준 기반 접근 방식은 관리가 어렵고, 웹 페이지 운영자가 통제할 수 없는 스크립트 공급망 내에서 유입되는 악성 페이로드에 대해 제한적인 보호 기능만 제공합니다. 이로 인해 기업에 사각지대가 발생해 민감한 데이터를 훔치는 유해 코드가 며칠, 몇 주 또는 몇 달 동안 탐지되지 않을 수 있습니다. Client-Side Protection & Compliance는 각 스크립트의 동작, 취약점, 도달 범위, 영향은 물론 접속된 데이터나 제기된 위협을 포함해 웹 사이트의 클라이언트측 공격표면에 대한 탁월한 가시성을 제공합니다.

작동 방식

Client-Side Protection & Compliance는 최종 사용자의 브라우저에서 실행되어 보호된 웹 페이지에서 클라이언트측 스크립트 실행을 모니터링합니다. 스크립트에서 행동의 변화가 나타나면 머신 러닝 기술을 사용해 무단 또는 부적절한 행동의 리스크를 평가합니다. 잠재적 위협을 즉시 조사하고 방어할 수 있도록 리스크가 높은 이벤트를 보안 팀에 알립니다.

설정 성능에 의미 있는 영향을 주지 않는 간단한 스크립트가 모니터링되는 각 페이지에 삽입됩니다.

모니터링 및 평가 사용자의 웹 브라우저에서 자바스크립트 활동 데이터를 수집하고 모니터링합니다. 머신 러닝 기법을 사용해 무단 작업이나 부적절한 작업이 발견될 경우 리스크를 평가합니다.

알림 활성 위협이나 공격이 발견되면 위협을 방어하기 위한 자세한 정보가 포함된 실시간 알림이 전송됩니다.

방어 클릭 한 번으로 악성 자바스크립트가 보호된 페이지의 민감한 데이터에 접속하고 유출하지 못하도록 즉시 제한합니다.

PCI DSS v4.0 스크립트 보안 컴플라이언스 가속

스크립트 무결성 및 권한(6.4.3)

보호된 결제 페이지에 로드된 모든 스크립트의 무결성 및 권한을 보장합니다.

스크립트 인벤토리 및 정당화(6.4.3)

보호된 결제 페이지에 로드된 스크립트를 추적하고 인벤토리를 관리합니다. 사전 정의된 정당화 및 자동화된 룰을 활용해 모든 스크립트를 신속하게 정당화합니다.

결제 페이지 보호(11.6.1)

보호된 결제 페이지에서 무단 변경을 즉시 탐지하고 대응할 수 있습니다.

직관적인 대시보드

스크립트 보안 요구 사항 6.4.3 및 11.6.1에 대한 관련 작업과 알림에 대한 자세한 정보가 포함된 전용 대시보드를 통해 PCI DSS v4.0 컴플라이언스 및 감사 프로세스를 간소화합니다.

실행 가능한 PCI 알림

무단 스크립트, 결제 데이터 유출, 결제 페이지 변조 등 PCI 컴플라이언스 관련 이벤트에 대한 자세한 알림을 수신하고 기록합니다.

자세한 내용은 제품 페이지를 방문하거나 Akamai 영업 담당자에게 문의하시기 바랍니다.