


WHITEPAPER

# A strategic approach to maintaining PCI DSS 4.0 compliance



# Content

- 3 Overview**
  - 4 Challenges of PCI DSS compliance**
  - 5 Keeping up with sophisticated cyberthreats**
  - 6 Solution: A new approach to PCI DSS 4.0**
  - 7 Key areas where Cloudflare can help**
  - 8 Summary**
- 

# Overview

**All organizations that process credit, debit, or prepaid cards must comply with the Payment Card Industry Data Security Standard (PCI DSS). This includes small merchants, retailers, ecommerce websites, banks, and large enterprises. However, the shift to the cloud and to hybrid work, combined with evolving standards as PCI DSS 4.0 is rolled out, make it difficult to comply in an efficient way.**

**A new approach for this digitally modernized world is needed to streamline the compliance process in a scalable way, enabling organizations to keep up with the dynamic regulatory landscape as it keeps pace with enterprise digital modernization.**



# Challenges of PCI DSS compliance for today's organizations

PCI compliance is crucial, with violators subject to fines, lawsuits, and government investigations. Yet compliance presents several challenges for financial institutions, ecommerce merchants, and others subject to its regulations.

And as IT teams have lost control of their digital environments due to an increased reliance on cloud computing and remote work, the process of solving those challenges has become more complex.



## **Time and resource allocation:**

53% of organizations say technical privacy roles are understaffed, making compliance challenging.<sup>1</sup>



## **Data security in diverse environments:**

With the rise of cloud computing and mobile payments, ensuring compliance in diverse and often less-controlled environments is increasingly hard.



## **Complexity with technology stack integration:**

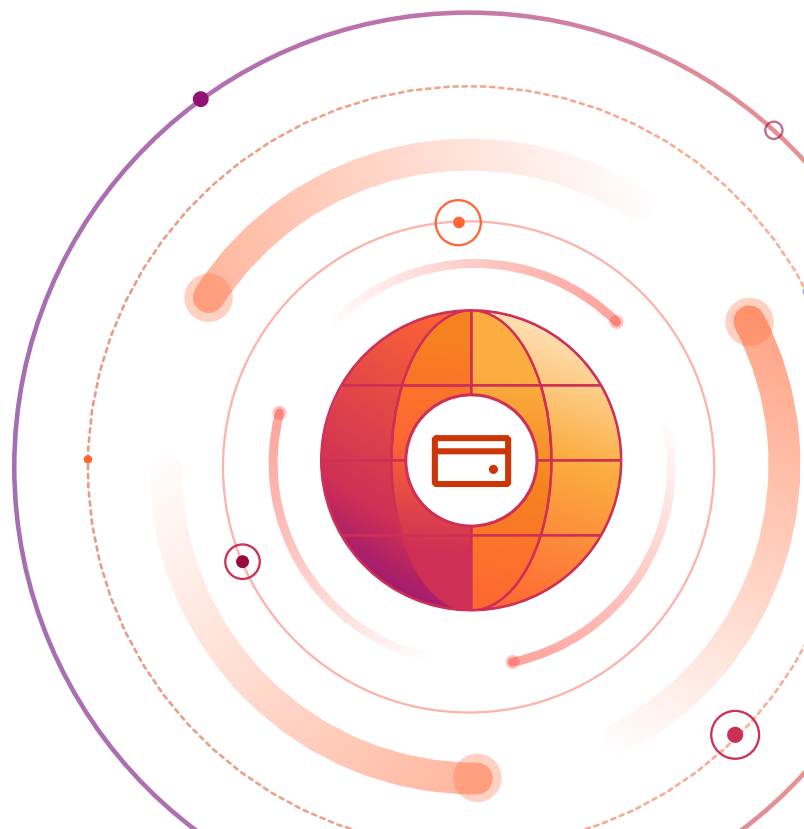
Integrating and maintaining the necessary technologies to meet compliance standards, such as encryption and firewall configurations, is often complex. This challenge is compounded in organizations with legacy systems or those undergoing digital transformation.



**Auditing:** IT teams must maintain an up-to-date audit trail across all infrastructure and systems to ensure compliance.



**Vendor compliance:** Ensuring that third-party service providers and vendors comply with PCI standards adds another layer of complexity.



# Keeping up with sophisticated cyberthreats with PCI DSS 4.0

PCI DSS 4.0 was released on March 31, 2022, coming into effect on March 31, 2024 with additional requirements to go into effect on March 31 2025. The goals of PCI DSS 4.0 are to:<sup>2</sup>

## 1. Continue to meet the security needs of the payment industry

- **Enhanced authentication requirements:** There is a stronger emphasis on authentication, particularly multi-factor authentication for all access into Cardholder Data Environment (CDE). Password requirements are also more stringent, increasing from 8 to 12 characters minimum.
- **Stronger encryption requirements:** PCI DSS 4.0 mandates the use of "strong" encryption for storing and transmitting cardholder data, such as TLS that is not vulnerable to known exploits.
- **New supply chain and phishing requirements to address ongoing threats:** PCI 4.0 has additional requirements for client-side security and for defending against phishing and social engineering.

## 2. Promote security as continuous process

- **Additional focus on risk analysis and management:** Organizations are encouraged to implement continuous risk analysis and management processes to identify and address vulnerabilities promptly.
- **Greater emphasis on accountability and governance:** The new version places a stronger focus on the governance of cardholder data and accountability for maintaining security controls.
- **More guidance for implementing and meeting security requirements:** PCI 4.0 clarifies the intent of the standard, and the timeframes used.

## 3. Add flexibility for different methodologies

- **Integration of new technologies:** PCI DSS 4.0 addresses the security of emerging technologies like cloud and mobile payment systems.
- **More flexibility for how organizations can achieve security objectives:** Organizations can use a "customized approach," a wider range of methods to meet requirements. And PCI 4.0 offers more flexibility to establish how frequently they perform actions based on targeted risk analyses.

## 4. Enhance validation methods

- **Continuous monitoring and testing:** The new standard encourages a shift from annual compliance validation to continuous security and compliance monitoring.
- **Increased alignment between assessments and attestations of compliance:** The information in self-assessment questionnaires or reports on compliance are more aligned with what is summarized in Attestations of Compliance.



## Solution: A new approach to PCI requirements via Cloudflare's connectivity cloud

Security and IT teams need to address PCI requirements in a simple and programmable way that integrates easily with their current security and technology stack, and continues to do so as their infrastructure and PCI DSS evolve.

The answer is not a mishmash approach with many legacy and point security solutions. Instead, teams need a unified platform of cloud-native security and networking services designed to help enterprises regain control over their IT environments and meet various compliance requirements, including PCI. Such a unified platform is called a connectivity cloud.

### The Cloudflare connectivity cloud offers:

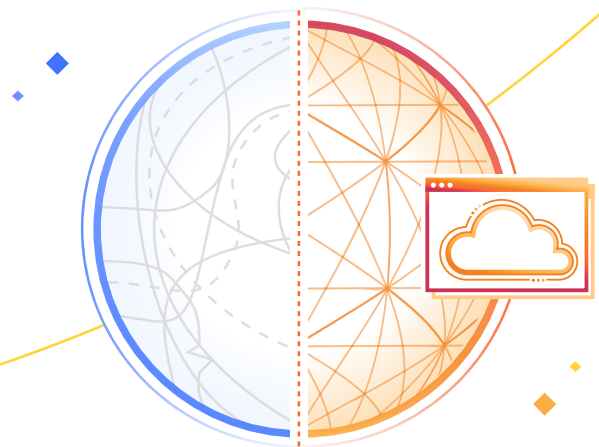
- A platform that is architected for data compliance
- A unified policy engine
- Data sovereignty without compromise
- Intelligent reporting to satisfy audits

Cloudflare allows IT teams to apply consistent controls across any location, converging multiple security services into a single control plane that manages private networking, web traffic, user access to business critical as well as SaaS applications, data protection, and email security.

Cloudflare's visibility at-scale into internet traffic means it can automatically identify and defend against new web-based threats, especially in context of traffic aimed at a critical website or application. Cloudflare also generates detailed audit logs at its edge, and allows users to send them to any preferred SIEM or cloud destination, along any path required to remain compliant with regional data governance laws.

Cloudflare itself is PCI compliant and natively supports PCI DSS 4.0 requirements. In addition to being built in a compliant manner with PCI ourselves, Cloudflare also helps customers meet their own PCI DSS 4.0 requirements. For example PCI calls for orgs to restrict cardholder access on a "need to know basis." Cloudflare can enforce least-privilege, granular access controls, no matter where users are located or data is stored."

A summary mapping of PCI DSS requirements to Cloudflare connectivity cloud capabilities can be found on the next page:



## Key areas where Cloudflare can help address PCI requirements\*

PCI Requirement	Cloudflare Capability
1. Install and maintain network security controls (previously "install and maintain a firewall").	Cloudflare protects networks, applications, and cloud deployments alike from malicious network traffic. Cloudflare uses threat intelligence from hundreds of billions of daily threats to protect websites and web applications from web-based threats, including the OWASP top 10 and zero-day attacks. Its security platform is cloud-native, deploys in minutes, and allows users to roll out global policy changes in seconds.
2. Apply secure configurations to all system components.	Users, devices, and applications behind Cloudflare are strongly encrypted and masked from potential attackers on the web. Cloudflare's API Gateway remediates vulnerabilities in customer APIs by identifying common sequences and enforcing policies surrounding API transactions.
3. Protect stored data via encryption or other data protection methods.	Cloudflare can identify PII at rest, and it meets the requirements for cardholder log retention time.
4. Encrypt cardholder data across open, public networks.	Traffic sent across Cloudflare's global network meets the encryption standards specified in this requirement, and Cloudflare can block the transmission of PII the user needs to identify.
5. Protect all systems and networks from malicious software.	Cloudflare serves over 55 million HTTP requests per second, giving us a uniquely wide-ranging view of the latest attacks in the wild. Cloudflare provides users a suite of anti-malware protections, including antivirus, cloud email security, and remote browser isolation.
6. Develop and maintain secure systems and software.	Cloudflare can rank and weight user security violations, as well as misconfigurations it detects within SaaS applications. Cloudflare's security services can protect all public web-facing applications against known attacks and exploits, as well as monitor and alert on supply chain risk of third party scripts loaded in the browser.
7. Restrict cardholder data access on a "need to know" basis.	Cloudflare can enforce least-privilege, granular access controls, no matter where users are located or data is stored.
8. Identify users and authenticate access to system components.	Cloudflare can enforce identity-based policies and security posture checks (e.g. whether MFA was used) for any traffic crossing its global network.
10. Log and monitor all access to system components and cardholder data.	Cloudflare provides granular audit logs across all products in its platform and integrates with most major SIEMs.
11. Test security of systems and networks regularly.	Cloudflare provides limited access policy testing and intrusion detection service functionality, in addition to providing in-depth logs for all of its major products.

\*Cloudflare does not assist with PCI DSS 4.0 requirements 9 and 12, which pertain to physical security and organizational structure.

## Summary: Rely on Cloudflare to help address PCI compliance requirements

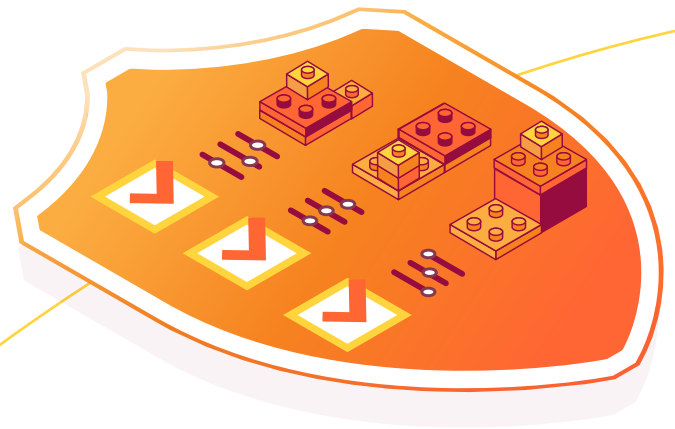
Cloudflare is PCI compliant and has capabilities that help customers address compliance requirements themselves, no matter what their infrastructure looks like.

In fact, the use of Cloudflare can result in a 65%<sup>3</sup> reduced likelihood of a data breach, a 24%<sup>4</sup> reduction on annual cyber insurance premiums, and 59%<sup>4</sup> reduced time spent on managing systems and processes.

“

Our enterprise customers contractually require Stax to meet very specific compliance standards. That led us to enforce security controls like Zero Trust across our infrastructure....Cloudflare did exactly what we needed it to. It protected our endpoints and locked down our security.”<sup>5</sup>

Troy Ridgewell  
[Stax Head of Security](#)



Discover Cloudflare [data compliance solutions](#) today.  
[Talk to our experts](#) to get started.



# References

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. IBM Cost of Breach 2022 report
4. 2023 Cloudflare TechValidate Survey of Cloudflare App Service Customers
5. <https://www.cloudflare.com/case-studies/stax>



© 2024 Cloudflare Inc. All rights reserved.  
The Cloudflare logo is a trademark of Cloudflare. All other  
company and product names may be trademarks of the  
respective companies with which they are associated.

1 888 99 FLARE | [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [Cloudflare.com](https://cloudflare.com)

REV: BDES-5776.2024APR29