Protecting Cardholder Data

How Cyera Supports PCI DSS Compliance

cyera

Table of Contents

Introduction 3

Build and Maintain a Secure Network and Systems 4

Protect Account Data 5

Maintain a Vulnerability Management Program 6

Implement Strong Access Control Measures 7

Regularly Monitor and Test Networks 8

Maintain an Information Security Policy 9

Introduction

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. Any business of any size must comply with PCI DSS if they store, process or transmit cardholder data. Compliance is validated annually or quarterly through a PCI assessment, a process that includes self-assessment questionnaires and network scans.

About Cyera

Cyera is a unified, AI-native data security platform that empowers organizations to discover, classify, and protect their most sensitive data—wherever it lives. Built for the cloud era, Cyera delivers real-time visibility, automated risk prioritization, and streamlined compliance at scale.

The platform's agentless, cloud-native design gives enterprises a comprehensive inventory of sensitive data across structured, unstructured, and semi-structured environments—including data lakes, SaaS applications, and AI training pipelines—without disrupting performance or requiring endpoint agents.

By combining data security posture management (DSPM) with data loss prevention (DLP) capabilities, Cyera helps security teams reduce their attack surface, enforce policies consistently, and respond to threats faster.

Introduction

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. Any business of any size must comply with PCI DSS if they store, process or transmit cardholder data. Compliance is validated annually or quarterly through a PCI assessment, a process that includes self-assessment questionnaires and network scans.

About Cyera

Cyera is a unified, AI-native data security platform that empowers organizations to discover, classify, and protect their most sensitive data—wherever it lives. Built for the cloud era, Cyera delivers real-time visibility, automated risk prioritization, and streamlined compliance at scale.

The platform's agentless, cloud-native design gives enterprises a comprehensive inventory of sensitive data across structured, unstructured, and semi-structured environments—including data lakes, SaaS applications, and AI training pipelines—without disrupting performance or requiring endpoint agents.

By combining data security posture management (DSPM) with data loss prevention (DLP) capabilities, Cyera helps security teams reduce their attack surface, enforce policies consistently, and respond to threats faster.

Build and Maintain a Secure Network and Systems

1. Install and Maintain Network Security Controls

PCI DSS Requirements	Cyera Capabilities
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Cyera's Identity Risk Graph provides a unified view of identities and their access to sensitive data across cloud environments. It maps human, machine, and non-human identities to the data they can access, helping you identify excessive permissions, dormant accounts, and risky access paths.
1.2 Network security controls (NSCs) are configured and maintained.	Cyera's Data Access Governance (DAG) enables you to set and enforce policies that restrict access to sensitive data based on user roles, data classifications, and compliance requirements. It integrates with your identity and access management (IAM) systems to automate policy enforcement.
1.3 Network access to and from the cardholder data environment is restricted.	Cyera's Data Access Governance (DAG) helps you limit unnecessary access to cardholder data by identifying and remediating overprivileged accounts. It provides recommendations for reducing access rights and integrates with your IAM systems to automate the process.
1.4 Network connections between trusted and untrusted networks are controlled.	Cyera's DSPM can discover and classify cardholder data wherever it resides, even in unexpected locations like shadow IT applications or misconfigured cloud storage. This helps you identify and secure all instances of cardholder data, reducing the risk of unauthorized access.
1.5 Risks to the CDE from computing devices able to connect to both untrusted networks and the CDE are mitigated.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.

2. Apply Secure Configurations to All System Components

PCI DSS Requirements	Cyera Capabilities
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Cyera's DSPM can discover misconfigurations in cloud storage services, databases, and other systems that could expose cardholder data. It provides alerts and recommendations for remediation, helping you maintain secure configurations.
2.2 System components are configured and managed securely.	Cyera's DSPM can identify and classify cardholder data wherever it resides, even in unexpected locations like shadow IT applications or misconfigured cloud storage. This helps you maintain an accurate inventory of cardholder data.
2.3 Wireless environments are configured and managed securely.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.

Protect Account Data

3. Protect Stored Account Data

PCI DSS Requirements	Cyera Capabilities
3.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Cyera's DSPM can discover and classify cardholder data wherever it resides, even in unexpected locations like shadow IT applications or misconfigured cloud storage. This helps you maintain an accurate inventory of cardholder data.
3.2 Storage of account data is kept to a minimum.	Cyera's DSPM automates data discovery and classification, helping you identify and remediate instances of cardholder data that are stored unnecessarily. This helps you minimize the amount of data you need to protect.
3.3 Sensitive authentication data (SAD) is not stored after authorization.	Cyera's DSPM can identify and classify SAD, helping you ensure that it is not stored after authorization. It can also provide alerts and recommendations for remediation.
3.4 Access to displays of full PANs and ability to copy PAN is restricted.	Cyera's Data Access Governance (DAG) enables you to restrict access to sensitive data, including cardholder data, based on user roles and permissions. This helps you minimize the risk of unauthorized access.
3.5 PAN is secured wherever it is stored.	Cyera can help you identify and classify cardholder data, but it does not provide encryption or tokenization capabilities. You will need to implement these separately.
3.6 Cryptographic keys used to protect stored account data are secured.	Cyera does not manage cryptographic keys. You will need to use a separate key management solution.
3.7 How key cryptographic events are managed is documented and included in all relevant processes.	Cyera does not manage cryptographic keys. You will need to use a separate key management solution.

4. Protect Cardholder Data with Strong Cryptography During Transmission over Open, Public Networks

PCI DSS Requirements	Cyera Capabilities
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.	Cyera discovers PAN and other sensitive data stored in cloud environments, helping you identify where cardholder data might be transmitted insecurely.
4.2 PAN is protected with strong cryptography during transmission.	Agent Auditor ensures that all data flow through approved channels, preventing unauthorized transmission of sensitive data.

Maintain a Vulnerability Management Program

5. Protect all Systems and Networks from Malicious Software

PCI DSS Requirements	Cyera Capabilities
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	While Cyera doesn't directly scan for malware, it can help you identify systems that may be vulnerable to malware attacks by discovering misconfigurations and unpatched software.
5.2 Malicious software (malware) is prevented, or detected and addressed.	Cyera can help you identify systems that may be vulnerable to malware attacks by discovering misconfigurations and unpatched software.
5.3 Anti-malware mechanisms and processes are active, maintained and monitored.	Cyera can help you identify systems that may be vulnerable to malware attacks by discovering misconfigurations and unpatched software.
5.4 Anti-phishing mechanisms protect users against phishing attacks.	Cyera can help you identify systems that may be vulnerable to phishing attacks by discovering misconfigurations and unpatched software.

6. Develop and Maintain Secure Systems and Software

PCI DSS Requirements	Cyera Capabilities
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	Cyera's DSPM and Shield AI can help you identify vulnerabilities in your systems and software, including those that could be exploited to gain access to cardholder data.
6.2 Bespoke and custom software are developed securely.	Cyera can help you identify vulnerabilities in your systems and software, including those that could be exploited to gain access to cardholder data.
6.3 Security vulnerabilities are identified and addressed.	Cyera's DSPM and Shield AI can help you identify vulnerabilities in your systems and software, including those that could be exploited to gain access to cardholder data.
6.4 Public-facing web applications are protected against attacks.	Cyera can help you identify vulnerabilities in your systems and software, including those that could be exploited to gain access to cardholder data.
6.5 Changes to all system components are managed securely.	Cyera can help you identify vulnerabilities in your systems and software, including those that could be exploited to gain access to cardholder data.

Implement Strong Access Control Measures

7. Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS Requirements	Cyera Capabilities
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Cyera's Identity Risk Graph provides a unified view of identities and their access to sensitive data across cloud environments. It maps human, machine, and non-human identities to the data they can access, helping you identify excessive permissions, dormant accounts, and risky access paths.
7.2 Access to system components and data is appropriately defined and assigned.	Cyera's Data Access Governance (DAG) enables you to set and enforce policies that restrict access to sensitive data based on user roles, data classifications, and compliance requirements. It integrates with your identity and access management (IAM) systems to automate policy enforcement.
7.3 Access to system components and data is managed via an access control system(s).	Cyera's Data Access Governance (DAG) helps you limit unnecessary access to cardholder data by identifying and remediating overprivileged accounts. It provides recommendations for reducing access rights and integrates with your IAM systems to automate the process.

8. Identify Users and Authenticate Access to System Components

PCI DSS Requirements	Cyera Capabilities
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	Cyera's Identity Risk Graph provides a unified view of identities and their access to sensitive data across cloud environments. It maps human, machine, and non-human identities to the data they can access, helping you identify excessive permissions, dormant accounts, and risky access paths.
8.2 User identification and related accounts for users and administrators are strictly managed throughout the user account lifecycle.	Cyera can help you identify dormant accounts with access to cardholder data, which can be a security risk. It provides recommendations for disabling or removing these accounts.
8.3 Strong authentication for users and administrators is established and managed.	Cyera's Data Access Governance (DAG) enables you to set and enforce policies that require strong authentication for access to sensitive data. It integrates with your identity and access management (IAM) systems to automate policy enforcement.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	Cyera's Identity Risk Graph can help you identify accounts that are not using MFA, which can be a security risk. It provides recommendations for enabling MFA on these accounts.
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	Cyera can help you identify accounts that are not using MFA, which can be a security risk. It provides recommendations for enabling MFA on these accounts.
8.6 Use of application and system accounts and associated authentication factors is strictly managed.	Cyera's Identity Risk Graph can help you identify and manage application and system accounts, which can be a security risk. It provides recommendations for reducing access rights and integrates with your IAM systems to automate the process.

9. Restrict Physical Access to Cardholder Data

Cyera does not provide physical access controls.

Regularly Monitor and Test Networks

10. Log and Monitor All Access to System Components and Cardholder Data

PCI DSS Requirements	Cyera Capabilities
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	Cyera continuously monitors your data security posture, including access to sensitive data. It can help you identify and investigate suspicious activity that may indicate a breach.
10.2 Audit logs are implemented to support detection of anomalies and suspicious activity, and forensic analysis of events.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
10.3 Audit logs are protected from destruction and unauthorized modifications.	Cyera's Data Access Governance (DAG) helps you restrict access to sensitive data, including audit logs, based on user roles and permissions. This helps you prevent unauthorized modification or deletion of audit logs.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
10.5 Retention of audit log history is kept to support immediate analysis and provide assistance as needed.	Cyera's Data Access Governance (DAG) helps you restrict access to sensitive data, including audit logs, based on user roles and permissions. This helps you prevent unauthorized modification or deletion of audit logs.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.

11. Test Security of Systems and Networks Regularly

PCI DSS Requirements	Cyera Capabilities
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.	Cyera offers ongoing discovery that can help you maintain an accurate inventory of your cardholder data environment.
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Cyera's DSPM can identify and classify cardholder data wherever it resides, even in unexpected locations like shadow IT applications or misconfigured cloud storage. This helps you maintain an accurate inventory of cardholder data.
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.
11.5 Network intrusions and unexpected file changes are detected and responded to.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.
11.6 Unauthorized changes on payment pages are detected and responded to.	Cyera's DSPM can monitor network traffic to and from cardholder data environments, detecting anomalous activity that may indicate a breach. It can also integrate with existing network security tools to provide a more comprehensive view of network traffic.

Support Information Security with Organizational Policies and Programs

12. Support Information Security with Organizational Policies and Programs

PCI DSS Requirements	Cyera Capabilities
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	Cyera's DSPM can help you identify and classify cardholder data, which is a key component of your information security policy. It can also help you monitor for unauthorized access to this data.
12.2 Acceptable use policies for end-user technologies are defined and implemented.	Cyera's Data Access Governance (DAG) enables you to set and enforce policies that restrict access to sensitive data based on user roles, data classifications, and compliance requirements. It integrates with your identity and access management (IAM) systems to automate policy enforcement.
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.	Cyera's DSPM can help you identify and classify cardholder data, which is a key component of your risk assessment process. It can also help you monitor for unauthorized access to this data.
12.4 PCI DSS compliance is managed.	Cyera can help you identify and classify cardholder data, which is a key component of your PCI DSS compliance program. It can also help you monitor for unauthorized access to this data.
12.5 PCI DSS scope is documented and validated.	Cyera can help you identify and classify cardholder data, which is a key component of your PCI DSS scope. It can also help you monitor for unauthorized access to this data.
12.6 Security awareness education is an ongoing activity.	Cyera can help you identify and classify cardholder data, which is a key component of your security awareness education program. It can also help you monitor for unauthorized access to this data.
12.7 Personnel are screened to reduce risks from insider threats.	Cyera can help you identify and classify cardholder data, which is a key component of your personnel screening process. It can also help you monitor for unauthorized access to this data.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	Cyera's Identity Risk Graph can help you identify and manage third-party access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Cyera's Data Access Governance (DAG) helps you restrict access to sensitive data, including data accessed by third-party service providers, based on user roles and permissions. This helps you minimize the risk of unauthorized access.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.

12. Support Information Security with Organizational Policies and Programs

PCI DSS Requirements	Cyera Capabilities
12.10.1 An incident response plan exists and is ready to activate in the event of a suspected or confirmed incident.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.2 At least once every 12 months, the security incident response plan is reviewed and the content is updated as needed.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed incidents.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.4 Personnel responsible for handling suspected or confirmed incidents are appropriately and periodically trained.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.5 The incident response plan includes monitoring and responding to alerts from security monitoring systems.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.6 The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.
12.10.7 Incident response procedures are in place to address the storage of PAN anywhere it is detected.	Cyera's Identity Risk Graph can help you identify and investigate suspicious activity related to user access to sensitive data. It provides a timeline of events and integrates with your SIEM system.