COALFIRE

WHITE PAPER

Red Hat OpenShift Applicability for PCI DSS 4.0

Applicability to Assist Customers in PCI DSS 4.0 Compliance

COALFIRE OPINION SERIES – FINAL V1.5

MICHAEL BURKE, PHD, CISSP, CISA, C|CISO, PCI-QSA
PRINCIPAL CONSULTANT

Red Hat OpenShift

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Executive summary

Red Hat has engaged Coalfire Systems, Inc. (“Coalfire”), a respected Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent technical review of Red Hat OpenShift.

This Product Applicability Guide (PAG) examines an entity’s adoption of Red Hat OpenShift Platform Plus in alignment with technical requirements to the Payment Card Industry Data Security Standard (PCI DSS) version 4.0. This PAG outlines Coalfire’s methodology for assessment and the approach used for its review, summarizes findings from Coalfire’s review of product capabilities, provides context for the use of these capabilities, defines parameters to form a common basis of understanding, and states an opinion as to the usefulness of OpenShift within a program of compliance for PCI DSS 4.0.

Coalfire PAGs provide a specific Coalfire opinion of a product’s applicability to PCI DSS through the “eyes of the assessor” and should not be construed as a specific endorsement. PAGs are provided as an element of Coalfire’s payment advisory and/or cloud services and are authored solely to inform prospective customers who are interested in using OpenShift.

Coalfire opinion

Coalfire reviewed the Red Hat OpenShift Platform Plus, comprising the following product modules: Red Hat OpenShift Container Platform, Red Hat Advanced Cluster Management, Red Hat Advanced Cluster Security, and Red Hat Quay. Throughout this paper, the term “OpenShift" will be used to refer to all components of Red Hat OpenShift Platform Plus.

Coalfire has determined that OpenShift is effective when employed properly in PCI DSS 4.0 assessed environments. OpenShift comes integrated with many security features and functions that can effectively support numerous PCI DSS technical control requirements.

This opinion is also dependent on many underlying presumptions (i.e., caveats), which are included in the complete Coalfire conclusion section at the end of this report.

Introducing PCI DSS 4.0

PCI DSS 4.0 is a framework that defines the baseline physical, technical, and operational security controls, known as requirements and sub-requirements, necessary for protecting payment card account data. PCI DSS 4.0 defines two categories of payment card account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and sensitive authentication data (SAD), which includes full track data (magnetic stripe data or equivalent on a chip), card security code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs/PIN blocks). (PCI DSS v4.0, 2022)

PCI DSS is intended for all entities that store, process, or transmit CHD and/or SAD or that could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing, including merchants, processors, acquirers, issuers, and other service providers. (PCI DSS v4.0, 2022)

The PCI DSS security requirements apply to components included in, connected to, or impacting the security of the CDE. The CDE is comprised of:

- System components, people, and processes that store, process, and transmit CHD/SAD
- System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD. (PCI DSS v4.0, 2022)

PCI DSS defines 12 requirements designed to address 6 objectives, as shown in the high-level overview below:

PCI Data Security Standard – High-Level Overview (PCI DSS v4.0, 2022)	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls (NSCs) **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 and Cardholder Data by Business Need to Know **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 of Systems and Networks Regularly
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs

Table 1: Principal PCI DSS 4.0 Requirements

For each principal requirement, PCI DSS includes detailed security requirements and corresponding testing procedures that collectively serve as a baseline for compliance.

This PAG is intended to provide an authoritative perspective for the use of OpenShift Platform Plus according to the PCI DSS principles, procedures, and guidance required for assessment and compliance. Industry-recognized authorities (e.g., Coalfire) commonly use de facto analysis of PCI systems (people, process, and technologies) to document the effects of use as part of an overall technical approach to PCI DSS compliance. Coalfire PAGs have been used since 2014 by various participants in the PCI community to understand how products may be successfully used in accordance with PCI DSS compliance.

Important updates to definitions

The PCI SSC has updated the PCI DSS to reflect changes within the industry and to clarify the intent of controls. This white paper utilizes language that reflects the changes that were made to the standard. Some of these changes have a direct impact on important features that are integral to the OpenShift solution, and are highlighted here:

- *Network Security Controls* - The PCI SSC has adopted the use of the term Network Security Control, or NSC, to refer to technology that is restricting, controlling, or policing network traffic between systems, networks, or devices. This technology is frequently referenced using terms such as; firewalls, access control lists, and security groups. The update to the DSS reflects a professionalization of this language, advancements in technology and acknowledges advances in cloud computing architectures. Network Security Controls can be now utilized to refer to any implementation of technology that places a control on network traffic within the infrastructure.
- *Trusted networks* - The council has also eliminated the references to the demilitarized zone, or DMZ, and instead adopted concepts of “trusted” and “untrusted” networks. Trusted networks are within the entity’s ability to control or manage and that meet the applicable PCI DSS requirements. Untrusted networks are all others.
- Scope - Defining the CDE has not changed, although every organization must now ensure that there is a process to ensure that the CDE is defined correctly, and that the process is enacted upon significant changes to the environment.

- *Significant change* - The council has provided a baseline definition, which clarifies which types of events are categorized as significant changes. This will impact organizations' change management processes and trigger additional vulnerability management activities.

Suggestions for the use of this PAG

This white paper is intended for PCI entities considering, or currently using, OpenShift, as well as other interested parties involved in sales, architecture, operation, and assessment of the platform or by its consumers. This document is intended to help Red Hat customers understand the controls that may be leveraged by the customer to support and implement OpenShift in a PCI DSS-compliant manner. The following sections explain how this review may be used by various entities throughout the PCI DSS life cycle.

Merchants and financial institutions

PCI DSS requirements provide a framework of standards that, when implemented, supports security for the payment card transactions from the merchant point-of-use, where payment and authorization transactions are initiated, to the financial institutions that provide the acquisition and settlement of a customer's purchase. OpenShift may be used for merchants and financial entities as a supporting platform for delivering services where CHD is stored, processed, or transmitted. This white paper is primarily intended to highlight where an OpenShift customer could supplement security controls using OpenShift and how those controls align with PCI DSS 4.0 requirements.

Service providers, designated entities, and shared PCI DSS responsibility

PCI DSS makes provisions for payment industry entities to use service providers to store, process, or transmit CHD on behalf of the payment entity or to manage components such as routers, firewalls, databases, physical security, or servers. CHD security is impacted while providing services to payment industry entities, and therefore, such service providers are responsible for compliance with PCI DSS. This is also true of shared service providers who provide services to multiple payment entities. Requirements under section 12.8 of PCI DSS 4.0 are focused on managing "service providers with whom CHD is shared, or that could affect the security of CHD." (PCI DSS v4.0, 2022) Service provider requirements, in addition to PCI DSS requirements, are listed in Appendix A1 of PCI DSS 4.0. This white paper may be useful for service providers using or planning to use OpenShift as a supporting platform for delivering services where CHD is stored, processed, or transmitted.

This white paper may also be useful where a designated entity is involved in the storage, processing, or transmission of CHD. Designated entities constitute an additional category of entity for which PCI DSS 4.0 is applicable. A designated entity may be any payment entity, including merchants or service providers, that a payment brand or acquirer determines requires additional supplemental validation of existing PCI DSS requirements. Examples of designated entities include those storing, processing, or transmitting large volumes of CHD; those providing aggregation points for CHD; or those who have suffered significant or repeated CHD breaches. Additional requirements for designated entities are found in Appendix A3 of PCI DSS 4.0.

PCI DSS qualified security assessors

This white paper and supporting materials may be useful to assist a PCI DSS Qualified Security Assessor (QSA) in evaluating the use of OpenShift during assessment activities that contribute to a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). In the section titled "OpenShift applicability to PCI DSS 4.0," Coalfire aligns the technical controls referenced in PCI DSS 4.0 with findings for how OpenShift can support or meet those requirements. Additionally, a designation of origination of control is provided with commentary on how the system's integrator would implement appropriate controls. Where applicable, Coalfire references the additional implementation steps documented in this white paper to be performed by the customer when deploying and supporting a PCI DSS compliance program.

Other products used in conjunction with OpenShift to provide relevant security controls, such as customer edge firewalls to secure the boundary between the untrusted network (Internet) and the internal, trusted networks, are noted where applicable.

The guidance in this white paper and supporting materials is intended to provide Coalfire's opinion and is not meant to supplant or compromise the independent judgment required to perform PCI DSS assessments. The PCI SSC Code of Professional Responsibility requires QSACs and employees to adhere to high standards of ethical and professional conduct. (PCI SSC Code of Professional Responsibility, 2014). Coalfire supports and upholds independent QSA judgments that might differ from this opinion.

Objectives of this white paper

This white paper's primary objective is to render an opinion on OpenShift's suitability to assist entities with meeting the requirements of PCI DSS 4.0. The following process is intended to illustrate Coalfire's findings and satisfy the following objectives:

- Convery functions and limitations of OpenShift for use by PCI entities.
- Evaluate the key features of OpenShift for their ability to support the control requirements.
- Make relevant observations and recommendations about each control family and the suggested implementation approaches to support meeting the objectives of controls.
- Render Coalfire's opinion on the applicability of OpenShift to PCI DSS 4.0 requirements.
- Provide a representative overview of relevant aspects of the PCI DSS process and practices.

Red Hat OpenShift

Introduction

This white paper intends to demonstrate to OpenShift customers how Red Hat OpenShift can assist organizations in achieving PCI DSS compliance with the use of varying OpenShift Platform Plus modules. This paper guides OpenShift customers in understanding how PCI DSS 4.0 compliance can be achieved and how OpenShift provides strategic tools to address compliance challenges presented by PCI DSS 4.0. The following sections provide an example of how this review may be utilized by ancillary and various entities in compliance with PCI DSS 4.0.

Overview

OpenShift is a comprehensive and fully scalable private cloud security platform that provides a gateway to realizing more sophisticated private cloud architectures. OpenShift, at its core, is a comprehensive Kubernetes-based application platform that has been meticulously crafted to meet the demands of modern, private cloud architectures. It simplifies the complexities of managing containerized applications by automating many of the tedious processes involved in deployment and scaling. However, OpenShift goes a step further. It is not just about container orchestration; it is an all-encompassing solution designed to tackle the specific needs of businesses venturing into or expanding their private cloud environments.

The following figure illustrates the full suite of modules within the OpenShift Platform Plus.

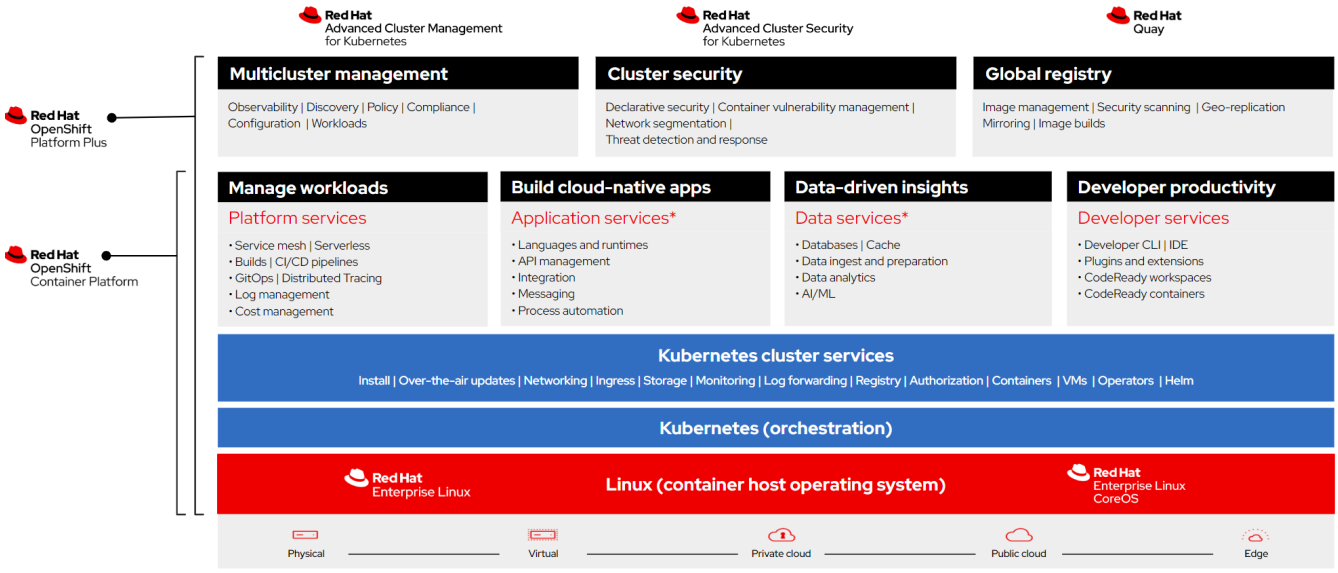

Figure 1 OpenShift Platform Plus

OpenShift Platform Plus architecture

The beauty of OpenShift Platform Plus lies in its integrated approach. It combines the foundational excellence of Red Hat OpenShift with advanced features that cater to the heightened demands of security, compliance, and multi-cluster management. OpenShift is engineered to provide a secure, enterprise-grade environment that is crucial for handling sensitive data and applications, making it an ideal choice for organizations implementing the controls prescribed in PCI DSS.

What truly sets OpenShift apart is its strategic implementation. It is not just a platform; it provides the mechanism that is essential to implement sophisticated private cloud architectures. From enhanced security protocols to streamlined management of multiple Kubernetes clusters, OpenShift offers a level of control and efficiency that is vital for businesses looking to leverage the full potential of cloud computing while maintaining a private, secure environment.

OpenShift is positioned as a strategic tool for businesses seeking to innovate and excel in the digital era. For information technology (IT) professionals, developers, or business leaders, understanding the capabilities of OpenShift is key to unlocking new possibilities in a company's cloud journey.

The foundation of the OpenShift architecture is built on the Red Hat Enterprise Linux operating system, with orchestration provided by Kubernetes. The foundation is a "tried and true" engine that provides the basis for cloud services. The foundation enables additional modules to be implemented in a secure, robust, and manageable way that cloud architectures require.

The OpenShift Platform Plus modules give organizations a single, trusted partner for the critical functions required by compliance and security frameworks, integrated within a single platform with industry recognized customer support.

Kubernetes and PCI DSS

Challenges

Kubernetes has become a cornerstone in modern software development, offering scalable, efficient container orchestration. However, as with any technology, it brings unique challenges, especially in the context of compliance with PCI DSS. Some of the challenges include:

- Kubernetes environments are highly dynamic, with containers constantly being created and destroyed. This dynamism can make it challenging to maintain a consistent security posture.
- Kubernetes often hosts multiple applications on the same cluster, which can lead to potential security risks and expansion of the scope of PCI DSS assessments.
- Ensuring that data is stored securely and encrypted, both at rest and in transit, is a key aspect of PCI DSS compliance.
- Managing access in a Kubernetes environment, where numerous users and services interact with resources, can be complex.
- Manual compliance checks are error-prone and not feasible in fast-paced Kubernetes environments, leading to higher costs and risk.

Growth and Kubernetes

Kubernetes is Application Programming Interface (API) driven architecture that is both enhanced and limited by its design. Controlling and limiting who can access a cluster is a first line of defense. As the cluster increases in complexity, management expands into a myriad of ports, API authenticators, roles for access control (RBAC), Node restrictions, and integration with identity management solutions. As a best practice, it is recommended that RBAC and Node restrictions are utilized together. As the power of the cluster is realized, the Kubernetes cluster quickly expands to support workflows throughout the organization. Organizations quickly realize that Kubernetes can be extended across disparate hardware, further complicating the management of the Kubernetes environment as multi cluster management is not native to Kubernetes, and the application of PCI controls becomes cumbersome.

An overwhelming majority of enterprises expect to leverage hybrid and multi-cloud architectures to support their applications in the near term. In addition, an even larger percentage of these organizations are using, or evaluating the use of, containerized applications to support future revisions of business-critical applications. Balancing the optimization of business agility, cost containment, and security management now must also consider the use of on-premises and cloud technology. At the time of this writing, less than one in five organizations had developed strategies for the leveraging and management of containerized infrastructure throughout their enterprise.

How OpenShift addresses the challenges

OpenShift Platform Plus comprises the products OpenShift Container Platform, Advanced Cluster Management for Kubernetes, Advanced Cluster Security for Kubernetes, OpenShift Data Foundation, and Red Hat Quay. Each of these play an important role in effectively managing the performance and security of the OpenShift Container Platform cluster.

Containerization and isolation

OpenShift Container Platform provides isolation capabilities at multiple layers of the platform. OpenShift Container Platform runs on Red Hat Enterprise Linux CoreOs, a container optimized host OS. Red Hat CoreOs only contains the packages required to run OpenShift, providing a minimized attack surface. OpenShift runs with Security Enhanced Linux

(SELinux) on in enforcing mode. SELinux has demonstrated the ability to prevent or mitigate container escapes to the host filesystem.

OpenShift secures hosts from network threats by enabling users to allow or block network traffic in accordance with organization policies. OpenShift supports Kubernetes Network Policies and OpenShift Service Mesh for microsegmentation of pod-to-pod traffic within the cluster. OpenShift also offers multiple options for cluster ingress and egress control.

OpenShift projects, which are Kubernetes namespaces with SELinux annotations, in combination with OpenShift RBAC and Network Policies, isolate users and applications from each other on the OpenShift platform.

The combination of OpenShift, Red Hat Advanced Cluster Security and Red Hat Advanced Cluster Management provides the ability to automate creation and deployment of Kubernetes Network Policies. Red Hat Advanced Cluster Management can automate deployment of both Network Policies and the OpenShift Service Mesh Operator.

- OpenShift includes the Network Observability Operator for monitoring network activity within an individual cluster. Red Hat Advanced Cluster Security provides observability of network traffic for a fleet of clusters and will identify and alert on network traffic anomalies.

Policy and configuration management

OpenShift operators deploy OpenShift platform components in an opinionated, pre-hardened configuration. Configuration changes are managed by the cluster admin via the operators. OpenShift operators monitor for configuration drift and will reset unsupported configuration changes for individual clusters.

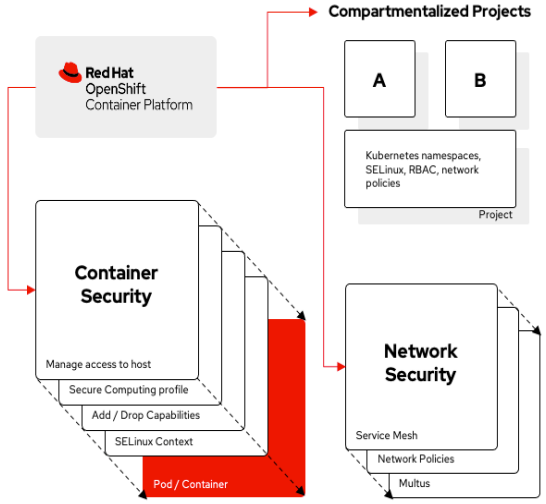

Figure 2 OpenShift Platform Plus Containerization and Isolation

Red Hat Advanced Cluster Security and Red Hat Advanced Cluster Management provide additional automation of policies and configuration management across a fleet of clusters. The combination of Red Hat Advanced Cluster Security and Red Hat Advanced Cluster Management delivers real-time usage data easily accessed via pre-built dashboards. Alerts and dashboards allow customers to see how their policies will impact users before rolling them out.

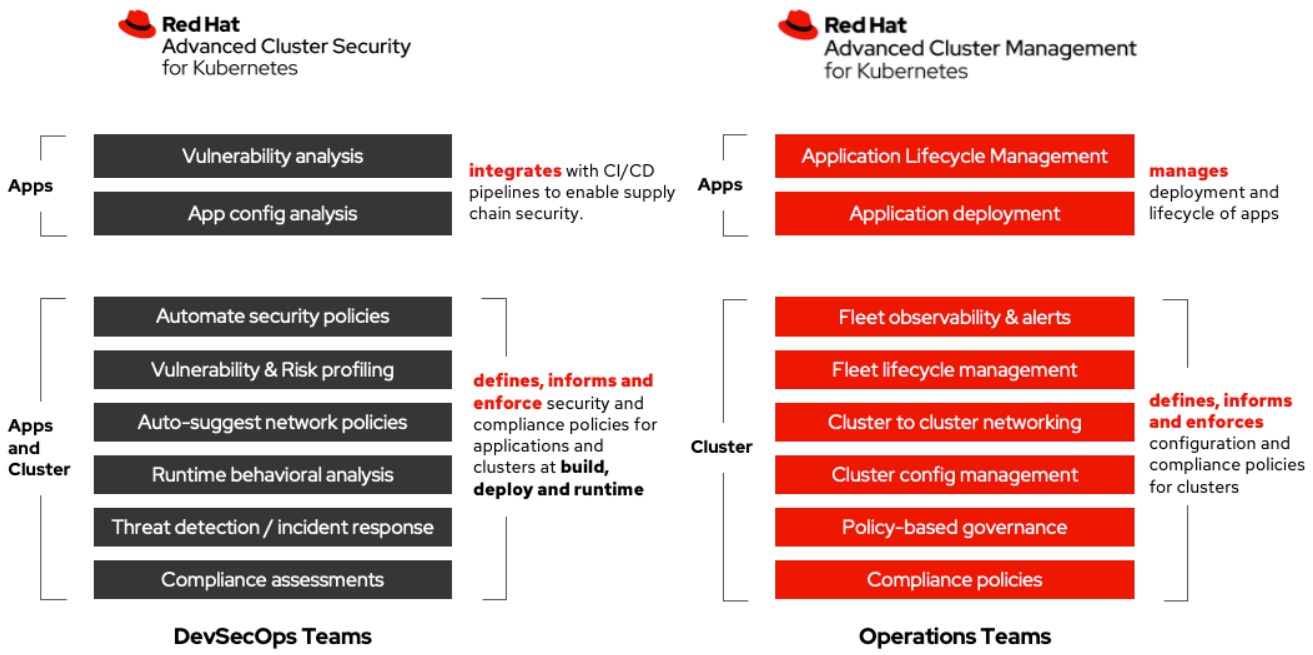

Figure 3: Red Hat Advanced Cluster Management and Red Hat Advanced Cluster Security Policy Control

Red Hat Advanced Cluster Management provides the lifecycle management necessary for regulatory level governance and compliance, ensuring that workloads are placed upon nodes based upon capacity and policy. Policy management of workloads ensures that "scope creep" is managed for PCI workloads by the appropriate policies and procedures established under the organization's PCI compliance program. Equally important are the contributions of Red Hat Advanced Cluster Security, as it provides behavioral analysis and the network policy enforcement that is essential in the control of PCI scope.

Third party solutions

One of the areas that the updated PCI DSS 4.0 is focused upon is the integration of third-party software and solutions. There are three aspects to consider. First, the use of container inventory and container management through Red Hat Quay provides the ability to ensure that only validated images are to be utilized in production. Second, the use of continuous integration/continuous deployment (CI/CD) within OpenShift enables the ability to scan images, custom and third party, with Red Hat Advanced Cluster Security prior to deployment and prevent the deployment of third-party software components that have not been approved. Third, Red Hat works with partner solutions to certify their integration with OpenShift. In this last case, certified partner solutions are available from the Red Hat Ecosystem Catalog. enabling customers to deploy additional, complementary security solutions with confidence.

Support for hybrid computing infrastructures

Ability to leverage legacy hardware

While not a requirement of PCI, a feature of OpenShift that is compelling is the ability for OpenShift to future-proof IT infrastructure by offering the same capabilities and experience across a wide range of infrastructure, both on premises and in public clouds. This includes the IBM Power Series and the IBM Z series hardware, which enables organizations to leverage centrally managed private clouds that can seamlessly integrate with compute infrastructure across architectures. Utilizing the centralized repositories that are managed using Red Hat Quay, enterprises can quickly mobilize container images to new clusters deployed to any supported infrastructure.

Leveraging the centralized repositories in Red Hat Quay

The centralized repositories contained within Red Hat Quay offer not only centralized container image governance to ensure that gold image containers are utilized. Red Hat Quay and Red Hat Advanced Cluster Security together provide additional risk mitigation against potential for attacks through vulnerability analysis across the container lifecycle. Red Hat Quay provides vulnerability analysis for images at rest and Red Hat Advanced Cluster Security provides vulnerability analysis for images as they move through the container lifecycle: at build, deploy and runtime. In addition, Red Hat Advanced Cluster Security recognizes behavioral problems within the cluster, workloads providing additional risk assessment.

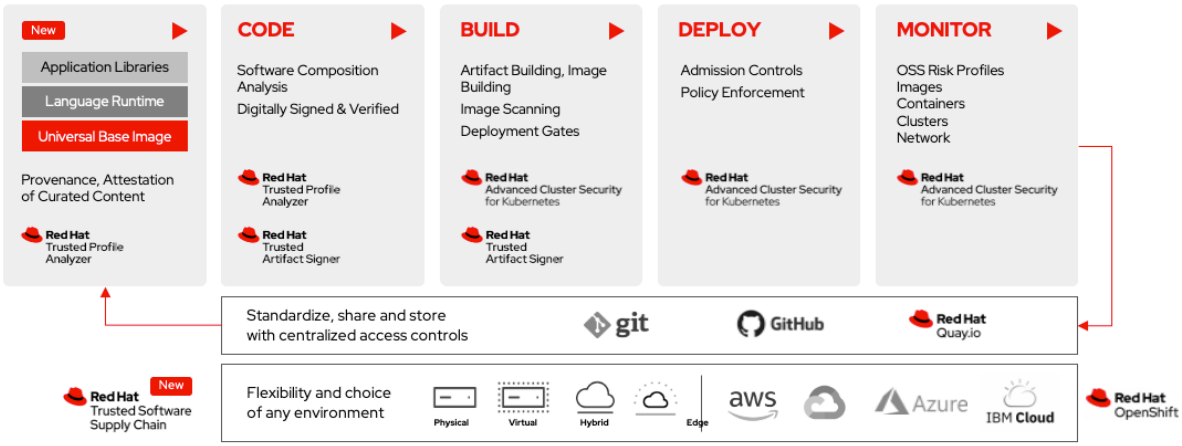

Figure 4: Trusted Software Supply Chain

The concept of a trusted software supply chain has implications within the newly revised PCI DSS 4.0. Requirement 6.3.2 relates to the security of the software supply chain and is one of the high impact changes to the PCI DSS. Leveraging the centralized container repository of Red Hat Quay provides a framework to control change management. OpenShift Platform Plus applicability to PCI DSS 4.0.

This section details Coalfire's findings and the corresponding customer requirements and responsibilities for OpenShift elements, as reviewed in Coalfire's analysis of use.

It is essential to understand that platforms and technologies do not themselves provide PCI compliance but can support and assist with a customer's compliance. Coalfire's review of OpenShift's applicability to PCI DSS is based on the platform's capacity to either provide compliance with the specific PCI DSS control or support an entity's requirements in concert with other operational and technical means necessary to meet PCI DSS testing requirements.

OpenShift

Requirement 1: Install and Maintain Network Security Controls

Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on predefined policies or rules. NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices and Kubernetes-native network controls. The ability to visualize communications and verify the expected communications between systems is an invaluable tool to assist network operations in the validation of

controls within requirement 1, particularly requirements 1.2.5 and 1.2.6 relating to the identification and documentation of business need; requirement 1.2.8, as the NSC configurations are maintained within the secure control plane of OpenShift; and requirements 1.3.1 through 1.4.3, providing flexible NSC configuration and placement capabilities.

Req #	PCI DSS Requirement	Platform Supporting Comments
1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Red Hat Advanced Cluster Security provides information on open ports and listening ports and the ability to generate Kubernetes Network policies based upon real time cluster information. Policies can be utilized to secure communications both within the cluster and within each pod, as a technical control, and these policies can be compared with the defined business justifications supporting procedural controls. Red Hat Advanced Cluster Management provides a way to centrally set and enforce policies for security, applications, and infrastructure including underlying network configurations for OpenShift clusters at scale.
1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated for insecure ports.	OpenShift provides multiple capabilities to handle mitigation of risk, such as Kubernetes Network Policies as well as multiple options for managing cluster ingress and egress, including encryption options. OpenShift also offers Service Mesh, providing an easy way to create Service-to-service authentication. Red Hat Advanced Cluster Security provides information on open ports and listening ports and the ability to generate Kubernetes Network policies based upon real time cluster information. Policies can be utilized to secure communications both within the cluster and within each pod, as a technical control, and these policies can be compared with the defined business justifications supporting procedural controls. Red Hat Advanced Cluster Management provides a way to centrally set and enforce OpenShift policies for security, applications, and infrastructure including underlying network configurations for OpenShift clusters at scale.
1.2.8	Configuration files for Network Security Controls (NSCs) are: • Secured from unauthorized access. • Kept consistent with active network configurations.	For user authentication to the platform, OpenShift includes an integrated OAuth server and the ability to integrate with an external identity provider for managing human users. OpenShift's RBAC is available to define which users or groups may make changes to configurations. Red Hat Advanced Cluster Security also provides the ability to integrate with external identity providers along with scoped access control for authorization. OpenShift includes options for managing and securing clusters. For a single cluster, the Ingress Operator's controller function ensures that ingress configurations are synchronized throughout the cluster.

Req #	PCI DSS Requirement	Platform Supporting Comments
		For multiple clusters, Red Hat Advanced Cluster Management can automate implementation of configuration governance policies that notify or auto-remediate configurations that violate best practices for both user management and network configurations. Red Hat Advanced Cluster Management user management is provided via the identity provider integrated with the underlying cluster as well as OpenShift RBAC. Red Hat Advanced Cluster Security provides visibility across your fleet of clusters for security policy compliance for user privileges and network communication.
1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	OpenShift provides restrictions for only necessary ingress traffic and explicitly denying all other traffic is made possible with the use of ingress configuration, network policy objects. Red Hat Advanced Cluster Security provides the ability to generate Kubernetes Network Control policies based upon real time cluster information. Policies can be utilized to secure communications both within the cluster and within each pod, as a technical control, and these policies can be compared with the defined business justifications supporting procedural controls. Red Hat Advanced Cluster Management provides a way to centrally set and enforce policies for security, applications, and infrastructure including underlying network configurations for OpenShift clusters at scale.
1.3.2	Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Red Hat Advanced Cluster Management provides the ability to generate Kubernetes Network Control policies based upon real time cluster information. Policies can be utilized to secure communications both within the cluster and within each pod, as a technical control, and these policies can be compared with the defined business justifications supporting procedural controls. OpenShift supports the creation of an egress network policy that can prevent unauthorized outbound traffic from the CDE. Restrictions for only necessary egress traffic and explicit denial of all other traffic is made possible within OpenShift with the use of network policy objects, and egress policy (egress firewall) rules. Red Hat Advanced Cluster Management provides a way to centrally set and enforce policies for security, applications, and infrastructure including underlying network configurations for OpenShift clusters at scale.
1.4.1	NSCs are implemented between trusted and untrusted networks.	Where a container may represent trusted, and untrusted, elements within a project, any project containers may

Req #	PCI DSS Requirement	Platform Supporting Comments
		represent a secure internal network element of a service will need to be placed on nodes residing on the internal network. Additionally, the payment entity can consider the integration of OpenShift Container Platform with proxy solutions to enhance the security and ensure adequate control for outbound connections to the internet. Red Hat Advanced Cluster Security provides the ability to generate Kubernetes Network Control policies based upon real time cluster information. Policies can be utilized to secure communications both within the cluster and within each pod, as a technical control, and these policies can be compared with the defined business justifications supporting procedural controls. Red Hat Advanced Cluster Management provides a way to centrally set and enforce policies for security, applications, and infrastructure including underlying network configurations for OpenShift clusters at scale.
1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. All other traffic is denied.	The cluster nodes in the trusted project networks will contain an OpenShift router for ingress with routes that direct traffic served from the OpenShift cluster. Additionally, for inbound traffic with a load balancer in front of the routers, the load balancer virtual IP (VIP) must belong to the network zone designated by the customer for this requirement. OpenShift recommends using dedicated router nodes in combination with Kubernetes Network Policies to create access zones within the cluster. This involves deploying and configuring a router instance to manage traffic and using Network Policies to create logical zones in the cluster SDN. Configuration of the OpenShift clusters should be carefully considered for production and should be configured accordingly. Ingress controls such as routes specify whether exposed services, ports, and protocols may respond to requests. Red Hat Advanced Cluster Security provides visibility into Kubernetes Network Control policies based upon real time cluster information which can be utilized to secure communications both within the cluster and within each pod, as a technical control. These policies can be compared with the defined business justifications supporting procedural controls. Red Hat Advanced Cluster Management provides a way to centrally set and enforce policies for ingress controls, including underlying network policy configuration for OpenShift clusters at scale.

Requirement 2: Apply Secure Configurations to All System Components

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information. Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords; removing unnecessary software, functions, and accounts; and disabling or removing unnecessary services all help to reduce the potential attack surface. The ability to define standards and control the Kubernetes nodes and clusters through policy is useful for the ability to address specific Requirement 2 controls. Utilizing the utilities within the OpenShift Platform Plus, organizations can develop configuration standards to be enforced by system policy through securing the container registry, securing the build pipeline, and securing the containers and the container platform. Utilizing Red Hat Quay, organizations can establish policies that can support the rigor of Requirement 2.2 and most of its sub requirements.

Req #	PCI DSS Requirement	Platform Supporting Comments
2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	The combination of Red Hat Advanced Cluster Security, Red Hat Quay, and pipeline workflows, organizations can configure the infrastructure in a way that permits only approved images for deployment. Approved container images are defined within Red Hat Quay, and components can be defined within pipeline services. Red Hat Advanced Cluster Security provides the ability to scan containers for PCI compliance and can be further configured to prevent the deployment of a container that fails compliance checks. Red Hat Advanced Cluster Management provides visibility into the PCI compliance posture based on user defined standards
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	OpenShift and Red Hat Enterprise Linux CoreOS do not come pre-configured with a default password. At the conclusion of the installation, a randomly generated password is provided for initial administrative access. Administrators are expected to integrate OpenShift with an Identity Provider (IDP) and subsequently disable the generated administrative account.
2.2.3	Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with different security levels that exist on the same system component are isolated from each other, OR • Primary functions with different security levels on the same system component are all secured to the level required by the function with the highest security needs.	OpenShift provides the means to separate application workloads within an OpenShift cluster onto separate hosts within the cluster. This allows the payment entity to separate CDE from non-CDE pods. Red Hat Advanced Cluster Management governance and placement policies can be configured across a fleet of clusters to notify of deviations from the desired configuration, and auto-remediate the configuration of workload placement if desired. As part of registered containers within Red Hat Quay, process controls are supported providing organizations the ability to ensure that containers are meeting the intent of this control.
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Red Hat Enterprise Linux CoreOS comes pre-hardened with the minimum necessary functionality to support running containers. All additional functionality available

Req #	PCI DSS Requirement	Platform Supporting Comments
		from OpenShift as layered on Red Hat Enterprise Linux CoreOS is necessary for the function of the platform and is described in detail in the product documentation. Red Hat Quay provides a process control to ensure that approved containers are eligible for deployment, these containers can be “organization approved” and have been hardened appropriately. Red Hat Advanced Cluster Security also provides the ability to scan the containers to ensure that only the appropriate services, protocols, and daemons are running. The optional Compliance Operator can be used to audit an OpenShift Container Platform cluster for the configuration of technical controls. Red Hat Advanced Cluster Security also implements default security policies that are centered around least-privileges, container immutability at runtime, and suggests only containers with a default read-only root filesystem. This prevents anyone from modifying files, scripts, or drivers and subsystems in the runtime environment if access is compromised.
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Red Hat Quay provides a process control to ensure that approved containers are eligible for deployment, these containers can be “organization approved” and have been hardened appropriately. Red Hat Advanced Cluster Security also provides the ability to scan the containers to ensure that only the appropriate services, protocols, and daemons are running.
2.2.6	System security parameters are configured to prevent misuse.	OpenShift Container Platform and Red Hat Enterprise Linux CoreOS can be configured and hardened per best practices. The Compliance Operator can be used to audit an OpenShift cluster for the configuration of technical controls. The Compliance Operator uses OpenSCAP, a NIST-certified tool, to scan and enforce security policies provided by the compliance profiles. Red Hat Advanced Cluster Security implements default security policies that are centered around least-privileges, container immutability at runtime, and suggests only containers with a default read-only root filesystem. This prevents anyone from modifying files, scripts, or drivers and subsystems in the runtime environment if access is compromised. Red Hat Advanced Cluster Management can be used to enforce governance of cryptography across OpenShift clusters to ensure this is enabled by default and has not been modified by users or administrators.

Req #	PCI DSS Requirement	Platform Supporting Comments
2.2.7	All non-console administrative access is encrypted using strong cryptography.	OpenShift and Red Hat Advanced Cluster Security utilize TLS 1.2, or higher, for all API and UI communication. Non-console access to OpenShift Control Plane or OpenShift cluster hosts is facilitated through SSH and enabled by default. Red Hat Advanced Cluster Management can be used to enforce governance of cryptography across OpenShift clusters to ensure this is enabled by default and has not been modified by users or administrators

Requirement 3: Protect Stored Account Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as email and instant messaging.

In the Coalfire use case, Requirement 3 controls would be supplied by a system outside of the OpenShift Platform Plus and considered notional controls for Coalfire's review.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and nonrepudiation. To protect against compromise, PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to CDE. Any transmissions of CHD over an entity's internal network brings that network into scope for PCI DSS since that network stores, processes, or transmits cardholder data. Any such network must be evaluated and assessed against applicable PCI DSS requirements. Configured appropriately, Red Hat Advanced Cluster Security can monitor to ensure that protected PCI workloads accessible to the Internet or other open public networks are only communicated over secured channels, and support HTTPS TLS configurations with the Ingress Operator (HAProxy) using a tlsSecurityProfile of intermediate or modern. Additionally, OpenShift Service Mesh supports mutual TLS (mTLS) enforcement capabilities that can be used to transparently encrypt inter-pod traffic. As of OpenShift 4.7, OVN-IPsec allows for encrypting all node-to-node traffic with IPsec when using Open Virtual Network (OVN).

Requirement 5: Protect All Systems and Networks from Malicious Software

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, and rootkits, as well as malicious code, scripts, and links. Malware can enter the network during many business-approved activities, including employee email (for example, via phishing) and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Using anti-malware solutions that address all types of malware helps to protect systems from current and evolving malware threats. The behavioral analysis and threat detection

of Red Hat Advanced Cluster Security and Red Hat Quay support control objectives within requirement 5 as part of a well-defined malware detection and mitigation program.

Requirement 6: Develop and Maintain Secure Systems and Software

Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software. Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software life cycle (SLC) processes and secure coding techniques.

Code repositories that store application code, system configurations, or other configuration data that can impact the security of account data or the CDE are in scope for PCI DSS assessments. Support for requirement 6.3.2 is provided in the management of container images through Red Hat Quay and the pipeline management architectures included within OpenShift Platform Plus.

Req #	PCI DSS Requirement	Platform Supporting Comments
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Red Hat Advanced Cluster Security scans the assets for known vulnerabilities and uses the Common Vulnerabilities and Exposures (CVE) data to assess the impact of a known vulnerability. Red Hat Advanced Cluster Security can be configured to perform continuous assessments on OpenShift Container Platforms providing industry recognized risk rankings enabling organizations to prioritize and act on vulnerabilities in their environment. The default policy enabled for Red Hat Advanced Cluster Security measures fixable CVEs of a severity of “Important” or greater, providing an important part of an overall vulnerability management program.
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Red Hat Quay and the pipeline management architectures provide support for this control by ensuring that components and containers are registered and approved prior to deployment. This provides the organization with the ability to strengthen inventory controls within the environment.
6.5.3	Separate development/test environments from production environments and enforce the separation with access controls. and enforce the separation with access controls.	OpenShift can be implemented, using tenant separation to allow for isolation between development/test clusters, and production clusters. Along with physical separation of clusters, OpenShift leverages RBACs, OpenShift projects, service mesh and network policy rules to enforce this separation within the individual clusters.
6.5.4	Separation of roles and functions between production and pre-production is intended to provide accountability so that only approved changes are deployed.	Access controls for the administration and management of OpenShift can be established to support the separation of duties; different levels of access can be granted to development and test projects and users as opposed to production projects and users.

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

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure that critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. Access or access rights are created by rules that provide users access to systems, applications, and data, while privileges allow a user to perform a specific action or function in relation to that system, application, or data. For example, a user may have access rights to specific data, but whether they can only read that data, or can also change or delete the data, is determined by the user's assigned privileges. Need to know refers to providing access to only the least amount of data needed to perform a job. Least privileges refers to providing only the minimum level of privileges needed to perform a job.

These requirements apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties (for example, for providing support or maintenance services). Certain requirements also apply to application and system accounts used by the entity (also called service accounts). OpenShift Platform Plus provides a centralized management control plane to define role-based access and ease the management of accounts and integration with the organization's identity and access management system.

Req #	PCI DSS Requirement	Platform Supporting Comments
7.3.1	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities. Default "deny-all" setting.	OpenShift leverages the external identity provider to support the customer's standards for access control based on minimum access requirements. For users to interact with OpenShift Container Platform, they must first authenticate to the cluster through the IDP. The authentication layer identifies the user associated with requests to the OpenShift Container Platform API. The authorization layer then uses information about the requesting user to determine if the request is allowed.
7.3.2	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	As an administrator, you can configure authentication for OpenShift Container Platform. RBACs can be implemented to establish authorization with a granular level of control for interaction with and/or administration of OpenShift and the underlying OS. Red Hat Advanced Cluster Security provides mechanisms to support enforcement of RBAC through security policies that can be configured to support specific requirements for access. Red Hat Advanced Cluster Management can be used to enforce RBAC policies across a fleet of clusters in production.

Requirement 8: Identify Users and Authenticate Access to System Components

Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be. Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as accounts) fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures

that there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes. OpenShift Platform Plus provides a centralized control plane to ease the management of authorized users and processes utilized in all work streams within the DevOps or DevSecOps models.

OpenShift Platform Plus provides mechanisms to support enforcement of RBAC through security policies that can be configured to support specific requirements for access and leverages the organizations' central identity management system.

Requirement 9: Restrict Physical Access to Cardholder Data

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

Requirement 9 lists three different requirement areas (PCI DSS v4.0, 2022):

- Requirements that specifically refer to sensitive areas are intended to apply to those areas only.
- Requirements that specifically refer to the CDE are intended to apply to the entire CDE, including any sensitive areas residing within the CDE.
- Requirements that specifically refer to "the facility" are referencing the types of controls that may be managed more broadly at the physical boundary of a business premise (such as a building) within which CDEs and sensitive areas reside. These controls often exist outside a CDE or sensitive area (for example, a guard desk that identifies, badges, and logs visitors). The term "facility" is used to recognize that these controls may exist at different places within a facility (for instance, at building entry or at an internal entrance to a data center or office space).

In the Coalfire use case, Requirement 9 controls would be supplied by a system outside of the OpenShift Platform Plus and considered notional controls for Coalfire's review of the platform.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, and minimizing the impact of a data compromise. The presence of logs on all system components and in the CDE allows thorough tracking, alerting, and analysis when an incident occurs. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

OpenShift provides the capability to export all system events that are required by the PCI DSS (Requirement 10.2 and 10.3) to a central logging server as required by Requirement 10.3.3.

This requirement applies to user activities, including those by employees, contractors, consultants, internal and external vendors, and other third parties (for example, those providing support or maintenance services). These requirements do not apply to the user activity of consumers (cardholders).

Requirement 11: Test Security of Systems and Networks Regularly

Vulnerabilities are discovered continually by malicious individuals and researchers and are introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure that security controls continue to reflect a changing environment.

OpenShift Platform Plus provides the ability for vulnerability scanning of container images as part of the CI/CD models and can prevent the deployment of applications that would introduce known vulnerabilities to a production system. While

this does not directly address controls within Requirement 11, it provides a supporting role to a well-formed vulnerability management program.

Req #	PCI DSS Requirement	Platform Supporting Comments
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	With OpenShift Platform Plus, the addition of the File Integrity Operator allows for close monitoring of any file changes on the nodes.

Requirement 12: Support Information Security with Organizational Policies and Programs

The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

For the purposes of Requirement 12, personnel refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of account data. Centralized control plane management, as previously discussed, plays an essential role in assuring that user inventories are maintained and support requirement 12.7, the screening of internal threats from users.

Customer considerations for PCI DSS use

Maintaining optimal PCI DSS scoping and avoiding scope creep are paramount to achieving and maintaining compliance status. When adopting new technologies and services, architecture design and general control considerations of shared and customer-owned requirements are often overlooked, negatively impacting scope. Consideration of the following guidance helps ensure minimal impact on OpenShift Platform Plus customers' compliance initiatives and maintain the existence of the CDE within customer boundaries.

A summary of PCI DSS customer responsibilities for consideration is provided below, with reference to the related PCI requirements:

- *(All Reqs)* Write and disseminate policies, procedures, and standards representing all PCI requirements.
- *(Req 1)* Configure and maintain network security controls such that:
    - Network access to and from the customer CDE is restricted.
    - Network connections between trusted and untrusted networks are controlled.
    - Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.
- *(Req 2)* Devise baseline standards and implement all system components for secure configuration and management.
- *(Req 3)* Implement protections for stored account holder data, including:
    - Keep storage and access to a minimum.
    - Secure (e.g., encrypt, mask) account holder data where stored/displayed, including log files, according to access policies.

    - Employ secure cryptography and key management processes and implementation.
- *(Req 4)* Protect the transmission of CHD using strong encryption with secure implementation.
- *(Req 5)* Protect systems and networks from malicious code.
- *(Req 6)* Securely develop and maintain systems and software.
- *(Reqs 7 and 8)* Restrict access to CDEs by need-to-know with mechanisms enforcing:
    - Life cycle management of user/resource identities and related accounts.
    - Strong authentication, including secure implementation of MFA.
    - Life cycle management of authentication factors for application and system accounts.
- *(Req 9)* Employ physical access restrictions to CDEs.
- *(Req 10)* Log and monitor access to CHD and system components such that:
    - Audit log history is retained and available for analysis.
    - Time-synchronization mechanisms support consistent time settings across all systems.
- *(Req 11)* Perform regular testing of systems and network security, including:
    - Vulnerability scanning
    - Penetration testing
    - Intrusion detection and prevention
- *(Req 12)* Devise organizational-level information security processes, including:
    - Risk management
    - Security awareness training
    - Acceptable use
    - PCI compliance and scope management
    - Screening of personnel
    - Third-party service provider management and shared responsibility agreements
    - Incident response

Coalfire conclusion

The OpenShift Platform Plus is a container orchestration platform that extends the capabilities of Kubernetes and OpenShift. Coalfire reviewed the capabilities included within the product and their value in assisting entities with PCI DSS 4.0 compliance.

Coalfire concludes with the opinion that the reviewed OpenShift Platform Plus solution is effective in providing significant and substantial support for PCI DSS payment entities' objectives and requirements, and is capable of streamlining the effort required to establish the effective application of controls and lower the overall effort required to demonstrate and maintain compliance. OpenShift Platform Plus provides a centralized management control plane for container orchestration that provides the ability to establish and enforce governance on a scalable and highly flexible Kubernetes container orchestration platform. The capabilities of the platform provide effective methods for organizations to achieve the highest level of maturity in governance, risk management, and compliance reporting. The capabilities can assist to reduce operational stress on the required risk management teams and associated information technology staff to support the cybersecurity program, workloads, and business operations.

A comment regarding regulatory compliance

Coalfire disclaims the generic suitability of any product to establish regulatory compliance strictly by use of that product. Agencies and entities attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not via the use of a specific product. This is true for merchants and service providers subject to PCI DSS and for customers targeting compliance with other regulations.

Legal disclaimer

Additional information, resources, and references

This section contains a description of the links, standards, guidelines, and reports used to identify and discuss the features and security capabilities of the OpenShift Platform Plus.

PCI SSC references

- As of the time of this white paper, there are two concurrent, active, versions of the PCI DSS: v3.2.1 (May 2018) and v4.0 (March 2022). This white paper references PCI DSS v4.0, which may be accessed via the following link:

  https://www.pcisecuritystandards.org/document_library/

- The PCI DSS v4.0 Quick Reference Guide helps gain an understanding of how PCI DSS can help protect payment processing environments and how to apply the standard. The Quick Reference Guide may be found at the following link:

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf

- The PCI SSC provides the Prioritized Approach to help organizations understand how they can reduce risk earlier in their PCI DSS journey. The Prioritized Approach may be found at the following link:

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Prioritized-Approach-For-PCI-DSS-v4-0.pdf

Coalfire references

- The Coalfire corporate payment card references and the Solutions Engineering offerings may be found at the following links:
  - https://www.coalfire.com/industries/payments
  - https://www.coalfire.com/solutions/cyber-engineering
- Coalfire corporate information is available at the following link:
  - https://www.coalfire.com/about

OpenShift Platform Plus refe rences

The following OpenShift Platform Plus materials were used as references during the research and writing phase of this white paper:

- https://www.redhat.com/en/resources/openshift-platform-plus-datasheet
- https://www.redhat.com/en/topics/containers/kubernetes-approach#red-hat-approach
- https://www.redhat.com/en/technologies/cloud-computing/openshift/platform-plus

Acknowledgements

The author would like to acknowledge the following individuals from Red Hat for their contributions to this paper: Eric Bannon and Ramon Villarreal. The author recognizes Dan Stocker, Kerry Steele, and Joanie South-Shelley for their contributions to the development of this paper. The author is also thankful to Maribel King for managing the project efficiently.

About Red Hat

Red Hat (NYSE: IBM), an International Business Machines (IBM) company, is the world's leading provider of enterprise open source solutions — including Linux, cloud, container, and Kubernetes. Delivers hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.

For More Information : **https://www.redhat.com/**

About the author

Michael Burke, Ph.D., *CISSP, CISA, C|CISO, PCI-QSA* | Principal Consultant, Payments and Cloud Advisory

With over three decades of information technology management and information security compliance experience, Michael is responsible for thought leadership and advocating solutions to the complex requirements of business risk and compliance mandates. Michael's direction, which synthesizes the importance of cybersecurity and sustainable business operation, has helped numerous organizations strengthen their cybersecurity posture.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.