



Qualys PCI DSS

Compliance Playbook














July 28, 2025

Copyright 2025 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Document Version History	5
Overview	6
Importance of PCI-DSS Compliance	6
Preparation for PCI Compliance	6
Analyze PCI DSS 4.0 Requirements	7
Review your Organization's Security Posture	7
Gap analysis	8
Implement Solution.....	8
Qualys Solution for PCI Compliance	9
Setup Qualys Security Solution.....	9
Step – 1: Create a Qualys User Account	9
Step – 2: Install Cloud Agent and Scanners.....	9
Step – 3: Configuration	10
Protect your Assets and Network.....	12
 Qualys Vulnerability Management, Detection, and Response (VMDR).....	12
 Continuous Monitoring (CM)	13
 Policy Compliance (PC)	13
 File Integrity Monitoring (FIM).....	13
 Web Application Scanning (WAS).....	14
 Endpoint Detection and Response (EDR).....	14
 Security Configuration Assessment (SCA).....	14
 Patch Management (PM).....	15
 Unified Dashboard (UD).....	15
 Security Assessment Questionnaire (SAQ).....	15
 Custom Assessment and Remediation (CAR)	16
 Certificate View.....	16
 Administration	16



Qualys TotalCloud	17
-------------------------	----

PCI Compliance Support	18
-------------------------------------	-----------

PCI DSS Requirement 1	18
PCI Compliance Support for Requirement 1	19
PCI DSS Requirement 2	20
PCI Compliance Support for Requirement 2	20
PCI DSS Requirement 3	21
PCI Compliance Support for Requirement 3	22
PCI DSS Requirement 4	23
PCI Compliance Support for Requirement 4	24
PCI DSS Requirement 5	24
PCI Compliance Support for Requirement 5	25
PCI DSS Requirement 6	26
PCI Compliance Support for Requirement 6	27
PCI DSS Requirement 7	28
PCI Compliance Support for Requirement 7	29
PCI DSS Requirement 8	30
PCI Compliance Support for Requirement 8	31
PCI DSS Requirement 9	32
PCI DSS Requirement 10	33
PCI Compliance Support for Requirement 10	34
PCI DSS Requirement 11	35
PCI Compliance Support for Requirement 11	36
PCI DSS Requirement 12	38
PCI Compliance Support for Requirement 12	39

Document Version History

Release Version	Release Date	Change Description
4.0.0	July 30, 2024	Initial Draft
4.0.0	February 04, 2025	<p>The document is updated with the following changes</p> <ul style="list-style-type: none">• Section – Requirement 12<ul style="list-style-type: none">- Added new requirement 12.3.3 in the compliance support diagram- Added new requirement 12.3.3 in the compliance support diagram
4.0.1	July 28, 2025	<p>The document is updated with the following changes</p> <ul style="list-style-type: none">• Section – Overview<ul style="list-style-type: none">- Updated the heading from Importance of PCI-DSS 4.0 to Importance of PCI-DSS Compliance• Section – Requirement 6<ul style="list-style-type: none">- Added new requirement 6.4.3 in the compliance support diagram- Added new requirement 6.4.3 in the compliance support table• Section – Requirement 11<ul style="list-style-type: none">- Added new requirement 11.6.1 in the compliance support diagram- Added new requirement 11.6.1 in the compliance support table

Overview

The Payment Card Industry Security Standard Council (PCI-SSC) has mandated that all organizations and entities handling, processing, and transferring cardholder data comply with the PCI Data Security Standard 4.0 (PCI-DSS 4.0).

PCI-DSS 4.0 is the latest version of the series, which focuses on evolving security threats and technology. The standard also defines the operational and technical requirements to protect the cardholder's data.

The affected organizations are required to implement these requirements in two phases:

- **Immediate requirements:** Implement by 31st March 2024.
- **Additional best practices:** Implement by 31st March 2025.

Importance of PCI-DSS Compliance

Compliance with the PCI DSS requirements ensures that:

1. Your organization has best security practices in place to protect cardholder's data.
2. Boost the brand image of your business.
3. It acts as a baseline for your security program.
4. Ensures that your business does not attract any federal penalties due to non-compliance.

Preparation for PCI Compliance

The following are the steps to achieve PCI compliance for your organization.

1. [Analyze PCI DSS 4.0 Requirements](#)
2. [Review your Organization's Security Posture](#)
3. [Gap Analysis](#)
4. [Implement Solution](#)

Analyze PCI DSS 4.0 Requirements

Let us now check the main requirements you must meet to achieve PCI DSS compliance.

PCI DSS 4.0 Goals	PCI DSS 4.0 Requirements
Build and maintain a secure network and systems	1. Install and maintain network security controls
	2. Apply secure configurations to all system components
Protect account data	3. Protect stored account data
	4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a Vulnerability Management program	5. Protect all systems and networks from malicious software
	6. Develop and maintain secure systems and software
Implement strong access control measures	7. Restrict access to system components' cardholder data by business need
	8. Identify users and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data
	11. Test security systems and networks regularly
Maintain an information security policy	12. Support information security with policies and programs

Identify the requirements applicable to your organization. For more information about PCI DSS requirements, refer to the [PCI DSS V4.0 Standard](#).

Review your Organization's Security Posture

Following are the steps to review the security posture of your organization:

1. **Define the security requirements:** Clearly define the security requirements for your organization according to business needs.
2. **Test the security controls:** Test the security policies and controls to ensure that they meet the security requirements.
3. **Identify the security risks:** Perform security scans on all of your assets to identify security risks.

4. **Generate a security posture report:** You should document all your security posture findings for the planned actions and future reference.

Gap analysis

Once you review your organization's security posture, compare the findings of your security posture report with the PCI-DSS 4.0 requirements. This analysis will help you identify gaps and required improvements to meet the PCI-DSS requirements.

Implement Solution

Based on your gap analysis, find the vendor or develop a solution measure internally to meet the PCI DSS requirements.

The following section describes how you can meet the various PCI DSS requirements using Qualys applications.

Qualys Solution for PCI Compliance

The integrated Qualys application suite contains over 20 applications designed to monitor and protect your assets against any possible risk. This section describes the role of different Qualys applications in PCI DSS compliance and the procedure to set up Qualys solutions for your organization.

Setup Qualys Security Solution

The following are the steps to set up Qualys Security Solution for your organization.

Step - 1: Create a Qualys User Account

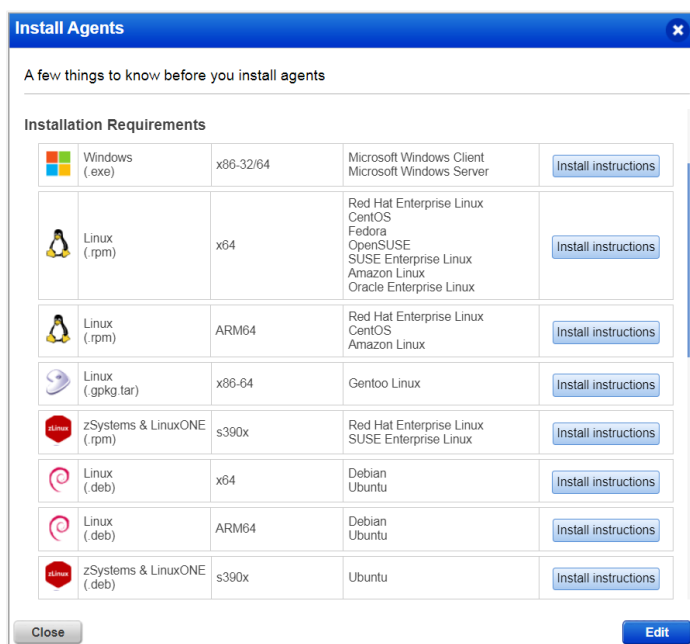
1. Sign up at <https://www.qualys.com> to create a new user account. If you already have an account, log in to the Qualys cloud platform using your Qualys credentials.
2. You must have all the required licenses to start using the Qualys applications. If you do not have the required licenses, contact your Qualys representative.

Step - 2: Install Cloud Agent and Scanners

The Cloud Agents and Scanners help you build the inventory of your assets. It also establishes a connection with the Qualys Cloud Platform and uploads asset data.

Install Qualys Cloud Agent

1. In the Qualys user account, open the Cloud Agent application.
2. From the Cloud Agent UI, download the Cloud Agent installer package based on the system architecture of the host.

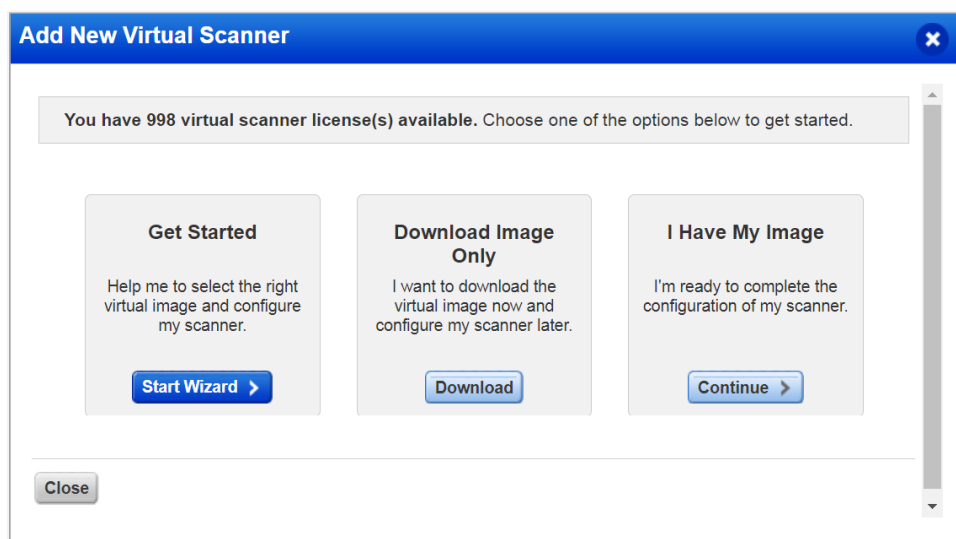


3. Install the Cloud Agent on the required assets. The Cloud Agent UI gives detailed steps for Cloud Agent installation.
4. To learn more about Cloud Agent, refer to [Qualys Cloud Agent Online Help](#).

Scanner Appliance Deployment

You also need to deploy the scanner appliances to get a holistic view of your asset inventory. The following are the steps to deploy scanner appliances.

1. From the scanner appliances UI, Install the scanner appliance in your network.
2. Configure the network settings and ensure that the scanner is connected to Qualys Cloud Platform.



3. To learn more about Scanner Appliances, refer to the [Scanner Appliance User Guide](#) and [Virtual Scanner Appliance User Guide](#).

Step - 3: Configuration

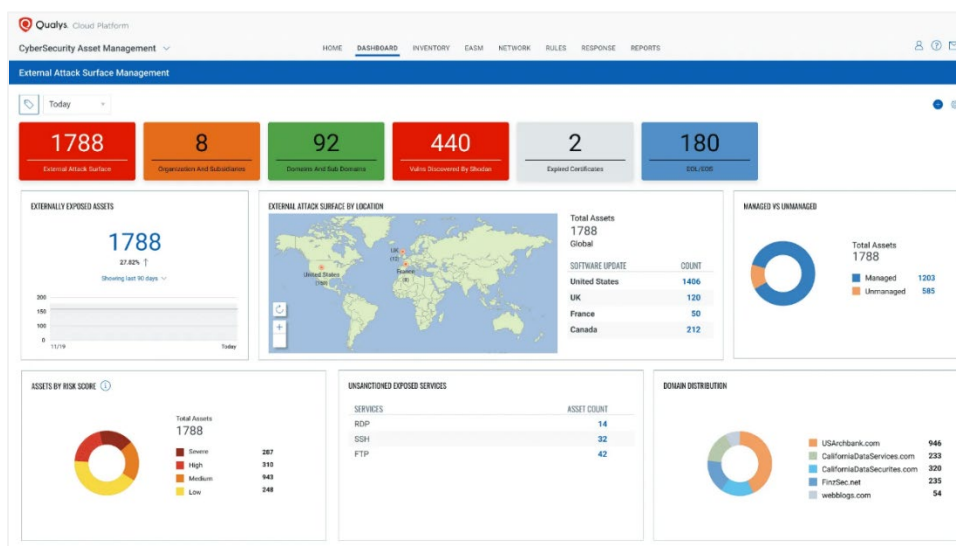
The next step is to configure your account and build asset inventory, create configuration profiles, and apply these profiles to assets. Following are the important sub-steps for this step.

Asset Management

The CSAM dashboard provides an overview of your asset inventory. To manage it, go to the Global AssetView application and start categorizing assets according to your requirements.

Perform the following steps to start with asset management.

1. Categorize the assets and tag them based on criteria like function, location, and importance.
2. Set up the asset groups for scanning and reporting.



3. To learn more about asset management, refer to the [CSAM Online Help](#) and [Global AssetView Online Help](#).

Create Configuration Profiles

The option to create a configuration profile is available on the Cloud Agent UI.

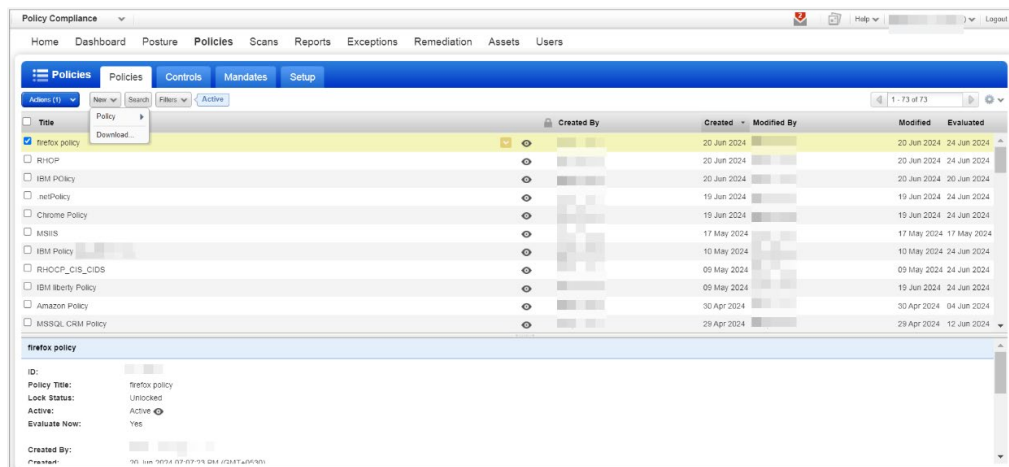
1. Create the configuration profiles with different scan configurations.

The screenshot shows the 'Create New: Configuration Profile' form. It has a sidebar with steps 1 through 8, with '1 Basic Details' currently selected. The main form area is titled 'Basic Details' and includes a description: 'Provide basic information for the configuration profile to manage Cloud Agent behavior.' There are two input fields: 'Profile Name' and 'Description'. Below these is a section for 'Additional Settings' with four checkboxes: 'Make this the default profile for the subscription', 'Suspend data collection for VM, PC, SCA and inventory for all agents using this profile', 'In-Memory SQLite Databases', and 'Enable QGS'. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

2. Apply these configuration profiles to the assets using their tags and groups.
3. To learn more about creating configuration profiles, refer to the [Create Configuration Profile](#).

Create Policy Compliance Scan Profile

1. In the Policy Compliance application, define the rules based on your requirements.
2. Apply these Policy Compliance profiles to assets using tags.



3. To learn more about the PC, refer to the [Policy Compliance Online Help](#).

Protect your Assets and Network

Once you set up the Qualys Security solution, the next step is to ensure that your networks and assets are continuously secured. The following applications help you protect your networks and assets.

VMDR Qualys Vulnerability Management, Detection, and Response (VMDR)

You can use the following VMDR functions to protect your assets and network:

- Qualys VMDR gives you a collective view of all the vulnerabilities; you can set up the prioritization rules and responses for these vulnerabilities.
- VMDR maps all assets on your network with details such as Operating Systems (OS), ports, services and certificates, and scans them for vulnerabilities.
- VMDR also assigns remediation tickets, manages exceptions, lists patches for each host, and integrates with existing IT ticketing systems to remediate the detected vulnerabilities effectively.
- VMDR generates comprehensive reports to document the network status. You can integrate these reports with other security and compliance systems using VM APIs.

To learn more about Qualys VMDR, refer to [Qualys VMDR Online Help](#).

CM

Continuous Monitoring (CM)

You can use the following Qualys CM functions to continuously monitor your assets and network:

- Qualys Continuous Monitoring (CM) watches your global network from the cloud and generates targeted alerts to notify the appropriate stakeholders of potential risks.
- With CM, you can monitor your on-premises systems, mobile devices, and public cloud instances.
- You can also configure the rules for alerts to accommodate different conditions, entities, and recipients.

To learn more about Qualys CM, refer to [Qualys Continuous Monitoring Online Help](#).

**PC
SCA**

Policy Compliance (PC)

You can use the following Qualys PC functions to define the policy compliance rules:

- Qualys Policy Compliance (PC) is a single platform for complete policy compliance.
- It reduces the risk of security breaches and misconfigurations.
- Qualys PC ensures that all the network components are securely configured and compliant with industry-accepted standards.

To learn more about Qualys PC, refer to [Qualys Policy Compliance Online Help](#).

GAV

File Integrity Monitoring (FIM)

You can use the following Qualys FIM functions to protect your assets and network:

- Qualys File Integrity Monitoring (FIM) monitors integrity violations and compliance across your global IT systems.
- It helps you eliminate alert noise and prioritize the most critical incidents, changes, and malicious events.
- FIM includes File Access Monitoring (FAM) to trigger alerts when critical host files are accessed. With its agentless network support, FIM generates alerts when any network configuration deviation is noticed.
- FIM also has pre-configured monitoring profiles to comply with PCI-DSS 4.0 and other compliance standards.

To learn more about Qualys FIM, refer to [Qualys File Integrity Monitoring Online Help](#).

WAS

Web Application Scanning (WAS)

You can use the following Qualys WAS functions to protect your web applications:

- Qualys Web Application Scanning (WAS) tool helps you minimize risks and reduce the attack surface for modern web applications and APIs.
- It uncovers runtime vulnerabilities, OWASP top 10, misconfigurations, PII exposures, and web malware and provides quick remediation steps.

To learn more about Qualys WAS, refer to [Qualys Web Application Scanning Online Help](#).

EDR

Endpoint Detection and Response (EDR)

You can use the following Qualys EDR functions to protect endpoints in your network:

- EDR monitors endpoints for suspicious activity and potential threats.
- It provides real-time detection and response to protect endpoints against malignant software.

To learn more about Qualys EDR, refer to [Qualys Endpoint Detection and Response Online Help](#).

PC
SCA

Security Configuration Assessment (SCA)

You can use the following Qualys SCA functions to protect your assets and network:

- Qualys Security Configuration Assessment (SCA) allows you to assess, report, monitor, and remediate security-related issues based on the Center for Internet Security (CIS) benchmarks.
- With SCA, you can continuously check if your IT assets are configured securely as per CIS guidelines.
- SCA not only serves as a security configuration tool but also helps you comply with standards like PCI-DSS, HIPPA, and others.

To learn more about Qualys SCA, refer to [Qualys Security Configuration Assessment Online Help](#).

PM

Patch Management (PM)

You can use the following Qualys PM functions to keep your assets updated:

- You can deploy the patches using PM to ensure that your systems and networks are updated.
- You can also create the Patch Jobs, select patches, and select assets to deploy patches.

To learn more about Qualys PM, refer to [Qualys Patch Management Online Help](#).

UD

Unified Dashboard (UD)

You can use the following Qualys UD functions to view the security compliance posture:

- UD provides a consolidated view of an organization's security and compliance posture.
- It integrates data from various Qualys modules into customizable dashboards, offering real-time insights and visualizations.
- You can track key metrics, monitor vulnerabilities, and assess compliance status from a single interface.

To learn more about Qualys UD, refer to [Qualys Unified Dashboard Online Help](#).

SAQ

Security Assessment Questionnaire (SAQ)

Qualys SAQ offers you the following functions:

- SAQ streamlines and automates the process of conducting security assessments and compliance surveys.
- You create, distribute, and analyze questionnaires to gather information about security practices, compliance status, and risk management from internal teams, partners, and vendors.
- SAQ helps ensure thorough and consistent assessments, supports regulatory compliance, and aids in identifying and mitigating security risks through comprehensive data collection and analysis.

To learn more about Qualys SAQ, refer to [Qualys Security Assessment Questionnaire Online Help](#).

CAR**Custom Assessment and Remediation (CAR)**

Qualys CAR offers you the following functions to manage security and compliance assessments.

- CAR allows you to create and automate custom security and compliance assessments and remediation workflows.
- It helps to define specific security checks, generate detailed reports, and automate remediation tasks tailored to their unique environment and requirements.
- CAR helps improve security posture by providing real-time visibility and control over security configurations and vulnerabilities across various assets.

To learn more about Qualys CAR, refer to [Qualys Custom Assessment and Remediation Online Help](#).

CERT**Certificate View**

Qualys Certificate View offers you the following functionalities to manage certificates:

- Certificate View provides comprehensive visibility and management of digital certificates across an organization's IT environment.
- It helps identify, track, and monitor SSL/TLS certificates to ensure they are properly configured and not expired.
- Certificate View offers automated scanning, detailed reporting, and alerts to help maintain a secure and compliant certificate infrastructure.

To learn more about Qualys Certificate View, refer to [Qualys Certificate View Online Help](#).

ADMIN**Administration**

Qualys Administration offers the following functions for system management:

- Qualys Administration helps you manage user access, roles, and permissions across the Qualys Cloud Platform.
- It allows administrators to configure and control security settings, assign user roles, manage assets, and monitor platform usage.
- Qualys Admin helps ensure secure and efficient platform management and facilitates the enforcement of security policies and compliance requirements within an organization.

To learn more about Qualys Administration, refer to [Qualys Administration Online Help](#).

Qualys TotalCloud offers the following functions to protect your assets and network:

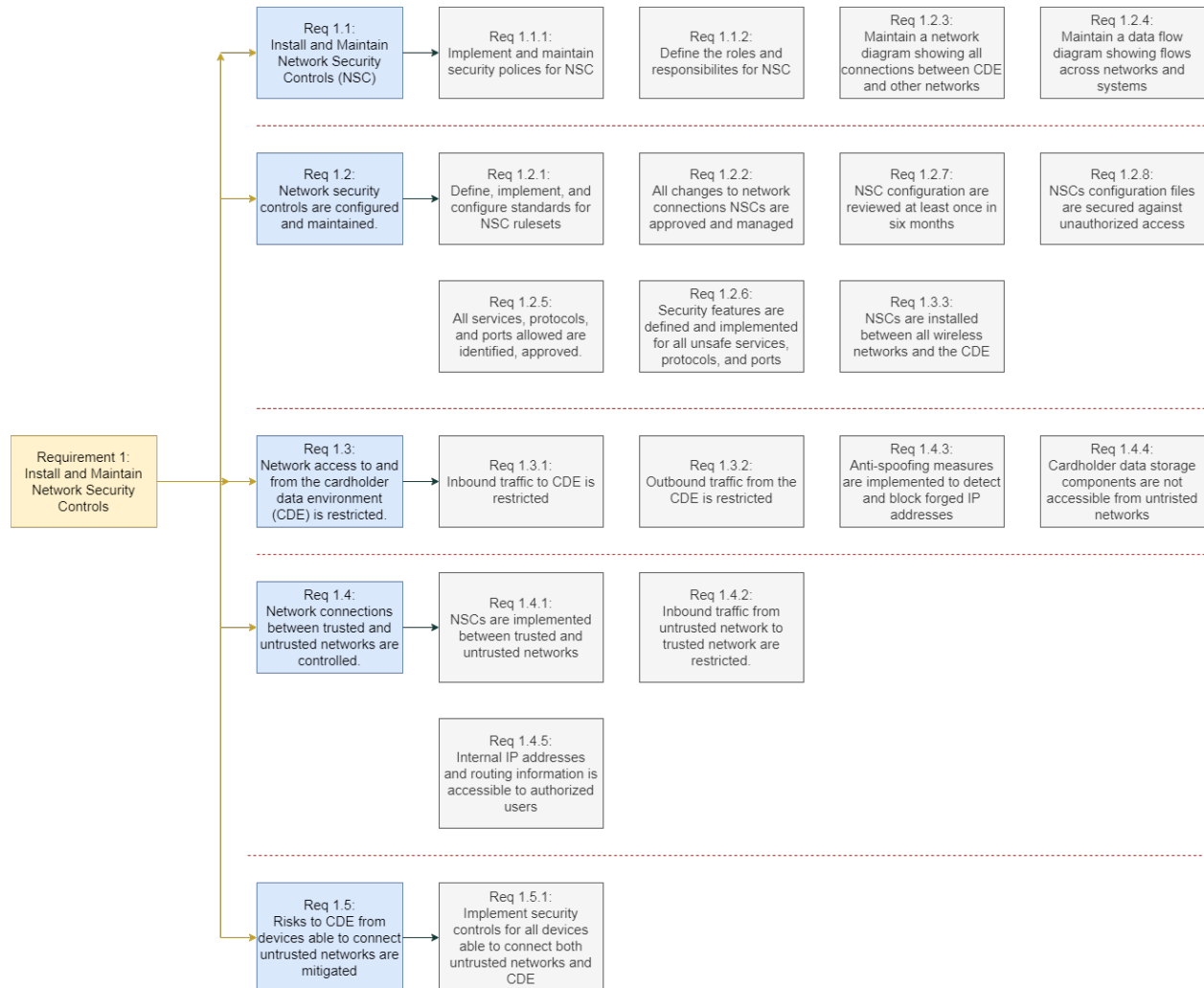
- Qualys TotalCloud is a comprehensive cloud security solution designed to provide visibility, compliance, and protection for cloud environments.
- It integrates with various cloud platforms to offer real-time monitoring, vulnerability management, and compliance checks.
- TotalCloud helps you secure your cloud infrastructure by detecting misconfigurations, identifying vulnerabilities, and ensuring compliance with industry standards.
- It simplifies cloud security management with automated workflows and centralized controls, enhancing the overall security posture of cloud assets.

To learn more about Qualys Total Cloud, refer to [Qualys TotalCloud Online Help](#).

PCI Compliance Support

PCI DSS Requirement 1

Install and maintain network security controls: It is important to establish and maintain a secure network infrastructure that protects cardholders' data from unauthorized access, controls connections between trusted and untrusted networks, and mitigates risks posed by devices that can connect to both the untrusted networks and Cardholder Data Environment (CDE).



Qualys Solution for Requirement 1

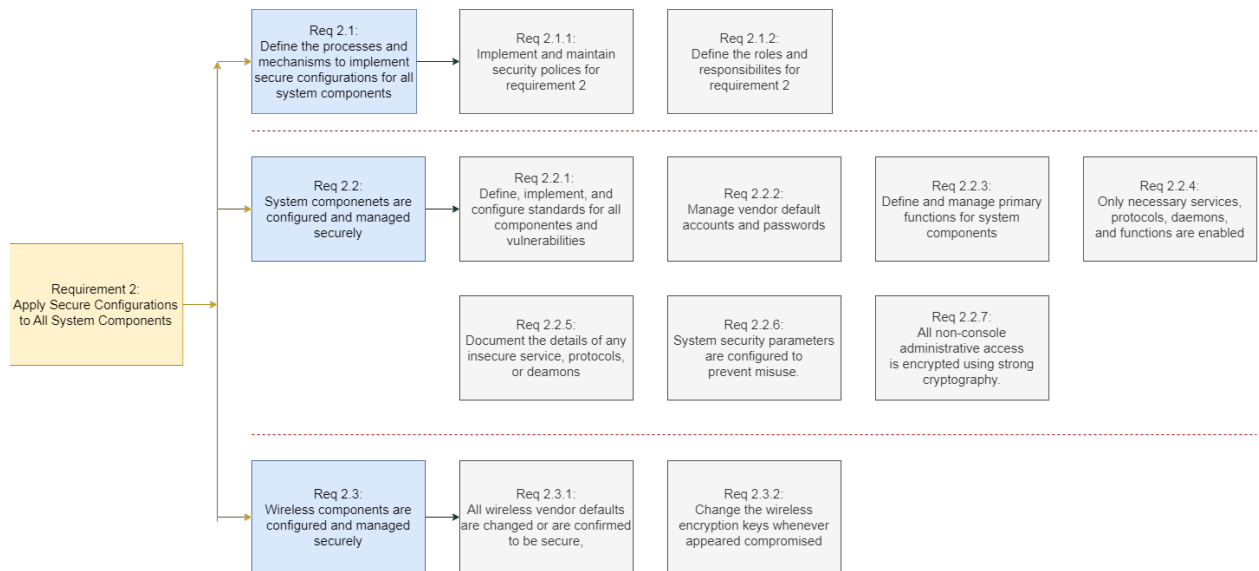
VMDR, CM, PC, FIM, EDR, SCA, PM, UD, GAV, CSAM

PCI Compliance Support for Requirement 1

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
1.2.1	✓								✓			
1.2.2			✓		✓							
1.2.6	✓		✓		✓	✓			✓			
1.2.8		✓	✓								✓	
1.3.1		✓	✓		✓				✓			
1.3.2		✓			✓						✓	
1.3.3		✓			✓				✓			
1.4.1		✓	✓		✓				✓			
1.4.2		✓			✓							
1.4.3	✓	✓			✓				✓			
1.4.4		✓	✓		✓				✓			
1.4.5		✓	✓								✓	
1.5.1	✓	✓	✓		✓	✓	✓	✓	✓		✓	

PCI DSS Requirement 2

Apply secure configurations to all system components: Implement secure configurations for all your system components and wireless environments to prevent malicious actors from exploiting the persistent weaknesses of default system configurations.



Qualys Solution for Requirement 2

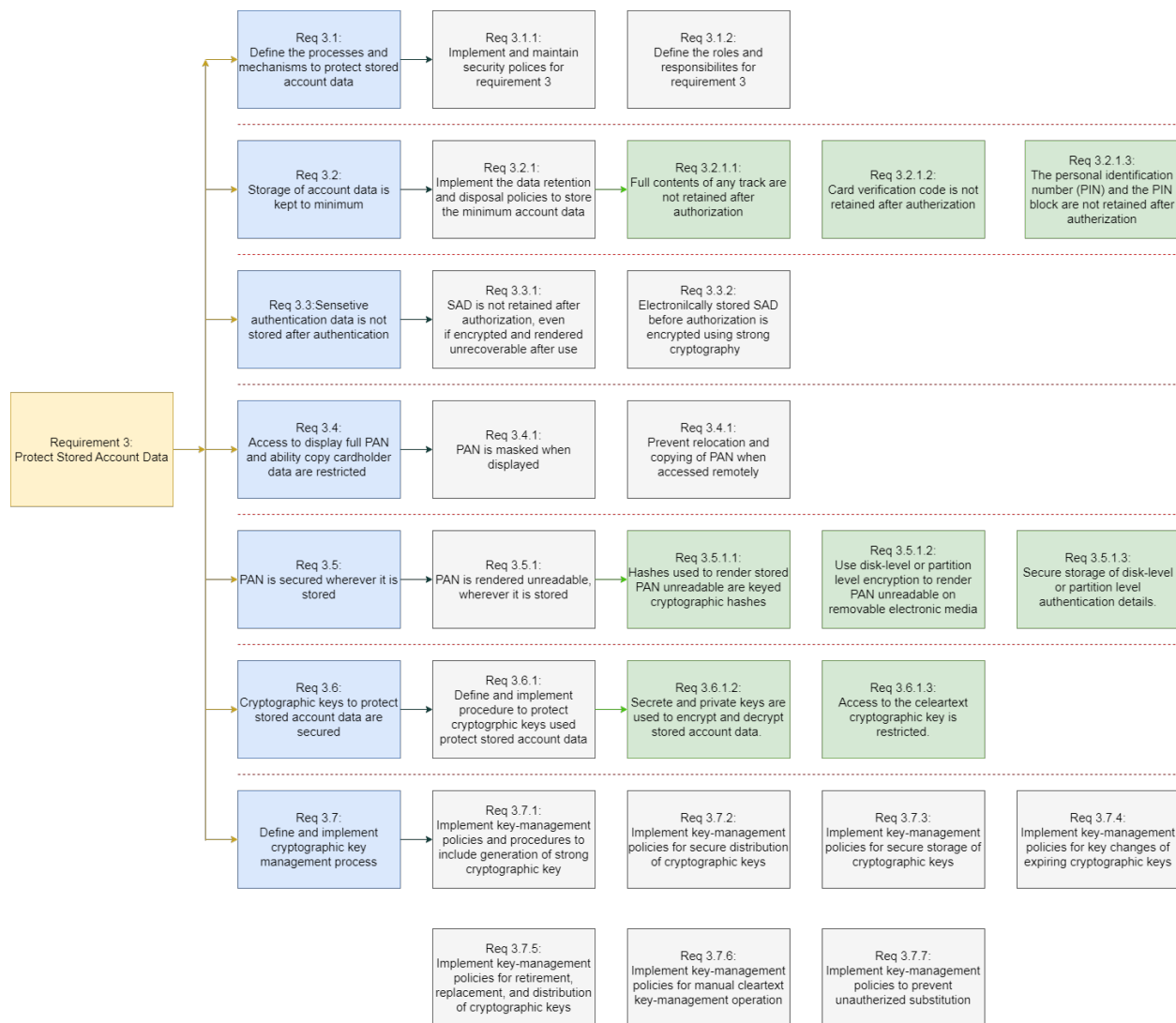
VMDR, CM, PC, FIM, WAS, EDR, SCA

PCI Compliance Support for Requirement 2

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
2.2.1	✓	✓							✓		✓	
2.2.2	✓	✓	✓								✓	
2.2.3		✓									✓	
2.2.4		✓									✓	
2.2.6		✓	✓						✓			
2.2.7			✓		✓						✓	
2.3.2		✓									✓	

PCI DSS Requirement 3

Protect stored account data: Implement measures to minimize storing account data, remove sensitive authentication data (SAD), restrict access to cardholder data, encrypt, truncate, and tokenize it to ensure security for cardholder data.



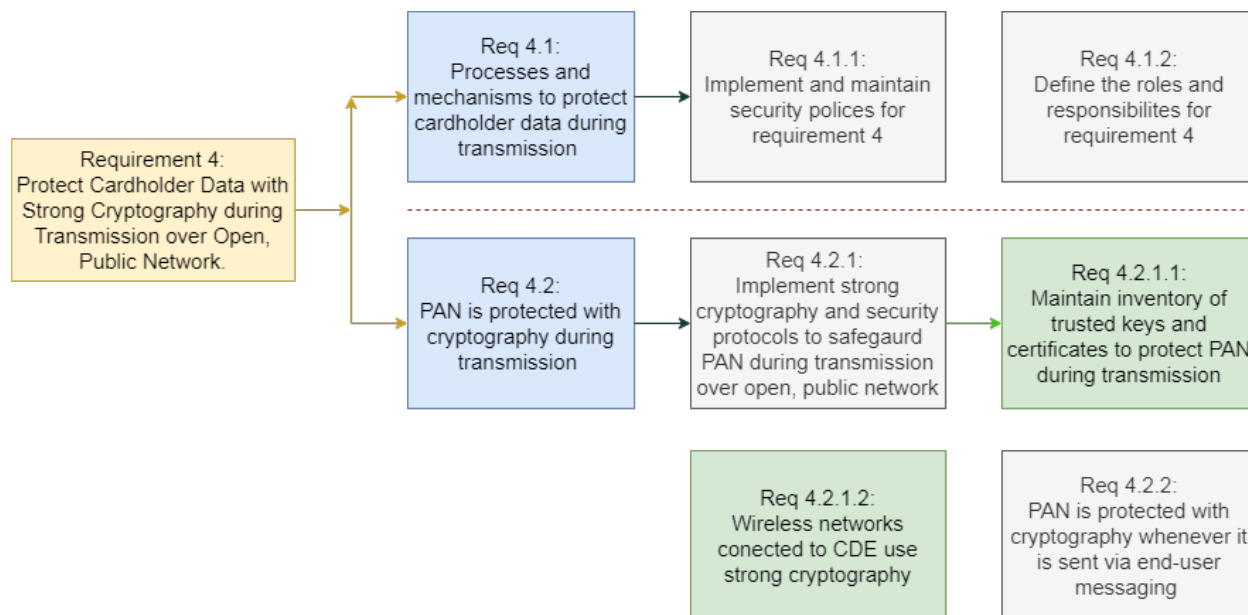
- Qualys employs strong security measures to protect the stored data against unauthorized access, security breaches, and other security threats.
- Data stored within the Qualys Cloud Platform is encrypted using the Advanced Encryption Standard (AES) with a 256-bit key.
- Qualys also employs methods like secure key storage using Hardware Security Modules (HSM), role-based access control, multi-factor authentication, separation of data environments, network segmentation, and continuous monitoring and auditing.

PCI Compliance Support for Requirement 3

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	CertView	WAS
3.2.1	✓								✓			
3.2.1.1		✓										
3.2.1.2		✓										
3.2.1.3			✓									
3.3.1		✓										
3.3.2		✓	✓									
3.4.2		✓	✓									
3.5.1		✓										
3.5.1.2		✓										
3.5.1.3			✓				✓	✓	✓			
3.6.1.2			✓									
3.7.1		✓										
3.7.2			✓									
3.7.3			✓									
3.7.4			✓									
3.7.5		✓										
3.7.7			✓									

PCI DSS Requirement 4

Protect cardholder data with strong cryptography during transmission over open, public networks: Ensure that cardholder data is protected with strong cryptography over an open and public network.



- Qualys employs comprehensive data encryption practices to secure data in transit and at rest.
- For data in transit, Qualys uses Transport Layer Security (TLS) and HTTPS to protect data transferred from your assets and applications to Qualys Cloud Platform. TLS uses strong encryption protocols and algorithms, such as Advanced Encryption Standard (AES) with 256-bit key.
- Data stored within Qualys Cloud Platform is protected with AES-256, ensuring high-level security.
- Qualys also employs robust key management practices to generate, store, and protect encryption keys.
- In addition to these encryption methods, Qualys implements additional security measures such as access control, data segmentation, and continuous monitoring.

Qualys Solution for Requirement 4

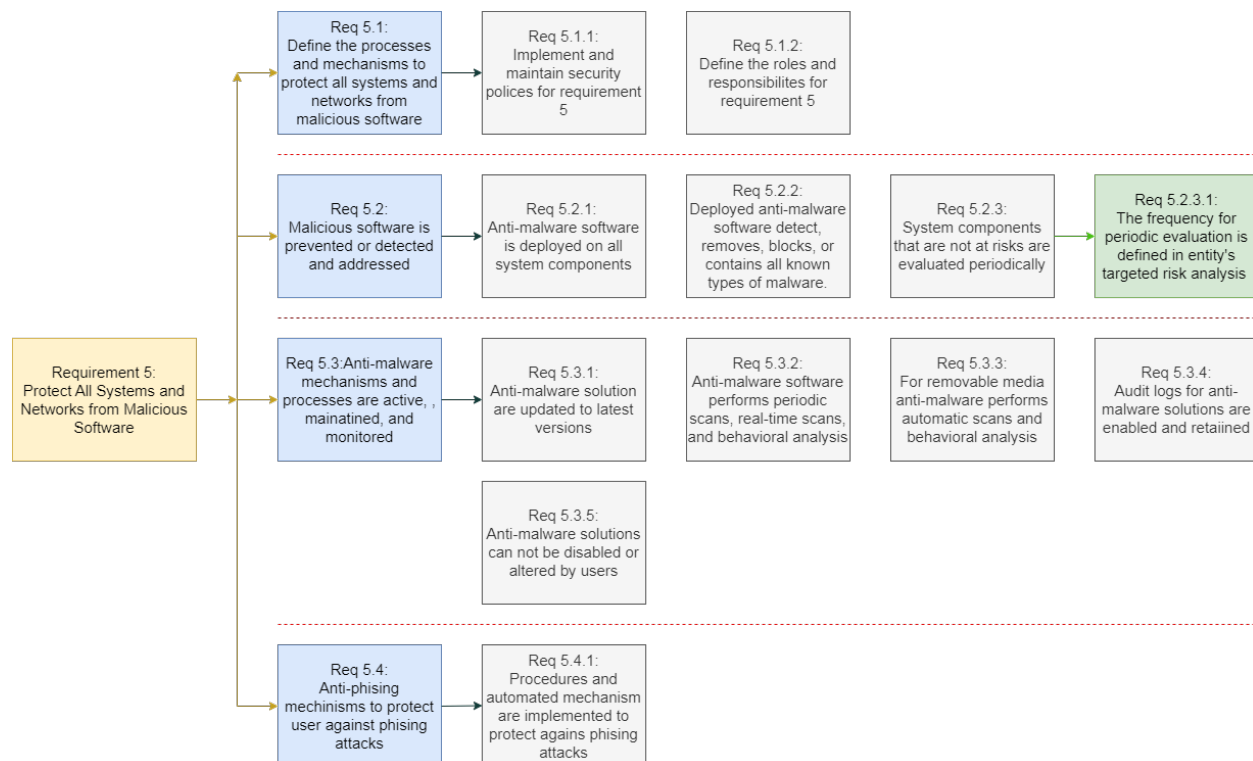
PC, EDR, CertView

PCI Compliance Support for Requirement 4

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	CertView	WAS
4.2.1		✓			✓						✓	
4.2.1.1											✓	
4.2.1.2		✓			✓							
4.2.2		✓			✓							

PCI DSS Requirement 5

Protect all systems and networks from malicious software: You must have clearly defined processes and mechanisms to protect your systems and networks against malware, phishing attacks, and other security threats. It is also important to continuously monitor and maintain these processes to provide protection against evolving threats.



Qualys provides comprehensive protection for your systems and network against malicious software through an integrated Cloud Platform service. To learn more, check out the following points.

- Qualys employs **malware detection** capabilities to scan for known malicious software on endpoints and servers.
- **Qualys threat intelligence** keeps your systems protected against the latest malware trends and threats.

Qualys Solution for Requirement 5

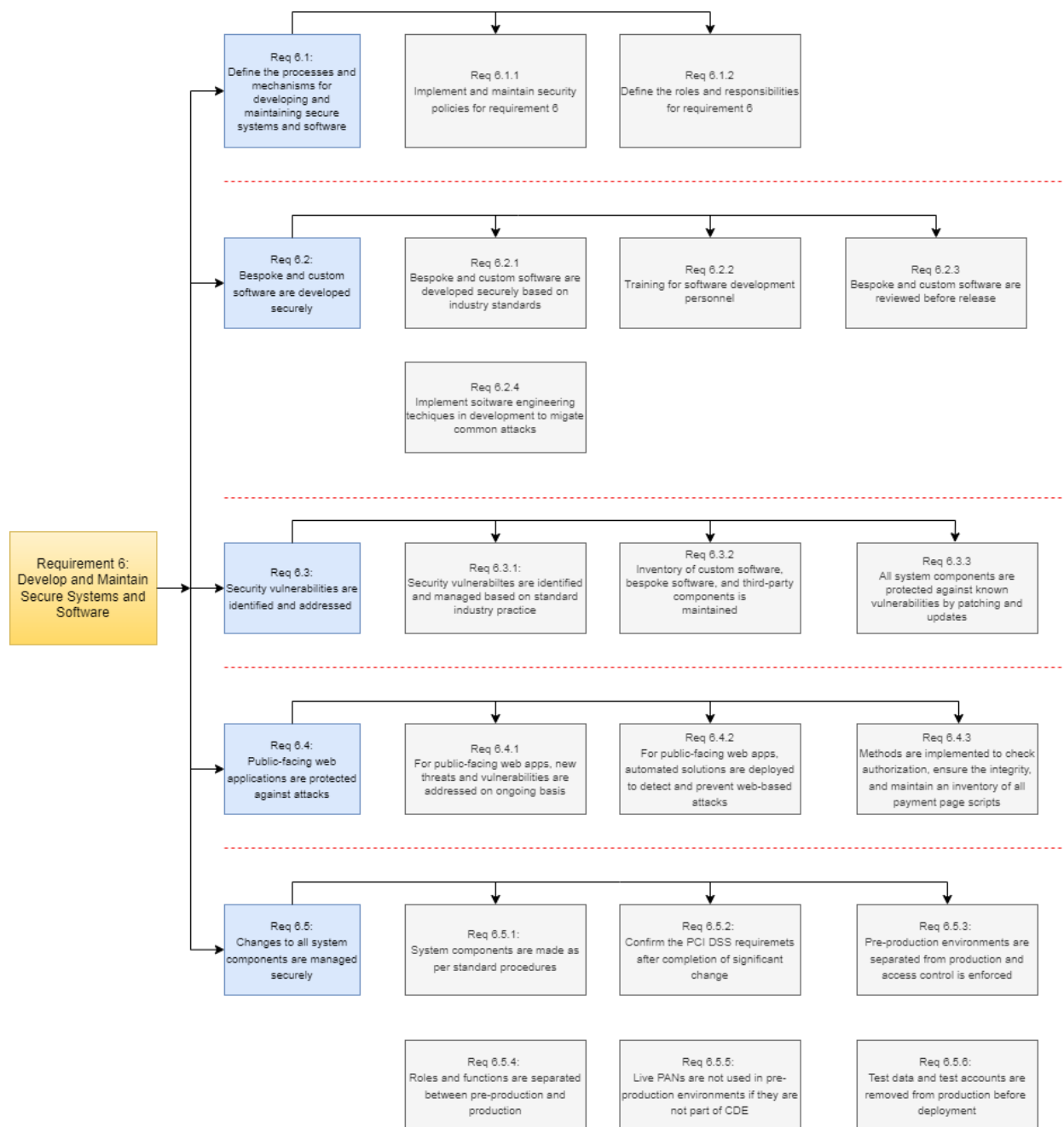
VMDR, CM, PC, FIM, EDR, SCA, PM, UD, CertView, GAV, CSAM

PCI Compliance Support for Requirement 5

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
5.2.1	✓				✓	✓			✓			
5.2.2	✓				✓							
5.2.3		✓							✓		✓	
5.2.3.1	✓											
5.3.1	✓	✓	✓		✓	✓			✓			
5.3.2	✓				✓				✓			
5.3.3	✓										✓	
5.3.4							✓	✓		✓		
5.4.1									✓			

PCI DSS Requirement 6

Develop and maintain secure systems and software: Security vulnerabilities risk payment data. Regularly install vendor-supplied patches and follow secure coding practices. Ensure timely updates based on risk analysis and manage system changes securely. Protect public-facing applications against attacks.



Qualys ensures the maintenance of secure systems and software for customers through proactive monitoring, automated tools, compliance enforcement, and continuous improvement practices.

You can leverage the following Qualys services to develop and maintain secure systems and software.

Qualys provides detailed reports and analytics to help customers understand their security posture and track improvements, including:

- Real-time visibility into security status and trends.
- Detailed reports to demonstrate compliance with various regulations and standards.

Qualys Solution for Requirement 6

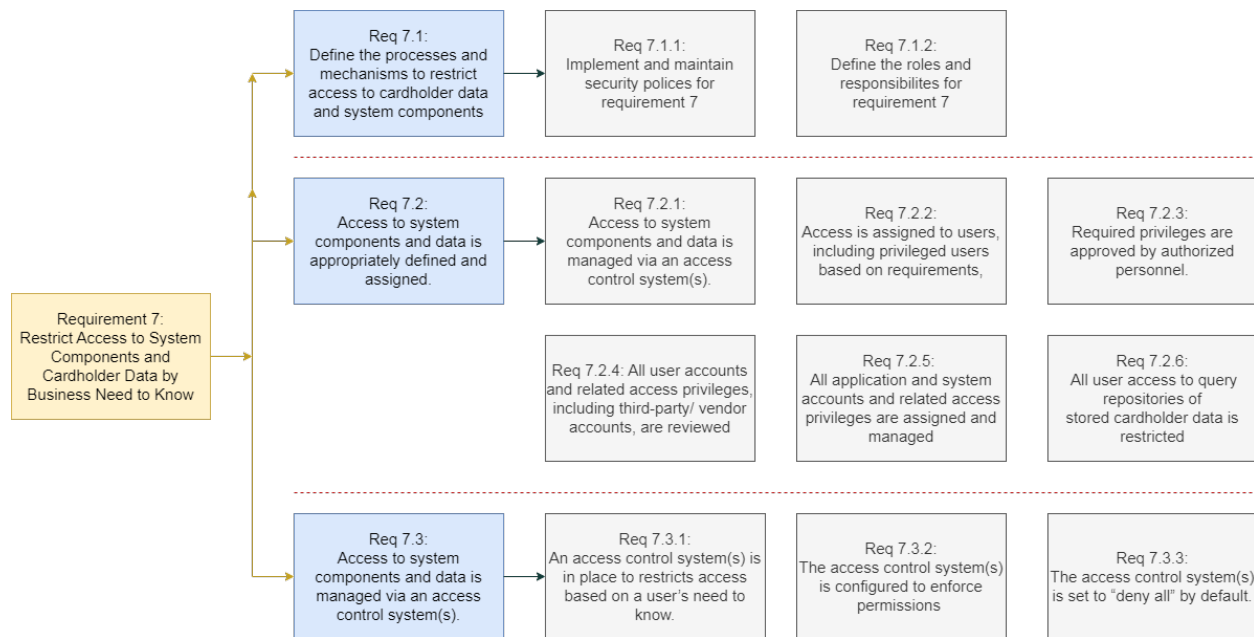
VMDR, CM, PC, FIM, WAS, SCA, PM, CAR, CertView, Admin, GAV, CSAM

PCI Compliance Support for Requirement 6

Req.	VMDR	PC	FIM	CAR	Admin	PM	GAV	SCA	CM	UD	WAS
6.2.1		✓									
6.3.1	✓										
6.3.2											✓
6.3.3	✓					✓			✓		
6.4.1									✓		✓
6.4.2		✓				✓		✓			
6.4.3											✓
6.5.2		✓									
6.5.3		✓			✓						
6.5.4					✓						

PCI DSS Requirement 7

Restrict access to cardholder data by business need-to-know: Ineffective access control can allow unauthorized access to critical data. Implement systems restricting access based on need-to-know and least privileges to authorized personnel, aligned with job responsibilities. Access control processes must be clearly defined and managed.



- Qualys ensures restricted data access based on the business need-to-know principle through a combination of robust access control mechanisms.
- Qualys employs strategies like detailed role-based access policies, granular permissions, continuous monitoring, and maintaining detailed audit logs.

Qualys Solution for Requirement 7

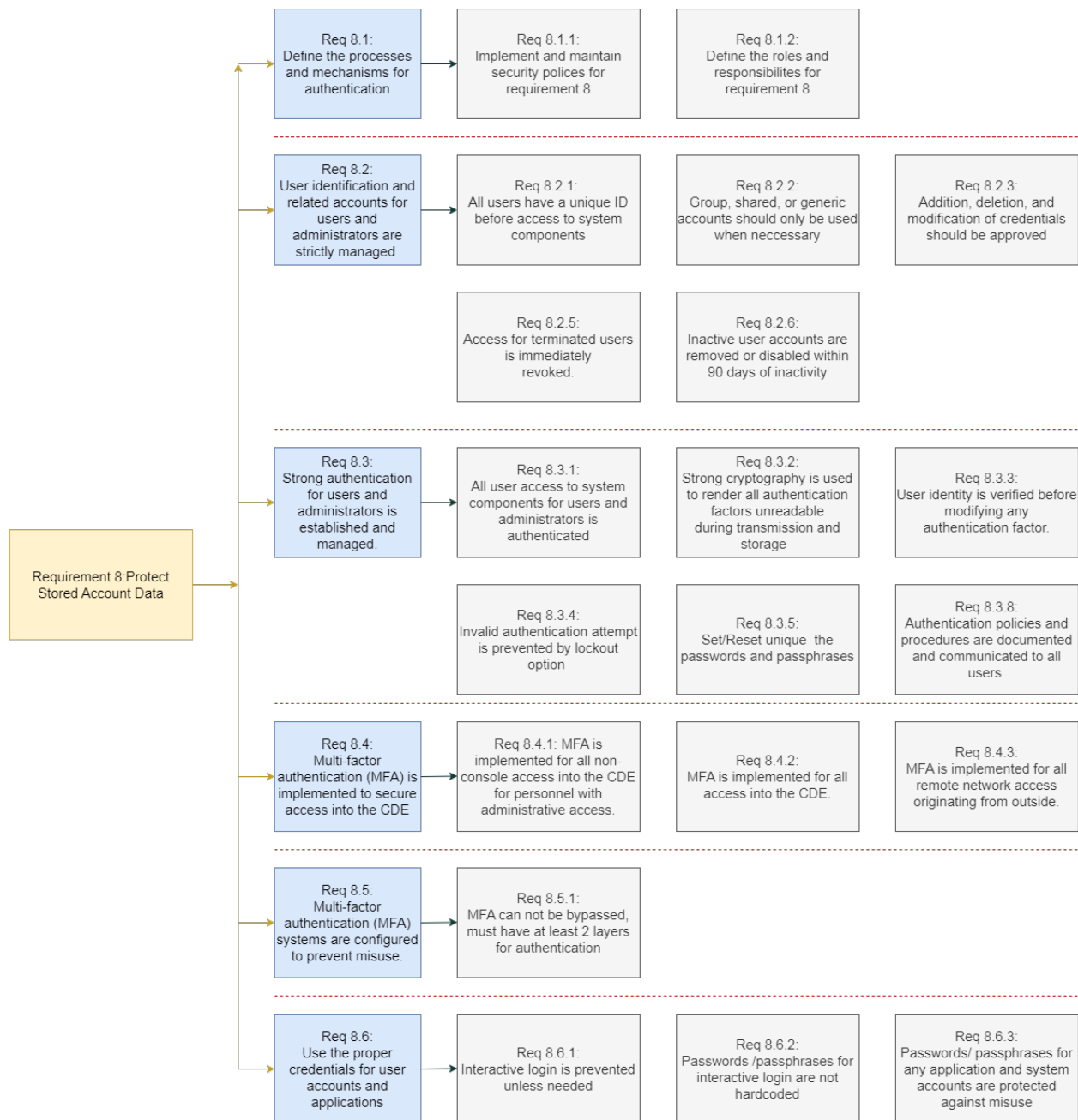
CM, PC, Admin

PCI Compliance Support for Requirement 7

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
7.2.1		✓										✓
7.2.2		✓										✓
7.2.3												✓
7.2.4												✓
7.2.5		✓										✓
7.2.6		✓										✓
7.3.1		✓							✓			
7.3.2		✓										✓

PCI DSS Requirement 8

Identify users and authenticate access to system components: Allocate unique identification to each account so that actions performed on critical data can be attributed to the known and authorized users. It is also important to implement and maintain strong authentication mechanisms and policies, such as multi-factor authentication.
















Qualys helps you implement comprehensive user authentication mechanisms to safeguard your critical data in any security situation. The following Qualys Services can help you meet this compliance requirement.

- Qualys Authentication APIs provide secure authentication for integration with other systems through a secure API key management system and an industry-standard regulatory protocol like OAuth2.0.
- Qualys also employs policies such as session management, account lockout mechanism, audit logs and monitoring, and periodic access review.

These practices protect your data and system components against unauthenticated intrusions.

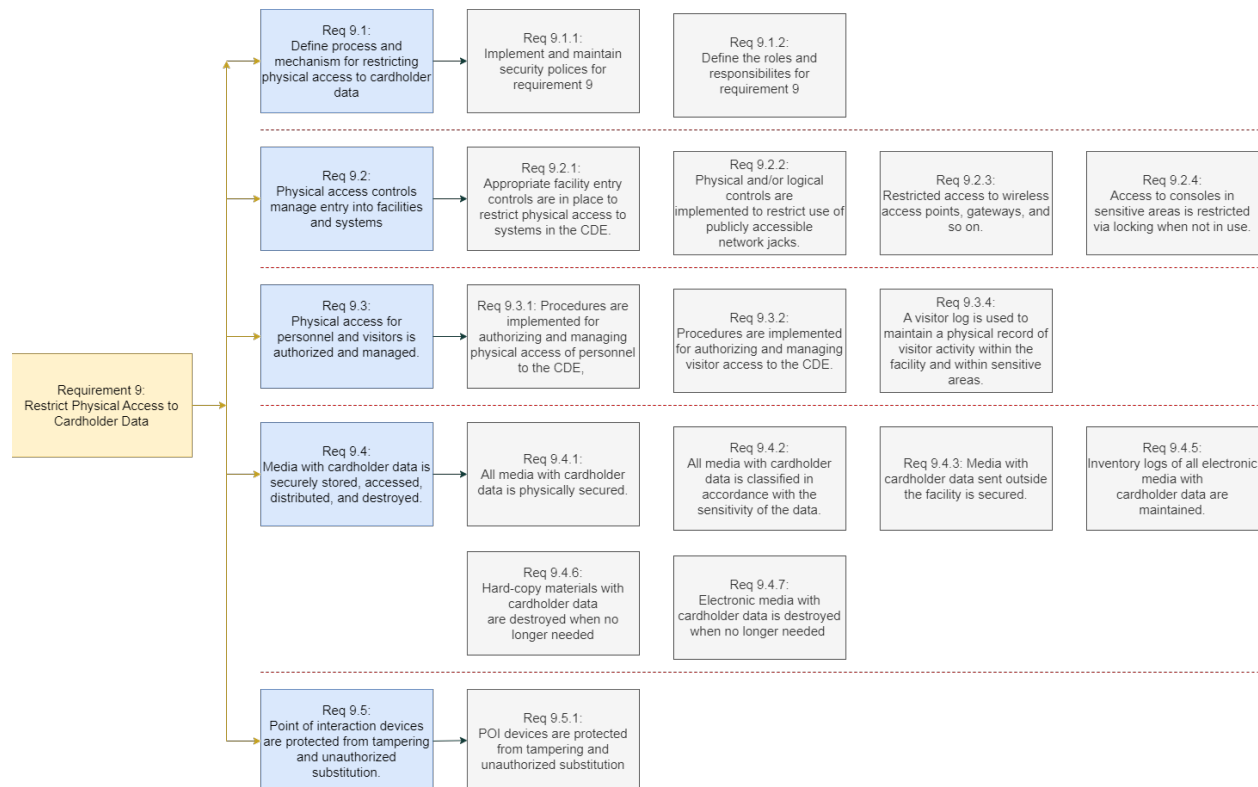
Qualys Solution for Requirement 8: [CM](#), [PC](#), [Admin](#)

PCI Compliance Support for Requirement 8

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
8.2.1												
8.2.2												
8.2.4												
8.2.5												
8.2.6												
8.3.1												
8.3.4												
8.4.1												
8.4.2												
8.4.3												
8.6.1												

PCI DSS Requirement 9

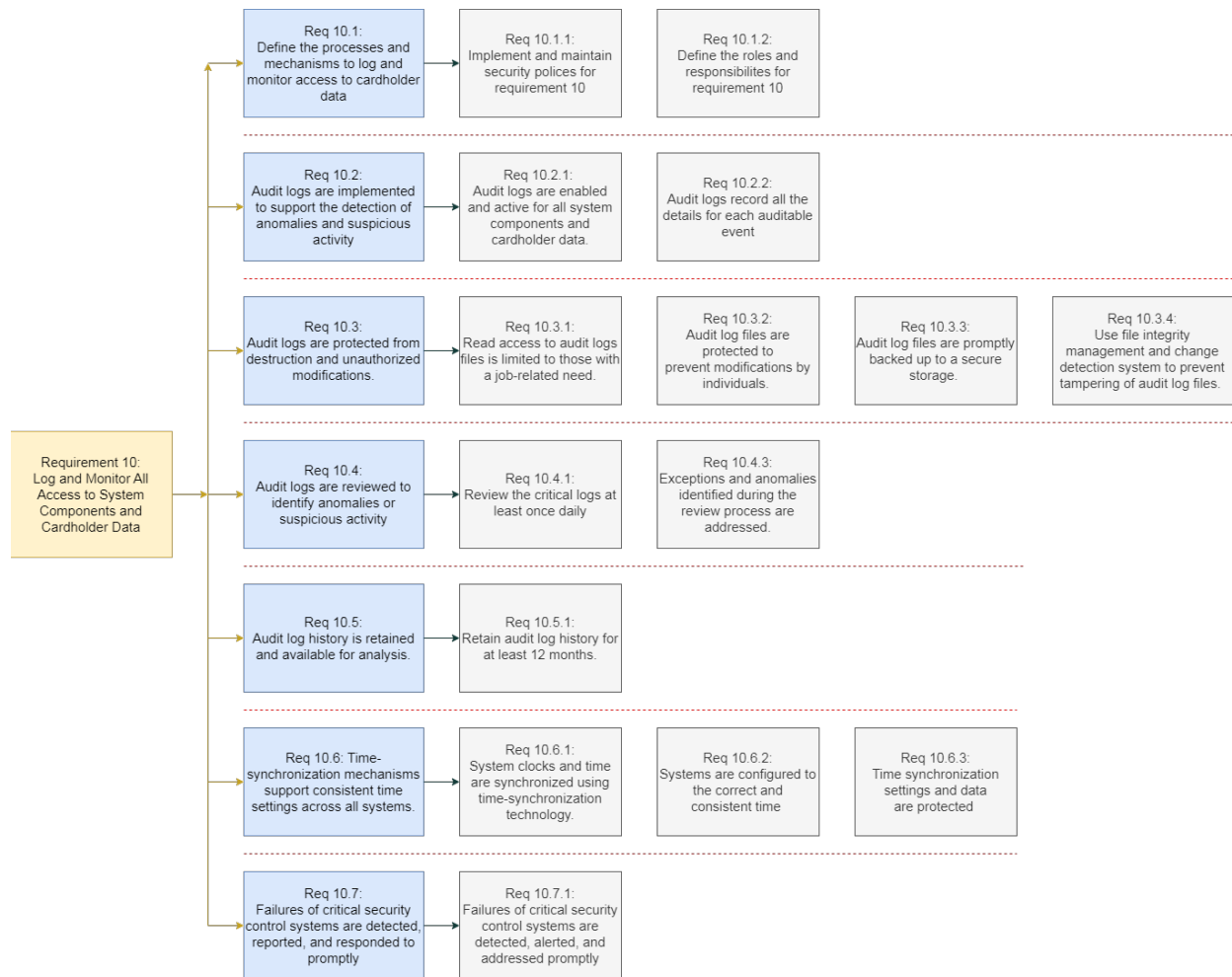
Restrict physical access to cardholder data: Physical access to cardholder data or to the systems that store, process, or transmit this data should be completely protected against unauthenticated physical intrusion by malicious actors. Implement policies and mechanisms to access, store, and destroy media associated with cardholders and protect point-of-interaction devices from tampering.



While Qualys focuses on digital security, organizations must implement physical security controls to restrict access to areas where cardholder data is stored.

PCI DSS Requirement 10

Log and monitor all access to system components and cardholder data: Implement the policies and mechanisms to monitor all access and maintain logs for tracking and evaluation. Organizations must set up an alert mechanism to report the failure of critical security controls. Also, ensure that all the access logs are protected from unauthorized destruction and modifications.



Qualys Solution for Requirement 10

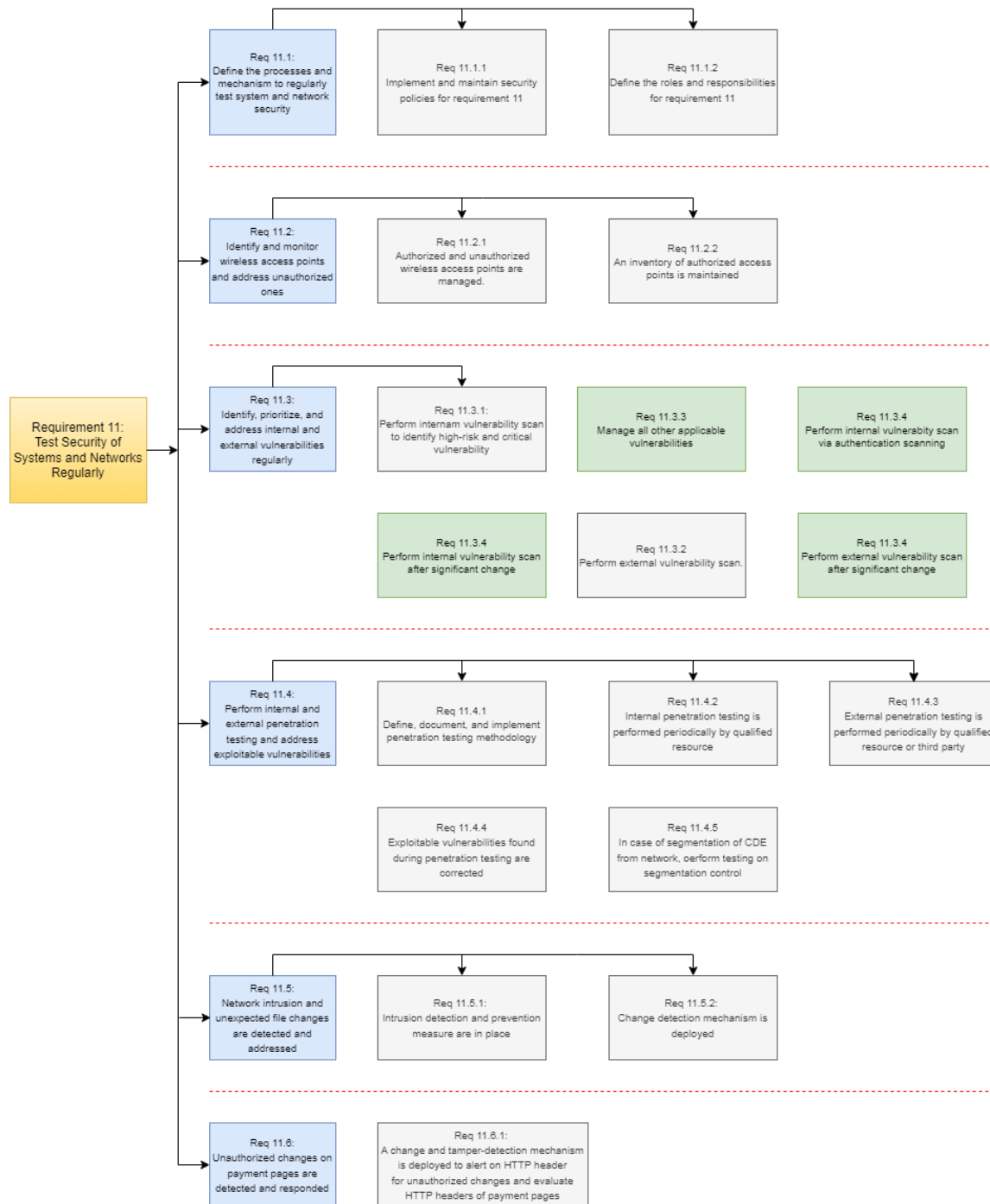
VMDR, CM, PC, FIM, SCA, PM, UD, GAV, Admin

PCI Compliance Support for Requirement 10

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
10.2.1		✓							✓			✓
10.2.2							✓			✓		
10.3.1												✓
10.3.3		✓										
10.3.4			✓									
10.4.1		✓									✓	
10.4.2	✓					✓						
10.6.3			✓									✓
10.7.1		✓	✓						✓			

PCI DSS Requirement 11

Test the security of systems and networks regularly: Organize the test procedures to ensure all the security policies and mechanisms are effective and up to date. This includes testing all the systems and networks, identifying both internal and external vulnerabilities, regularly performing penetration testing, and detecting and responding promptly to unauthorized changes to critical system files and software.



Qualys Solution for Requirement 11

VMDR, CM, PC, WAS, EDR, PM, GAV, CSAM, WAS

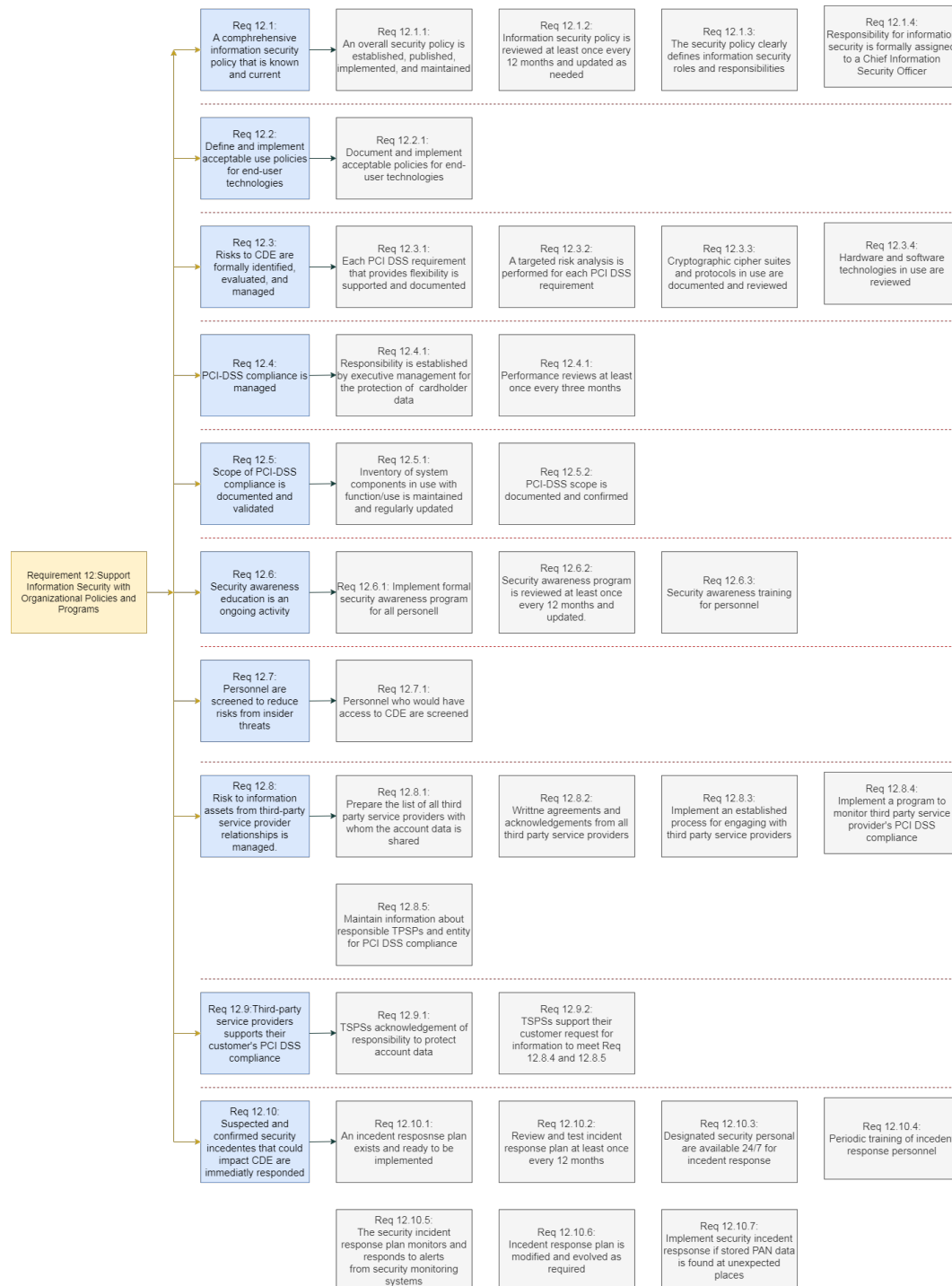
PCI Compliance Support for Requirement 11

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	WAS	Admin
11.2.1					✓				✓			

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	WAS	Admin
11.2.2							✓	✓				
11.3.1	✓	✓										
11.3.1.1	✓	✓										
11.3.1.2		✓										
11.3.1.3		✓										
11.3.2	✓		✓		✓				✓			
11.3.2.1	✓				✓							
11.4.4						✓			✓			
11.5.1	✓		✓		✓	✓			✓			
11.5.2			✓									
11.6.1											✓	

PCI DSS Requirement 12

Support information security with organizational policies and programs: Implement a strong information security policy to ensure that all stakeholders involved in maintaining the organization's security are aware of the security risks and PCI DSS compliance policies. The policy should be thorough and identify, report, and remediate any security incidents.



PCI Compliance Support for Requirement 12

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
12.2.1		✓										
12.3.2		✓									✓	
12.3.3	✓	✓							✓			
12.3.4		✓										
12.5.1							✓	✓				
12.10.1		✓							✓			
12.10.5		✓	✓		✓	✓			✓		✓	
12.10.7		✓							✓			