CLOUDFLARE

백서

PCI DSS 4.0 규제 준수를 유지하기 위한 전략적 접근법

목차

개요

신용 카드, 직불 카드 또는 선불 카드를 처리하는 모든 조직에서는 지불 카드 산업 데이터 보안 표준(PCI DSS)을 준수해야 합니다. 여기에는 소규모 판매자, 소매업체, 전자 상거래 웹 사이트, 은행, 대기업이 포함됩니다. 하지만 클라우드 및 하이브리드 업무로의 변화, PCI DSS 4.0 도입과 더불어 표준까지 발전하면서 규제를 효율적으로 준수하기가 어려워졌습니다.

이와 같은 디지털 최신화 세상에서는 확장 가능한 방식으로 규제 준수 프로세스를 간소화하여, 조직에서 기업 디지털 최신화에 발맞추는 동시에 역동적인 규제 환경을 따라갈 수 있도록 하는 새로운 접근법이 필요합니다.

오늘날 조직에서 겪는 PCI DSS 규제 준수 문제

PCI 규제 준수는 중요하며, 규제를 위반하면 벌금이 부과되거나, 소송에 걸리거나, 정부 조사를 받을 수 있습니다. 하지만 금융 기관, 전자 상거래 판매자, 규정이 적용되는 기타 대상들은 규제 준수로 인해 몇 가지 문제를 겪습니다.

또한 클라우드 컴퓨팅과 원격 근무 의존도가 높아지면서 IT 팀에서는 디지털 환경에 대한 제어력을 잃었고, 문제 해결 프로세스는 더 복잡해졌습니다.

시간 및 리소스 할당: 53%의 조직에서는 기술적 개인정보 보호 역할을 맡을 인력이 부족해 규제 준수가 어렵다고 답변했습니다.[1]

다양한 환경에서의 데이터 보안: 클라우드 컴퓨팅과 모바일 결제가 증가함에 따라, 다양하면서도 통제력이 낮은 경우가 많은 환경에서 규제 준수를 보장하기란 점점 더 어려워지고 있습니다.

기술 스택 통합에 따른 복잡성: 암호화, 방화벽 구성과 같이 규제 준수 표준에 필요한 기술을 통합하고 유지하는 과정은 복잡한 경우가 많습니다. 레거시 시스템을 갖추고 있는 조직이나 디지털 전환을 진행하고 있는 조직에서 이러한 문제는 더 복잡해집니다.

감사: IT 팀은 규제를 준수하기 위해 모든 인프라와 시스템 전반에서 최신 상태로 감사를 추적해야 합니다.

벤더 규제 준수: 타사 서비스 공급자와 벤더가 PCI 표준을 준수하도록 하면 더욱더 복잡해집니다.

PCI DSS 4.0으로 정교한 사이버 위협에 대응하기

PCI DSS 4.0은 2022년 3월 31일에 발표되어 2024년 3월 31일에 발효되었으며, 추가 요구 사항은 2025년 3월 31일에 발효됩니다. PCI DSS 4.0의 목표는 다음과 같습니다.[2]

1. 지불 업계의 보안 요구 사항을 지속적으로 충족하기

- **인증 요구 사항 강화:** 인증, 특히 카드 소지자 데이터 환경(CDE)에 액세스하는 모든 경우에 적용되는 멀티 팩터 인증이 크게 강조되고 있습니다. 비밀번호 요구 사항 역시 최소 8자에서 12자까지로 늘어나며 더욱 엄격해졌습니다.
- **더욱 강력한 암호화 요구 사항:** PCI DSS 4.0은 카드 소지자의 데이터를 저장하고 전송하기 위해, 알려진 악용에 대한 취약점이 없는 TLS와 같은 "강력한" 암호화를 사용하도록 요구합니다.
- **지속적인 위협 해결을 위한 새로운 전자 상거래 및 피싱 요구 사항:** PCI 4.0은 클라이언트 측 보안, 피싱, 소셜 엔지니어링을 방어하기 위한 추가 요구 사항을 마련하고 있습니다.

2. 지속적인 프로세스로서 보안 장려하기

- **위험 분석 및 관리에 더욱 집중:** 조직에서는 지속적인 위험 분석 및 관리 프로세스를 구현하여 취약점을 즉시 식별하고 해결하는 것이 좋습니다.
- **책임성 및 거버넌스를 더욱 강조:** 새로운 버전은 보안 제어를 유지하기 위해 카드 소지자 데이터의 거버넌스와 책임에 더욱 중점을 두고 있습니다.
- **보안 요구 사항의 구현과 충족을 위한 지침 추가:** PCI 4.0은 해당 표준의 의도 및 사용 기간을 명확히 합니다.

3. 다양한 방법론에 유연성 추가하기

- **새로운 기술 통합:** PCI DSS 4.0은 클라우드 및 모바일 결제 시스템 등 새롭게 부상하는 기술의 보안을 다루고 있습니다.
- **조직의 보안 목표 달성 방법에 유연성 추가:** 조직은 요구 사항을 충족하기 위해 더 광범위한 방법인 "맞춤형 접근법"을 사용할 수 있습니다. 또한 위험 대상 분석을 바탕으로 얼마나 자주 조치를 취할 지 정하는 과정에서 PCI 4.0으로 유연성이 높아집니다.

4. 유효성 검사 방법 강화

- **지속적인 모니터링 및 테스트:** 새로운 표준에 따르면, 매년 규제 준수 유효성을 검사하는 대신 보안 및 규제 준수를 지속적으로 모니터링하는 것이 좋습니다.
- **규제 준수의 평가와 증명 간의 연관성 향상:** 규제 준수에 대한 자체 평가 설문지 또는 보고서에 나온 정보가 규제 준수 증명에 요약된 내용과 더욱 부합하게 됩니다.

솔루션: PCI 요구 사항에 Cloudflare의 클라우드 연결성을 통해 접근하는 새로운 방식

보안 및 IT 팀은 최신 보안 및 기술 스택에 손쉽게 통합되는 간단하고 프로그래밍 가능한 방식으로 PCI 요구 사항을 해결해야 하며, 인프라와 PCI DSS가 진화하므로 이 과정을 계속 진행해야 합니다.

여러 레거시 솔루션과 포인트 보안 솔루션이 뒤죽박죽 섞여 있는 접근법은 정답이 아닙니다. 그 대신, 기업에서 IT 환경에 대한 제어 능력을 되찾고 PCI 등 다양한 규제 준수 요건을 충족하도록 지원하기 위해 설계된 클라우드 네이티브 보안 및 네트워킹 서비스 통합 플랫폼이 팀에 필요합니다. 이러한 통합 플랫폼을 클라우드 연결성이라고 합니다.

Cloudflare 클라우드 연결성에서 제공하는 것:

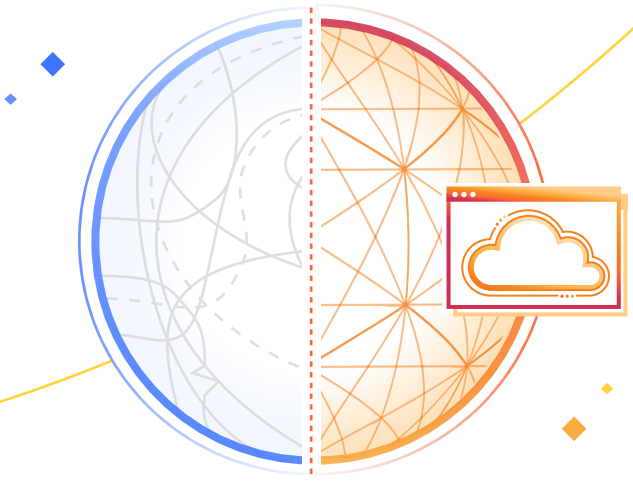
- 데이터 규제 준수를 위해 설계된 플랫폼
- 통합 정책 엔진
- 손상 없는 데이터 주권
- 감사 요건을 충족시키기 위한 지능적인 보고 기능

IT 팀은 Cloudflare를 통해 하나의 제어판을 사용하여 모든 위치에 일관적인 제어를 적용하고 어디서든 제어를 활성화할 수 있습니다.

팀은 Cloudflare 에지에서 선호하는 SIEM 또는 클라우드 목적지로 감사 목적의 로그를 직접 전송할 수 있습니다. 또한, Cloudflare는 인터넷 트래픽 가시성이 방대하므로 새로운 위협을 자동으로 식별하고 방어할 수 있습니다.

Cloudflare는 자체적으로 PCI 규제를 준수하고 있으며 PCI DSS 4.0 요구 사항을 기본적으로 지원합니다. 예를 들어, Cloudflare는 PCI DSS 4.0에서 주로 강조하는 멀티 팩터 인증을 IT 팀에서 손쉽게 시행할 수 있도록 합니다. 또한 Cloudflare에서는 최신 암호화 표준을 지원하고 암호화 표준에 기여하는 경우도 많으므로, 고객은 중요한 정보를 암호화하는 데 적용되는 PCI DSS 4.0 요구 사항을 충족할 수 있습니다.

Cloudflare 클라우드 연결성 기능에 대한 PCI DSS 요구 사항의 매핑 요약은 다음 페이지에서 확인하실 수 있습니다.



PCI 요구 사항을 해결하는 과정에서 Cloudflare가 도움을 줄 수 있는 주요 영역*

PCI 요구 사항	Cloudflare 역량
1. 네트워크 보안 제어를 설치하고 유지 관리합니다(이전에는 "방화벽 설치 및 유지 관리"였음).	Cloudflare는 악성 네트워크 트래픽 등으로부터 네트워크, 앱, 클라우드 배포를 보호합니다. Cloudflare는 매일 수천억 건의 위협을 통해 얻은 위협 인텔리전스를 사용하여 OWASP 상위 10대 및 Zero-day 공격을 비롯한 웹 기반 위협으로부터 웹 사이트와 웹 앱을 보호합니다. Cloudflare의 보안 플랫폼은 클라우드 네이티브 방식이며 몇 분 안에 배포되고, 사용자가 몇 초 만에 전역적인 정책 변경 사항을 도입할 수 있습니다.
2. 보안 구성을 모든 시스템 구성 요소에 적용합니다.	Cloudflare에서 보호하는 사용자, 장치, 앱은 강력하게 암호화되어 웹에 있는 잠재적인 공격자로부터 마스킹됩니다. 사용자는 Cloudflare의 API Shield를 사용하여 시퀀스를 식별하고 API 트랜잭션 관련 정책을 시행하여 API 취약점을 보호할 수 있습니다.
3. 암호화 또는 기타 데이터 보호 방법을 통해 저장된 데이터를 보호합니다.	Cloudflare는 미사용 PII를 식별할 수 있으며 카드 소지자 로그 유지 시간에 대한 요구 사항을 충족합니다.
4. 개방형 공용 네트워크에서 카드 소지자 데이터를 암호화합니다.	Cloudflare의 전역 네트워크로 전송된 트래픽은 이러한 요구 사항에 정해진 암호화 규칙을 충족하며, Cloudflare는 사용자가 식별해야 하는 PII가 전송되는 것을 차단할 수 있습니다.
5. 악성 소프트웨어로부터 모든 시스템과 네트워크를 보호합니다.	Cloudflare는 초당 5,500만 건이 넘는 HTTP 요청을 처리하므로 외부의 최신 공격에 대해 독보적으로 폭넓은 관점을 제공합니다. Cloudflare는 사용자에게 바이러스 백신, 클라우드 이메일 보안, 원격 브라우저 격리 등 맬웨어 방지를 위한 보호용 제품군을 제공합니다.
6. 보안 시스템과 소프트웨어를 개발하고 유지합니다.	Cloudflare는 사용자 보안 위반 사항뿐만 아니라 SaaS 앱 내에서 감지된 잘못된 구성의 순위를 매기고 가중치를 둘 수 있습니다. Cloudflare의 보안 서비스로 알려진 공격과 악용으로부터 웹에 공개된 모든 공용 앱을 보호할 수 있습니다.
7. "알아야 할 필요"에 따라 카드 소지자의 데이터 액세스를 제한합니다.	Cloudflare는 사용자 위치 또는 데이터 저장 위치와 관계없이 권한을 최소화한 세부 접근 제어를 시행할 수 있습니다.
8. 사용자를 식별하고 시스템 구성 요소에 대한 액세스를 인증합니다.	Cloudflare는 전역 네트워크를 통과하는 모든 트래픽에 ID 기반 정책을 시행하고 보안 상태 검사(예: MFA 사용 여부)를 진행할 수 있습니다.
10. 시스템 구성 요소와 카드 소지자 데이터에 대한 모든 액세스를 로그로 남기고 모니터링합니다.	Cloudflare는 플랫폼 내 모든 제품에 세부적인 감사 로그를 제공하며, 이를 대부분의 주요 SIEM과 통합합니다.
11. 시스템과 네트워크의 보안을 정기적으로 테스트합니다.	Cloudflare는 모든 주요 제품에 대한 심층 로그뿐만 아니라 제한된 액세스 정책 테스트와 침입 감지 서비스 기능을 제공합니다.

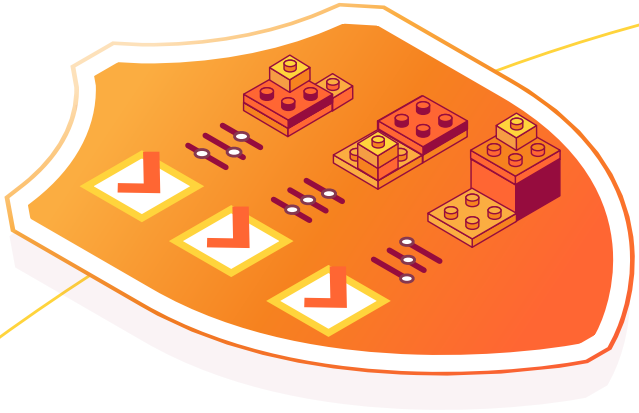
*Cloudflare는 물리적 보안 및 조직적 구조에 관한 PCI DSS 4.0 요구 사항 9 및 12를 지원하지 않습니다.

요약: PCI 규제 준수 요구 사항을 해결하기 위해 Cloudflare 활용하기

Cloudflare는 PCI를 준수하며, 인프라 형태와 관계없이 고객이 스스로 규제 준수 요구 사항을 해결할 수 있도록 지원하는 능력을 갖추고 있습니다.

실제로 Cloudflare를 사용하여 데이터 유출 가능성이 65%[3] 감소했고, 연간 사이버 보험료가 24%[4] 감소했으며, 시스템 및 프로세스 관리 소요 시간이 59%[4] 감소했습니다.

> **Stax의 기업 고객은 매우 구체적인 규제 준수 표준을 충족할 것을 계약으로 요구합니다. 그래서 Stax는 인프라 전반에서 Zero Trust와 같은 보안 제어를 시행하게 되었습니다...Cloudflare는 필요한 것을 정확하게 해냈습니다. 엔드포인트를 보호하고 보안을 강화한 것입니다."** [5]
>
> **Troy Ridgewell**
> **Stax 보안 책임자**
>
> STAX



Cloudflare의 데이터 규제 준수 솔루션을 지금 바로 만나보세요. 전문가들과 상의하여 시작하세요.

참고자료

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. 2022년 IBM 유출 비용 보고서
4. Cloudflare 앱 서비스 고객을 대상으로 한 2023년 Cloudflare TechValidate 설문조사
5. https://www.cloudflare.com/ko-kr/case-studies/stax/

CLOUDFLARE

007-9814-2030-192 | enterprise@cloudflare.com | cloudflare.com/ko-kr

REV:BDES-5776.2024APR09