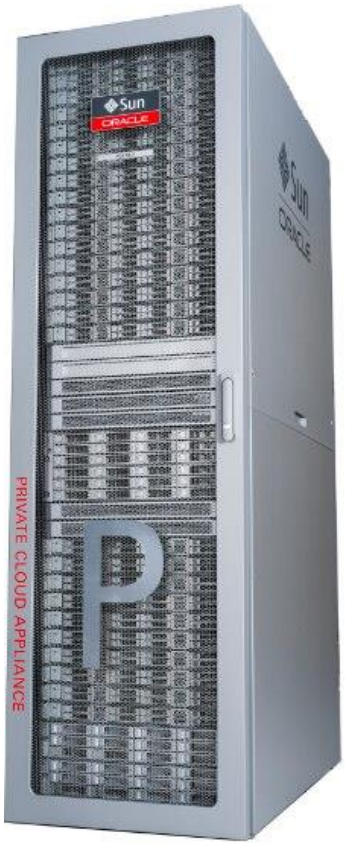
COALFIRE



ORACLE PRIVATE CLOUD APPLIANCE AND PCI COMPLIANCE

A QUALIFIED SECURITY ASSESSOR (QSA) PERSPECTIVE

February 27, 2020

Ryan McGovern PCI-QSA
Senior Consultant, Coalfire

COALFIRE

Table of Contents

COALFIRE

Executive Summary

Organizations that process, transmit, or store payment card data are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) on an ongoing basis. For organizations to meet these security requirements, they must deploy security measures across all the components of the network and systems that process, store, or transmit payment card information. Merchants as well as payment card service providers are required to attest to compliance with requirements of the PCI DSS annually.

Introduction

The intent of this white paper is to provide information to IT professionals implementing Oracle Private Cloud Appliance (PCA) within a Cardholder Data Environment (CDE), as well as a Qualified Security Assessor (QSA) tasked with assessing them. PCA features and published controls were compared with the PCI DSS 3.2.1 and analyzed for meeting or supporting compliance requirements. The Detailed Notes section reports how these controls meet or support PCI compliance.

Requirements that are not relevant for use of the PCA product, features, or controls were omitted from the published detailed analysis in the interest of brevity. Furthermore, PCA controls were not independently tested by Coalfire. The opinions in this whitepaper represent Coalfire's judgment of documented PCA features and controls, from published information sources supplied by Oracle.

Description

Oracle PCA is an integrated hardware and software system, engineered to enable rapid deployment of private cloud. It delivers a converged infrastructure, complete with compute, networking, virtualization and internal storage, for hosting mixed applications. PCA supports workloads across multiple platforms, to include Linux, UNIX, Oracle Solaris and Microsoft Windows. Automating deployment, scaling and management of application containers in a Oracle Linux Cloud Native Environment is also fully supported using Oracle PCA.

In combination with customer-provided storage from Oracle or other storage vendors, Oracle PCA incorporates server and network hardware with Oracle operating system, virtualization, and orchestration software to automate the discovery, configuration, deployment, and management of converged infrastructure for hosting virtual machines (VMs).

Oracle PCA incorporates high-speed Ethernet or InfiniBand connectivity and Oracle Software Defined Networking (SDN) software to provide a converged, wire-once, software-defined networking and storage fabric for all servers and storage in the appliance. Users can leverage the software-defined network fabric to rapidly and dynamically create or modify private or public networks without having to manually re-cable connections, saving time and reducing the risk of human error. Furthermore, the consolidation of network connections results in substantially fewer cables and cards.

In addition to rapid infrastructure provisioning, Oracle PCA accelerates complete application stack deployment through Oracle Virtual Machine (Oracle VM) Templates and Assemblies. These are preconfigured applications, middleware, and databases packaged as ready-to-run VMs dynamically configured at deployment time. The result is an unparalleled ability to go from "bare-metal" infrastructure power-on to logging in to a newly deployed application within days or hours, instead of weeks or months.

Private Cloud Appliance Architecture

The following diagram (see Figure 1) represents the architecture of Oracle PCA, including internal components and external access points.

Customer access to the typical Oracle PCA deployment is provided through an external-facing network and an internal management network. This supports better separation of back-end system administration and overall network administration duties.

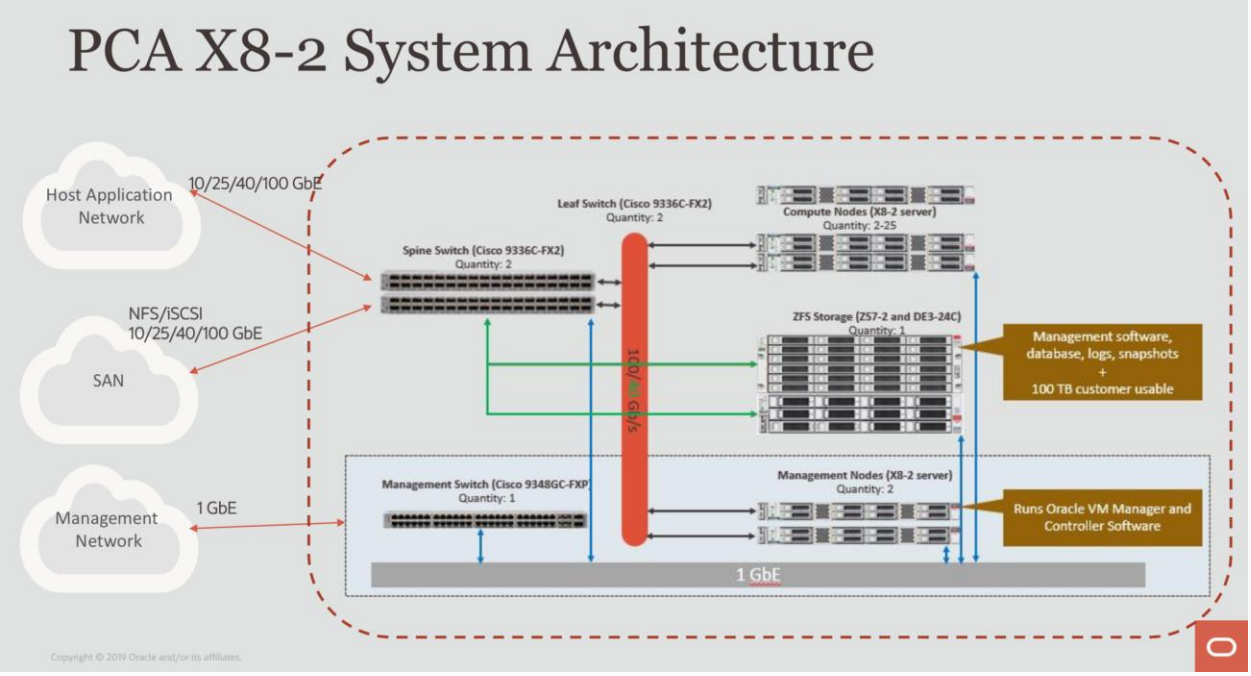


Figure 1. Oracle Private Cloud Appliance

Several individual hardware and software components make up the complete Oracle PCA engineered solution. In addition, there are some supporting technologies that are relevant to PCI DSS compliance in the Oracle PCA environment. All components described below are in scope for PCI DSS compliance and must be configured appropriately.

Hardware Components

Oracle PCA is composed of the following featured hardware components as part of the base rack:

- Two Oracle Server Management Nodes – Oracle Server X8-2
- Two – Twenty-Five Oracle Server Compute Nodes – Oracle Server X8-2
- Two Leaf/Data Switches - Cisco Nexus 9336C-FX2
- Two Spine Switch – Cisco Nexus 9336C-FX2
- One Management Switch - Cisco Nexus 9348GC-FXP
- One Oracle ZFS Storage Appliance – ZS7-2

Software Components

Oracle PCA includes the Oracle VM, Oracle Software Defined Network (Oracle SDN), and Oracle PCA controller software components as part of the standard installation.

Oracle VM provides an application-driven server virtualization environment that supports scalable and rapid server, appliance, and application deployment using pre-built templates and assemblies. The Oracle VM is a Type I hypervisor. As with other virtualization technologies, it abstracts basic system services such as processing, memory, and I/O management to virtual system instances. The hypervisor enables this abstraction and ensures that applications cannot directly manipulate the system resources and thus limits their ability to adversely affect those resources and other applications.

Oracle VM provides the primary management interface for managing guest operating systems and applications. However, once the Oracle PCA is in place, it is generally accessed indirectly through the Oracle VM Manager or through Oracle Enterprise Manager which can be installed separately.

Oracle SDN supports dynamic connection of virtual servers to networks and storage using virtual network interface cards (vNICs).

Oracle PCA controller software orchestrates and supports the management of hardware components and virtual resources, software upgrades, and monitoring of system utilization metrics.

Supporting Oracle Technologies

While there are several products that are either integrated into the Oracle PCA or can be utilized to facilitate compliance with the PCI DSS requirements, the key supporting technology is the Oracle Enterprise Manager.

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product, which provides a complete, integrated and business-driven enterprise cloud management solution. By adding Oracle Enterprise Manager to the Oracle PCA deployment, customers can quickly build and manage a Private Cloud within the data center and offer services like Infrastructure as a Service (IaaS) and Database as a Service (DBaaS). Oracle Enterprise Manager enables business users, developers, and testers rapid and self-service access to cloud services while allowing administrators to govern the cloud services. Both self-service users and administrators can access usage data and create chargeback reports to assess the service consumption.

The Payment Card Industry Data Security Standards

The PCI DSS is a framework of information security requirements that enforce the minimal set of information security controls necessary to protect an environment of computer systems that process, store, or transmit cardholder data.

Any organization that processes, stores, or transmits cardholder data (payment card data) must comply with the PCI DSS and must attest to their compliance annually. Currently, organizations are required to comply with the PCI DSS version 3.2.1 as of June 2018.

The PCI DSS framework is composed of twelve requirements and each requirement has multiple sub-requirements (controls) that provide a detailed description of the control as well as its verification procedures. The PCI DSS requires that organizations define their cardholder data environment (CDE) and that the requirements of the PCI DSS be assessed against the organization's cardholder data environment.

COALFIRE

PCI DSS v3.2.1 DETAILED NOTES

Key Definitions

Meets PCI: Oracle PCA is equipped with capabilities which allow it to meet the intent of the PCI DSS requirement without user configuration or after initial setup.

Supports PCI: Oracle PCA is equipped with capabilities which allow it to support compliance with the PCI DSS requirement. This includes user-required configuration, customer processes, or customer documentation where a shared responsibility model is leveraged for meeting PCI DSS requirements.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

The Oracle PCA must be deployed within a PCI DSS compliant environment, and thus this requirement will not generally apply directly to the appliance. Typically, compliance with this requirement is met by placing appliances such as the Oracle PCA behind a firewall(s) deployed elsewhere in the infrastructure.

However, there may be situations in which segmentation is created within the appliance to:

- Reduce the cardholder data environment scope
- Segment public-facing systems and internal systems
- Segment testing, development, and production environments

For those situations in which segmentation is used, the ability of the Oracle PCA to both support virtual machines configured as firewalls and to create separate physical networks through the dedication of network ports facilitates compliance with Requirement 1. It is important to note that the validity of any segmentation must be validated by technical review and penetration testing in order to meet PCI DSS compliance.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	Firewalls running as virtual machines on the compute nodes can be configured within the Oracle PCA environment to perform firewall functions. The Oracle PCA Private Virtual Interconnects (PVI) fabrics can also be used to provide private networks that do not leave the Oracle PCA rack.	Supports

1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	Services, protocols, and ports used within the Oracle PCA to support internal functions meet this requirement. Services, protocols, and ports used for hosted VMs are out of scope for the Oracle PCA.	Supports and/or Meets
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Individual network zones can be created within the Oracle PCA, segregated with virtual firewalls, to facilitate compliance with this requirement.	Supports

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Oracle PCA facilitates changing default accounts and credentials at system implementation by virtual machine templates and Enterprise Manager. Virtual machine templates can be built to mirror industry-accepted hardening standards and reduce/eliminate errors caused by manual component configurations. Any administrative access to the Oracle PCA is through SSH or SSL encrypted channels.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc*.	All accounts required for administration of the Oracle PCA can be configured to support this requirement. In addition, utilization of Oracle Enterprise Manager can support centralized management of vendor and internal accounts.	Supports and/or Meets
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Virtual machines can be created using secure guidance from applicable standards then saved as templates. These templates can then be deployed for all future device needs, saving time and minimizing human error, thus	Supports

Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	facilitating compliance with this requirement.	
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	Oracle PCA supports the implementation of one primary function per virtual server. In addition, Oracle PCA facilitates more cost and resource effective separation of systems, as resources can be shifted between virtual machines within the larger system.	Supports and/or Meets
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Only those services and protocols necessary for management of the Oracle PCA environment are enabled by default. Management of services and protocols on virtual machines is outside of the scope of the Oracle PCA compliance environment, but the use of secure templates can facilitate more secure virtual machine deployments.	Supports and/or Meets
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure **Note**: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed*	While the management of additional security features and system security parameters on deployed virtual machines is out of scope for the Oracle PCA compliance environment, the implementation of additional security features in place for virtual machines can be facilitated by the development of secure machine templates.	Supports
2.2.4 Configure system security parameters to prevent misuse.		Supports
2.3 Encrypt all non-console administrative access using strong cryptography.	Administrative access to the Oracle PCA is conducted through SSH and TLS encrypted channels.	Meets

Note: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*		
2.4 Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of the components function/use.	Oracle Enterprise Manager supports this requirement when used to manage access to the Oracle PCA management infrastructure.	Supports

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. 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 cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

The protection of cardholder data stored within the Oracle PCA is the sole responsibility of the customer. This requirement is a typical customer responsibility excluded from infrastructure or appliance solutions like Oracle PCA.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

The Oracle PCA will typically be deployed in an environment in which no data is transmitted over open, public networks. However, customer deployment needs vary and data transmission from hosted virtual machines may need to travel over open, public networks. Encryption for such transmission will be implemented at the guest OS level and is supported by the Oracle PCA, subject only to any limitations of the guest OS and applications.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:	The Oracle PCA will typically be deployed in an environment in which no data is transmitted over open, public networks. However, customer deployment needs vary and data transmission from hosted virtual machines may need to travel over open, public networks. Encryption for such transmission will be implemented at the guest OS	Meets

• Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. **Note:** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications	level and is supported by the Oracle PCA subject only to any limitations of the guest OS and applications.	

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

The operating system used for the management of the Oracle PCA environment, Oracle Linux, is typically considered "to be not commonly affected by malicious software", but may be managed as any other OS and protected by antivirus if deemed necessary by the organization. Organizations must address the malware risk to the management OS using their own formal IT Risk Assessment processes and consultation with their QSA.

While any virtual machine hosted within the Oracle PCA environment is subject to this requirement and must be managed accordingly, management of this requirement is out of scope for the Oracle PCA compliance environment.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals 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 systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

The Oracle PCA implementation supports requirements for PCI DSS through features such as VM templates in patching and network segmentation for separation of test and production environments. Additional requirements such as development processes, change management, code review, and application vulnerability testing are typical customer responsibilities excluded from infrastructure or appliance solutions like Oracle PCA.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. **Note**: *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	The Oracle PCA supports single patch bundles allowing it to be maintained as a single unit for patching and reduces patch time to a few hours. Additionally, the Oracle VM Manager templates accelerates deployment of patch bundles to virtual operating systems.	Supports
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	Separate test, development, and production environments can be created within the Oracle PCA using the segmentation options discussed in requirement one.	Supports

Requirement 7: Restrict access to cardholder data by business need-to-know

To ensure 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.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Oracle PCA Enterprise Manager provides granular access controls and default deny-all capability.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Oracle Enterprise Manager supports this requirement when used to manage access to the Oracle PCA management infrastructure. Oracle Enterprise Manager's ability to manage access to the environment both supports and facilitates compliance with features such as granular system access and default "deny-all" settings for newly provisioned accounts.	Supports and/or Meets
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		
7.1.3 Assign access based on individual personnel's job classification and function.		
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:		
7.2.1 Coverage of all system components		
7.2.2 Assignment of privileges to individuals based on job classification and function.		
7.2.3 Default "deny-all" setting.		

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Oracle PCA leverages Enterprise Manager to manage accounts and access controls.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Oracle Enterprise Manager manages access to the Oracle PCA environment including usernames and passwords. The central management provided by Oracle Enterprise Manager, while not directly related to the Oracle PCA implementation, also facilitates central user management. Virtual machines deployed as templates can be configured to require automatic password changes, further facilitating compliance with this requirement.	Meets
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		Meets
8.1.3 Immediately revoke access for any terminated users.		Supports and/or Meets
8.1.4 Remove/disable inactive user accounts within 90 days.		Meets
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.		Meets
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.		Meets
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		Meets
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.		Meets
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at		Meets

least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.		
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.		Meets
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. • Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.		Meets
8.2.4 Change user passwords/passphrases at least once every 90 days.		Meets
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.		Meets
8.2.6 Set passwords/passphrases for first-time use and upon reset to		Meets

a unique value for each user, and change immediately after the first use.		

Requirement 9: Restrict physical access to cardholder data

Requirement 9 states, "Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data."

The Oracle PCA must be deployed in a physically secure environment to meet this compliance requirement, which is a customer's responsibility. This requirement is a typical customer's responsibility excluded from infrastructure or appliance solutions like Oracle PCA.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

The integrated monitoring and audit capabilities of Enterprise Manager enables Oracle PCA to meet compliance requirements for monitoring access to hypervisors and VMs.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
10.1 Implement audit trails to link all access to system components to each individual user.	While the Oracle PCA alone will not generally support compliance with these requirements, all logs associated with the Oracle PCA can be exported to a log management tool to support compliance with these requirements.	Supports
10.2 Implement automated audit trails for all system components to reconstruct the following events:		
10.2.1 All individual user accesses to cardholder data		
10.2.2 All actions taken by any individual with root or administrative privileges		
10.2.3 Access to all audit trails		

10.2.4 Invalid logical access attempts		
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges		
10.2.6 Initialization, stopping, or pausing of the audit logs		
10.2.7 Creation and deletion of system-level objects		
10.3 Record at least the following audit trail entries for all system components for each event:		
10.3.1 User identification		
10.3.2 Type of event		
10.3.3 Date and time		
10.3.4 Success or failure indication		
10.3.5 Origination of event		
10.3.6 Identity or name of affected data, system component, or resource.		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	The Oracle PCA can be configured to synchronize with the organization's NTP source of choice to support compliance with this requirement. Guest VMs can be configured in accordance with the operating system NTP settings.	Supports
10.4.1 Critical systems have the correct and consistent time.		
10.4.2 Time data is protected.		
10.4.3 Time settings are received from industry-accepted time sources.		
10.5 Secure audit trails so they cannot be altered.		Supports

10.5.1 Limit viewing of audit trails to those with a job-related need.	All logs associated with the Oracle PCA can be exported to a log management tool to support compliance with these requirements.	Supports
10.5.2 Protect audit trail files from unauthorized modifications		Supports
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		Supports
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.		Supports
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).		Supports
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).		Supports

Requirement 11: Regularly test security systems and processes

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

The Oracle PCA leverages Enterprise Manager (EM) to support file-integrity monitoring capability. EM agents can be deployed to in scope components and monitor for changes in near real-time, performs hash comparison, and can generate alerts. This capability is more efficient than traditional file-integrity solutions which can bring management systems to a crawl.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
11.5 Implement audit trails to link all access to system components to each individual user.	EM agents can be deployed to monitor for changes in critical files, executables, and applications. EM performs hash comparisons, generates alerts, and interfaces with “auditd” in near real-time.	Supports

Requirement 12: Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of 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 who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

The requirements detailed throughout requirement 12 of the PCI DSS v3.2.1 cover the policy and procedures necessary to enforce the technical and process controls of all the PCI DSS requirements. This requirement is a typical customer's responsibility excluded from infrastructure or appliance solutions like Oracle PCA.

CONCLUSION

The Oracle PCA can be implemented as part of a cardholder data environment. When deployed with controls described in this paper, Oracle PCA supports and often meets PCI DSS compliance requirements. While there are additional factors unique to a virtualized solution, these factors are in no way insurmountable. In fact, many features of the Oracle PCA easily support compliance with PCI DSS requirements and assists organizations with both a more secure and cost-effective solution.

REFERENCES

1. Oracle (2019). Oracle Private Cloud Appliance Administrator's Guide for Release 2.4
2. Oracle (2019). Oracle Private Cloud Appliance Installation Guide for Release 2.4
3. Oracle (2019). Oracle Private Cloud Appliance Data Sheet
4. Cloud Special Interest Group PCI Security Standards Council (2018). Information Supplement: PCI DSS Cloud Computing Guidelines
5. PCI Security Standards Council, LLC (2018), Payment Card Industry (PCI) Data Security Standard, v3.2.1

ACKNOWLEDGMENTS

The author would like to acknowledge the following individuals from Oracle for their contributions to this paper: Krishna Srinivasan and Bill Jacobs. In addition, the author recognizes Allen Mahaffy of Coalfire for his contributions to this paper.