

Akamai Client-Side Protection & Compliance의 PCI DSS v4.0 자바스크립트 보안 체크리스트

PCI DSS(Payment Card Industry Data Security Standard)는 결제 카드 데이터의 온라인 보안과 전 세계적으로 일관성 있는 데이터 보안 조치의 광범위한 채택을 촉진하기 위해 개발된 글로벌 보안 표준입니다. 가장 중요한 보안 표준 중 하나이며, 결제 카드 데이터를 온라인으로 처리하는 기업은 해당 표준을 준수해야 합니다.

최신 버전의 PCI DSS(영어로만 제공), 버전 4.0은 2025년에 발효됩니다. 여기에는 새롭게 진화하는 사이버 보안 위협을 해결하기 위한 지침으로 업데이트된 12개의 핵심 데이터 보안 요구사항이 포함되어 있습니다. PCI DSS v4.0, 6.4.3 및 11.6.1에 추가된 2개의 주요한 요구사항은 브라우저 내에서 민감한 최종 사용자 정보를 훔치는 클라이언트 측 웹 스키밍 공격에 대한 자바스크립트 보안과 방어와 관련되었습니다. 이 공격은 최근 몇 년간 계속 증가하고 있으며, 정교한 기술로 인해 점점 더 탐지하기 어려워지고 있습니다. 이 공격의 피해자가 된 기업은 과중한 벌금, 브랜드 평판 훼손, 수익 손실, 고객 신뢰 저하와 같은 상당한 피해를 입을 수 있습니다.

새로운 PCI DSS v4.0 스크립트 보안 요구사항 내용과 Client-Side Protection & Compliance가 필요한 이유에 대한 체크리스트를 확인하시기 바랍니다.

PCI DSS v4.0 요구사항	Client-Side Protection & Compliance의 유용한 기능
<p>요구사항 6.4.3 - 공격에 대한 일반 웹 애플리케이션 보호</p> <ul style="list-style-type: none">✓ 브라우저에 로드되어 실행되는 각 스크립트의 인가 여부를 확인하기 위한 방법 구현✓ 브라우저에 로드되어 실행되는 각 스크립트의 무결성을 보장하기 위한 방법 구현✓ 브라우저에 로드되어 실행되는 스크립트별 필요성에 대한 서면 근거를 통해 모든 스크립트의 인벤토리 유지	<p>클릭 한 번으로 권한 관리</p> <ul style="list-style-type: none">✓ 웹사이트 결제 페이지에서 실행하도록 허용된 스크립트를 통해서 직접 간편하게 관리 <p>선제적 무결성 보장</p> <ul style="list-style-type: none">✓ 행동 기반 기술을 통해 악성 활동 또는 데이터 탈취를 탐지하고 알리를 제공하도록 브라우저에서 실행되는 모든 스크립트 분석 <p>모든 스크립트의 자동 추적 및 인벤토리 유지</p> <ul style="list-style-type: none">✓ 미리 정의된 정당화 및 자동화된 룰을 통해 브라우저에 로드되어 실행되는 각 스크립트의 용도를 간편하게 정당화

요구사항 11.6.1 - 결제 페이지의 무단 변경 탐지 및 대응

다음과 같이 변경 및 변조 탐지 메커니즘이 배포됩니다.

- ✓ 소비자 브라우저에서 수신할 때 결제 페이지의 콘텐츠와 HTTP 헤더의 무단 수정(감염, 변경, 추가 및 삭제 징후) 알림 제공
- ✓ 수신된 HTTP 헤더 및 결제 페이지를 평가하기 위한 메커니즘 구성

메커니즘 기능은 최소 7일마다 또는 주기적으로 수행(요구사항 12.3.1에 명시된 모든 요소에 따라, 법인에서 목표로 하는 리스크 분석에 정의된 빈도)

결제 페이지 보호

- ✓ 최종 사용자의 소중한 데이터를 안전하게 보호하기 위해 결제 페이지에 대한 악성 변조 모니터링, 분석, 방어

즉각적인 유용한 알림을 통해 실시간 무단 수정 조사

- ✓ 즉각적인 탐지를 통해 보안 팀은 결제 페이지의 HTTP 헤더에 대한 무단 변경 또는 수정에 빠르게 대응

상시가동형 방어로 보안

- ✓ 상시 보호 체계로 결제 페이지에서 사용자 상호작용 보호

Akamai Client-Side Protection & Compliance는 자바스크립트 위협을 방어하고 브라우저에서 민감한 데이터를 보호하기 위해 클라이언트 측 공격에 대한 가시성을 제공합니다. 특별히 설계된 PCI DSS v4.0 기능은 보안 및 컴플라이언스 팀이 PCI DSS v4.0 감사 프로세스를 간소화하고 스크립트 보안 요구사항 6.4.3 및 11.6.1을 이행하는데 유용한 전용 워크플로우를 제공할 수 있게 지원합니다.

Akamai Client-Side Protection & Compliance는 유연한 배포 옵션을 제공하므로, Akamai Connected Cloud를 활성화하지 않아도 됩니다.

이 유용한 기능이 PCI DSS v4.0 준수 기업을 어떻게 지원하는지 [자세히 알아보세요.](#)