AKAMAI-LÖSUNGSÜBERBLICK

# PCI DSS v4.0-Compliance mit Akamai

PCI-Compliance bedeutet die Erfüllung globaler Sicherheitsanforderungen, um Umgebungen zu schützen und zu sichern, die Daten von Zahlungskartenkonten verarbeiten. Jedes Unternehmen, das Karteninhaberdaten online verarbeitet, überträgt oder speichert, trägt Verantwortung für die Compliance des Payment Card Industry Data Security Standard (PCI DSS). Der 2004 entwickelte Standard wird regelmäßig aktualisiert, um Branchenänderungen und sich weiterentwickelnden Cybersicherheitsbedrohungen gerecht zu werden. Die neueste Version dieses Standards, PCI DSS v4.0, brachte bei ihrer Veröffentlichung im März 2022 erhebliche Änderungen mit sich und enthält 12 Kernanforderungen, die Unternehmen bis März 2025 erfüllen müssen.

## Sind Sie bereit für PCI DSS v4.0?

Auch wenn die Nichteinhaltung der PCI-Standards rechtlich nicht strafbar ist, können Kreditkartenunternehmen Geldbußen gegen Firmen verhängen, die dem Standard nicht gerecht werden. Darüber hinaus können nicht geschützte Marken anfällig für Cyberangriffe sein, die zu verheerenden Datenschutzverletzungen mit hohen Geldstrafen und einem dauerhaften Verlust des Kundenvertrauens führen.

Wir helfen Ihnen gern. Akamai hält nicht nur die PCI-DSS-Compliance auf Stufe 1 ein, sondern bietet auch eine breite Palette branchenführender Sicherheitslösungen, die Unternehmen bei der Einhaltung der PCI DSS v4.0-Compliance unterstützen. Einige Lösungen tragen sogar dazu bei, den Umfang eines PCI-Audits zu reduzieren. Dies spart Ihnen wertvolle Zeit und Geld für die Erfüllung der Zertifizierungsanforderungen.

## App & API Protector mit Malware-Schutz

Stellen Sie die Compliance bei Protokollen sicher und schützen Sie sich vor Datenlecks, Zero-Day-Angriffen und CVEs sowie anderen Edge-basierten Angriffen, um die Anforderungen 6.4.2, 6.5.3 und 11.5 zu erfüllen.

> **„Jeden Tag werden 560.000 neue Malware-Varianten entdeckt, die zu den bereits im Umlauf befindlichen hinzukommen und sich auf über eine Milliarde Malware-Programme summieren.“**
>
> Quelle: Getastra | 30+ Malware Statistics You Need to Know In 2023

## Vorteile

- **Optimieren Sie Workflows** für Sicherheits- und Compliance-Teams
- **Reduzieren Sie den Auditaufwand** mit speziell entwickelten und dedizierten PCI-Funktionen
- **Erhalten und protokollieren Sie PCI-Warnungen** für Compliance-bezogene Ereignisse
- **Konsolidieren Sie Anbieter** mit dem umfassenden Portfolio an Sicherheitslösungen von Akamai und erfüllen Sie PCI-Anforderungen


| Veröffentlicht: April 2024

## API Security

Erkennen und verringern Sie den Missbrauch von API-Verhalten und -Logik, protokollieren Sie API-Aktivitäten und implementieren Sie reaktionsschnellen, automatisierten Schutz für Ihre APIs, um die Compliance-Anforderungen 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1, 10.5.1 und 11.3.2 zu erfüllen.

> **„Bis 2024 werden sich API-Missbrauch und damit zusammenhängende Datenschutzverletzungen nahezu verdoppeln."**
>
> Quelle: Gartner-Bericht: Top 10 Aspects Software Engineering Leaders Need to Know About APIs (Nur in englischer Sprache verfügbar)

## Client-Side Protection & Compliance

Erfüllen Sie die neuen JavaScript-Sicherheitsanforderungen 6.4.3 und 11.6.1, indem Sie den Schutz vor clientseitigen Angriffen wie Web-Skimming oder Magecart stärken. Bei derartigen Angriffen wird über den Browser Schadcode in Seiten zur Kaufabwicklung injiziert, um nach Zahlungskartendaten zu suchen und diese zu extrahieren.

> **„81 % der großen Onlineeinzelhändler geben an, dass ihr Unternehmen im Jahr 2022 von verdächtigem Skriptverhalten betroffen war."**
>
> Quelle: From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 (Nur in englischer Sprache verfügbar)

## Akamai Guardicore Segmentation

Eine effizientere Segmentierung von regulierten Assets anhand von verschiedenen Technologien auf einer einzigen Plattform unterstützt Sie dabei, viele PCI-Anforderungen zu erfüllen. Transparenz von Netzwerk und Assets, eine verteilte Firewall, Richtliniendurchsetzung bis Layer 7 sowie Erkennung und Reaktion auf Sicherheitsverletzungen.

> **„Dank der softwaredefinierten Segmentierung konnten wir Segmentierungsrichtlinien auf Prozessebene erstellen und durchsetzen. Das hatte sowohl für unsere Sicherheit als auch für die Fähigkeit zur Erfüllung der technischen PCI-DSS-Anforderungen erhebliche Verbesserungen zur Folge."**
>
> – Senior Infrastructure Engineer, The Honey Baked Ham Company

**Wenn Sie mehr darüber erfahren möchten, wie Sie die PCI DSS v4.0-Compliance mit Akamai beschleunigen können, wenden Sie sich an unser Expertenteam.**