# PCI DSS COMPLIANCE

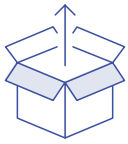
**If your business accepts credit cards, you've heard of PCI DSS 4.0 — a compliance standard with critical requirements for organizations that store, process or transmit credit card data. It impacts your customers and your business — a breach means a loss of revenue, customers, brand reputation or trust.**

## DISCOVER AND REMEDIATE CARDHOLDER DATA

Organizations that store, transmit or process cardholder data rely on Ground Labs to ensure discovery of personal data and gain PCI DSS 4.0 compliance. We invite you to learn how Ground Labs' network wide data discovery solution can help you comply with PCI DSS 4.0 and with trends like BYOD and multi-cloud storage frameworks -- meaning your data can be almost anywhere — on your network, in the cloud or on an employee's desktop.

Is your business ready for the PCI DSS 4.0 deadline? Book a complimentary sample data analysis with Ground Labs to find out.

## HOW GROUND LABS CAN HELP ENSURE PCI DSS COMPLIANCE

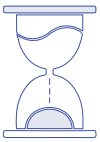


Out of the box cardholder discovery designed for PCI DSS 4.0

Trusted by PCI QSAs (Qualified Security Assessors) in 50+ countries

Simple, fast deployment without the need to ship any boxes or contact on-site engineers

Low resource requirements that allow mission critical system use



Reduce the time required to become compliant with major data security standards

Create detailed, actionable reports, keeping all business leaders informed

Search across the entire organization with support for Windows, macOS, Linux, FreeBSD, Solaris, HP-UX and IBM AIX

Search within both structured and unstructured data sources including servers, on desktops, email, and databases, on prem and in the cloud.

Book a complimentary sample data analysis with Ground Labs at
https://go.groundlabs.com/book-a-demo

GROUND LABS

## PCI DSS 4.0: What Organisations need to Know

According to the 2020 Verizon Payment Security Report, only 27.9% of global organizations maintained full compliance with the PCI DSS in 2019 — marking the third straight year that PCI DSS compliance has declined. The report also found that only about 50% of organizations successfully test security systems and processes. This is especially concerning with the accelerated adaptation of e-commerce and contactless payment.

PCI DSS 3.2.1 is currently the gold standard for organizations handling credit card information. Organizations, regardless of size, that accept, transmit, or store payment card data must achieve compliance under the PCI DSS 3.2.1 regulations by law or risk penalties of up to $500,000 per violation. If you missed our latest post, PCI DSS Compliance Levels: A Complete Guide, we recommend taking a step back to understand in greater detail what the regulatory requirements are currently. In this post, we'll go over expected changes for PCI DSS 4.0, slated to come into effect in mid-2021. across almost any network, including EBCDIC IBM mainframes.

## PCI DSS Version 4.0 Release Date & Timeline

According to the PCI SSC (Security Standards Council), the expected release date of PCI DSS 4.0 is Q1 2022. Based on this timeline, the slated enforcement date is still pending but historically comes within two quarters of the standard's release.

Therefore, businesses must plan how they will maintain compliance now. Organizations will need to accommodate budgetary changes to adapt to the new requirements and additional data management/security testing. Executing on these changes will likely require staffing changes, new tools and data discovery solutions, as well as overall organization-wide training efforts.

## When will my organization need to comply with PCI DSS 4.0?

Once PCI DSS 4.0 is released, an extended transition period will be provided for organizations to update from PCI DSS 3.2.1 to PCI DSS 4.0. To support this transition, PCI DSS 3.2.1 will remain active for 18 months once all PCI DSS 4.0 materials — that is, the standard, supporting documents (including SAQs, ROCs, and AOCs), training, and program updates — are released.

This extended period allows organizations to do a few things in preparation. It provides time to become familiar with the changes in PCI DSS 4.0, update reporting templates and forms, and plan for and implement necessary changes to meet the updated requirements. Upon completion of the transition period, PCI DSS 3.2.1 will be retired and 4.0 will become the only active version.

## WHAT WILL CHANGE WHEN PCI DSS 4.0 IS RELEASED?

PCI DSS 4.0 is evolving to support a range of payment environments, technologies, and methodologies, while ensuring its ability meet the security needs of the financial services industry.

PCI DSS 4.0 emphasizes security as a continuous process and will promote fluid data management practices that integrate with an organization's overall security and compliance posture.

The majority of changes involve changing the language what 'must' be implemented to the resulting security outcome. Other changes may include:

- **Authentication** – in order to reflect the latest industry best practices for password and multi-factor authentication.
- **Encryption** – including broader applicability for cardholder data on trusted networks and a need for a data discovery process.
- **Monitoring** – regarding requirements, regarding cardholder data environments, and taking into consideration recent technology advancement.
- **Testing of critical controls** – in greater frequency and perhaps incorporating some requirements from the Designated Entities Supplemental Validation (PCI DSS Appendix A3) into regular PCI DSS requirements