A COALFIRE WHITE PAPER

Oracle SuperCluster and PCI Compliance

Security Capabilities of Oracle SuperCluster that Support PCI Compliance

November 21th 2014

Daniel Sanchez – Senior Consultant, Coalfire

Oracle SuperCluster and PCI DSS v3.0

Executive Summary

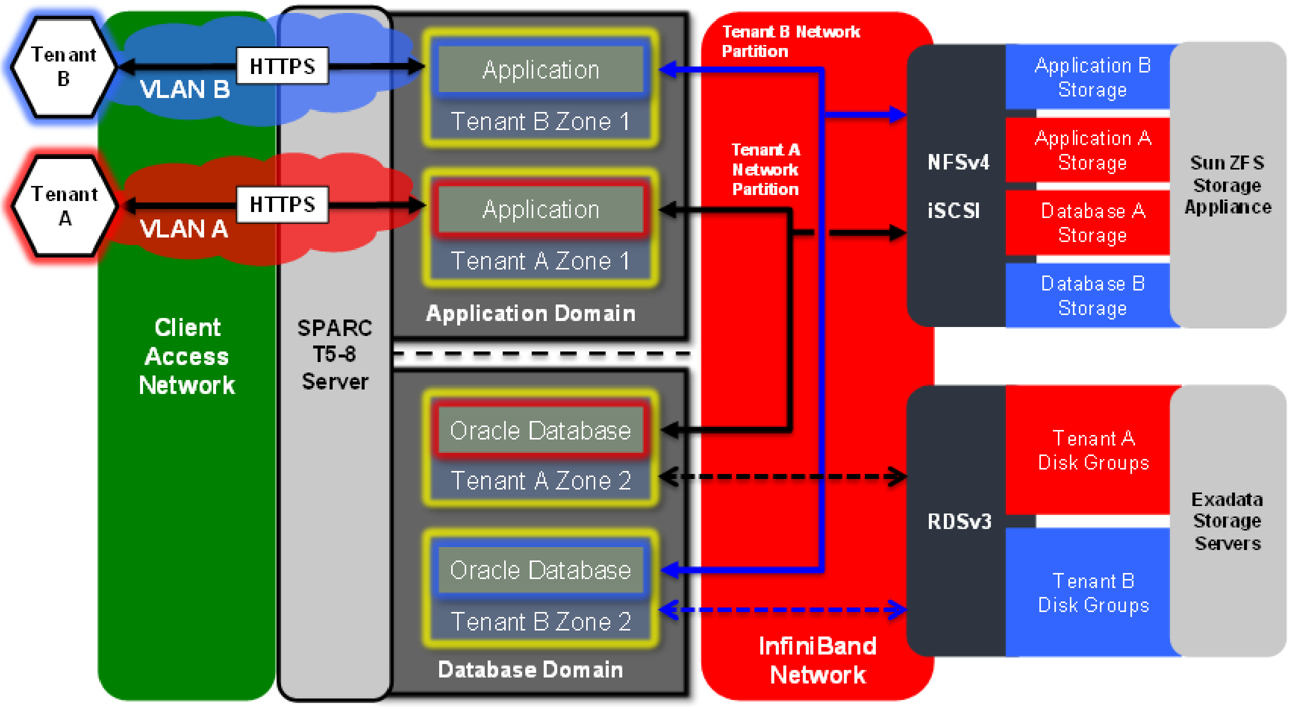
Organizations that process, transmit or store payment card data are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) on an ongoing basis. In order for organizations to meet these security requirements, they must deploy security measures across all the components of the network and systems that process, store or transmit payment card information. Merchants as well as payment card services providers are required to attest to compliance with requirements of the PCI DSS annually. This paper is written to elucidate those requirements of the PCI DSS that can be supported by the Oracle SuperCluster in both single tenant and multitenant configurations.

Introduction

This paper offers information for both the IT professional implementing Oracle SuperCluster within a Cardholder Data Environment (CDE), as well as to the Qualified Security Assessor (QSA) tasked with the assessment of those environments.

Oracle SuperCluster can be used to support enterprise IT service consolidation as well as the deployment of public or private clouds. It is designed to provide highly available multitier enterprise applications with web, database, and application components. Oracle SuperCluster implements secure isolation, strong access controls, monitoring and auditing as well as data protection capabilities across its compute, storage, network, database and application layers. Oracle SuperCluster's integrated security features and capabilities can be configured to satisfy or support many of the PCI DSS v3 requirements. Further, service providers and enterprise customers can configure SuperCluster to enable multitenant architectures and solutions. Both public and private cloud hosting service providers can configure Oracle SuperCluster to enforce the segmentation between hosted entities that is required to satisfy or support the various PCI DSS requirements that apply specifically to them (Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers).

Any organization that stores, processes, or transmits cardholder data must be in compliance with PCI DSS. Over the years, Oracle has demonstrated a steadfast commitment to providing solid and secure solutions. Oracle works with industry security organizations to stay apprised of the various security and compliance hurdles that many organizations face and uses that information to design a product meet the challenges. With its integrated security controls, Oracle SuperCluster can be configured to meet or support many information security requirements without the addition of any software or hardware. Oracle SuperCluster can integrate with existing network or other IT security controls thereby adding additional detective and preventative layers of defense directly in front of the sensitive information being protected.



A Oracle SuperCluster multitenant consolidation design enforces that all compute, storage, network, database and application components for each hosted entity are properly isolated to meet the PCI requirement to enforce isolation between hosted entities.

The Payment Card Industry Digital 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 2.0 but must begin to comply with the PCI DSS version 3.0 starting January 2015.

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 organizations cardholder data environment or an established sampling of it.

Build and Maintain a Secure Network

1. **Install and maintain a firewall configuration to protect cardholder data**

   Oracle SuperCluster can be configured to meet and/or support several of the controls associated with this requirement. For example, Oracle SuperCluster can be configured to use its integrated stateful packet filtering software to enforce inbound and outbound network traffic policy across its IP-based networks. Similarly, additional network flow protection can be implemented using service-specific functionality (e.g., Database, Web Server, etc.) as well as through cryptographic means such as with IPsec/IKE.

2. **Do not use vendor-supplied defaults for system passwords and other security parameters**

   Oracle SuperCluster can be configured to ensure compliance and support several controls of this requirement. For example, Oracle SuperCluster can be configured to comply with various security configuration baselines including those published by the U.S. Department of Defense (DoD Security Technical Implementation Guides) as well as Center for Internet Security (CIS) Benchmarks. Further, each of the components used by Oracle SuperCluster implements a network secure by default configuration to ensure that unnecessary services and functionality are not enabled by default. Finally, as part of the Oracle SuperCluster delivery process, all default passwords can be changed to values known only to the customer.

Protect Cardholder Data

3. **Protect stored cardholder data**

   For those organizations that store cardholder data, Oracle SuperCluster implements integrated security controls can be configured to satisfy or support several of the controls of this requirement. Oracle SuperCluster includes secure isolation technology to ensure strong isolation of cardholder data at the compute, network, storage and database levels. These capabilities can be combined as needed to support a diverse set of architectures, workloads and security requirements. Further, strong authentication and role-based access control technologies help to ensure that cardholder data can only be accessed by authorized individuals and services. Finally, cardholder data flowing over the network and stored in databases or on disks is protected using strong encryption. Together, these controls help to ensure the confidentiality and integrity of sensitive cardholder information.

4. **Encrypt transmission of cardholder data across open, public networks**

Oracle SuperCluster can be configured to protect cardholder data flowing into and out of the platform using strong cryptographic means. Protocols such as TLS (SSL), SSH, and IPsec are all used to help ensure that sensitive data processed by Oracle SuperCluster is always encrypted when flowing over a network. These capabilities extend beyond application and cardholder data to include the protocols and services used to manage and monitor the Oracle SuperCluster platform as well.

Maintain a Vulnerability Management Program

5. **Protect all systems against malware and regularly update anti-virus software or programs**

   The PCI DSS requires organizations to "Deploy anti-virus software on all systems commonly affected by malicious software" and although SuperCluster does not meet any requirement it can support this requirement in several ways. For example, Oracle SuperCluster is built upon compute nodes running the Oracle Solaris operating system. The Oracle Solaris operating system includes support for a VSCAN service that provides real-time anti-malware scanning of content stored on ZFS file systems. The VSCAN service integrated is with external servers using an industry standard ICAP protocol. In addition, Oracle Solaris supports a number of integrated anti-malware capabilities including immutable non-global zones, non-executable stacks, address space layout randomization, as well as data link protections. Collectively, these integrated security controls support the creation of high integrity environments on Oracle SuperCluster.

6. **Develop and maintain secure systems and applications**

   Oracle SuperCluster can satisfy or support controls of this requirement that call for separation of duties between development/test and production environments. SuperCluster can also support several other controls of this requirement that call for a program for vulnerability management and timely application of vendor supplied security patches. Oracle SuperCluster's inherent security controls combined with Oracle's Critical Patch Updates and Security Alerts ensure that SuperCluster can provide secure multitenant and single tenant designs.

Implement Strong Access Control Measures

7. **Restrict access to cardholder data by business need-to-know.**

   Oracle SuperCluster includes strong authentication as well as user and role based access controls across its compute, storage, network and database components. Together, the access control policies enforced across these components help to ensure that access to sensitive information and functions is limited to only those intended. Because of this, Oracle SuperCluster access controls can satisfy and/or support many of the controls (sub-requirements) of this requirement.

8. **Assign a unique ID to each person with computer access**

   Oracle SuperCluster can be configured to satisfy and/or support many of the controls of this requirement. More importantly, Oracle SuperCluster can be configured to satisfy the additional access-controls requirements the PCI DSS imposes on service providers whose customers' store, process or transmit cardholder data. Oracle SuperCluster's integrated user and role based access controls (RBAC) can be used to control and limit access to compute, storage, network, database and application services. These fine-grained access controls help to minimize the availability and use of administrative privilege across both multitenant and single tenant environments.

9. **Restrict physical access to cardholder data**

   Oracle SuperCluster does not directly satisfy any of these requirements but supports many of them with its ability to consolidate information assets in places with increased detective and preventative physical security controls.

Regularly Monitor and Test Networks

10. **Track and monitor all access to network resources and cardholder data.**

    Oracle SuperCluster's inherent auditing and monitoring features can be configured to monitor administrative actions and activities across all compute, storage, network, database and application assets to satisfy and/or support many of the controls detailed in this requirement. This applies to Oracle SuperCluster configured as a multitenant consolidated solution allowing the customer segmentation required by the PCI DSS Appendix A: Requirement for Service providers.

11. **Regularly test security systems and processes.**

    Oracle SuperCluster can satisfy the controls of this requirement that call for file integrity monitoring on critical files on systems within the cardholder data environment. This can be accomplished using the integrated Basic Audit and Reporting Tool (BART) delivered by the Oracle Solaris operating system. The ZFS file system used by the Oracle SuperCluster compute nodes also supports the ability to create read-only snapshots of file system content. These snapshots can be compared with each other or with the actual file system to detect whether changes have been made. Further, the use of immutable non-global zones further helps prevent unauthorized change to operating system and application components.

12. Maintain a policy that addresses information security for all personnel

The controls detailed in this requirement deal mainly with the process, policy and procedure controls necessary to enforce the requirements of PCI DSS and information security best practice. Because of this, Oracle SuperCluster does not satisfy or support this requirement directly.

Requirement A.1: Shared hosting providers must protect the cardholder data environment

Detailed in its Appendix A, PCI DSS contains requirements applicable specifically to service providers that the Oracle SuperCluster can satisfy and or support by tying together its multitenant secure isolation technology to its integrated access-control, data protection and monitoring/auditing capabilities. This allows the disparity of critical information required by the PCI DSS of service providers of multitenant hosting solutions.

PCI DSS v3.0 Detail

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

Requirement 1 of the PCI DSS v3.0 states that "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"

Oracle SuperCluster's secure isolation technologies in combination with its stateful packet inspection firewall can be configured to empower customers to meet or support many of the controls of PCI DSS requirement 1. Through its integration of compute, storage, network, database and application components, Oracle SuperCluster provides an integrated collection of layered security controls. Together, a defense in depth architecture can be created to support many of the requirements of the PCI DSS for standalone and consolidated environments as well as public or private clouds.

Oracle SuperCluster allows customers to apply strong access controls to not just the network but to users, processes, storage, databases and applications. Network isolation, access control, stateful firewall encryption (IPsec, SSL/TLS) and transport layer access lists on VLANs at layer 2 or layer 3 can be applied to the Oracle SuperCluster's Infiniband Switch Fabric network, management network and client network so customers can apply a defense in depth posture to support existing security controls on the network. Oracle SuperCluster incorporates access controls, encryption, monitoring, and secure isolation across all of its storage, network, process and application layers and between layers so a defense in depth posture can be enforced at all layers and in between.

PCI DSS Requirement		SuperCluster Feature
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Satisfy and/or Support	In combination with traditional network based firewall controls, Oracle SuperCluster's secure isolation and stateful packet inspection technologies can be enabled to support existing controls to ensure compliance with the PCI DSS requirements for a firewall at any demilitarized zone (DMZ) and the internal network. In the cloud or in the private datacenter, SuperCluster's secure isolation and access

		control technologies can be applied to the Infiniband IP network, management networks, and client network to ensure the isolation required in multitenant environments.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Satisfy and/or Support	Oracle Solaris IP Filter can be configured to ensure that any connection from untrusted networks can be restricted with stateful firewall access controls.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic	Satisfy and/or Support	Oracle Solaris IP Filter can be configured to limit traffic inbound and outbound only to that which is necessary, and deny any other traffic by default.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Support	Oracle Solaris IP Filter can be leveraged as a stateful packet inspection firewall to ensure that any wireless networks outside the SuperCluster are firewalled away from any cardholder data environment networks located on the SuperCluster. If access is required, SuperCluster's stateful firewalls can provide access to the cardholder data environment with the same maximum granularity of any network based stateful packet inspecting firewall.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Support	Oracle Solaris IP Filter can be combined with network based firewalls or border router firewall features and access control lists to prohibit any direct access between the cardholder data environment.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Support	Oracle Solaris IP Filter access lists can be configured to ensure that access only over authorized protocols/ports is allowed to DMZ or internal networks.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ	Satisfy and/or Support	Oracle Solaris IP Filter can be configured to limit inbound internet traffic to IP addresses within a DMZ network that is built upon a SuperCluster network. Additionally, SuperCluster enables transport

		layer (layer 4) access controls to be deployed between VLANS (Layer 3) and at layer 2 (data-link layer) to limit access between hosts on the same VLAN. Access controls can be applied to the SuperCluster's client (outward facing), management and Infiniband Switch IP networks as well as its storage.
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	Satisfy and/or Support	Oracle Solaris IP Filter stateful firewall can be combined with network based firewalls or border router firewall features and access controls to prohibit any direct access between the cardholder data environment, internal networks or DMZ networks. Solaris Kernel SSL Proxy can be enabled to prevent direction network connections and to accelerate cryptographic operations of web and application servers running on the Oracle SuperCluster.
1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	Satisfy and/or Support	Anti-spoofing features can be enabled with Oracle Solaris Link Protection in combination with the application of Solaris IP Filter firewall access control lists to apply ingress anti-spoof detective and preventative controls to meet this requirement.
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Satisfy and/or Support	Oracle SuperCluster's IP Filter stateful packet inspection firewalls can be configured with egress access control lists to only allow authorized outbound traffic from the cardholder data environment to the internet.
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	Satisfy and/or Support	Oracle SuperCluster's IP Filter stateful packet inspection firewalls can be configured to meet compliance with this requirement. Over Ethernet or IP over InfiniBand, stateful packet filtering is supported.
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks	Satisfy and/or Support	Oracle SuperCluster's network isolation technology combined with its IP Filter stateful packet inspection firewall can be configured to ensure that system components that store cardholder data in

		virtualized hosts can be segregated from the DMZ and other untrusted networks.
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties	Satisfy and/or Support	Oracle SuperCluster's IP Filter can be configured to provide Network Address Translation and Port Address Translation to prevent the disclosure of any private IP addresses and routing information to unauthorized parties.
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	Satisfy and/or Support	Oracle Solaris IP Filter Firewall can be installed as a host based firewall on hosted virtual guest computers. A predefined set of specific configuration settings can be configured to ensure that the firewall is actively running and its configuration is not alterable by users.

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

Requirement 2 of the PCI DSS v3.0 states that “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.”

SuperCluster combines a posture of Secure by Default with integrated security controls that allow customers to support many of the controls of this requirement.

PCI DSS Requirement		SuperCluster Feature
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, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	Support	When Oracle Solaris is installed, most network services are disabled by the Secure by Default feature that ensures that no access other than SSH is available remotely and elevated (root) access is only available locally by default. Oracle virtualization can be leveraged to ensure that all new virtual components satisfy compliance with configuration standards that ensure best practice hardening is enforced on all new and existing system components.
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.)	Support	Oracle virtualization technology allows virtual hosts to be created to serve only one primary function. Oracle SuperCluster Service Management Facility (SMF) can be leveraged to ensure consistent service management of virtual resources within the cardholder data environment.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Satisfy	Oracle Solaris Secure by Default posture ensures that no unnecessary services, protocol, daemons/servers are running, SSH is

		the only listening for remote connections, and only local access can be elevated.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc	Satisfy and/or Support	Oracle SuperCluster only leverages secure services by default so no additional security features are required for the default configuration of Oracle SuperCluster. For an additional layer of defense to the hardening (securing) any services, protocols, or daemons (servers) that are considered to be insecure, SuperCluster access controls, stateful packet inspection, secure zone isolation, strong authentication and logging can be enabled to satisfy or support this requirement.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Support	With Oracle SuperCluster's Secure by Default reduced attack surface posture, unnecessary functionality in the form of a large set of networking services are disabled, elevated access (root) is only available locally and only SSH is enabled to accept inbound network connections. Oracle Solaris has no web servers listening for connections by default and other Oracle SuperCluster components have web servers that have already been hardened by default.
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	Satisfy and/or Support	Oracle SuperCluster can leverage IPSec, SSL/TLS, SSH or any combination of these secure communications between zones, domains, servers, and other components on the Oracle SuperCluster's client access, management and InfiniBand networks. Solaris Kernel SSL Proxy can be enabled to offload cryptographic workload from web, application or other servers running on the SuperCluster
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet	Satisfy and/or Support	SuperCluster's integrated monitoring, access control, and encryption combined with its secure isolation technologies can be designed and

specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers		configured to ensure compliance with the Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement 3: Protect stored cardholder data

Requirement 3 of the PCI DSS v3 states that: "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."

Any organization that stores cardholder data must ensure that they have applied all the applicable controls of the PCI DSS Requirement 3. Oracle SuperCluster comes with the ability to encrypt data in the database with Transparent Database Encryption (TDE) or data at rest on the ZFS file system and supports redaction and masking of database information if needed.

PCI DSS Requirement		SuperCluster Feature
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely.	Support	Although the PCI DSS strictly prohibits the storage of sensitive authentication data, in the rare circumstances it is necessary with a valid business justification or because the organization is an issuer. If sensitive authentication data must be stored for a valid business reason, SuperCluster can be leveraged to ensure that all sensitive information is encrypted either in the database tables with Transparent Database Encryption or where it is stored on disk with the ZFS file system security. Additionally, where redaction or masking of data is required, Oracle Solaris 11 Data Redaction,

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3		sensitive information can be masked from low privileged users or applications.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.	Support	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures	Satisfy	SuperCluster can leverage multiple encryption algorithms and key strengths with its Transparent Database Encryption (TDE) to encrypt data within databases (file- or column-level database encryption) or at rest with ZFS disk encryption. Both Transparent Data Encryption (TDE) and ZFS encryption can be implemented in a way that complies with this control. Oracle Database can be leveraged to ensure that the entire data or just a portion of the data is replaced by a fixed or masked value.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Satisfy	ZFS encryption can be configured to ensure that disk encryption is implemented in a way that is not associated with user accounts. The Oracle SuperCluster provides integration support for the configuration of using "Oracle Key Manager" as a network HSM appliance to seamlessly provide cryptographic acceleration and to off load cryptographic key management duties. Oracle SuperCluster also provides integration support for several third party HSM products to offload cryptographic key management duties and provide cryptographic acceleration.

3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key • Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry accepted method	Satisfy	Oracle SuperCluster in combination with an HSM or other approved PKCS#11 device can be configured to seamlessly to provide cryptographic acceleration, minimize cryptographic keys storage locations, generate strong cryptographic keys and off load cryptographic key management and storage duties. Oracle Database and Oracle Solaris works seamlessly with the Oracle Key Manager 3 or another third party HSM product to enforce compliance with PCI cryptographic key management requirements.
3.5.3 Store cryptographic keys in the fewest possible locations.		
3.6.1 Generation of strong cryptographic keys.		
3.6.2 Secure cryptographic key distribution.		
3.6.3 Secure cryptographic key storage.		
3.6.4 Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).		

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

The PCI DSS states that: "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 SuperCluster can implement IPSec, SSL/TLS and SSH over its client network, management network and Infiniband IP switch network. The Oracle Secure by Default (SBD) posture ensures that SuperCluster can only be accessed remotely by SSH in its default configuration and SuperCluster allows all management traffic to be isolated to its management network.

PCI DSS Requirement		SuperCluster Feature
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • 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.	Satisfy	Oracle SuperCluster can secure the transmission of cardholder data between its components over its integrated client access, management and/or InfiniBand networks using one or more technologies such as TLS/SSL, SSH, and IPsec. Oracle SuperCluster can enforce IPSec, SSL/TLS or both against all transmissions across all of its networks and to secure all of its management interfaces.

Requirement 5: Use and regularly update antivirus software or programs

Requirement 5 of the PCI DSS states that: "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."

Oracle SuperCluster or Oracle Solaris support virus scanning of the ZFS file system with up to three 3rd party anti-virus scanners through VSCAN.

PCI DSS Requirement		SuperCluster Feature
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Support	VSCAN can be implemented to enforce real-time anti-malware scans for content stored on the ZFS file systems. Oracle Solaris and the integrated Oracle ZFS Storage Appliance both support virus scanning of content stored on ZFS file systems. Virus scanning is accomplished through an integration between the component's VSCAN service and a pre-existing (external) virus scanning service using the industry standard Internet Content Adaptation Protocol (ICAP).
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Support	
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	Support	

PCI DSS Requirement 6: Develop and maintain secure systems and applications

The PCI DSS v3.0 Requirement 6 States: "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".

Oracle SuperCluster has 24/7 access for critical updates through Oracle's Critical Patch Updates and to ensure that vulnerabilities are managed throughout the lifecycle of the hardware and software. Oracle SuperCluster can help organizations establish isolation between their development and production environments through its secure isolation technologies and integrated security controls.

PCI DSS Requirement		SuperCluster Feature
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.	Satisfy	Oracle SuperCluster can be easily administered to meet this requirement by leveraging Oracle's Critical Patch Updates and security alerts which ensure that licensed users have 24/7 access to security updates and patches. All news and notices about SuperCluster updates are available to customers via Oracle Critical Patch Update Advisory. Critical security updates are available for all components and software/firmware. Oracle Software Security Assurance (OSSA) methodology ensures that all Oracle products have information security best practice controls baked into all phases of the security development lifecycle and are subject to an ongoing vulnerability management lifecycle from release to end of support.
6.4.2 Separation of duties between development/test and production environments	Satisfy	Oracle SuperCluster secure isolation as well as integrated access controls can be leveraged to ensure that development and production environments are separated at the compute, network, storage and application resource areas and that their associated access control systems are disparate from one another.

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Support	Oracle Audit Vault and Database firewall can be added to Oracle SuperCluster to enable the inspection of SQL statements inbound to the database against a highly accurate next-generation SQL grammar analysis engine to detect and prevent SQL injection attacks before they can affect the database. The Oracle Database firewall can be configured to alert, log, substitute, whitelist or blacklist, block or allow the SQL and exception lists controls can be applied. Although it does not satisfy this requirement completely, it augments any other security controls applied and enforces a defense in depth posture to support these requirements.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.		

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

The PCI DSS v3.0 Requirement 7 states: "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 SuperCluster provides fine-grained access controls across compute, storage, network and application resource areas.

PCI DSS Requirement		SuperCluster Feature
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Satisfy	All Oracle SuperCluster access controls can be applied to compute, network, storage, application and database layers, which translates into individual server, storage, virtualization, operating system and database access controls through Oracle's fine-grained RBAC (Role based access controls) facility and POSIX permissions. The SuperCluster allows customers to establish an access control system for operating system, database and application components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
7.1.1 Define access needs for each role, including: • System components and data resources that each role • needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.		
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 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 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: Assign a unique ID to each person with computer access

PCI DSS v3.0 Requirement 8 states: “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”.

Oracle SuperCluster and be configured to ensure that all of require users to have a unique ID in order to authenticate for authorization to access its workload, storage, network, application and database layer as well as in between layers. With Oracle SuperCluster, Kerberos is integrated with auditing, cryptography, and user management functions to secure the Kerberos-enabled applications. Oracle Solaris integrates flexible authentication extensibility through the use of Pluggable Authentication Modules (PAM) which enable Oracle SuperCluster to be integrated with an LDAP directory service such as Oracle Directory Server Enterprise Edition and/or multiple-factor authentication for any or all of the isolated zones it hosts.

PCI DSS Requirement		SuperCluster Feature
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Satisfy	With its integrated security features, Oracle SuperCluster can be configured to comply with these controls by implementing proper user identification management security policy configuration.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		
8.1.3 Immediately revoke access for any terminated users.		
8.1.4 Remove/disable inactive user accounts at least every 90 days.		

8.1.5 Manage IDs used by vendors 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.		
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.		
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		
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.		
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 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.	Satisfy	SuperCluster can be configured to use strong authentication that can meet this control. SuperCluster can be configured to use authentication via Radius, Kerberos or SSL/TLS and 2nd factor authentication can be applied via multiple 3rd party products to enforce an additional factor of authentication.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.		Oracle Solaris uses the SHA-256 algorithm by default for all user and role passwords. Similarly, Oracle Database uses SHA-1 by default. These algorithms can be changed to others if required. Password security properties can be set to ensure that accounts that are provided access to hardware and software within the CDE are

8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.		required to adhere to all password properties required by these controls.
8.2.4 Change user passwords/passphrases at least every 90 days.		
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.		
8.2.6 Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.		
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).	Satisfy	SuperCluster can be configured to use a 2nd factor of authentication applied to authentication for remote access originating from outside the network and allowing SuperCluster to meet this requirement.
8.5.1 Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.		Service providers can ensure they meet this requirement by configuring SuperCluster access controls to restrict each hosted tenant entity to its own cardholder data environment. Access controls are leveraged with sufficient granularity with RBAC so it can be configured to ensure that all hosted entities are only permitted to access those resources that are their own.

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).		Whether SuperCluster is designed as a single instance in a physical domain or as a multitenant system in the cloud, fine-grained access controls can be applied to all user access to any database containing cardholder data. Users can be granted permissions to meet all of the controls of this requirement even in complex multitenant environments.

Requirement 9: Restrict physical access to cardholder data

PCI DSS v3.0 Requirement 9 states that “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.”

Although SuperCluster itself provides no physical security controls other than providing administrators with the ability to set an EEPROM (boot loader) password, computing and storage consolidation and cloud service offerings mean that engineered systems like Oracle SuperCluster can be physically consolidated in datacenters with better physical security controls.

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

PCI DSS v3.0 Requirement 10 states that "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 Oracle SuperCluster can enable organizations to meet compliance requirements for monitoring access to cardholder resources across the compute, storage, network, database, and application areas. Shared hosting providers can configure the secure isolation technologies built into SuperCluster to build highly available multitenant systems while ensuring and each hosted entities monitoring is disparate from any other hosted entity. This empowers customers to configure the Oracle SuperCluster to comply with many of the monitoring requirements of PCI for single tenant or multitenant designs without addition cost or software/hardware.

PCI DSS Requirement		SuperCluster Feature
10.1 Implement audit trails to link all access to system components to each individual user.	Satisfy	Oracle SuperCluster audits the entire system, including activities in Solaris non-global zones and can be configured to implement audit trails to link all access to system components to each individual user for the entire system as well as any zones on the system. Oracle SuperCluster auditing can be performed on each zone as well as the entire system as if they were separate systems. Isolation between zones ensures that the required individual tenant zones and databases can each have their own isolated set of users, groups, roles, authentication mechanisms, logging and auditing. This enables the ability to service providers to configure the SuperCluster to satisfy some of the requirements in PCI DSS Appendix A Additional PCI DSS Requirements for Shared Hosting Providers A.1.3.
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		In addition, at the database level, Oracle Database provides an equivalent fine-grained and conditional auditing capability to ensure critical users and activities are audited while also helping to minimize the amount of unnecessary "noise" in the audit logs.
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.	Satisfy Or Support	Oracle SuperCluster leverages the Network Time Protocol (NTP) service to support synchronized time across the platform. The NTP service combined with the monitoring and auditing capabilities of SuperCluster can be configured to comply with this requirement.
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.	Satisfy	Access to Oracle SuperCluster storage is controlled through a variety of authentication and access control techniques including user and role-based access controls. Further, database and file system storage can be encrypted to further prevent unauthorized access to data at rest. Finally, if required, Oracle Solaris and

		Oracle Database audit data can be offloaded to an external storage and processing capability.
10.5.1 Limit viewing of audit trails to those with a job-related need.	Satisfy	Oracle SuperCluster can be configured to meet this control with role-based access controls applied to allow only those with the role that has been authorized with a need to know to access the logs. Note that this applies to both Solaris and Database audit trails.
10.5.2 Protect audit trail files from unauthorized modifications.	Satisfy	Beyond user and role-based access controls, Oracle SuperCluster can be configured to meet this control through the use of BART (Basic Audit Reporting Tool) which can be enabled to provide file integrity monitoring on archived logs to ensure that any unauthorized modifications are logged for detection. The use of ZFS read-only snapshots can also preserve point-in-time records of audit data that can be used and/or restored as needed.
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).	Satisfy	In order to achieve compliance with this requirement, BART (Basic Audit Reporting Tool) can be enabled on Oracle SuperCluster to ensure that file integrity monitoring requirements are achieved without incurring the additional cost of deploying a separate file integrity monitoring solution. Again, the use of read only ZFS data sets and Solaris immutable non-global zones can also serve to limit the areas of the file system that can be modified at all.
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).	Satisfy	Oracle SuperCluster's monitoring and logging allow audit trails to be configured for the necessary retention requirements to achieve compliance with this control.

Requirement 11: Regularly test security systems and processes

PCI DSS v3.0 requirement 11 states that: “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”.

Oracle SuperCluster can support detective and preventative control, complementing dedicated IDS/IPS systems with its integrated fine-grained auditing at both the compute and database level and through its use ability to use BART (Basic Audit Reporting Tool) enable file integrity monitoring on critical files within the cardholder data network. Additional preventive and anti-malware controls such as Solaris immutable non-global zones, non-executable stacks, and address space layout randomization further serve to reinforce the integrity of the cardholder environment.

PCI DSS Requirement		SuperCluster Feature
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Support	As an additional control to augment traditional intrusion detection and/or intrusion prevention systems, Oracle SuperCluster includes fine-grained auditing at both the compute (Solaris) and database levels. This helps to ensure that all administrative, service and end-user actions are monitored in accordance with the PCI DSS requirements and site policy. Further, this data is augmented by network event information generated by the Solaris IP Filter stateful packet filter technology.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Satisfy	SuperCluster BART (Basic Audit Reporting Tool) can be configured to meet this requirement by ensuring that file integrity monitoring policies are enforced without incurring the additional cost of deploying a separate file integrity monitoring solution. To further promote the integrity of the cardholder environment, Solaris immutable non-global zones can be deployed to ensure that critical operating system configuration files, binaries, libraries and other file system elements cannot be changed from within the non-global zone itself.

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

The requirements detailed throughout requirement 12 of the PCI DSS v3.0 cover the policy and procedure necessary to enforce the technical and process controls of all the PCI DSS requirements and best practice and hence, no controls of this requirement can be satisfied or supported by Oracle SuperCluster

PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

Requirement 2 of the PCI DSS v3.0 states that "As referenced in Requirement 12.8 and 12.9, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix."

To meet the growing demand for secure and highly available computing in the public and private cloud, Oracle has designed Oracle SuperCluster specifically with multitenant environment security in mind. Oracle SuperCluster's data protection, secure isolation, monitoring and access control technologies are pervasive across all of its compute, network, storage and database/application resources. This enables SuperCluster customers to design solutions using a comprehensive defense in depth strategy at every layer and in between. Secure isolation and strong access controls combined with the ability to monitor each user/customer zone as disparate entities allows Oracle SuperCluster to be configured to satisfy the Additional PCI DSS Requirements for Shared Hosting Providers.

PCI DSS Requirement		SuperCluster Feature
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.	Support	See A.1.1 through A.1.4 for details
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	Satisfy	Secure multitenant isolation can be leveraged on Oracle SuperCluster to ensure that process separation is achieved. Physical isolation, electrical isolation (Physical Domains) and hypervisor-mediated isolation (Logical Domains) as well as Solaris non-global zones can be configured to ensure secure isolation for any compute service including both database and application workloads.
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	Satisfy	Oracle SuperCluster access controls span compute, storage, network, database and application resources. Oracle SuperCluster can be configured to restrict the access of each hosted tenant entity to its own cardholder data environment. SuperCluster fine-grained access control are easily applied with RBAC so it can be configured to ensure that all hosted entities are only permitted to access those resources that are their own. Isolation between zones ensures that the required individual tenant zones can each have their own isolated set of users, groups, roles, authentication mechanisms, logging and audit trails.
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's	Satisfy	Oracle SuperCluster monitoring can be configured to comply with this control since monitoring of compute, storage, database, network and

cardholder data environment and consistent with PCI DSS Requirement 10.		applications can be enabled while ensuring that data associated each entity hosted is isolated and access is limited to only the service provider. Configured correctly, secure multitenant isolation ensures that every entity hosted cannot affect and other entity hosted on the Oracle SuperCluster.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Support	Oracle SuperCluster can be configured to support this requirement through its inherent monitoring and audit controls combined with the built in detective, preventive and corrective services of Solaris such as immutable non-global zones, file integrity scanning, fine-grained auditing and logging and virus scanning (VSCAN). Further, database and application specific controls can further provide additional insight and records of administrative actions, user activity and other data.

Conclusion

Oracle SuperCluster includes integrated security controls that can be applied to assist organizations meet or support many of the PCI DSS v3.0 requirements without the need for additional hardware or software. Its integrated security controls combined with Oracle SuperCluster's ability to provide highly available solutions over the enterprise or in the cloud makes SuperCluster an exceptional value.

References & Resources

1. Brunette G., Nagappan R., Weise J. (2013). *Secure Database Consolidation Using the*
2. *Oracle SuperCluster T5-8 Platform.*
3. Brunette G., Nagappan R., Weise J. (2013). *Secure Database Consolidation Using the*
4. *SPARC SuperCluster T4-4 Platform.*
5. Brunette, G. (2014). *Oracle Engineered Systems Security Capability Technical Overview.*
6. Mandalika G., Vasudevan S., Moazeni R., and Nagappan R. (2012). *Best Practices for Deploying Oracle Solaris Zones with Oracle Database 11g on SPARC SuperCluster*
7. Combs, G. (2013). *A Technical Overview of Oracle SuperCluster*
8. Virtualization Special Interest Group PCI Security Standards Council. (2011). *Information Supplement:*
9. *PCI DSS Virtualization Guidelines.*
10. Oracle. (2013). *Complete Support Services for Oracle SuperCluster.*
11. Oracle. (2013). *Oracle Key Manager 3.*
12. Oracle. (2014). *Oracle Audit Vault and Database Firewall.*
13. Oracle. (2014). *Overview and Frequently Asked Questions Oracle SuperCluster.*
14. Oracle. (2012). *Oracle Solaris 11.2 Security Compliance Guide.*
15. Oracle. (2014). *Securing Systems and Attached Devices in Oracle Solaris 11.2.*
16. Oracle. (2011). *Overview and Frequently Asked Questions Oracle SPARC SuperCluster T4- 4.*
17. Oracle. (2014). *Overview and Frequently Asked Questions Oracle SuperCluster.*
18. Scarfone K., Souppaya M., Hoffman P. (2010). *Guide to Security for Full Virtualization Technologies.*
19. PCI Security Standards Council, LLC. (2013., *Payment Card Industry (PCI) Data Security Standard, v3.0*
20. Cloud Special Interest Group PCI Security Standards Council (2013). *Information Supplement: PCI DSS Cloud Computing Guidelines*
21. Virtualization Special Interest Group PCI Security Standards Council (2011). *Information Supplement: PCI DSS Virtualization Guidelines*
22. Oracle (2012). *Reduce Risk with Oracle Solaris*

Acknowledgments

The author would like to acknowledge the following individuals from Oracle for their contributions to this paper: Glenn Brunette and Ramesh Nagappan. In addition, the author recognizes Matt Getzelman and Adam Shnider of Coalfire for their contributions to this paper.