AKAMAI SOLUTION BRIEF

PCI DSS v4.0 Compliance with Akamai

PCI compliance means adhering to a global set of security requirements to protect and secure environments with payment card account data. Any business that processes, transmits, or stores cardholder data online holds the responsibility of adhering to the Payment Card Industry Data Security Standard (PCI DSS). Developed in 2004, the standard is regularly updated to meet industry changes and evolving cybersecurity threats. The latest standard, PCI DSS v4.0, was released in March 2022 with significant changes and contains 12 core requirements that organizations need to meet by March 2025.

Are you ready to meet PCI DSS v4.0?

Although failing to comply with PCI standards is not punishable by law, credit card companies can impose fines on businesses that do not adhere to the standard. In addition, failing to secure cardholder data can leave brands vulnerable to cyberattacks that result in devastating data breaches with hefty fines and permanent loss in customer trust.

We are here to help. Not only does Akamai maintain PCI DSS Level 1 compliance, we also offer a breadth of industry-leading security solutions to help organizations meet PCI DSS v4.0 compliance. Some solutions even help to reduce the scope of a PCI audit, saving valuable time and money spent on meeting certification requirements.

App & API Protector with Malware Protection

Maintain log compliance and protect against personally identifiable information data leakage, zero-day attacks, and CVEs, as well as other edge-based attacks to comply with requirements 6.4.2, 6.5.3, and 11.5.

> “Every day, 560,000 new pieces of malware are detected, adding to the over 1 billion malware programs already in circulation.”
>
> Source: Getastra | 30+ Malware Statistics You Need to Know In 2023

API Security

Detect and mitigate API behavior and logic abuse, log API activity, and implement responsive, automated protection for your APIs to help meet compliance requirements 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1,10.5.1, and 11.3.2.

> “By 2024, API abuses and related data breaches will nearly double.”
>
> Source: Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs

Benefits

- **Streamline workflows** for security and compliance teams
- **Reduce the auditing burden** with purpose-built and dedicated PCI capabilities
- **Receive and log actionable PCI alerts** for events related to compliance
- **Consolidate vendors** to meet PCI requirements with Akamai’s comprehensive portfolio of security solutions

Akamai

| Support | | Published 04/24

Client-Side Protection & Compliance

Meet new JavaScript security requirements 6.4.3 and 11.6.1 by helping to protect against client-side attacks, such as web skimming or Magecart, that skim and exfiltrate payment card data from online checkout pages through malicious code injection executed in the browser.

> “81% of large online retailers report that their organization had been targeted by suspicious script behavior in 2022.”
>
> Source: From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023

Akamai Guardicore Segmentation

Segment regulated assets more efficiently by leveraging several technologies integrated within a single platform to help meet many PCI requirements. Get network and asset visibility, a distributed firewall, policy enforcement up to Layer 7, and breach detection and response.

> “Software-defined segmentation allowed us to create and enforce segmentation policies at the process level, significantly improving both our security posture and the ability to meet PCI-DSS technical requirements.”
>
> — Senior Infrastructure Engineer, The Honey Baked Ham Company

To learn more about how to accelerate PCI DSS v4.0 compliance with Akamai, reach out to our team of experts.