imperva

THALES
Building a future we can all trust
CYBERSECURITY

PCI DSS 4.0 준수를 위한 클라이언트 측 보호

솔루션 개요

PCI DSS 4.0 준수를 위한 클라이언트 측 보호

오늘날의 웹사이트는 기능 향상 및 결제 처리를 위해 타사 스크립트에 크게 의존하고 있으며, 이는 의도치 않게 신뢰할 수 없거나 모니터링되지 않는 코드를 노출시켜 공격 표면을 확대합니다.

스크립트가 손상되면 공격자는 고객의 브라우저에서 직접 민감한 데이터를 은밀히 탈취할 수 있으며, 이는 수개월간 탐지되지 않는 경우가 많습니다. 이러한 침해는 고객 신뢰를 위협하고 PCI DSS 준수를 저해합니다. PCI DSS는 이제 증가하는 위협에 대응하기 위해 요구사항 6.4.3 및 11.6.1을 통해 클라이언트 사이드 보안에 대한 더욱 엄격한 요구사항을 시행하고 있습니다.

요구 사항 6.4.3은 결제 페이지에서 실행되는 모든 스크립트를목록화하고 승인하며 정당성을 입증하고, 무결성을 보장하는 프로세스를 요구합니다.

요구 사항 11.6.1은 데이터 유출을 방지하기 위해 보안에 영향을 미치는 HTTP 헤더 및 스크립트의 무단 변경을 탐지하고 경고하도록 규정합니다.

PCI DSS 6.4.3 및 11.6.1 준수 간소화

최종 사용자 데이터 유출로부터 결제 페이지를 보호하고 PCI DSS 요구사항 6.4.3 및 11.6.1 준수를 간소화하십시오. 클릭 한 번으로 Client-Side Protection은 모든 스크립트 활동에 대한 완전한 가시성을 제공하고, 스크립트 검색을 자동화하며 무결성을 보장하는 동시에 보안에 영향을 미치는 HTTP 헤더를 지속적으로 모니터링하여 승인되지 않거나 위험한 동작을 손쉽게 차단할 수 있습니다.

Client-Side Protection은 Imperva 애플리케이션 보안 플랫폼의 일부입니다. 클라우드, 온프레미스 또는 하이브리드 구성 등 애플리케이션이 위치한 곳 어디서나 심층 방어를 제공하는 베스트 솔루션을 결합합니다.

주요 장점

포괄적인 스크립트 인벤토리
결제 페이지의 모든 스크립트를 자동으로 식별하고 전체 목록을 유지하여, PCI DSS 6.4.3의 스크립트 승인 및 무결성 검사 요구사항을 완벽하게 충족합니다.

AI 기반 스크립트 분석기
AI를 활용하여 스크립트의 출처, 동작, 위험도에 대한 즉각적이고 상세한 인사이트를 확보함으로써, 보안팀의 신속한 스크립트 평가 및 승인을 지원합니다.

실시간 경보 및 차단
승인되지 않은 스크립트 동작과 보안에 영향을 미치는 HTTP 헤더 변경 을 지속적으로 모니터링하여, PCI DSS 11.6.1 하의 준수 위반을 사전에 방지합니다.

통합 준수 대시보드
맞춤형 실행 계획과 함께 준수 현황을 실시간으로 제공하여, 기업이 PCI 심사를 간소화하고 표준을 손쉽게 유지할 수 있도록 지원합니다.

포괄적인 스크립트 관리 (PCI DSS 6.4.3)

결제 페이지의 모든 클라이언트 사이드 스크립트를 실시간으로 자동 탐지 및 목록화하고 무결성을 보증하여 PCI DSS 6.4.3 준수를 지원합니다. 기존 스크립트와 새로 추가된 스크립트를 실시간으로 지속 모니터링하며, 새 버전을 탐지하여 알리고 변경 사항을 강조 표시하여 손쉬운 검토가 가능합니다. 스크립트를 승인하고 사용 목적을 명확히 할 수 있는 정밀한 도구를 제공하여, 보안 팀이 신뢰할 수 있는 스크립트만 승인하는 동시에 승인되지 않거나 악성 코드를 차단할 수 있습니다.

변조 탐지, 경보 및 모니터링 (PCI DSS 11.6.1)

HTTP 헤더 및 클라이언트 사이드 요소의 무단 변경을 자동으로 탐지합니다. 브라우저 레벨에서 강제 적용되는 CSP(Content-Security-Policy) 헤더를 활용하여, PCI DSS 요구사항에서 규정한 주간 단위 검사를 넘어 실시간 지속 모니터링을 제공합니다. 이메일, SIEM 또는 API를 통해 실시간 이상 징후 경보를 수신하여, 보안 팀에 실행 가능한 인사이트를 제공하고 잠재적 악의적 활동에 대한 신속한 대응을 지원합니다.

PCI DSS 심사 준비 대시보드

PCI 컴플라이언스 대시보드는 PCI DSS 요구사항 충족을 위한 단계별 가이드를 제공하여, 심사 준비에 필요한 명확한 방향성을 제시합니다. 요구사항 6.4.3 및 11.6.1이 대시보드에 완전히 통합되어 있어, 온보딩된 각 결제 경로별로 맞춤화된 실행 단계를 확인할 수 있습니다. 진행 상황 추적, 완료 작업 표시, 체계적인 준수 현황 관리가 가능하며, 불확실성을 제거하여 심사 부담을 줄이고 완벽한 심사 준비 환경을 보장합니다.

다운로드 가능한 리포트를 통해 심사 프로세스를 간소화할 수 있습니다. 필요한 모든 데이터를 단일 문서로 통합하여 심사자에게 명확하고 검증 가능한 증적을 제공합니다.

안전한 원클릭 배포

Imperva 클라우드 애플리케이션 보안 솔루션의 일부인 Client-Side Protection은 안전하고 간편하며 신속하게 배포됩니다. 공격 표면을 확대하고 클라이언트 측 실행에 의존하는 JavaScript 배포 방식과 달리, CSP 헤더는 서버에서 정의하고 브라우저에서 강제 실행하는 보안 메커니즘으로 승인되지 않은 스크립트를 사전 차단하면서 성능을 향상시키고 위험을 최소화합니다.

온보딩 완료 후 몇 분 내에 탐지가 시작되며, 추가 지연 없이 향상된 클라이언트 사이드 보안의 모든 이점을 활용할 수 있습니다. 더욱 중요한 점은 코드 변경이 불필요하여 웹사이트 운영에 전혀 영향을 주지 않는다는 것입니다.

Thales 소개

Thales는 글로벌 사이버보안 분야 선도 기업으로, 전 세계에서 가장 신뢰받는 기업과 조직들이 중요 애플리케이션, 민감 데이터, 신원 정보를 어디서나 대규모로 보호할 수 있도록 지원합니다. 혁신적인 서비스와 통합 플랫폼을 통해 고객사의 위험 가시성을 높이고, 사이버 위협을 방어하며, 컴플라이언스 격차를 해소하고, 매일 수십억 명의 소비자에게 신뢰할 수 있는 디지털 경험을 제공합니다.

Imperva 애플리케이션 보안

Client-Side Protection은 Imperva의 웹 애플리케이션 및 API 보호(WAAP)의 핵심 구성 요소로, 최적의 사용자 경험을 제공하면서 위험을 감소시킵니다.

당사의 솔루션은 다음을 통해 온프레미스 및 클라우드의 애플리케이션을 보호합니다.

- 웹 애플리케이션 방화벽(WAF)
- API 보안
- 분산 서비스 거부(DDoS) 방어
- 고급 봇 방어
- 계정 탈취 방어
- 런타임 애플리케이션 자체 보호(RASP)
- 실행 가능한 보안 인사이트
- 보안이 적용된 애플리케이션 배포

Imperva는 조직이 중요한 애플리케이션, API 및 데이터를 어디서나 대규모로, 그리고 최고의 ROI로 보호할 수 있도록 지원하는 사이버보안 리더입니다.

Imperva 애플리케이션 보안에 대해 자세히 알아보려면 +1.866.926.4678로 문의하거나 imperva.com을 방문하십시오.