GROUND LABS

A practical guide

Data discovery for PCI DSS compliance

CONTENTS

Introduction

PCI DSS v4.0.1 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.

Cardholder data discovery is no longer merely a pre-compliance activity reserved only to organizations starting out on their compliance journey. While discovery remains a fundamental tool for organizations undertaking compliance for the first time, it is now 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 the enterprise means they have more ways than ever before to conduct business.

Traditional networks have been replaced by software-defined networking and software-as-a-service (SaaS) offerings.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 to achieve and maintain compliance.

In total, data discovery has the potential to support 27 controls across four requirements of the latest version of PCI DSS.

This guide explains how data discovery can support your compliance process, whether you're a merchant, service provider or QSA. From initial scoping to incident response, data discovery scanning for PCI DSS offers visibility of account data across the digital estate for proactive, sustainable compliance.

Data discovery and PCI DSS

Data discovery directly supports 27 controls across four requirements of PCI DSS – 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.

Data discovery supports compliance across four PCI DSS requirements

Req 1. Install and maintain network security controls
Data discovery validates the network boundaries of scope and demonstrates data flows are up to date.

Req 3. Protect stored acccount data
Discovery scans identify cardholder data, including SAD, wherever it is stored. Periodic scans can confirm that data has been deleted when it has passed its retention period.

Req 6. Develop and maintain secure systems and software
Discovery scans verify that account data is not present in non-production environments.

Req 12. Support information security with 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 tech for PCI DSS

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 requirement.

With the enhancements of the most recent version of PCI DSS, 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	Data discovery scanning	Identity and access management	Malware protection	Log monitoring (SIEM)	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 without stored cardholder data, merchants can use periodic data discovery to support compliance with 14 PCI DSS controls.

Merchants must particularly be aware of incident response control 12.10.7., which requires 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.

SAQ type	Data discovery	Description
SAQ A	Yes	Verifying no cardholder data is stored in merchant systems
SAQ A-EP	Yes	Validating network boundaries, verifying no cardholder data is stored, confirming no live PAN present in non-production environments
SAQ B	No	
SAQ B-IP	Yes	Verifying no cardholder data is stored in merchant systems
SAQ C	Yes	Verifying no cardholder data is stored in merchant systems
SAQ C-VT	No	
SAQ D	Yes	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	Yes	Verifying no cardholder data is stored in merchant systems

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.

Periodic data discovery can help service providers meet their PCI DSS compliance obligations and, with advanced discovery solutions, remediation-in-place capabilities can help to address issues of non-compliance when these occur.

Requirement 1. Install and maintain network security controls

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 cardholder data

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

Data discovery can help in verifying that a significant change has not impacted scope boundaries, and that CHD is not present in non-production environments.

Requirement 12. Support information security with organizational policies and programs

Data discovery scanning can be used to confirm that operational procedures involving cardholder data are being followed so cardholder data is not leaking beyond the cardholder data environment (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 also support identification and remediation for account data in unexpected locations.

Data discovery for DESV organizations

The PCI Security Standards Council introduced the PCI DSS Designated Entities Supplemental Validation (DESV) in June 2015, as part of PCI DSS v3.1. 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 and continuously.

The latest version of PCI DSS 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.

DESV-eligible companies 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.

Data discovery for PCI QSAs

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

PCI QSAs and ISAs often use scripts to sample their clients' environments for rogue account data. The problem with these methods is that they rely on known patterns of data and defined network locations. Prone to inaccurate findings, script-based discovery is not robust enough to satisfy the latest PCI DSS requirements.

Industry-leading Data Discovery for PCI DSS from Ground Labs

For merchants: Ground Labs' Card Recon provides 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.

For service providers: 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 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.

For DESV organizations: 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.

For PCI QSAs: 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.

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.

groundlabs.com