E-BOOK

GROUND LABS

DATA DISCOVERY AND PCI DSS 4.0

CONTENTS

Introduction 3

Data Discovery and PCI DSS 4.0 4

Compliance Technologies for PCI DSS 4.0 5

Data Discovery for Merchants 6

Data Discovery for Service Providers 7

Data Discovery for DESV Eligible Organizations 8

Data Discovery for Assessors 9

Industry-leading Data Discovery for PCI DSS from Ground Labs 10

Introduction

PCI DSS 4.0 is the latest evolution of the card data security standard that has revolutionized the payments industry. Of the 64 controls introduced in the latest update, eight are directly supported by data discovery.

No longer can card data discovery be considered merely a pre-compliance activity; an activity relevant only to organizations starting out on their compliance journey. Data discovery remains a fundamental tool for organizations undertaking compliance for the first time – after all, you can't secure what you don't know – but is now also embedded in controls throughout the standard.

The rapid evolution in the technology landscape and the increased accessibility to smaller organizations to technologies that were previously restricted to Enterprises means that organizations have more ways than ever before to conduct business. Traditional networks have been replaced by software-defined networking and Infrastructure-as-a-Service or Platform-as-a-Service offerings. Data is no longer held in static locations as organizations migrate to more flexible and dynamic storage solutions in virtualized server environments and cloud-based solutions. With added flexibility comes greater potential for data proliferation, increasing the emphasis organizations need to place on understanding where and how their data is processed. In total, data discovery has the potential to support compliance with 27 controls across four requirements of the new standard.

This e-book explains how data discovery can support your compliance process, whether you're a merchant, service provider or assessor. From initial scoping to incident response, data discovery scanning for PCI DSS offers the situational awareness of account data necessary to support compliance over time.

Data Discovery and PCI DSS 4.0

Data discovery directly supports 27 PCI DSS 4.0 controls and sub-controls across four requirements, from periodic scope revalidation to incident response. Of the 64 new controls introduced in PCI DSS 4.0, eight are directly or indirectly supported by periodic data discovery scanning.

Frequent data discovery scans can be used to verify compliance across multiple requirements in PCI DSS 4.0.

Requirement 1:

Install and maintain network security controls

Data discovery validates the network boundaries of scope and demonstrates data flows are up to date.

Requirement 3:

Protect stored account data

Discovery scans identify account data, including SAD, wherever it is stored. Periodic scans can confirm that data has been deleted when it has passed its retention period.

Requirement 6:

Develop and maintain secure systems and software

Discovery scans verify that account data is not present in non-production environments.

Requirement 12:

Support information security with organizational policies and programs

As part of periodic scope revalidation, data discovery verifies in-scope systems and data repositories. Advanced discovery solutions offer remediation-in-place for data found in unexpected locations.

Compliance Technologies for PCI DSS 4.0

PCI DSS compliance requires the implementation of a range of technical solutions and capabilities, from malware protection to vulnerability scanning, all considered fundamental to good security practice. Many of these technologies support a single control or controls within a single requirements.

With the enhancements of PCI DSS 4.0 and the global movement toward data protection and privacy legislation and regulation, data discovery is increasingly recognized as an essential component of effective data management.

PCI DSS compliance requires the implementation of a range of technical solutions and capabilities.

PCI DSS 4.0	Data discovery scanning	Identity and access management	Malware protection monitoring	Automated log monitoring	Vulnerability scanning
Req. 1	✓	×	×	×	×
Req. 2	×	✓	×	×	×
Req. 3	✓	✓	×	×	×
Req. 4	×	×	×	×	×
Req. 5	×	✓	✓	×	×
Req. 6	✓	✓	×	×	✓
Req. 7	×	✓	×	×	×
Req. 8	×	✓	×	×	×
Req. 9	×	×	×	×	×
Req. 10	×	✓	×	✓	×
Req. 11	×	×	×	×	✓
Req. 12	✓	×	×	✓	×

Data Discovery for Merchants

While many payment solutions remove data from merchant environments, card data storage remains prevalent, particularly in larger organizations. Even where there is no card data storage, up to 14 controls are supported by periodic data discovery scanning.

Merchants must particularly be aware of the new incident response control 12.10.7. requiring organizations to have an incident response plan for account data identified in unexpected locations. As part of this plan, organizations need to be able to locate and remediate this data quickly. Advanced discovery solutions such as Ground Labs' Enterprise Recon PCI support remediation-in-place for data found outside authorized and in-scope systems.

Merchants eligible for self-assessment also have compliance obligations that may benefit from periodic data discovery scanning.

Data discovery scanning for merchants eligible for self-assessment against PCI DSS v4.0.

SAQ type	Data discovery	
SAQ A	✓	Verifying no cardholder data is stored in merchant systems
SAQ A-EP	✓	Validating network boundaries, verifying no cardholder data is stored, confirming no live PAN present in non-production environments
SAQ B	×	
SAQ B-IP	✓	Verifying no cardholder data is stored in merchant systems
SAQ C	✓	Verifying no cardholder data is stored in merchant systems
SAQ C-VT	×	
SAQ D	✓	Validating network boundaries, verifying cardholder data is stored only in authorized locations, confirming no live PAN present in non-production environments, supporting incident response for data in unexpected locations.
SAQ P2PE	✓	Verifying no cardholder data is stored in merchant systems

Ground Labs' Card Recon and Card Recon Plus solutions provide self-service discovery solutions to meet merchants' needs whatever their size. Card Recon offers Desktop and Server editions, specifically designed for card data discovery for small and medium-sized organizations. Supporting all major operating systems, server and database platforms, and file types including audio and Optical Character Recognition (OCR).

Card Recon Plus is the benchmark self-service data discovery solution available online for up to 10TB of scanning capacity. Based on the GLASS Technology™ that powers Ground Labs' industry-leading Enterprise Recon solution, Card Recon Plus offers data discovery for cloud services and email platforms in an unobtrusive and flexible package.

Data Discovery for Service Providers

While merchants are able to outsource payment processing and account data handling, it's service providers that have the responsibility for managing these critical functions on their behalf.

Service providers have up to 64 new controls to meet when PCI DSS 4.0 becomes mandatory from March 31, 2024. Eight of these can be supported with periodic data discovery scanning, and with advanced discovery solutions, remediation-in-place capabilities may help to address issues of non-compliance when these occur.

Across PCI DSS 4.0, data discovery supports up to 22 controls and sub-controls including some that are applicable only to service providers.

Data discovery scanning for service providers in PCI DSS v4.0.

Requirement 1	**Install and maintain network security controls**
1.2.3. 1.2.4.	Data discovery scanning can be used to validate the network boundaries of the CDE, as well as demonstrating that data flows map account data accurately.
Requirement 3	**Protect stored account data**
3.2.1. 3.3.1. (3.3.1.1, 3.3.1.2., 3.3.1.3.) 3.3.2. 3.3.3. 3.4.2.	Data discovery scanning identifies any cardholder data including sensitive authentication data wherever it is stored. Periodic discovery scanning can be used to confirm that data has been deleted when it has exceeded its retention period. Organizations that store sensitive authentication data must be able to verify that it is removed following authentication, or when no longer required.
Requirement 6	**Develop and maintain secure systems and software**
6.5.2. 6.5.5.	Verifying that a significant change has not impacted scope boundaries, and that CHD is not present in non-production environments is supported by data discovery scanning.
Requirement 12	**Support information security with organizational policies and programs**
12.4.2. (12.4.2.1.) 12.5.1. (12.5.2.1.) 12.5.2. 12.5.3. 12.10.7.	Data discovery scanning can be used to confirm that operational procedures involving cardholder data are being followed so CHD remains in the CDE. As part of periodic scope revalidation and following organizational change, data discovery scanning is essential to confirm in-scope systems, network boundaries, data flows and data repositories. Advanced discovery solutions support remediation-in-place for data found in unexpected locations.

Ground Labs' Enterprise Recon PCI provides comprehensive data discovery with remediation capabilities suitable for organizations with complex processing environments including cloud-, virtualized- and on-premises-based networks. Enterprise Recon PII and Enterprise Recon Pro build on these capabilities to provide discovery and data management across a range of PII and custom-defined data types in structured and unstructured systems.

Data Discovery for DESV Eligible Organizations

The PCI Security Standards Council introduced the PCI DSS Designated Entities Supplemental Validation (DESV) in June 2015, alongside PCI DSS 3.1. The DESV placed additional obligations on organizations at the discretion of payment brands and acquirers. Designed for high-risk organizations such as those processing very high volumes of account data or those that had suffered serious or repeated data breaches, the DESV aimed to provide greater assurance that these organizations were able to maintain compliance effectively, on a continuous basis.

PCI DSS 4.0 maintains the same basic set of requirements introduced in June 2015, with a number of these focusing on frequent scope validation and data discovery. Eight of the 25 controls defined in the DESV relate to scoping, scope validation and data discovery.

Scoping, scope validation and data discovery for DESVs in PCI DSS v4.0.

Appendix A3	Designated Entities Supplemental Validation (DESV)
A.3.2.1. A.3.2.2. A.3.2.3. A.3.2.5. (A.3.2.5.1., A3.2.5.2.) A.3.2.6. A.3.3.3.	DESVs are required to revalidate their PCI DSS scope every three months, as part of any organizational restructure, and following any significant change to the in-scope environment, systems or networks including the addition of new systems and network connections. This cannot be done efficiently without an effective data discovery solution. Advanced discovery solutions support remediation-in-place for data identified in cleartext, unauthorized and unexpected locations.

For the most comprehensive data discovery service tailored to the compliance requirements of PCI DSS, Ground Labs' Enterprise Recon PCI offers unbeatable performance across all major operating systems, server and database platforms, on-premises and cloud-hosted, as well as cloud storage and email service scanning capabilities. Remediation-in-place and robust reporting capabilities support the enhanced scoping and discovery requirements of the DESV in a flexible and lightweight solution.

Data Discovery for Assessors

As part of the assessment process, assessors have to verify the boundaries of the cardholder data environment and establish that their client has defined their scope for compliance correctly.

QSAs and ISAs often use scripts or RegExes to sample their clients' environments for rogue account data. The problem with these methods is that they are dependent on known patterns of data and defined network locations. Prone to false positives and – even worse in PCI DSS terms – false negatives, data discovery using scripts and RegExes is not robust enough to satisfy the updated requirements of PCI DSS 4.0.

Ground Labs' Card Recon offers QSA companies a cost-effective solution enabling QSAs to conduct comprehensive scope verification as part of the assessment process. Trusted by over 300 QSA companies worldwide, Card Recon is a portable, lightweight and unobtrusive data discovery tool designed for the payment card industry. Using Card Recon as part of the scope verification stage of an assessment will save assessors and their clients time and resources whatever the findings.

Industry-leading Data Discovery for PCI DSS from Ground Labs

Effective data discovery goes beyond scripted and RegEx searches, which are prone to false positives (and negatives) and typically exclude parts of the network or are incompatible with business systems. Advanced data discovery offerings such as Ground Labs' Enterprise Recon PCI and Card Recon Server edition provide remediation-in-place capabilities to help streamline compliance efforts.

ENTERPRISE RECON PCI

Ground Labs' Enterprise Recon PCI offers enterprise data discovery tailored for PCI DSS compliance. Powered by GLASS Technology™, Enterprise Recon provides fast, accurate results identifying account data from all major card brands.

To find out more and to book a demo, visit **groundlabs.com/enterprise-recon** ▶

CARD RECON

Ground Labs' Card Recon products are designed with small- and medium-sized organizations in mind. Coming in both Desktop and Server editions, Card Recon is a flexible and lightweight data discovery solution, developed specifically to support PCI DSS compliance.

To find out more and to book a demo, visit **groundlabs.com/card-recon** ▶

GROUND LABS

Established in 2007 and trusted by more than 4,500 companies in 85 countries, Ground Labs offers award-winning data discovery and management solutions for all industry sectors.

www.groundlabs.com

CONTACT:

US	**+1 737 212 8111**
UK	**+44 203 137 9898**
Ireland	**+353 1 903 9162**
Australia	**+612 8459 7092**
Asia	**+65 3133 3133**
Email	**info@groundlabs.com**

COPYRIGHT NOTICE

DOCUMENT LAST UPDATED:
APRIL 2023